



User Manual



© Doctor Web, 2018. All rights reserved

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

Trademarks

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

Disclaimer

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

Dr.Web for Linux
Version 11.0
User Manual
9/3/2018

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

Conventions and Abbreviations	7
Introduction	8
About this Product	9
Main Functions	9
Program Structure	11
Quarantine Directories	12
File Permissions and Privileges	13
Operation Modes	14
Testing Product Operation	17
System Requirements	19
Licensing	23
Key File	25
Connection Settings File	27
Installing and Uninstalling Dr.Web for Linux	28
Installing Dr.Web for Linux	29
Installing Universal Package	29
Installing in Graphical Mode	31
Installing from Command Line	36
Installing from the Repository	38
Upgrading Dr.Web for Linux	42
Getting Current Upgrades	42
Upgrading to a Newer Version	43
Uninstalling Dr.Web for Linux	47
Uninstalling Universal Package	47
Uninstalling in Graphical Mode	48
Uninstalling from Command Line	50
Uninstalling the Product Installed from the Repository	52
Additional Information	55
Product Files Location	55
Custom Component Installation and Uninstallation	55
Configuring Security Systems	59
Configuring SELinux Security Policies	60
Configuring the Permissions of PARSEC (Astra Linux)	63



Working with Dr.Web for Linux	65
Operating in Graphical Mode	66
Integration with Desktop Environment	70
Starting and Shutting Down Graphical Interface	73
Threat Detection and Neutralization	74
Scanning on Demand	75
Scheduled scanning	78
Managing Scan Tasks	79
File System Monitoring	81
Monitoring of Network Connections	83
Viewing Detected Threats	85
Managing Quarantine	88
Updating Antivirus Protection	90
License Manager	91
Managing Application Privileges	101
Help and Reference	102
Operation Settings	103
Main Settings	104
Scanner Settings	106
File System Monitoring Settings	108
Monitoring Settings of Network Connections	109
Configuring Exclusions	112
Excluding Files and Directories	112
Exclusion of Applications	113
Black and white Lists of Websites	114
Scheduler Settings	115
Preventing Threats Distributing over Network	117
Mode Settings	119
Configuring Dr.Web Cloud	121
Additional Information	122
Command Line Parameters	122
Starting the Autonomous Copy	123
Working from Command Line	123
Call Format	125
Usage Examples	141
Appendices	145
Appendix A. Types of Computer Threats	145





Appendix B. Neutralizing Computer Threats	149
Appendix C. Technical Support	152
Appendix D. Known Errors	153
Appendix E. Building Kernel Module for SpIDer Guard	199
Index	201



Conventions and Abbreviations

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

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



Command-line commands, which are entered via 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 execution of the specified command. According to the standard convention for UNIX-based systems

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

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



Introduction

Thank you for purchasing Dr.Web for Linux. It offers reliable protection from various types of [computer threats](#) using the most advanced virus [detection](#) and neutralization technologies.

This manual is intended to help users of computers running **GNU/Linux** family OSes (hereinafter, the **Linux** convention will be used), install and use GUI of Dr.Web for Linux version 11.0.

If the previous version of Dr.Web for Linux is already installed on your computer and you wish to upgrade the product to version 11.0, follow the steps described in the upgrade procedure (see section [Upgrading to a Newer Version](#)).



About this Product

Dr.Web for Linux is an anti-virus solution created to protect computers under **GNU/Linux** OS from viruses and other malware targeting different platforms.

Main program components (anti-virus engine and virus databases) are not only highly effective and resource-sparing, but also cross-platform, which lets Doctor Web specialists create reliable anti-virus solutions protecting computers and mobile devices under popular operating systems from threats that target different platforms. Currently, along with Dr.Web for Linux, Doctor Web offers anti-virus solutions for **UNIX**-based operating systems (such as **FreeBSD** and **Solaris**), **IBM OS/2**, **Novell NetWare**, **macOS** and **Windows**. Moreover, other anti-virus products have been developed to deliver protection for devices that run **Android**, **Symbian**, **BlackBerry**, and **Windows Mobile**.

Components of Dr.Web for Linux are regularly updated and Dr.Web virus databases are supplemented with new signatures to ensure up-to-date protection. For additional protection against unknown viruses, heuristic analysis methods are implemented in the anti-virus engine. The product also contacts the Dr.Web Cloud service, which collects up-to-date information about threats and helps prevent users from visiting unwanted websites and protect operating systems from infected files.

Main Functions

Dr.Web for Linux main functions:

1. **Detection and neutralization** of malicious programs (for example, viruses, including those that infect mail files and boot records, Trojans, mail worms) and unwanted software (for example, adware, joke programs, dialers). For details on methods used to neutralize threats, refer to [Appendix A. Types of Computer Threats](#).

The product uses several malware detection methods simultaneously:

- *Signature analysis*, which allows detection of known threats
- *Heuristic analysis*, which allows detection of threats that are not present in virus databases
- *Dr.Web Cloud* service that collects up-to-date information about recent threats and sends it to Dr.Web products.

Note that the heuristics analyzer may raise false alarms. Thus, objects that contain threats detected by the analyzer are considered "suspicious". It is recommended to quarantine such files and send them for analysis to Doctor Web anti-virus laboratory. For details on methods used to neutralize threats, refer to [Appendix B. Neutralizing Computer Threats](#).

File system scanning can be started in two ways: on demand and automatically, according to the schedule. There are two modes of scanning: full scan (scan of all file system objects) and custom scan (scan of selected objects: directories or files). Moreover, the user can start a separate scan of volume boot records and executable files that ran currently active processes. In the latter case, if a malicious executable file is detected, it is neutralized and all processes run by this file are forced to terminate.



For operating systems that have a graphic desktop environment, there is the [integration](#) of scanning functions with control panel as well as with file manager. In operating systems with mandatory access to files with several different access levels, the scanning of files, which are unavailable on the current access level, can be performed in [autonomous copy](#) mode.

Command-line [management tool](#) included in the product allows to scan for threats file systems of remote network hosts, that provide remote terminal access via SSH.



The remote scanning can be used only for detection of malicious and suspicious files on a remote host. To eliminate detected threats on the remote host, it is necessary to use administration tools provided directly by this host. For example, for routers and other "smart" devices, a mechanism for a firmware update can be used; for computing machines, it can be done via a connection to them (as an option, using a remote terminal mode) and respective operations in their file system (removal or moving of files, etc.), or via running an anti-virus software installed on them.

2. **Monitoring of file reference.** File events and attempts to run executable files are monitored. This feature allows to detect and neutralize malware at its attempt to infect the computer.
3. **Monitoring of network connections.** All attempts to access Internet servers (web servers, mail servers, file servers) are monitored in order to block access to the websites of the unwanted categories, and to prevent the transfer of email messages with infected files, unwanted links or spam. Check of email messages and files downloaded for viruses and other threats from the web is performed on the fly. To restrict access to unwanted websites, Dr.Web for Linux supports a database of web resource categories that is automatically updated, and black and white lists that are edited by the user. Dr.Web Cloud service is also used to check whether the requested web resource is marked malicious by other anti-virus products of Dr.Web.



Depending on a distribution, the anti-spam library could be unavailable. In this case, scanning of email messages for signs of spam is not performed.

If any email messages are falsely detected by the anti-spam library, it is recommended that they are forwarded to special addresses for analysis and improvement of spam filter quality:

- email messages, incorrectly *assessed as spam*, should be forwarded to vrnonspam@drweb.com;
- spam email messages, which were *not detected as spam*, should be forwarded to vrspam@drweb.com.

Each email message that is subject to analysis should be preliminary saved in the .eml format. Saved files should be attached to the email message sent to the required service address.

4. **Reliable isolation of infected or suspicious objects.** Such objects are moved to a special storage, quarantine, to prevent any harm to the system. When moved to quarantine, objects are renamed according to special rules and, if necessary, they can be restored to their original location only on demand.



5. **Automatic updating** of Dr.Web virus databases and of the anti-virus engine to support a high level of protection against malware.
6. **Operation under the control of a central protection server** (such as a Dr.Web Enterprise Server, or through a subscription to the Dr.Web AV-Desk service). This mode makes it possible to implement a unified security policy on computers within the protected network. It can be a corporate network, a private network (VPN), or a network of a service provider (for example, of an Internet service provider).



Use of the information stored in the service Dr.Web Cloud requires transfer of data on user activity (for example, addresses of visited websites). Thus, Dr.Web Cloud can be used only after the corresponding user agreement is received. When necessary, the use of Dr.Web Cloud can be disabled at any time in the program settings.

Program Structure

Dr.Web for Linux consists of the following components:

Component	Description
Scanner	The component which performs scanning of file system objects (files, directories, boot records) at user's request or as scheduled to detect threats. The user can start scans when operating in graphical mode or from the command line .
The file system monitor SpIDer Guard	The component which operates in resident mode and monitors file operations (creation, opening, closing, and running of a file). It sends Scanner tasks to scan new and modified files or executable files upon a program startup. It operates with the OS file system via the system mechanism fanotify or via the special kernel module (<i>LKM – Linux Kernel Module</i>) developed by Doctor Web.
The network connection monitor SpIDer Gate	<p>The component which works in resident mode and monitors all network connections.</p> <ul style="list-style-type: none">• It checks whether the requested URL falls into the unwanted category of web resources or in the user's black list, and, if so, blocks access to the resource.• Blocks transfer of email messages if they contain malicious objects or unwanted links.• The component also sends Scanner tasks to scan files downloaded from the Internet (from servers whose access is not restricted) and blocks their download if they contain threats. <p>Additionally, if it has the permission from the user, the component sends URL to Dr.Web Cloud service for a check.</p>
Anti-virus Engine	The core component of the anti-virus protection. It is used by Scanner to detect viruses and malicious programs as well as algorithms to analyze suspicious behavior.



Component	Description
Virus database	Automatically updated database used by anti-virus engine. The database contains information for detection and curing of known threats.
Database of web resource categories	Automatically updated database. The database contains information on web resources assigned to pre-defined categories. SpIDer Gate uses them to block access to web resources of categories that are marked as unwanted.
Updating component	It automatically downloads updates of the virus databases, databases of web resource categories and anti-virus engine from Doctor Web servers (both scheduled and on demand).
Graphical management interface	The component that provides a window graphical interface for management of Dr.Web for Linux. It allows users to run scanning of file system objects in the graphical mode, manage operation of SpIDer Guard and SpIDer Gate, view the quarantine contents, launch receiving of updates, and also configure Dr.Web for Linux's operation.
Notification agent	The component that works in a background mode. It displays pop-up notifications on events and Dr.Web for Linux's indicator in the notification area, runs scheduled scanning. By default it is launched when user's session starts in the desktop environment.
License Manager	The component simplifies work with licenses in graphical mode. It allows to activate license or demo period, view information about the current license, renew it, and install or remove the license key file.

Apart from the additional service components, Dr.Web for Linux also includes additional service components running in background. They do not require any user intervention.



SpIDer Guard, the file system monitor, can operate in one of the following modes:

- **FANOTIFY**—using the **fanotify** monitoring interface (not all **GNU/Linux**-based OSes support this mode)
- **LKM**—using the loadable **Linux** kernel module (compatible with any **GNU/Linux**-based OS with kernel 2.6.x and newer)

By default, the file system monitor automatically chooses the appropriate operation mode according to the environment. If SpIDer Guard cannot be started, [build and install](#) a loadable kernel module by using the supplied source codes.

Quarantine Directories

Quarantine directories serve for isolation of files that pose a threat to system security and cannot be currently cured. Such threats are those that are unknown to Dr.Web for Linux (that is, a virus is detected by the heuristic analyzer but the virus signature and method to cure are absent in the databases) or those that caused an error during scanning. Moreover, a file can be quarantined on



demand if the user selected this [action](#) in the list of detected threats or specified this action in Scanner or SpIDer Guard settings as reaction to this threat [type](#).

When a file is quarantined, it is renamed according to special rules. Renaming of isolated files prevents their identification by users or applications and complicates access to them in case of attempt to bypass quarantine management tools implemented in Dr.Web for Linux. Moreover, when a file is moved to quarantine, the execution bit is reset to prevent an attempt to run this file.

Quarantine directories are located in

- *user home directory* (if multiple user accounts exist on the computer, a separate quarantine directory can be created for each of the users)
- *Root directory of each logical volume* mounted to the file system

Dr.Web for Linux quarantine directories are always named as `.com.drweb.quarantine` and are not created until the *Quarantine (Isolate)* [action](#) is applied. At that, only a directory required for isolation of a concrete object is created. When selecting a directory, the file owner name is used: search is performed upwards from the location where the malicious object resides and if the owner home directory is reached, the quarantine storage created in this directory is selected. Otherwise, the file is isolated in the quarantine created in the root directory of the volume (which is not always the same as the file system root directory). Thus, any infected file moved to quarantine always resides on the volume, which provides for correct operation of quarantine in case several removable data storages and other volumes are mounted to different locations in the system.

Users can manage objects in quarantine both in [graphical](#) mode and from the [command line](#). Every action is applied to the consolidated quarantine; that is, changes affect all quarantine directories available at the moment. From the viewpoint of the user, the quarantine directory located in the user home directory is considered *User quarantine* and other directories are considered *System quarantine*.





Operation with quarantined objects is allowed even if no [active license](#) is found. However, isolated objects cannot be cured in this case.

File Permissions and Privileges

To scan objects of the file system and neutralize threats, Dr.Web for Linux (or rather the user under whom it runs) requires the following permissions:

Action	Required rights
<i>Listing all detected threats</i>	Unrestricted. No special permission required.
<i>Output of container contents (an archive, email file, etc.)</i>	Unrestricted. No special permission required.



Action	Required rights
(display only corrupted or malicious elements)	
<i>Moving to quarantine</i>	Unrestricted. The user can quarantine all infected files regardless of read or write permissions on them.
<i>Deleting threats</i>	<p>The user needs to have write permissions for the file that is being deleted.</p> <div> If threat is detected in a file located in a container (an archive, email message, etc.), its removal is replaced with moving of a container to quarantine.</div>
<i>Curing</i>	<p>Unrestricted. The access permissions and owner of a cured file remain the same after curing.</p> <div> The file can be removed if deletion can cure the detected threat.</div>
<i>Restoring a file from quarantine</i>	The user should have permissions to read the file and to write to the restore directory.
<i>Deleting a file from quarantine</i>	The user must possess write permissions to the file that was moved to quarantine.

To temporarily elevate permissions of Dr.Web for Linux, run in graphical mode, you can use the [corresponding button](#) in Dr.Web for Linux window (which is available only if the elevation of permissions is necessary to complete an operation successfully). To run Dr.Web for Linux in [graphical mode](#) or the command-line management [tool](#) with superuser privileges, you can use the **su** command, which allows to change the user, or the **sudo** command, which allows you to execute a command as another user.



Scanner cannot check file which size exceeds 4 GB (on attempt to scan such files, the following error message will be displayed: *"The file is too large"*).

Operation Modes

Dr.Web for Linux can operate both in Standalone mode and as a part of an *anti-virus network* managed by a *central protection server*. Operation in *Central protection mode* does not require installation of additional software or Dr.Web for Linux re-installation or uninstallation.

- *In Standalone mode*, the protected computer is not connected to an anti-virus network and its operation is managed locally. In this mode, configuration and license key files are located on



local disks and Dr.Web for Linux is fully controlled from the protected computer. Updates to virus databases are received from Doctor Web update servers.

- *In Central protection mode*, protection of the computer is managed by the central protection server. In this mode, some functions and settings of Dr.Web for Linux can be adjusted in accordance with the general (corporate) anti-virus protection policy implemented on the anti-virus network. The license [key file](#) used for operating in Central protection mode is received from the central protection server. The key file stored on the local computer, if any, is not used. Statistics on virus events together with information on Dr.Web for Linux operation are sent to the central protection server. Updates to virus databases are also received from the central protection server.
- *In Mobile mode*, Dr.Web for Linux receives updates from Doctor Web update servers, but operation of the product is managed with the local settings. The used key file is received from the central protection server.

When Dr.Web for Linux is operating in Central protection mode or Mobile mode, the following options are blocked:

1. Deletion of a license key file in License Manager
2. Manual start of an update process and adjustment of update settings
3. Configuration of file system scanning parameters

Configuration of SpIDer Guard settings as well as an option to enable or disable SpIDer Guard when Dr.Web for Linux is running under control of the central protection center is dependent on permissions specified on the server.



In the Central protection mode, scanning of files according to a [set schedule](#) is not available.

Note that if launch of scanning on demand is prohibited on the used central protection server, the [page for starting scanning](#) and **Scanner** button of the Dr.Web for Linux window will be disabled.

Central Protection Concept

Doctor Web's solutions for central protection use client-server model (see the figure below).

Workstations and servers are protected by *local anti-virus components* (herein, Dr.Web for Linux) installed on them, which provides for anti-virus protection of remote computers and allows connection between the workstations and the central protection server.

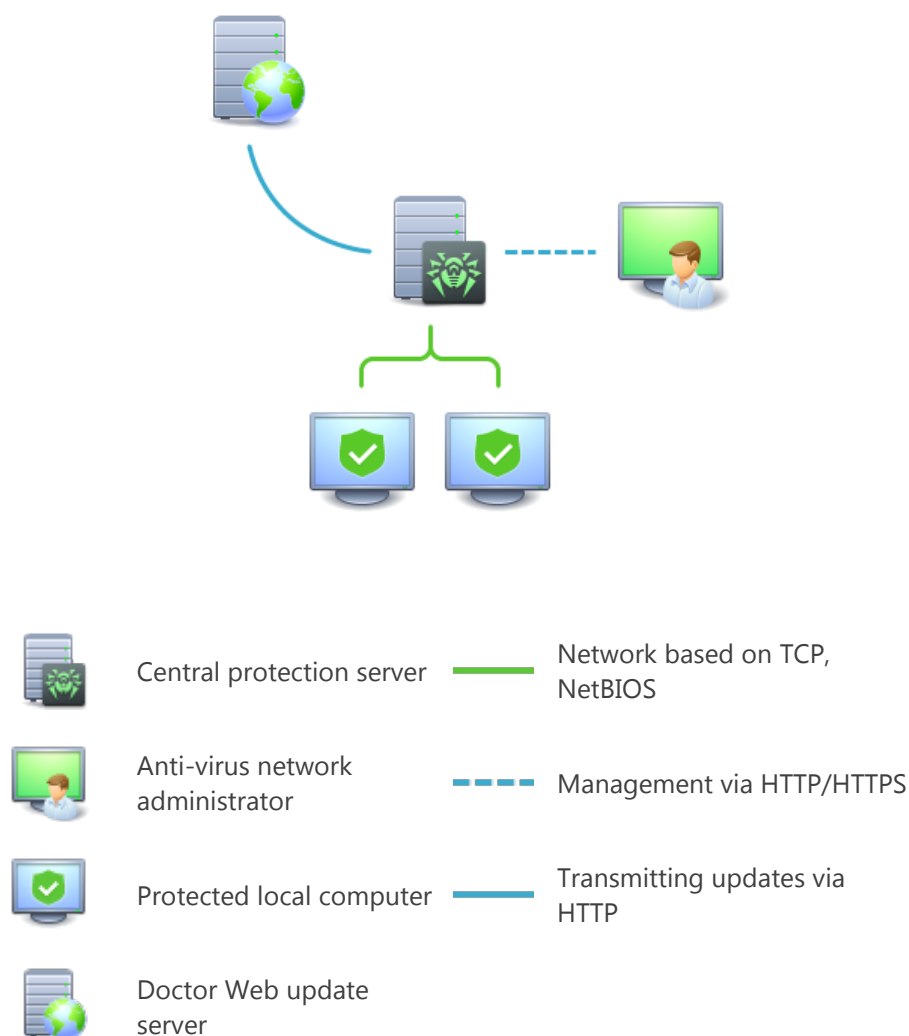


Figure 1. Logical structure of the Anti-virus Network

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

All necessary updates are downloaded to the central protection server from Doctor Web update servers.

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



Local anti-virus components are not compatible with anti-virus products of other companies or anti-virus solutions of Dr.Web if the latter do not support operation in central protection mode (for example, Dr.Web for Linux version 5.0). Installation of two anti-virus programs on the same computer can cause a system crash and loss of important data.

Connecting to Anti-Virus Network

Dr.Web for Linux can be connected to an anti-virus network in one of the following ways:

- On the **Mode** [tab](#) of the [settings window](#) in the Dr.Web for Linux graphical interface.
- Using the `esconnect` [command](#) of the command-line management tool (**drweb-ctl**).

Disconnecting from Anti-Virus Network

Dr.Web for Linux can be disconnected to an anti-virus network in one of the following ways:

- On the **Mode** [tab](#) of the [settings window](#) in the Dr.Web for Linux graphical interface.
- Using the `esdisconnect` [command](#) of the command-line management tool (**drweb-ctl**).

Testing Product Operation

The *EICAR* (*European Institute for Computer Anti-Virus Research*) test helps testing performance of anti-virus programs that detect viruses using signatures. This test was designed specially so that users could test reaction of newly-installed anti-virus tools to detection of viruses without compromising security of their computers.

Although the *EICAR* test is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", Dr.Web anti-virus products report the following: **EICAR Test File (NOT a Virus!)**. Other anti-virus tools alert users in a similar way. The **EICAR** test file is a 68-byte COM-file for **MS DOS/MS Windows** that outputs the following line on the terminal screen or to the console emulator when executed:

```
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
```

The EICAR test contains the following character string only:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To create your own test file with the "virus", you may create a new file with the line mentioned above.

If Dr.Web for Linux operates correctly, the test file is detected during a file system scan regardless of the scan type and the user is notified on the detected threat: **EICAR Test File (NOT a Virus!)**.



An example of a command that checks operation of the program by means of **EICAR** test from the command line:

```
$ tail /opt/drweb.com/share/doc/drweb-common/readme.eicar | grep X50 >  
testfile && drweb-ctl scan testfile && rm testfile
```

From the file `/opt/drweb.com/share/doc/drweb-common/readme.eicar` (supplied with the product), this command retrieves a string that represents the body of the **EICAR** test file, then writes it into a file named `testfile` created in the current directory, then scans the resulting file and removes this file afterwards.



The above-mentioned test requires write access to the current catalog. In addition, make sure that it does not contain a file named `testfile` (if necessary, change the file name in the command).

If a test virus is detected, the following message is displayed:

```
<path to the current directory>/testfile - infected with EICAR Test File (NOT a  
Virus!)
```

If an error occurs during the test, refer to the description of [known errors](#).




If SpIDer Guard is enabled, a malicious file can be immediately removed or quarantined (depending on the configuration of the component). In this case, the command **rm** will inform that the file is missing, which implies that the monitor operates in normal mode.



System Requirements

You can use Dr.Web for Linux on a computer that meets the following requirements:

Component	Requirement
Platform	CPU with the Intel/AMD architecture and command system are supported: 32-bit (IA-32, x86); 64-bit (x86-64, x64, amd64).
Space on hard disk	At least 512 MB of free disk space on a volume where the Dr.Web for Linux directories are located.
Operating system	<p>Linux for Intel x86/amd64 platform based on kernel ver. 2.6.37 or later, and using PAM and library glibc ver. 2.13 or later.</p> <p>Tested Linux distributions are listed below.</p> <div> For systems operating on 64-bit platforms, support of 32-bit applications must be enabled (probably, additional libraries must be installed for this, see below).</div> <hr/> <p>For the correct operation of SpIDer Gate, OS kernel must be built with inclusion of the following options:</p> <ul style="list-style-type: none">• <code>CONFIG_NETLINK_DIAG</code>, <code>CONFIG_INET_TCP_DIAG</code>;• <code>CONFIG_NF_CONNTRACK_IPV4</code>, <code>CONFIG_NF_CONNTRACK_IPV6</code>, <code>CONFIG_NF_CONNTRACK_EVENTS</code>;• <code>CONFIG_NETFILTER_NETLINK_QUEUE</code>, <code>CONFIG_NETFILTER_NETLINK_QUEUE_CT</code>, <code>CONFIG_NETFILTER_XT_MARK</code>. <p>The set of required options from the specified list can depend on the used distribution kit of GNU/Linux.</p>
Other	<p>The following valid network connections:</p> <ul style="list-style-type: none">• An Internet connection to download updates and for sending requests to the Dr.Web Cloud service (only if it is manually authorized by the user).• When operating in central protection mode, connection to the server on the local network is enough; connection to the Internet is not required.



Dr.Web for Linux is incompatible with other anti-virus software programs. To avoid system errors and data loss that may occur when installing two anti-viruses on one computer, uninstall all other anti-virus programs from the computer before the Dr.Web for Linux installation.



The product was tested on the following **Linux** distributions:

Linux distribution name	Versions	Platforms
Astra Linux Special Edition (Smolensk)	1.5	x86_64
CentOS	6.9, 7.4	x86, x86_64
Debian	7.11, 8.10, 9.3	x86_64
Fedora	27	x86, x86_64
Red Hat Enterprise Linux	7.4	x86_64
SUSE Linux Enterprise Server	11 SP4, 12 SP3	x86_64
Ubuntu	14.04, 16.04	x86_64

Other **Linux** distributions that meet the above-mentioned requirements have not been tested for compatibility with Dr.Web for Linux but may be supported. If a compatibility issue occurs, contact technical support on the official website at <https://support.drweb.com/request/>.

Required additional components and packages

- For **CentOS, Debian, Fedora, Red Hat Enterprise Linux, Ubuntu** on the platform `x86_64`, a package that enables support for 32-bit applications is required (**libc6-i386** or **glibc.i686** depending on the OS).
- To enable Dr.Web for Linux operation in graphical mode and startup of the program for product installation and uninstallation in graphical mode, **X Window System** graphic shell and any window manager is required. Moreover, for correct operation of the [indicator](#) for **Ubuntu Unity** desktop environment, the additional library may be required (by default, the library named **libappindicator1** is required).
- To start the product installer or uninstaller, designed for the command line, in graphical mode, a terminal emulator (such as **xterm**, **xvt**, etc.) is required.
- To enable privileges elevation during installation or uninstallation, one of the following utilities is required: **su**, **sudo**, **gksu**, **gksudo**, **kdesu**, **kdesudo**. For correct operation of the product, **PAM** must be used in the operating system.



For convenient work with Dr.Web for Linux in the [command line](#), you can enable command auto-completion in the used command shell (if disabled).

If you encounter any problem with installation of additional packages and components, refer to manuals for the used distribution of the operating system.



Compatibility with components of operating systems

- By default, SpIDer Guard uses the **fanotify** system mechanism, while on those operating systems on which the **fanotify** is not implemented or is unavailable for other reasons, the component uses a special *LKM module*, which is supplied in pre-built form within the product. The product distribution has LKM modules for all **GNU/Linux** systems mentioned above. If required, you can [build a kernel module](#) independently from the distributed source codes for any OS that uses the kernel **GNU/Linux** of version 2.6.x and later.



Operation of SpIDer Guard via **GNU/Linux** (LKM module) is not supported for operating systems launched in the **Xen** hypervisor environment. An attempt to load the LKM module used by SpIDer Guard during the OS operation in the **Xen** environment can lead to a [critical error](#) of the kernel (so called "*Kernel panic*" error).

- SpIDer Gate may conflict with other firewalls installed in your system:
 - Conflict with **Shorewall** and **SuseFirewall2** (for **SUSE Linux Enterprise Server**). In case of conflict with these firewalls, an error message of SpIDer Gate with a code x109 is displayed. A way to resolve this conflict is [described](#) in the Appendix "Known Errors".
 - Conflict with **Firewalld** (for **Fedora, CentOS, Red Hat Enterprise Linux**). In case of conflict with these firewall, the SpIDer Gate error message with a code x102 is displayed. A way to resolve this conflict is [described](#) in the Appendix "Known Errors".
- In case if the used OS includes the version of **NetFilter** less than 1.4.15, SpIDer Gate may operate incorrectly. This problem is related to the internal error of the **NetFilter**, and looks like as follows: after disabling SpIDer Gate, the network connections are broken and cannot be re-established. If you run into this problem, it is recommended to upgrade your OS to version that includes **NetFilter** 1.4.15 or above. How to resolve the problem, is [described](#) in the Appendix "Known Errors".
- Under normal operation, SpIDer Gate is compatible with all user applications that use network, including web browsers and mail clients. For the correct [scanning of secured connections](#), it is necessary to add the certificate Dr.Web for Linux to the list of trusted certificates of those applications that use the secured connections (for example, web browsers and mail clients).
- After [changing](#) operation of SpIDer Gate (enabling of the previously disabled monitor, change of the scanning mode of secured connections), it is necessary to *restart mail clients* that use the IMAP protocol to receive email messages from the mail server.

Compatibility with Security Subsystems

By default, Dr.Web for Linux does not support **SELinux**. In addition, Dr.Web for Linux operates in reduced functionality mode in the **GNU/Linux** systems that use mandatory access models (for example, in systems supplied with the **PARSEC** mandatory access subsystem that appends different privilege levels to users and files).

If installation of Dr.Web for Linux is required for systems with **SELinux**, as well as for systems that use mandatory access models, it is necessary to execute additional settings of security



subsystems so that Dr.Web for Linux operates in full functionality mode. For details, refer to the section [Configuring Security Systems](#).



Licensing

Permissions to use Dr.Web for Linux are granted by the license purchased from 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 product installation. The license contains information on the user and the vendor as well as usage parameters of the purchased product, including:

- List of components licensed to the user
- Dr.Web for Linux license period
- Other restrictions (for example, number of computers on which the purchased Dr.Web for Linux is allowed for use)

For evaluation purposes users may also activate a *demo period*. If activation terms of the demo period are complied with, a user gains rights to use Dr.Web for Linux with full functionality for the whole activated 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 the Dr.Web for Linux 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 (including cases when a validity of a purchased license or a demo period is expired), anti-virus functions of the Dr.Web for Linux components are blocked. Moreover, updates for the Dr.Web virus databases and components cannot be downloaded from Doctor Web update servers. However, you can activate the Dr.Web for Linux by connecting it to the central protection server as a part of the *anti-virus network* administered by the enterprise or Internet service provider. In this case, operation of the product and updating are managed by the central protection server.

Purchasing and Registering License

After a license is purchased, updates to product components and virus databases are regularly downloaded from Doctor Web update servers. Moreover, if the customer encountered any issue when installing or using the purchased product, they can take advantage of technical support service provided by Doctor Web or its partners.

You can purchase any Dr.Web product as well as obtain a product serial number either from our partners (see the list of partners on <https://partners.drweb.com/>) or in our online store <https://estore.drweb.com/>. For details on license periods and license types, visit the Doctor Web official website at <https://www.drweb.com/>.



License registration is required to prove that you are a legal user of Dr.Web for Linux and activate Dr.Web for Linux functions including virus database updating. It is recommended to register the product and activate the license once installation completes. A purchased license can be activated in one of the following ways:

- Via the [Registration Wizard](#) included in License Manager;
- On the Doctor Web's official website at <https://products.drweb.com/register/>.

During activation, it is required to enter the serial number. The serial number is supplied with the product or via email when purchasing or renewing the license online.



To renew the license, enter your registered serial number or provide a previous license key file. Otherwise, the period of license validity will be reduced by 150 days.

If you have several licenses for using Dr.Web for Linux on several computers, but choose to use Dr.Web for Linux only on one computer, you can specify this and, hence, license validity period will be automatically extended.

Obtaining Demo License

Users of Dr.Web can obtain a demo period for

- 3 months
- 1 month

To obtain a demo period for 3 months, register on the Doctor Web official website and provide the requested personal data. After registration completes, you will receive an email with a serial number for Dr.Web for Linux activation. Demo period for 1 month can be received in the Registration wizard window of License Manager. To obtain a demo period for 1 month, you do not need to provide your personal data.

The Registration Wizard of License Manager opens upon the first Dr.Web for Linux startup (usually Registration Wizard starts once installation of Dr.Web for Linux completes). You can start registration or obtain a demo period from the License Manager window at any time by clicking the **Get new license** button on the [page](#) with information on the current license.



To activate a license using the serial number or request a demo license, a valid Internet connection is required.

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

When a demo period or license is activated via License Manager, the key file (license or demo) is automatically generated on the local computer in its target directory. If you register on the website, the key file is sent by email and you need to [install](#) the key file manually.



If the registration wizard is unavailable (for example, due the absence of operating system GUI), you can use the [command](#) of license management [of the command line interface](#) **drweb-ctl**, which allows to obtain the demo key file or license key file for the serial number of the license registered (including the serial number of demo period, obtained by email). The description of **drweb-ctl** can be found in user manual.



Full version of User Manual for Dr.Web for Linux is available

- At Doctor Web official website <https://download.drweb.com/doc/> (Internet connection is required).
- You can view a PDF file in the `/opt/drweb.com/share/doc` directory (the suffix in the name indicates the language).

Subsequent Registration

If a key file is lost but the existing license is not expired, you must register again by providing the personal data you specified during the previous registration. You may 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 requests in excess of that number are sent, no key file will be delivered. To receive a lost key file, contact [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.

Key File

The key file is a special file stored on the local computer. It corresponds to the purchased license or activated demo period for Dr.Web for Linux. The file contains information on the provided license or demo period and regulates usage rights in accordance with it.

The key file has `.key` extension and is valid if satisfies the following criteria:

- License or demo period is not expired.
- Demo period or license applies to all anti-virus components required by the product.
- Integrity of the key file is not violated.

If any of the conditions are violated, the license key file becomes invalid.



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

Components of Dr.Web for Linux regularly check whether the key file is available and valid. The key file is digitally signed to prevent its editing. So, the edited key file becomes invalid. It is not recommended to open your key file in text editors in order to avoid its accidental invalidation.

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 to 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 must use the same product serial number and customer data that you provided during the registration.



Dr.Web key files are usually packed in a ZIP archive if sent via email. The archive with a key file is named `agent.zip` (note that if there is *several* archives in an email message, you should use only `agent.zip`). In the Registration Wizard, you may specify the direct path to the archive without its unpacking. Before installing a key file, unpack it using any suitable tool and extract a key file to any directory (for example, to your home directory or to a USB flash drive).

Key File Installation

If you have a key file corresponding to the valid license for the product (for example, if you obtained the key file by email or if you want to use Dr.Web for Linux on another computer), you can activate Dr.Web for Linux by specifying the path to the key file. You can specify the key file path:

- In the [License Manager](#) by clicking **Other activation types** on the first step of the registration procedure and specifying a path to the key file or to the zip archive with the key.
- Manually. For that purpose
 1. Unpack the key file if archived
 2. Copy the key file to the `/etc/opt/drweb.com` directory and rename the file to `drweb32.key` if necessary.
 3. Execute the [command](#)

```
# drweb-ctl reload
```

to apply all changes.

You can also use the following [command](#):

```
# drweb-ctl cfset Root.KeyPath <path to a key file>
```



In this case, the key file will not be copied to the `/etc/opt/drweb.com` directory and will remain in its original location.



If the key file is not copied to the `/etc/opt/drweb.com` directory, the user becomes responsible for ensuring that the file is protected from corruption or deletion. This installation method is not recommended as the key file can be accidentally deleted from the system (for example, if the directory, where the key file resides, is periodically cleaned up). Remember that if a key file is lost, you can request the support for a new one, but the number of such requests is limited.

Connection Settings File

The connection settings file is a special file that stores parameters that configure connection between Dr.Web for Linux and the [central protection](#) server. This file is supplied by the administrator of the anti-virus network or the Internet service provider (if the latter provides support for the central anti-virus protection service).

You can use this file to activate Dr.Web for Linux when connecting it to the central protection server (in this case, you cannot use Dr.Web for Linux in Standalone mode without purchasing additional [license](#)).

Connecting to the Central Protection Server

If the Internet service provider or network administrator submitted a file with settings of connection to the central protection server, you can activate Dr.Web for Linux by specifying the file path. To specify a path to the connection settings file

- In the open program [settings window](#), go to the **Mode tab** and select the **Enable central protection mode** check box. On the appeared menu, select the *Load from file* item, specify the path to the connection settings file and click **Connect**.



Installing and Uninstalling Dr.Web for Linux

This section describes how to [install](#) and [uninstall](#) the Dr.Web for Linux version 11.0. In this section, you can also find information on how to obtain [current updates](#) and a procedure of [upgrading to a new version](#), if the previous version of Dr.Web for Linux is already installed on your computer.

Besides, this section describes the procedure of [custom installation and uninstallation](#) of the product components (for example, to resolve errors that occurred during the course of the Dr.Web for Linux operation) and [configuration of advanced security subsystems](#) (such as **SELinux**) that could be necessary for installation and operation of the product.

To perform these procedures, root permissions are required (i.e. privileges of the *root* user). To elevate privileges when installing or uninstalling the product, use the **su** command for changing the current user or the **sudo** command to execute the specified command with the privileges of another user.



Compatibility *is not guaranteed* for Dr.Web for Linux and anti-virus products of other developers. Due to the fact that installation of two anti-viruses on one machine can lead to *errors in the operation system and loss of important data*, before the installation of Dr.Web for Linux, *it is strongly recommended* that you delete anti-virus products of other developers from the computer.

If your computer *already has* other Dr.Web anti-virus product installed from the [universal package](#) (`.run`), and you want to install one more Dr.Web anti-virus product (for example, you have Dr.Web for UNIX File Servers installed from the universal package, and in addition you want to install Dr.Web for Linux), it is necessary to make sure that the version of the installed product is the *same* as the version of the product you want to install. If the product version that you plan on installing is newer than the installed product version, *before* installation, it is necessary to [update](#) the installed product to the version of the product you want to install additionally.



Installing Dr.Web for Linux

To install Dr.Web for Linux, do one of the following:

1. Download the installation file with the [universal package](#) for UNIX systems from the Doctor Web official website. The package is supplied with installers (both graphical and console) started depending on the environment.
2. Download the [native packages](#) from the corresponding package repository of Doctor Web.



After the installation of Dr.Web for Linux is performed using one of the specified ways, you need to activate the license or to install the key file. You can also connect Dr.Web for Linux to the central protection server. Anti-virus protection *will be disabled* unless you do that.

If a mail client runs in the system (such mail client as **Mozilla Thunderbird**) that uses the IMAP protocol to receive email messages, it is necessary to restart it after the anti-virus installation is complete to provide the scanning of incoming email messages.

After you installed the product by any of the mentioned means, you can [uninstall](#) or [update](#) it if there are fixes for its components available or if a new product versions is released. If required, you can also [configure security subsystems](#) of **Linux** for correct operation of the installed product. If there is a problem with functioning of any individual components, you can perform their [custom installation and uninstallation](#), without uninstalling the entire installed product.

Installing Universal Package

Dr.Web for Linux is distributed as an installation file named `drweb-<version>-av-linux_<platform>.run`, where `<platform>` is a platform for which the product is intended (x86 for 32-bit platforms and amd64 for 64-bit platforms). For example:

```
drweb-11.0.7-av-linux-amd64.run
```

Note that the installation file name corresponding to the above-mentioned format is referred to as `<file_name>.run`.

To install Dr.Web for Linux components:

1. Download the installation file from the Doctor Web official website.
2. Save it to the hard disk drive of the computer to any convenient and available directory (for example, `/home/<username>`, where `<username>`—name of the current user).
3. Go to the directory with the saved file and allow its execution, for example, with the following command:

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



4. Execute the archive using the following command:

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

or use the standard file manager of the graphical shell for both changing the file properties (permissions) and running the file.

First, this will run an integrity check of the archive, after which the archived files are unpacked to a temporary directory and an installation program is started. If the user does not have root privileges, the installation program attempts to elevate its privileges asking you for the root password (**sudo** is used). If the attempt fails, the installation process aborts.



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 an appropriate message is displayed. In this case, change the value of the `TMPTDIR` system environment variable so that it points to a directory with enough free space and repeat the installation. You can also use the `--target` option (for more details, see [Custom Component Installation and Uninstallation](#) section).

Depending on the environment where the distribution package is launched, one of the following installation programs runs:

- Installation Wizard for [graphical mode](#).
- Installer for [command-line mode](#).

At that, the installer for command-line mode is automatically started if the Installation Wizard for graphical mode fails to start.

5. Follow the installer's instructions.

You can also start the installation program in silent mode by executing the command:

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

In this case the installation program is started in the silent mode and will operate without a user interface (this means it also will not have any dialogs that are normally displayed in the command-line mode).

Note that

- Using this option means that you *accept* the terms of the Dr.Web License Agreement. The License Agreement's text is located in the `/opt/drweb.com/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.
- Administrative (root) privileges are required to start the uninstall program in silent mode. To elevate the privileges, you can use the **su** and **sudo** commands.



If the used **Linux** distribution features **SELinux**, the installation process can be interrupted by the security subsystem. If such situation occurs, set **SELinux** to the *Permissive* mode. To do this, enter the following command:

```
# setenforce 0
```

And restart the installer. After the installation completes, configure **SELinux** [security policies](#) to enable correct operation of the product components.

All unpacked installation files are deleted once the installation process completes.



It is recommended that you save the downloaded file `<file_name>.run`, from which the installation was performed, for the possibility of reinstallation of the product or its components without the need to update the product version.

After installation completes, the **Dr.Web** item displays on the **Applications** menu in the desktop graphical shell. This item contains two items:

- **Dr.Web for Linux** to start Dr.Web for Linux in [Graphical Mode](#).
- **Remove Dr.Web components** item to [uninstall](#) the components.

The program [indicator](#) automatically appears in the notification area after the user logs in again.



For correct operation of Dr.Web for Linux, it may be necessary to install packages specified in the [System Requirements](#) section (for example, the library that enables support for 32-bit applications installed on a 64-bit platform and **libappindicator1**, which is a library for correct display of the program [indicator](#) in the notification area).

Installing in Graphical Mode

Upon its startup, the installation program checks if there are any problems that can cause errors in Dr.Web for Linux operation or can render it inoperable. If such problems are found, an appropriate message is displayed on the screen listing the issues. You can cancel the installation by clicking **Exit** and resolve the problems. In this case, you will need to [restart](#) the installation program afterwards (after [required libraries](#) are installed, **SELinux** is temporarily [disabled](#), and so on). However, you may choose not to cancel the installation of Dr.Web for Linux by clicking **Continue**. After you click the button, the process starts and the window of the installation wizard is displayed. In this case, you will need to resolve the problems after the installation completes or if [errors](#) in Dr.Web for Linux operation occur.

After the installation program for graphical mode starts, a window of the Installation Wizard displays.



Figure 2. Welcome page of the Installation Wizard

To install Dr.Web for Linux on your computer, do the following:

1. To view the terms of the Doctor Web License agreement, click the corresponding link on the start page of the installation master. After that, a page with the License agreement text and copyright information for the installed components opens.

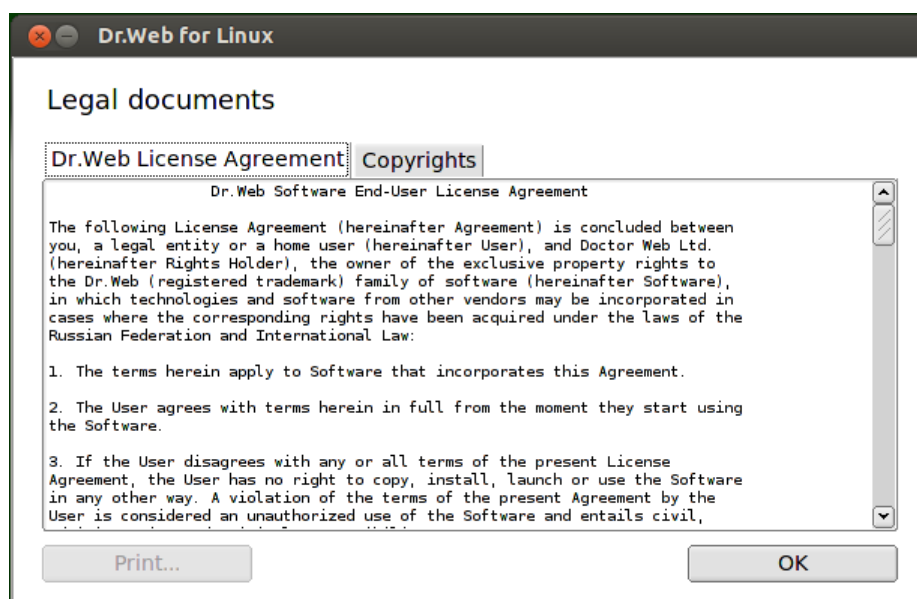


Figure 3. Viewing License Agreement

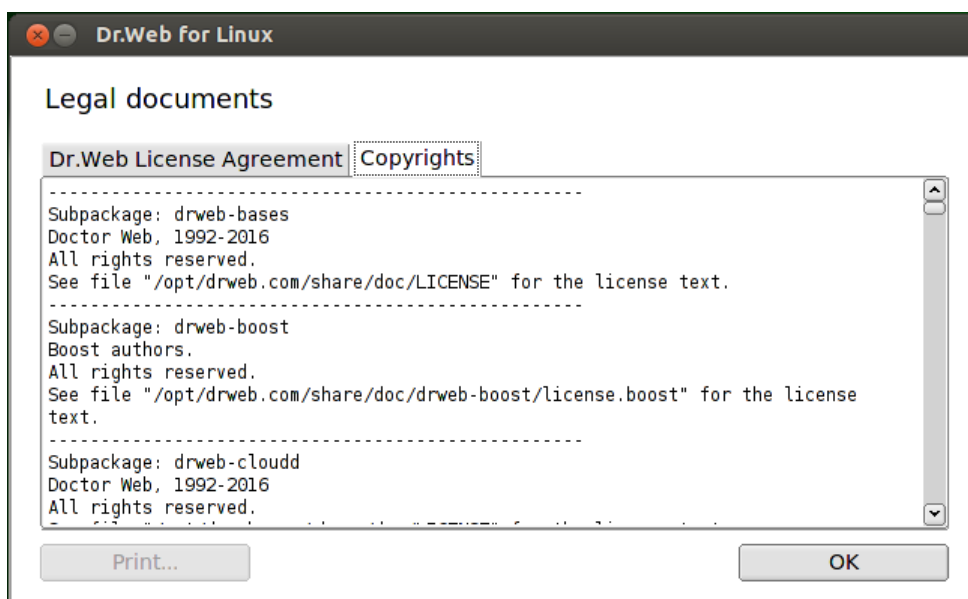


Figure 4. Copyright information page

When required, if a printer is installed and configured in your system, you can print off the License agreement terms and copyright information. To do that, open the corresponding tab of the License agreement page and click the **Print** button.

To close the page, click **OK**.

2. Before the setup starts copying files, you can enable Dr.Web for Linux to connect to Dr.Web Cloud automatically after the installation. To do so, enable the corresponding option (when you start the wizard, the option is enabled by default). If you do not wish Dr.Web for Linux to use the service Dr.Web Cloud, clear the check box. If necessary, you can allow Dr.Web for Linux to connect to the Dr.Web Cloud service in the program's [settings](#) at any time.
3. To continue the installation, click **Install**. By doing so, you also accept terms of Doctor Web License agreement. If you choose not to install Dr.Web for Linux on your computer, click **Cancel**. Once the button is clicked, the Installation Wizard exits.
4. After installation starts, a page with the progress bar opens. If you wish to view the logs during the installation, click the **Details** button.



Figure 5. Installation progress bar

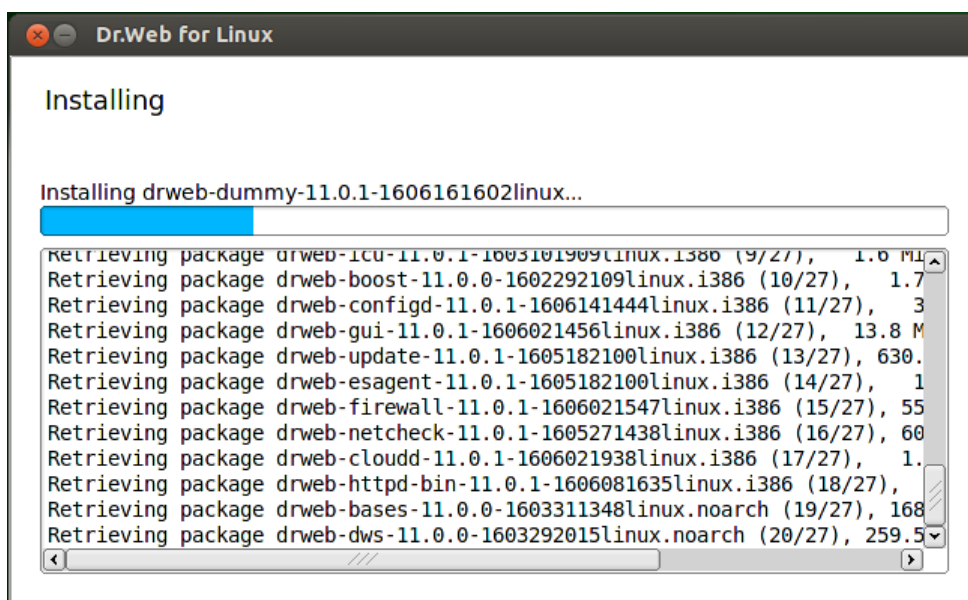


Figure 6. Viewing installation log file

5. After program files are successfully copied and all required adjustments to system settings are made, the final page with the installation results is displayed.

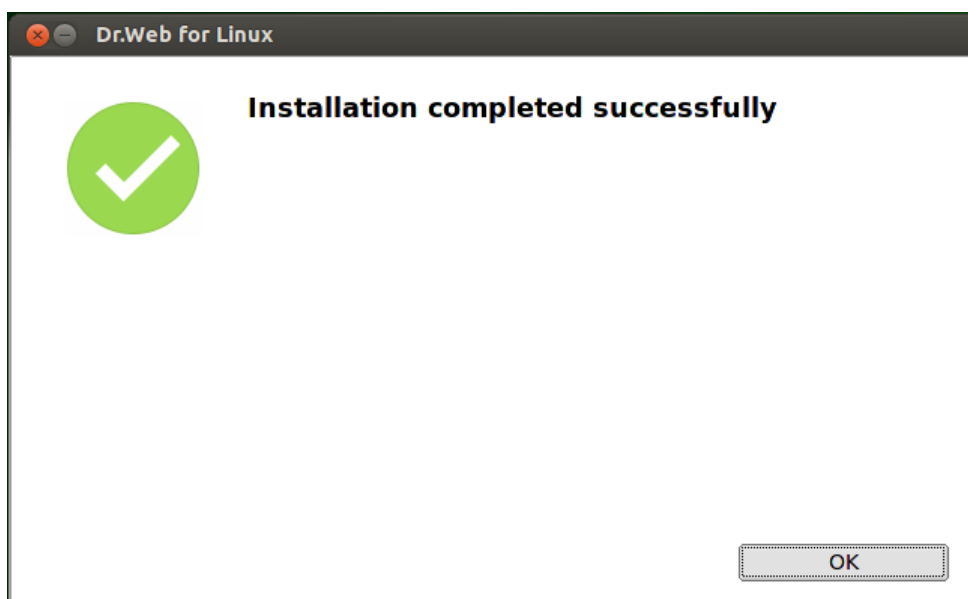


Figure 7. Installation results

6. To exit the Installation Wizard, click **OK**. If the desktop environment you are using supports this feature, in the final installation step you will be prompted to launch Dr.Web for Linux in [graphical mode](#). To run the program after installation, select the **Run Dr.Web for Linux now** check box and click **OK**.

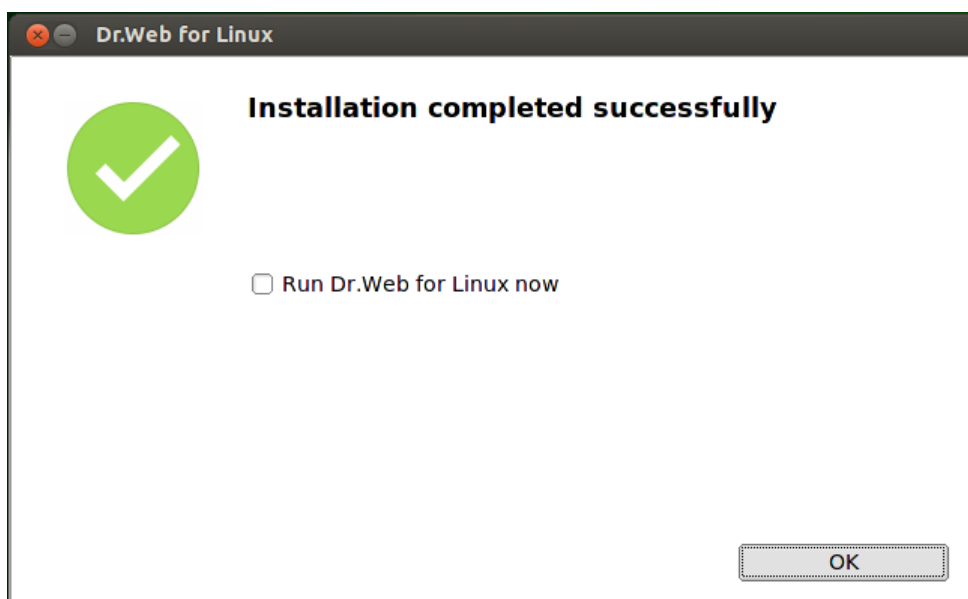


Figure 8. Suggestion to start Dr.Web for Linux after installation is completed

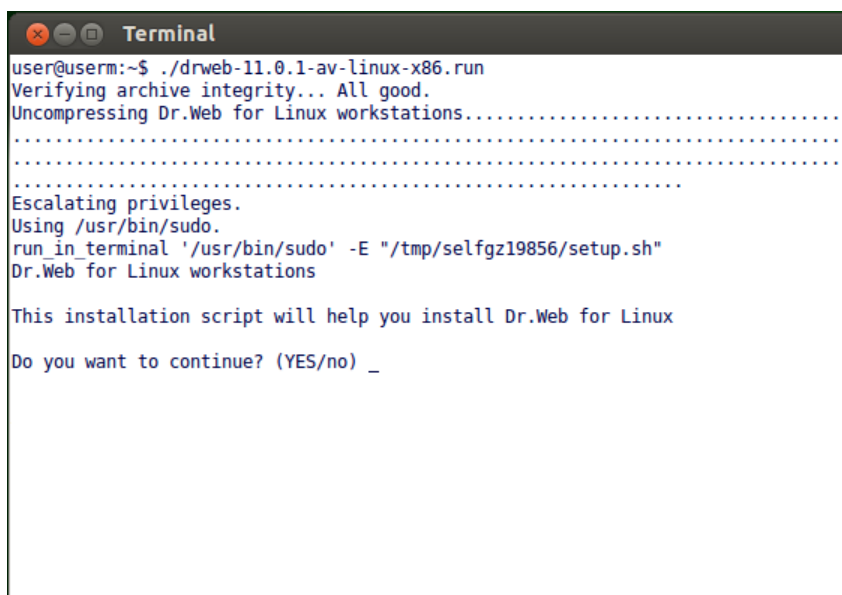
If the installation process fails due to an error, the final page of the Installation Wizard will contain the corresponding message. In this case, exit the Installation Wizard by clicking **OK**. Then remove the problems that caused this error and start an installation procedure again.



Installing from Command Line

Once the installation program for the command line starts, the command prompt displays on the screen.

1. To start installation, enter *Yes* or *Y* in response to the "Do you want to continue?" question. To exit the installer, enter *No* or *N*. In this case, installation is canceled.



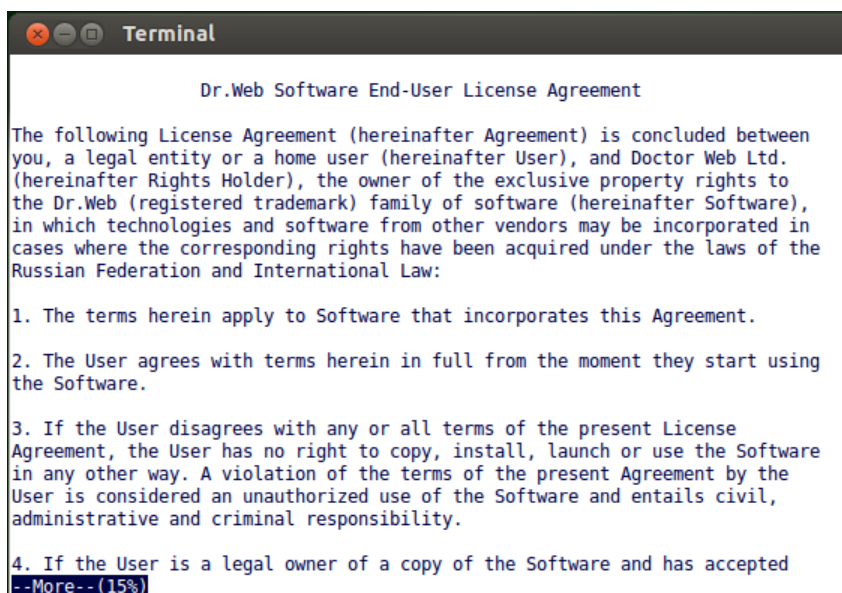
```
user@userm:~$ ./drweb-11.0.1-av-linux-x86.run
Verifying archive integrity... All good.
Uncompressing Dr.Web for Linux workstations.....
.....
Escalating privileges.
Using /usr/bin/sudo.
run_in_terminal '/usr/bin/sudo' -E "/tmp/selfgz19856/setup.sh"
Dr.Web for Linux workstations

This installation script will help you install Dr.Web for Linux

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

Figure 9. Command prompt to install the product

2. After that, you need to view the terms of the Doctor Web License agreement, which is displayed on the screen. Press ENTER to line down or SPACEBAR to page down the text. Note that options to line up or page up the License agreement text are not provided.



```
Dr.Web Software End-User License Agreement

The following License Agreement (hereinafter Agreement) is concluded between
you, a legal entity or a home user (hereinafter User), and Doctor Web Ltd.
(hereinafter Rights Holder), the owner of the exclusive property rights to
the Dr.Web (registered trademark) family of software (hereinafter Software),
in which technologies and software from other vendors may be incorporated in
cases where the corresponding rights have been acquired under the laws of the
Russian Federation and International Law:

1. The terms herein apply to Software that incorporates this Agreement.

2. The User agrees with terms herein in full from the moment they start using
the Software.

3. If the User disagrees with any or all terms of the present License
Agreement, the User has no right to copy, install, launch or use the Software
in any other way. A violation of the terms of the present Agreement by the
User is considered an unauthorized use of the Software and entails civil,
administrative and criminal responsibility.

4. If the User is a legal owner of a copy of the Software and has accepted
--More-- (15%)
```

Figure 10. Viewing License Agreement text

3. After you read the License agreement text, you are prompted to accept the terms. Type *Yes* or *Y* if you accept the License agreement. If you refuse to accept them, type *No* or *N*. In the latter case, the installer automatically exits.



```
Terminal
6. The Software, its components, and the accompanying documentation are
provided to the User as is, without any express or implied warranty of any
kind. The Rights Holder is not liable to the User for any problems that arise
or may arise, including but not limited to, while the User is installing,
updating, supporting, and maintaining the Software (including compatibility
issues with other software products, drivers, etc.), problems due to the
User's misinterpretation of guidance provided in the documentation, or failure
of the Software to meet the User's expectations.

7. The Rights Holder is not liable to you for possible negative consequences of
any kind, including (without limitation) those caused by the incompatibility or
conflict between the Software and other software products installed on the same
computer, incompatibility or conflict with the computer hardware.

8. The relations between the Rights Holder and the User under this Agreement
are governed by the law of the Russian Federation. All disputes related to
adherence to the terms herein are to be resolved in corresponding courts at
the Rights Holder's location.

9. The Rights Holder can change terms of this agreement unilaterally. A new
version of the agreement shall enter into force as soon as the user is
notified about changes to the agreement by the Rights Holder.

Do you agree with the terms of this license? (yes/NO) yes_
```

Figure 11. Accepting the License agreement terms

4. After you accept the terms of the License Agreement, installation of the Dr.Web for Linux components automatically starts. During the procedure, the information about the installation process (installation log), including the list of installed components, will be displayed on the screen.

```
Terminal
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following 27 NEW packages are going to be installed:
  drweb-bases drweb-boost drweb-clouddd drweb-common drweb-configd drweb-dws drwe
b-esagent drweb-filecheck drweb-firewall drweb-gated drweb-gui drweb-httpd-bin d
rweb-httpd-linkchecker drweb-icu drweb-icu-data drweb-netcheck drweb-openssl drw
eb-protobuf drweb-qt drweb-se drweb-spider drweb-spider-kmod drweb-uninst drweb-
update drweb-workstations drweb-workstations-doc drweb-ziplib

27 new packages to install.
Overall download size: 521.4 MiB. Already cached: 0 B After the operation, addi
tional 694.9 MiB will be used.
Continue? [y/n/? shows all options] (y): y
Retrieving package drweb-protobuf-11.0.1-1603101909linux.i386 (1/27), 1.1 MiB
( 4.1 MiB unpacked)
Retrieving package drweb-common-11.0.1-1604222044linux.noarch (2/27), 127.7 KiB
(179.8 KiB unpacked)
Retrieving package drweb-openssl-11.0.1-1605041332linux.i386 (3/27), 1.2 MiB (
3.1 MiB unpacked)
Retrieving package drweb-workstations-doc-11.0.0-1604261435linux.noarch (4/27),
20.2 MiB ( 20.8 MiB unpacked)
```

Figure 12. Component installation protocol

5. After the installation completes successfully, the installer exits automatically. If an error occurs, a message describing the error is displayed and the installer exits.



```
Terminal
Generating HTML doc index files...

(26/27) Installing: drweb-spider-kmod-11.0.1-1606211346linux [.....done]
Additional rpm output:
Reloading Dr.Web drweb-configd...
update-rc.d: warning: drweb-spider-kmod start runlevel arguments (2 3 4 5) do not match LSB Default-Start values (3 5)
Adding system startup for /etc/init.d/drweb-spider-kmod ...
/etc/rc0.d/K70drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc1.d/K70drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc6.d/K70drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc2.d/S30drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc3.d/S30drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc4.d/S30drweb-spider-kmod -> ../init.d/drweb-spider-kmod
/etc/rc5.d/S30drweb-spider-kmod -> ../init.d/drweb-spider-kmod
Install Dr.Web kernel module if needed...
Notice: Your system supports fanotify; the kernel module is not required.

(27/27) Installing: drweb-workstations-11.0.1-1607051625linux [.....done]
Removing repository 'dir:///tmp/selfgz19856/repo/yum' [...done]
Repository 'dir:///tmp/selfgz19856/repo/yum' has been removed.
user@userm:~$ _
```

Figure 13. Installation Complete message

6. To start working with the installed Dr.Web for Linux, run the product in one of the [available ways](#).

If the installation process fails due to an error, remove the problems that caused this error and start an installation procedure again.

Installing from the Repository

Dr.Web for Linux's native packages are stored in the Dr.Web official repository at <https://repo.drweb.com>. Once you have added the Dr.Web repository to the list of those used by your operating system's package manager, you can install the product from native packages as you install any other programs from the operating system's repositories. Required dependencies are automatically resolved. Besides, this case supports a detection procedure by an OS package manager of all Dr.Web components installed from the connected repository. It also supports a suggestion to install all detected updates.



To access Dr.Web repository, Internet access is required.

All the commands mentioned below—the commands used to add repositories, to import digital signature keys, to install and uninstall packages—must be performed with administrative privileges (by the **root** user). To elevate the privileges, use the **su** command (to change the current user) or the **sudo** command (to execute the specified command with another user's privileges).



Debian, Mint, Ubuntu (apt)



The Dr.Web for Linux anti-virus engine uses a 32-bit architecture *x86*; in 64-bit systems **Debian, Mint, Ubuntu** (for platforms *x86-64, x64, amd64*), a permission could be required for installation of packages for the platform *x86*. It could be obtained via the following command:

```
# dpkg --add-architecture i386
```

1. The repository for these operating systems is digitally signed by Doctor Web. To access the repository, import and add to the package manager storage the digital signature key via execution of the following command:

```
# apt-key adv --keyserver hkp://keyserver.ubuntu.com:80 --recv-keys 10100609
```

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

```
deb https://repo.drweb.com/drweb/debian 11.0 non-free
```



Besides, you can execute items 1 and 2 by downloading from the repository and installing a special DEB package.

Link to download the package: <https://repo.drweb.com/drweb-repo11.deb>.

3. To install Dr.Web for Linux from the repository, use the following commands:

```
# apt-get update
# apt-get install drweb-workstations
```

You can also use alternative package managers (for example, **Synaptic** or **aptitude**) to install the product. Moreover, it is recommended to use alternative managers, such as **aptitude**, to solve a package conflict if it occurs.

ALT Linux, PCLinuxOS (apt-rpm)

1. To add the repository, add the following line to the `/etc/apt/sources.list` file:

```
rpm https://repo.drweb.com/drweb/altlinux 11.0/<arch> drweb
```

where `<arch>`—representation of the used packet architecture:

- For the **32-bit** version: `i386`
- For **64-bit** version: `x86_64`



2. To install Dr.Web for Linux from the repository, use the following commands:

```
# apt-get update
# apt-get install drweb-workstations
```

You can also use alternative package managers (for example, **Synaptic** or **aptitude**) to install the product.

Mageia, OpenMandriva Lx (urpmi)

1. Connect the repository using the following command:

```
# urpmi.addmedia drweb https://repo.drweb.com/drweb/mandriva/11.0/<arch>/
```

where *<arch>*—representation of the used packet architecture:

- For the **32-bit** version: `i386`
- For **64-bit** version: `x86_64`

2. To install Dr.Web for Linux from the repository, use the following command:

```
# urpmi drweb-workstations
```

You can also use alternative package managers (for example, **rpmdrake**) to install the product.

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

1. Add a file `drweb.repo` with the contents described below to the `/etc/yum.repos.d` directory:

```
[drweb]
name=DrWeb - 11.0
baseurl=https://repo.drweb.com/drweb/e15/11.0/$basearch/
gpgcheck=1
enabled=1
gpgkey=https://repo.drweb.com/drweb/drweb.key
```



If you plan on logging the indicated above contents to a file using such commands as **echo** with redirecting of an output, a symbol `$` must be escaped: `\$`.

Besides, you can execute item 1 by downloading from the repository and installing a special RPM package.

Link to download the package: <https://repo.drweb.com/drweb-repo11.rpm>.

2. To install Dr.Web for Linux from the repository, use the following command:

```
# yum install drweb-workstations
```




In the **Fedora** operating system, starting from version 22, it is recommended that instead of manager **yum** the manager **dnf** is used, for example:

```
# dnf install drweb-workstations
```

You can also use alternative package managers (for example, **PackageKit** or **Yumex**) to install the product.

SUSE Linux (zypper)

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

```
# zypper ar -t YUM 'https://repo.drweb.com/drweb/el5/11.0/$basearch/' drweb
```

2. To install Dr.Web for Linux from the repository, use the following commands:

```
# zypper refresh
# zypper install drweb-workstations
```

You can also use alternative package managers (for example, **YaST**) to install the product.



Upgrading Dr.Web for Linux

There are two modes for updating Dr.Web for Linux:

1. [Getting updates of packages and components](#) released in the course of operation of the current product version (usually such updates contain error fixing and minor improvements in component functioning);
2. [Upgrading to a newer version](#). This upgrading option is used if Doctor Web released a new version of the product you use, and it has new features.

Getting Current Upgrades

After installation of the product using any method described in the [corresponding section](#), the package manager automatically connects to the Dr.Web package repository:

- If installation was performed from the [universal package](#) (file `.run`), and the system uses DEB packages (for example, such operating systems as **Debian**, **Mint**, **Ubuntu**), for operation with Dr.Web packages, an individual version of package managers **zypper** is used. It is automatically installed during the product installation.

To get and install the updated Dr.Web packages with this manager, go to the `<opt_dir>/bin` directory (for **GNU/Linux**—`/opt/drweb.com/bin`), and execute the following commands:

```
# ./zypper refresh
# ./zypper update
```

- In all other cases use commands for updating of the package manager used in your OS, for example:
 - For **Red Hat Enterprise Linux** and **CentOS**, use the command **yum**
 - For **Fedora**, use the command **yum** or **dnf**
 - For **SUSE Linux**, use the command **zypper**
 - For **Mageia**, **OpenMandriva Lx**, use the command **urpmi**
 - For **Alt Linux**, **PCLinuxOS**, **Debian**, **Mint**, **Ubuntu**, use the command **apt-get**.

You can also use alternate package managers developed for your operating system. If necessary, refer to the instruction manual for the package manager you use.

If a new product version is released, packages with its components are put into the section of the Dr.Web repository corresponding to the new product version. In this case, an update requires switching of the package manager to a new Dr.Web repository section (refer to [Upgrading to a Newer Version](#)).



Upgrading to a Newer Version

Introductory Remarks

The upgrade procedure for previous versions of the product to version 11.0 is supported. Please note that your version of Dr.Web for Linux should be upgraded the same way as it was used during the installation:

- If the current version was installed from the repository, an upgrade requires updating program packages from the repository.
- If the current version was installed from the universal package, then to upgrade the product, you need to install another universal package that contains a newer version of the product.



To identify how the product version was installed, check whether the Dr.Web for Linux executable directory contains `remove.sh` program uninstallation script. If so, the current version was installed from the universal package; otherwise it was installed from the repository.

If you cannot update the product the way you installed it initially, uninstall your current version of Dr.Web for Linux, and then install a new version using any convenient method. Installation and uninstallation procedures for previous Dr.Web for Linux versions are the same as [installation](#) and [uninstallation](#) described in the current manual for version 11.0. For additional information, see User manual for your current version of Dr.Web for Linux.



Note that upgrade of Dr.Web for Linux from version 6.0.2 to version 11.0 can be performed *only* by uninstalling the outdated product and [installing](#) the version 11.0.

If the current version of the product is operating in the [central protection](#) mode, it is recommended that you record the address of the used central protection server. For example, to determine the address to which Dr.Web for Linux of the version higher than 6.0.2, you can use the following command:

```
$ drweb-ctl appinfo
```

In the output provided by this command, from the line that looks like:

```
ESAgent; <PID>; RUNNING 1; Connected <address>, on-line
```

save the `<address>` part (which can look like `tcp://<IP address>:<port>`, for example: `tcp://10.20.30.40:1234`). In addition, it is recommended that you save the server public key file.



In case there are any problems with finding out the parameters of the connection that you are currently using, refer to the Administrator's Manual for the product version that you are currently using and to the administrator of your anti-virus network.

Upgrading Version 9.0 and Higher

Installing Universal Package for an Upgrade

Install Dr.Web for Linux 11.0 from the [installation file](#). During the installation, if it is necessary, you are prompted to automatically uninstall the older version installed from the distribution.

Upgrading from the Repository

To upgrade your current version of Dr.Web for Linux that was installed from the Doctor Web's repository, do one of the following, depending on the required type of packages:

- **In case of using RPM packages (yum):**

1. Change the used repository (from the package repository of your current version to the package repository 11.0).



You can find the name of the repository in the [Installing from the Repository](#) section. For details on how to change repositories, refer to help guides of the used operating system distribution.

2. Install the new version using the following command:

```
# yum update
```

or, if the manager **dnf** is used (similar to the **Fedora** OS of the version 22 and earlier):

```
# dnf update
```



If during the update of packages there is an error, uninstall and repeat the installation of the product. If necessary, see sections [Uninstalling the Product Installed from the Repository](#) and [Installing from the Repository](#) (items for the OS and the package manager that you are using).

- **In case of using DEB packages (apt-get):**

1. Change the used repository (from the package repository of your current version to the package repository 11.0).
2. Update the product using the following commands:

```
# apt-get update  
# apt-get dist-upgrade
```



Please note that for the **Ubuntu 14.04** (64-bit version) OS, the **apt-get** `dist-upgrade` command may fail. In this case use the **aptitude** package manager (to upgrade the product, issue the **aptitude** `dist-upgrade` command).

Key File Transfer

Regardless of the selected method to upgrade Dr.Web for Linux, the license [key file](#) is installed to the default location automatically.



If any problem occurs during automatic installation of the key file, you can [install it manually](#). The license key file of Dr.Web for Linux version 9.0 and older resides in the directory `/etc/opt/drweb.com`. If a valid license key file is lost, contact Doctor Web [technical support](#).

Restoring Connection to the Central Protection Server

If possible, after upgrading Dr.Web for Linux, if the upgraded product was connected to a central protection server, the connection is re-established automatically. If not, you can use any of the following ways (note that you should specify the saved address and server public key file):

- Select the check box on the **Mode** [tab](#) of the Dr.Web for Linux [settings window](#).
- Use the [command](#)

```
$ drweb-ctl esconnect <address> --Key <path to a file of the public server key>
```

In case there are any problems with the connection process, contact the administrator of your anti-virus network.

Upgrading Procedure Features

- If your current version of Dr.Web for Linux is active when upgrading the product from the repository, processes of the older version remain running until the user logs off the system after the upgrade is complete. At that, if Dr.Web for Linux is operating in graphical mode, the [icon](#) of the older version can display in the notification area.
- After upgrading Dr.Web for Linux, SpIDer Gate [settings](#) may be reset to default values.
- If a mail client runs in the system (such mail client as **Mozilla Thunderbird**) that uses the IMAP protocol to receive email messages, it is necessary to restart it after an update is complete to provide the scanning of incoming email messages.

Upgrading Version 6.0.2 and Older

Upgrade of Dr.Web for Linux from version 6.0.2 and older to version 11.0 can be performed only by uninstalling the outdated product version and installing version 11.0. For additional



information how to uninstall the old version, see User manual for your installed version of Dr.Web for Linux.

Key File Transfer

After upgrading Dr.Web for Linux, the license [key file](#) is not installed automatically to the default location, but you can install it [manually](#). The license key file of Dr.Web for Linux 6.0.2 and older, resides in the directory `/home/<user>/.drweb` (the directory is hidden). If a valid license key file is lost, contact Doctor Web [technical support](#).



Dr.Web for Linux 11.0 does not support Version of Dr.Web for Linux 9.0 and older! If any isolated files remain in quarantine of an older version, you can retrieve or delete these files manually. Dr.Web for Linux 6.0.2 (and earlier) uses as quarantine the following directories:

- `/var/drweb/infected` – system quarantine;
- `/home/<user>/.drweb/quarantine` – user quarantine (where `<user>` – user name).

To simplify processing of quarantined files, it is recommended to revise quarantine using old version of Dr.Web for Linux before starting an upgrade.



Uninstalling Dr.Web for Linux

Depending on the method that you used to install Dr.Web for Linux, you can remove the product in one of the following ways:

1. [Starting the uninstaller](#) to uninstall the universal package (in graphical or command-line mode, depending on the environment).
2. [Uninstalling the packages](#) installed from the Doctor Web repository via the package system manager.

Uninstalling Universal Package

Dr.Web for Linux that was installed from the [universal package](#) for UNIX systems can be uninstalled either via the application menu of the desktop environment or via the command line.



Note that the uninstallation tool uninstalls not only Dr.Web for Linux, but also *all the other* Dr.Web products installed on your computer.

If any other Dr.Web products are installed on your computer, besides Dr.Web for Linux, then, to uninstall only Dr.Web for Linux, use the custom [components installation and uninstallation](#) procedure, instead of running the automatic uninstallation tool.

Uninstalling the Product via the Application Menu

On the application menu, click the **Dr.Web** item and select **Remove Dr.Web components**. The uninstallation tool will be started.

Uninstalling the Product via the Command Line

To uninstall anti-virus, run the `remove.sh` script, which resides in the `/opt/drweb.com/bin` directory, using the following command:

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

Then an uninstallation tool will be launched (either in graphical or command-line mode, depending on the environment).

To run the uninstallation tool directly from the command line, use the following command:

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

Uninstallation of Dr.Web for Linux is described in the corresponding sections:

- [Uninstalling the Product in Graphical Mode.](#)



- [Uninstalling from the Command Line.](#)

You can also start the uninstallation tool in silent mode by executing the command

```
# /opt/drweb.com/bin/remove.sh --non-interactive
```

In this case, the uninstallation tool is run in silent mode and operates without the user interface (including program dialogs for command-line mode). Note that root privileges are required to start the uninstallation tool in silent mode. To elevate the privileges, you can use the **su** and **sudo** commands.

Uninstalling in Graphical Mode

Once the Uninstallation wizard starts in graphical mode, its welcome page is displayed.

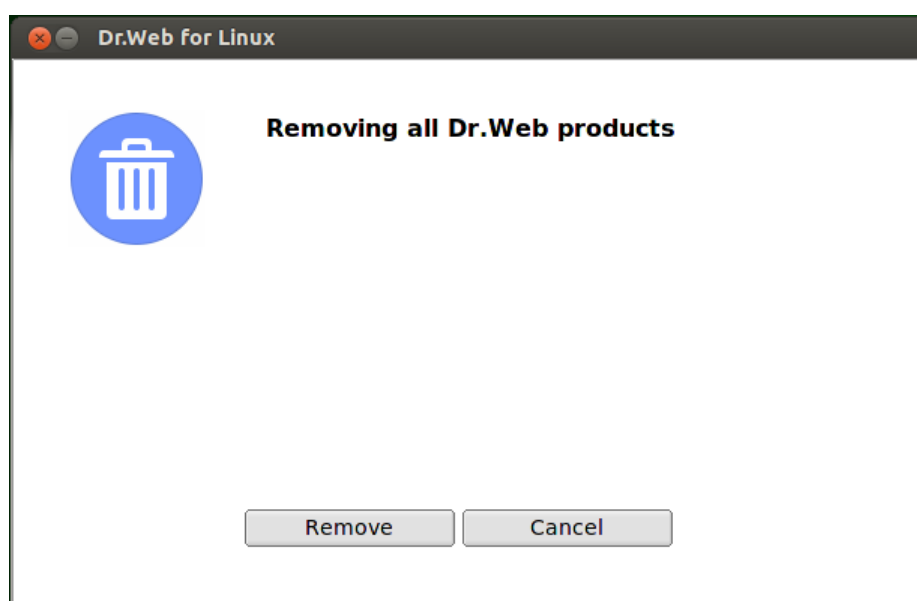


Figure 14. Welcome page

1. To uninstall Dr.Web for Linux, click **Delete**. To close the Uninstallation Wizard, click **Cancel**.
2. After the uninstallation starts, a page with the progress bar opens. To view the log, you can click the **Details** button.

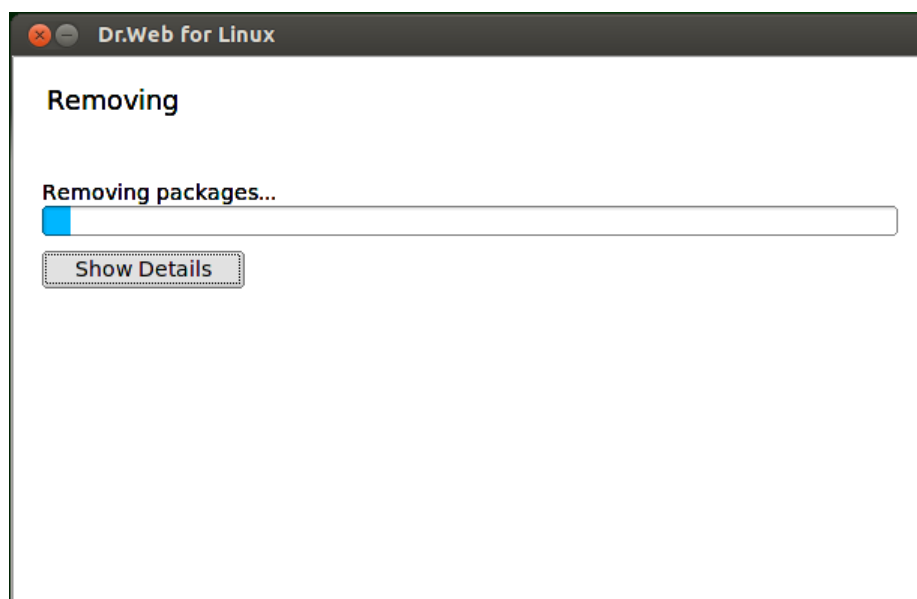


Figure 15. Uninstallation progress indicator

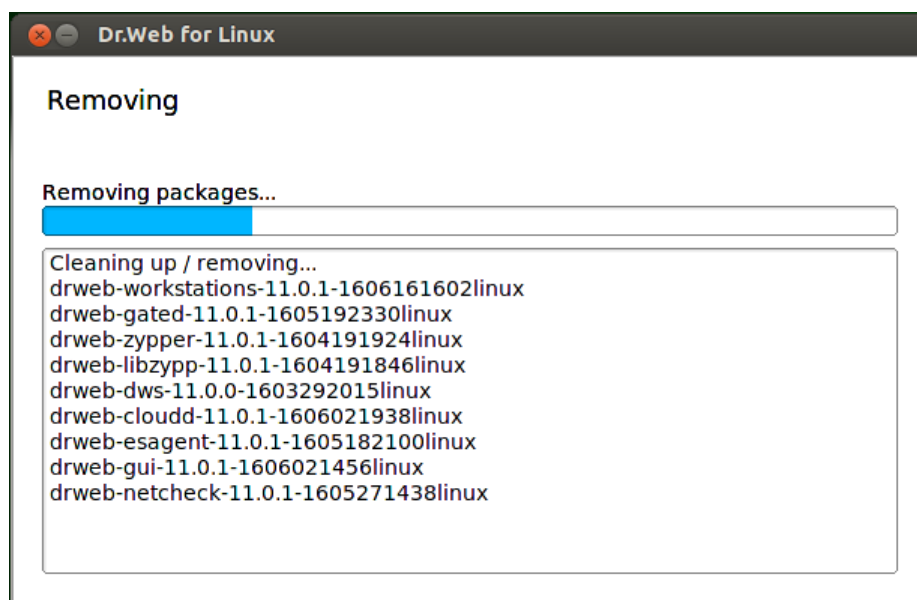


Figure 16. Viewing the log

3. After Dr.Web for Linux files are successfully uninstalled and all necessary changes are made to the system settings, the Uninstallation Wizard displays the final page notifying on successful operation results.

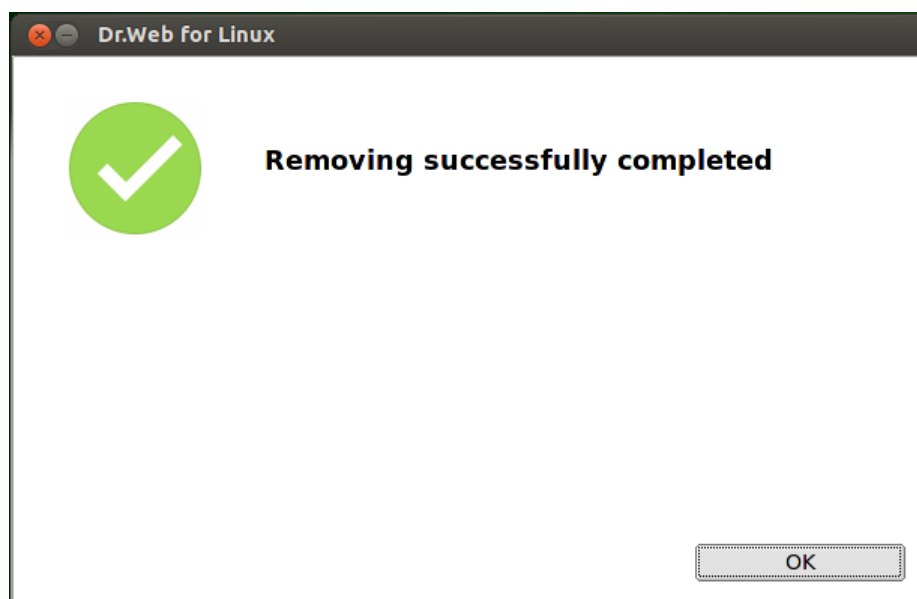


Figure 17. The Uninstallation Wizard results

4. To close the Uninstallation Wizard, click **OK**.

Uninstalling from Command Line

Once the command-line-based uninstallation program starts, an offer to remove the product is displayed in the command line.

1. To start uninstallation, enter *Yes* or *Y* in response to the "Do you wish to continue?" question. To exit the uninstallation program, type *No* or *N*. In this case, uninstallation will be canceled.

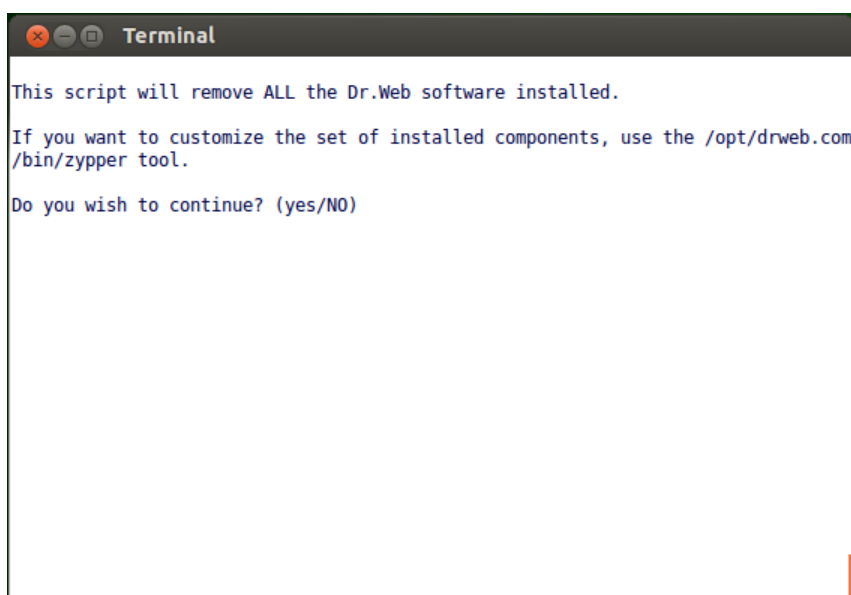


Figure 18. Offer to unistall the product

2. Once uninstallation of the selected components is launched, messages about the uninstallation process will be displayed on the screen and logged.



```
Terminal
Shutting down Dr.Web drweb-configd...
.
Removing any system startup links for /etc/init.d/drweb-configd ...
/etc/rc0.d/K70drweb-configd
/etc/rc1.d/K70drweb-configd
/etc/rc2.d/S30drweb-configd
/etc/rc3.d/S30drweb-configd
/etc/rc4.d/S30drweb-configd
/etc/rc5.d/S30drweb-configd
/etc/rc6.d/K70drweb-configd
22:drweb-configd-11.0.1-1606141444li##### [ 67%]
Generating HTML doc index files...
23:drweb-boost-11.0.0-1602292109linu##### [ 70%]
24:drweb-icu-11.0.1-1603101909linux ##### [ 73%]
25:drweb-icu-data-11.0.1-1603101909l##### [ 76%]
26:drweb-openssl-11.0.1-1605041332li##### [ 79%]
27:drweb-protobuf-11.0.1-1603101909l##### [ 82%]
28:drweb-ziplib-11.0.1-1603101909lin##### [ 85%]
29:drweb-libs-11.0.1-1606021505linux##### [ 88%]
30:drweb-common-11.0.1-1604222044lin##### [ 91%]
31:drweb-workstations-doc-11.0.0-160##### [ 94%]
32:pgp-pubkey-10100609-4bcc7a79 ##### [ 97%]
33:drweb-dummy-11.0.1-1606161602linu##### [100%]
root@userm:~# _
```

Figure 19. Uninstallation completion

3. Once the process is completed, the uninstallation program will automatically terminate.



Uninstalling the Product Installed from the Repository



All commands mentioned below for package uninstallation require superuser (root) privileges. To elevate the privileges, use the **su** command (to change the current user) or the **sudo** command (to execute the specified command with other user's privileges).

Debian, Mint, Ubuntu (apt)

To uninstall the root meta-package of Dr.Web for Linux, enter the following command:

```
# apt-get remove drweb-workstations
```

To uninstall all the installed Dr.Web packages, enter the following command (in certain operating systems, the '*' character must be escaped: '*'):

```
# apt-get remove drweb*
```

To automatically uninstall all packages that are no longer used, enter also the following command:

```
# apt-get autoremove
```



Please, note that uninstallation with the help of the **apt-get** command has the following special aspects:

1. The first command uninstalls only the `drweb-workstations` package; all other packages that could be automatically installed to resolve dependencies remain in the system.
2. The second command uninstalls all the packages whose name starts with "drweb" (the standard name prefix for Dr.Web products). Note that this command uninstalls all packages with this prefix, not only those of Dr.Web for Linux.
3. The third command uninstalls all packages that were automatically installed to resolve dependencies of other packages and are no longer necessary (e.g., due to their uninstallation). Note that this command uninstalls all packages that are not used, not only those of Dr.Web for Linux.

You can also use alternative managers (for example, **Synaptic** or **aptitude**) to uninstall packages.

ALT Linux, PCLinuxOS (apt-rpm)

In this case, uninstalling of Dr.Web for Linux is the same as on **Debian** and **Ubuntu** operating systems (see above).

You can also use alternative managers (for example, **Synaptic** or **aptitude**) to uninstall packages.



Mageia, OpenMandriva Lx (urpme)

To uninstall Dr.Web for Linux, enter the following command:

```
# urpme drweb-workstations
```

To automatically uninstall all packages that are no longer used, enter also the following command:

```
# urpme --auto-orphans drweb-workstations
```



Please, note that uninstallation with the help of the **urpme** command has the following special aspects:

1. The first command uninstalls only the `drweb-workstations` package; all other packages that could be automatically installed to resolve dependencies remain in the system.
2. The second command uninstalls the root meta-package `drweb-workstations` and all packages that were automatically installed to resolve dependencies of other packages and are no longer necessary (e.g., due to their uninstallation). Note that this command uninstalls all packages that are not used, not only those of Dr.Web for Linux.

You can also use alternative managers (for example, **rpmdrake**) to uninstall packages.

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

To uninstall all the installed Dr.Web packages, enter the following command (in certain operating systems, the '*' character must be escaped: '*'):

```
# yum remove drweb*
```

In the **Fedora** operating system, starting from version 22, it is recommended that instead of manager **yum** the manager **dnf** is used, for example:

```
# dnf remove drweb*
```



Please, note that uninstallation with the help of the **yum** (**dnf**) command has the following special aspects:

The indicated command uninstalls all the packages whose name starts with "drweb" (the standard name prefix for Dr.Web products). Note that this command uninstalls all packages with this prefix, not only those of Dr.Web for Linux.



You can also use alternative managers (for example, **PackageKit** or **Yumex**) to uninstall packages.

SUSE Linux (zypper)

To uninstall Dr.Web for Linux, enter the following command:

```
# zypper remove drweb-workstations
```

To uninstall all the installed Dr.Web packages, enter the following command (in certain operating systems, the '*' character must be escaped: '*'):

```
# zypper remove drweb*
```



Please, note that uninstallation with the help of the **zypper** command has the following special aspects:

1. The first command uninstalls only the `drweb-workstations` package; all other packages that could be automatically installed to resolve dependencies remain in the system.
2. The second command uninstalls all the packages whose name starts with "drweb" (the standard name prefix for Dr.Web products). Note that this command uninstalls all packages with this prefix, not only those of Dr.Web for Linux.

You can also use alternative managers (for example, **YaST**) to uninstall packages.



Additional Information

Product Files Location

After the installation of Dr.Web for Linux, its files are located in the `/opt`, `/etc`, and `/var` directories of the file system.

Structure of the used directories

Directory	Contents
<code>/opt/drweb.com</code>	Executable files of the product's components and main libraries necessary for Dr.Web for Linux operation
<code>/etc/opt/drweb.com</code>	Component setting files (by default) and a key file for Dr.Web for Linux operation in Standalone mode .
<code>/var/opt/drweb.com</code>	Virus databases, anti-virus engine, temporary files, and additional libraries necessary for Dr.Web for Linux operation.

Custom Component Installation and Uninstallation

If necessary, you can choose to install or uninstall only certain product components by installing or uninstalling the respective [packages](#). Custom component installation or uninstallation should be performed the same way the product was installed.

To reinstall a component, you can uninstall it first and then install again.

1. Installation and Uninstallation of Product Components Installed from Repository

If your product is installed from repository, for custom component installation or uninstallation use the respective command of the package manager, used in your OS. For example:

1. To uninstall SpIDer Gate (package `drweb-gated`) from the product installed on OS **CentOS**, use the command:

```
# yum uninstall drweb-gated
```

2. To additionally install SpIDer Gate (package `drweb-gated`) to the product installed on OS **Ubuntu Linux**, use the command:

```
# apt-get install drweb-gated
```



The Dr.Web for Linux anti-virus engine uses a 32-bit architecture x86; in 64-bit systems **Debian, Mint, Ubuntu** (for platforms x86-64, x64, amd64), a permission could be required for installation of packages for the platform x86. It could be obtained via the following command:

```
# dpkg --add-architecture i386
```

If necessary, use a help file of the package manager used in your OS.

2. Installation and Uninstallation of Product Components Installed from the Universal Package

If the product is installed from the universal package and you want to additionally install or reinstall a package of a component, you will need an installation file (with the `.run` extension), from which the product was installed. In case you did not save this file, download it from the Doctor Web's official website.

Unpacking the Installation File

When you launch the `.run` file, you can also specify the following command-line parameters:

`--noexec`—unpack the product's installation files instead of starting the installation process. The files will be placed to the directory that is specified in the `TMPDIR` environment variable (usually, `/tmp`).

`--keep`—do not delete the product installation files and the installation log automatically after the installation completes.

`--target <directory>`—unpack the product's installation files to the specified `<directory>`.

For a full list of command-line parameters that can be specified for an installation file, type the following command:

```
$ ./<file_name>.run --help
```

For a custom installation, you need to use the unpacked installation files. If there is no directory containing these files, you should first unpack them. To do that, enter the following command:

```
$ ./<file_name>.run --noexec --target <directory>
```

After the command is executed, a nested directory named `<file_name>` will appear in the directory `<directory>`.



Custom Installation of the Components

Installation RUN file contains packages of all components of Dr.Web for Linux (in the RPM format) and supporting files. Package files of each component have the following structure:

```
<component_name>_<version>~linux_<platform>.rpm
```

where *<version>* is a string that contains the version and time of the product's release, and *<platform>* is a platform for which the product is intended. Names of all the packages containing the components of Dr.Web for Linux start with the "drweb" prefix.

Package manager is enabled for the installation of packages to the installation kit. For the custom installation, you should use a service script `installpkg.sh`. To do that, first, you need to unpack the contents of the installation package to a directory.



To install packages, superuser permissions are required (i.e. privileges of the *root* user). To elevate your privileges, use the **su** command for changing the current user or the **sudo** command to execute the specified command with the privileges of another user.

To start installation or reinstallation of a component package, go to the directory which contains the unpacked installation kit, and execute the following command via the console (or via a console emulator—terminal for the graphical mode):

```
# ./scripts/installpkg.sh <package_name>
```

For example:

```
# ./scripts/installpkg.sh drweb-gated
```

If it is necessary to start the full product installation, launch the automatic installation script. To do that, use the following command:

```
$ ./install.sh
```

Besides that, you can install all product packages (to install the missing or accidentally deleted components as well) by launching the installation of the root meta-package of the product:

```
# ./scripts/installpkg.sh drweb-workstations
```



Custom Uninstallation of the Components

For the custom uninstallation of a component, use the appropriate uninstallation command of the package manager of your OS if your OS uses the RPM format of packages:

- In **Red Hat Enterprise Linux** and **CentOS**, use the command **yum remove <package_name>**
- In **Fedora**, use the command **yum remove <package_name>** or **dnf remove <package_name>**
- In **SUSE Linux**, use the command **zypper remove <package_name>**
- In **Mageia**, **OpenMandriva Lx**, use the command **urpme <package_name>**
- In **Alt Linux** and **PCLinuxOS**, use the command **apt-get remove <package_name>**.

For example (for **Red Hat Enterprise Linux**):

```
# yum uninstall drweb-gated
```

If your OS uses DEB packages, for the custom uninstallation you should use the package manager **zypper**, which is automatically installed within the product installation. To do that, go to the directory `/opt/drweb.com/bin` and execute the following command:

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

For example:

```
# ./zypper rm drweb-gated
```

If it is necessary to start the full product uninstallation, launch the automatic uninstallation script. To do that, use the following command:

```
# ./uninst.sh
```

To reinstall a component, you can uninstall it first and then install by launching the custom or full installation from the installation kit.



Configuring Security Systems

Presence of the **SELinux** enhanced security subsystem in the OS as well as the use of mandatory access control systems, such as **PARSEC** (as opposed to the classical discretionary model used by UNIX) causes problems in the work of Dr.Web for Linux when its default settings are used. To ensure correct operation of Dr.Web for Linux in this case, it is necessary to make additional changes to the settings of the security subsystem and/or to the settings of Dr.Web for Linux.

This section discusses the settings that ensure correct operation of Dr.Web for Linux in the following cases:

- [Configuring SELinux](#) Security Policies.
- [Setting up the permissions](#) of the **PARSEC** mandatory access control system (the **Astra Linux** OS)



Configuring the permissions of the **PARSEC** mandatory access control system for Dr.Web for Linux will allow the components of Dr.Web for Linux to bypass the restrictions of the set security policies and to get access to the files that belong to different privilege levels.

Note that even if you have not configured the permissions of the **PARSEC** mandatory access control system for Dr.Web for Linux, you still will be able to launch file scanning by the [Graphical management interface](#) of Dr.Web for Linux in the [autonomous copy](#) mode. For that, execute the **drweb-gui** [command](#) with the parameter `--Autonomous`. You can also launch the scanning directly from the [command line](#). To do this, use the **drweb-ctl** [command](#) specifying the same parameter (`--Autonomous`) in the command call. In this case, it will be possible to scan files that require a privileges level not higher than the level that the user that launched the scanning session. This mode has the following features:

- To run the Graphical management interface of Dr.Web for Linux as an autonomous copy, you will need a valid [key file](#), working in [Central protection](#) mode is not supported (an option to [install](#) the key file, exported from central protection server, is available). In this case, even if Dr.Web for Linux is connected to the central protection server, the autonomous copy *does not notify* the central protection server of the threats detected in the autonomous copy mode.
- All additional components, that are run to serve the work of the autonomous copy of the Graphical management interface, will be launched as the current user and will work with a configuration file, separately generated for this session.
- All the used temporary files and UNIX sockets are created only in the directory with an unique name, which is created when the autonomous copy is launched. The unique temporary directory is created in the system directory for temporary files (path to this directory is available in the `TMPDIR` environment variable).
- The autonomous copy of the Graphical management interface *does not launch* SpIDer Guard and SpIDer Gate monitors, only files checking and quarantine management functions, supported by Scanner, are available.
- All the required paths (to virus databases, anti-virus engine and executable files of the service components) are defined by default or retrieved from the special environment variables.



- The number of simultaneously running autonomous copies is unlimited.
- When the autonomous copy is shut down, the set of servicing components is also terminated.

Configuring SELinux Security Policies

If the used **Linux** distribution features **SELinux** (*Security-Enhanced Linux*), you may need to configure **SELinux** security policies to enable correct component operation (for example, operation of the scanning engine) after they are installed.

1. Universal Package Installation Issues

If **SELinux** is enabled, installation from the [installation file](#) (.run) can fail because an attempt to create the *drweb* user, under which Dr.Web for Linux components operate, can be blocked.

In case of failure, check the **SELinux** operation mode with the **getenforce** command. The command outputs one of the following:

- *Permissive*—protection is active but a permissive strategy is used: actions that violate the security policy are not denied but information on the actions is logged.
- *Enforced*—protection is active and restrictive strategy is used: actions that violate security policies are blocked and information on the actions is logged.
- *Disabled*—**SELinux** is installed but not active.

If **SELinux** is operating in *Enforced* mode, change it to *Permissive*. For that purpose, use the following command:

```
# setenforce 0
```

which temporarily (until the next reboot) enables *Permissive* mode for **SELinux**.



Note that regardless of the operation mode enabled with the **setenforce** command, after the restart of the operating system, **SELinux** returns to the safe operation mode specified in its settings (file with **SELinux** settings usually resides in the `/etc/selinux` directory).

After the successful product installation, enable *Enforced* mode again before starting the product. For that, use the following command:

```
# setenforce 1
```

2. Operation Issues

In some cases when **SELinux** is enabled, certain auxiliary Dr.Web for Linux components (for example, **drweb-se** and **drweb-filecheck** used by Scanner and SpIDer Guard) cannot start. If so, object scanning and file system monitoring become unavailable. When an auxiliary module fails



to start, the main Dr.Web for Linux window displays messages on *119* and *120* errors and information on these errors is also registered by **syslog** (the log is usually located in the `/var/log/` directory).



Messages on [119](#) and [120](#) errors can also indicate an attempt to start Dr.Web for Linux on 64-bit version of the operating system if the 32-bit application support library is missing (see [System Requirements](#)).

When the **SELinux** security system denies access, such an event is logged. In general, when the **audit** daemon is used on the system, the log of the audit is stored in the `/var/log/audit/audit.log` file. Otherwise, messages about blocked operations are saved to the general log file (`/var/log/messages` or `/var/log/syslog`).

If auxiliary modules do not function because they are blocked by **SELinux**, compile special security policies for them.



Note that certain **Linux** distributions do not feature the utilities mentioned below. If so, you may need to install additional packages with the utilities.

Configuring SELinux Security Policies:

1. Create a new file with the **SELinux** policy source code (a `.te` file). This file defines restrictions related to the described policy module. The policy's source code can be created in one of the following ways:

- 1) Using the **audit2allow** utility, which is the simplest method. The utility generates permissive rules from messages on access denial in system log files. You can set to search messages automatically or specify a path to the log file manually.

Note that you can use this method only if Dr.Web for Linux's components have violated **SELinux** security policies and these events are registered in the audit log file. If not, wait for such an incident to occur or force-create permissive policies by using the **policygentool** utility (see below).



The **audit2allow** utility resides either in the `policycoreutils-python` package or in the `policycoreutils-devel` package (for **RedHat Enterprise Linux**, **CentOS**, **Fedora** operating systems, depending on the version) or in the `python-sepolgen` package (for **Debian** and **Ubuntu** operating systems).

Example of using **audit2allow**:

```
# grep drweb-se.real /var/log/audit/audit.log | audit2allow -M drweb-se
```

In the given example, the **audit2allow** utility performs a search in the `audit.log` file to find access denial messages for **drweb-se** module.

The following two files are created: policy source file `drweb-se.te` and the `drweb-se.pp` policy module ready to install.



If no security violation incidents are found in the system audit log, the utility returns an error message.

In most cases, you do not need to modify the policy file created by the utility. Thus, it is recommended to go to [step 4](#) for installation of the `drweb-se.pp` policy module. Note that the **audit2allow** utility outputs invocation of the **semodule** command. By copying the output to the command line and executing it, you complete [step 4](#). Go to [step 2](#) only if you want to modify security policies which were automatically generated for Dr.Web for Linux components.

- 2) Using the **policygentool** utility. For that purpose, specify name of the module operation with which you want to configure and the full path to the executable file.



Note that the **policygentool** utility, included in the `selinux-policy` package for **RedHat Enterprise Linux** and **CentOS Linux** OS, may not function correctly. If so, use the **audit2allow** utility.

Example of policy creation using **policygentool**:

- For **drweb-se**:

```
# policygentool drweb-se /opt/drweb.com/bin/drweb-se.real
```

- For **drweb-filecheck**:

```
# policygentool drweb-filecheck /opt/drweb.com/bin/drweb-filecheck.real
```

You will be prompted to specify several common domain characteristics. After that, three files that determine the policy are created for each of the modules:

`<module_name>.te`, `<module_name>.fc` and `<module_name>.if`.

2. If required, edit the generated policy source file `<module_name>.te` and then use the **checkmodule** utility to create a binary representation (a `.mod` file) of this source file of the local policy.



Note that to ensure successful execution of the command, the `checkpolicy` package must be installed in the system.

Example usage

```
# checkmodule -M -m -o drweb-se.mod drweb-se.te
```

3. Create a policy module for installation (a `.pp` file) with the help of the **semodule_package** utility.

Example:

```
# semodule_package -o drweb-se.pp -m drweb-se.mod
```

4. To install the created policy module, use the **semodule** utility.

Example:



```
# semodule -i drweb-se.pp
```

For details on **SELinux** operation and configuration, refer to documentation for the used **Linux** distribution.

Configuring the Permissions of PARSEC (Astra Linux)

In operating systems equipped with the **PARSEC** security subsystem (mandate access control system), due to the variation in privilege levels required to access different files, SpIDer Guard working in its default mode (*AUTO*) cannot intercept file-access events for any files whose required access privilege level is higher than the one with which SpIDer Guard was launched. Moreover, if the user works at any privilege level other than the zeroth, the graphical interface of Dr.Web for Linux cannot interact with SpIDer Guard and with the Anti-virus service components if they work at a different privilege level; access to the consolidated [quarantine](#) may also become unavailable.

To perform these procedures, superuser permissions are required (i.e. privileges of the *root* user). To elevate your privileges, use the **su** command for changing the current user or the **sudo** command to execute the specified command with the privileges of another user.

Configuring SpIDer Guard to intercept attempts to access files with any privilege level

To give the SpIDer Guard file monitor an ability to detect attempted access, when any files that have any level of access privileges are accessed, it is necessary to switch SpIDer Guard into an *LKM* operating mode (this will use a special loadable kernel module for the **Linux** kernel; this module is supplied together with Dr.Web for Linux).

To switch SpIDer Guard into the *LKM* operating mode, execute the following [command](#):

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

To get additional information, use the following command:

```
$ man drweb-spider
```

Configuring the Correct Launch of Dr.Web for Linux at Any Privilege Level

In order for all the components of the Anti-virus (Scanner, SpIDer Guard and SpIDer Gate, [graphical interface](#) and the [management tool](#)) to be able to correctly interact with each other when they are launched with different privilege levels, it is necessary to modify the script that launches the Dr.Web for Linux configuration daemon (**drweb-configd**)—the product service component responsible for interaction of all anti-virus components between each other.



To do this, proceed as follows:

1. Log into the system using the privilege level zero
2. Open the `/etc/init.d/drweb-configd` script file in any text editor (root privileges are required).
3. In this file find the definition of the `start_daemon()` function and replace the line:

```
"$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

with the line:

```
execaps -c 0x100 -- "$DAEMON" -d -p "$PIDFILE" >/dev/null 2>&1
```

4. In some OSes, (for example, **Astra Linux SE 1.3**), an additional indication of component launch dependence from the **PARSEC** subsystem could be required. In this case, it is also necessary to modify a string in the file:

```
# Required-Start: $local_fs $network
```

Change this string in the following way:

```
# Required-Start: $local_fs $network parsec
```

5. Save the file and reboot the operating system



Working with Dr.Web for Linux

User's operation with Dr.Web for Linux can be performed both in graphical mode via the component that provides graphical interface for management and from the command line (including operation via terminal emulators for graphical mode).

To start Dr.Web for Linux's graphical management interface, select the **Dr.Web for Linux** item on the **Applications** or enter the following command in the operating system command line:

```
$ drweb-gui
```

In this case, if the desktop environment is available, Dr.Web for Linux' graphical management interface is started. To run file scanning at start the graphical interface or to start an [autonomous copy](#) of the interface, you can use this command with [parameters](#).

For details on managing the Dr.Web for Linux operation, refer to [Working from Command Line](#).

For the graphic desktop environments, Dr.Web for Linux allows you to start the scan from the task bar (such as **Unity Launcher** in **Ubuntu OS**) and from the graphic file manager (such as **Nautilus**). Moreover, the application status indicator appears in the notification area of the desktop and provides access to the application menu or displays pop-up notifications. The indicator is displayed as the notification agent, which, as well as all other service components, starts automatically and its operation does not require user intervention. For details, refer to [Integration with Desktop Environment](#).



Regardless of the selected way to install Dr.Web for Linux, after the installation completes, you need either to activate the license, or install the key file if already obtained, or connect Dr.Web for Linux to the central protection server (see [Licensing](#)). Until you do that, *anti-virus protection is disabled*.

Note that the IMAP mail protocol that is mostly used by mail clients (such as **Mozilla Thunderbird**) to receive email messages from the mail server works in sessions. Therefore after changing operation of the SpIDer Gate [monitor](#) (enabling of the previously disabled monitor, change of the scanning [mode](#) of secured connections), it is necessary to restart the mail client, so SpIDer Gate can scan incoming email messages after changing its operation mode.



Operating in Graphical Mode

Two components are responsible for Dr.Web for Linux's operation in the desktop environment:

- Notification agent—a component, which is automatically launched when user's session starts in the desktop environment. This component displays pop-up notifications on events in the product operation. It is also a status indicator of Dr.Web for Linux in the area of system notifications and the main menu for interaction with the product.
- Graphical management interface—a component that operates in the environment of graphical desktop and provides a window interface for management of Dr.Web for Linux's operation.

Notification Agent

Dr.Web for Linux's notification agent is designed to:

1. Display the [status indicator](#) of Dr.Web for Linux.
2. Manage monitors and an update, launch the graphical management interface.
3. Display pop-up notifications about events.
4. Launch scanning according to the specified schedule.

Graphical Management Interface

The graphical management interface of Dr.Web for Linux allows to solve the following tasks:

1. View the status of Dr.Web for Linux operation, including currency of the virus databases and a period of license validity.
2. [Start and stop](#) the file system monitor SpIDer Guard.
3. [Start and stop](#) the network connection monitor SpIDer Gate.
4. Start on-demand [file scanning](#):
 - *Express scan* to check system files and most vulnerable system objects.
 - *Full scan* to check all system files.
 - *Custom scan* to check only specified files and directories or special objects (boot records, active processes).

You can select the files to be scanned by specifying target directories and files before scanning and by dragging and dropping them with the mouse from the window of the file manager to the Main page (see below) or to the **Scanner** page of the Dr.Web for Linux window.

5. [View all threats](#) detected by Dr.Web for Linux during the current operation in graphical mode, including viewing neutralized and skipped threats and objects moved to quarantine.
6. [View objects](#) moved to quarantine, with possibility to remove or restore them.
7. [Configuration of operation parameters](#) of the Dr.Web for Linux components, including the following options:



- Actions that the Scanner and SpIDer Guard should apply to the detected threats (according to their type)
 - List of directories and files that must not be scanned by the Scanner and must not be controlled by the file system monitor SpIDer Guard.
 - Black and white lists of websites used by the monitor SpIDer Gate, and scanning parameters for the files downloaded from the Internet or received via email.
 - Schedule of planned of file system scanning, including the frequency, the type of scanning and the list of objects for custom scan according to a set schedule.
 - [Operation mode](#) (connect to the central protection server or disconnect from it)
 - [Network activity](#) monitoring parameters (enable or disable checking of the encrypted traffic).
 - [Permission](#) to use Dr.Web Cloud service.
8. License management (performed using [License Manager](#)).



To enable the correct operation of Dr.Web for Linux, it is necessary to start its service components before the operation; otherwise, it finishes immediately after startup with the corresponding warning message. In standard mode, all necessary service components are started automatically and do not require user interference.



Appearance of the Graphical Management Interface

Appearance of the Dr.Web for Linux's main window of the graphical management interface is shown in the figure below.

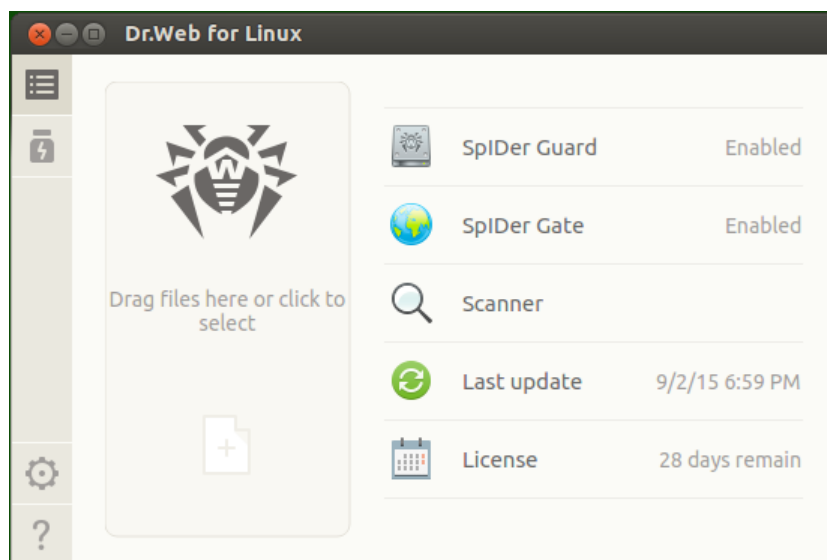
















Figure 20. Dr.Web for Linux's graphical management interface


The navigation panel is situated in the left part of the window. The buttons of the navigation panel allow to perform the following actions.

Button	Description
Continuously enabled	
	<p>Opens the main page where you can</p> <ul style="list-style-type: none">• Enable or disable the file system monitor SpIDer Guard.• Turn on or off SpIDer Gate network connection monitor.• Start scanning of the file system objects (files, boot records) and running processes.• Check whether the virus databases are up-to-date and update them, if necessary.• Start the License Manager to check the status of current license and register a new one, if necessary.
	<p>Opens the Quarantine page, where you can view the files moved to the quarantine and delete or restore them, if necessary.</p>
	<p>Opens Dr.Web for Linux settings window, in particular:</p> <ul style="list-style-type: none">• Scanner of file system objects• The file system monitor SpIDer Guard.• Monitoring of SpIDer Gate network connections• Start scanning as scheduled <p>In addition, you can configure the settings of the Central protection mode.</p>



Button	Description
	<p>Provides access to reference materials and supportive Doctor Web resources:</p> <ul style="list-style-type: none">• Product information• User manual• Dr.Web Updater• Technical support• Personal user webpage My Dr.Web <p>All links are opened in the browser installed in your system.</p>
Visible depending on certain conditions	
	<p>Opens the page of the scanning task list, where you can find uncompleted (running) scanning tasks.</p> <p><i>It is situated on the navigation panel only if scanning is performed.</i></p>
   	<p>Opens the page with the list of completed scans. The button changes its color depending on the scanning results:</p> <ol style="list-style-type: none">1. Green — all scanings are completed successfully; all detected threats are neutralized.2. Red — some of the detected threats are not neutralized.3. Yellow — at least one of the scanning tasks failed. <p><i>It is displayed in the navigation pane only if at least one scanning was started.</i></p>
	<p>Opens the page with threats detected by Scanner or by the file system monitor SpIDer Guard.</p> <p><i>It is displayed in the navigation pane only if at least one threat was detected.</i></p>
	<p>It is displayed in the navigation pane only if the scanning start page is open and active.</p> <p><i>When you go to any other page of the main window or scanning session is started, the update control page closes automatically, and the button is removed from the navigation pane.</i></p>
	<p>It is displayed in the navigation pane only if the SpIDer Guard control page is open and active.</p> <p><i>When you go to any other page of the main window, the SpIDer Guard control page closes automatically, and the button is removed from the navigation pane.</i></p>
	<p>It is displayed in the navigation pane only if the SpIDer Gate control page is open and active.</p> <p><i>When you go to any other page of the main window, the SpIDer Gate control page closes automatically, and the button is removed from the navigation pane.</i></p>
	<p>It is displayed in the navigation pane only if the update control page is open and active.</p>



Button	Description
	<i>When you go to any other page of the main window, the update control page closes automatically, and the button is removed from the navigation pane.</i>
	<p>It is displayed in the navigation pane only if the License Manager control page is open and active.</p> <p><i>When you go to any other page of the main window, the License Manager control page closes automatically, and the button is removed from the navigation panel.</i></p>

Main Page

On the main page of Dr.Web for Linux's graphical management interface, you can see the target pane where you can drag and drop files and directories to be scanned. The pane is marked with the **Drag files here or click to select** label. After objects are dragged and dropped from the file manager to the Dr.Web for Linux Main page, their [custom scanning](#) starts (if the Scanner is already scanning other objects, the new scanning task is [queued](#)).

Also on the main page of the window, there are the following buttons:

- **SpIDer Guard**—displays the current state of the file system monitor SpIDer Guard. Click the button to open the [control page](#), where you can start or stop SpIDer Guard and see its operation statistics.
- **SpIDer Gate**—displays the current state of the SpIDer Gate network connection monitor. Click the button to open the [control page](#), where you can start or stop SpIDer Gate and see its operation statistics.
- **Scanner**—allows to open the page where you can [start scanning](#) of files and other objects of the file system (for example, boot records).
- **Last update**—displays the current status of virus databases. Click the button to open the [update control page](#), where you can start an updating process (if required).
- **License**—displays the status of the current license. Click this button to open the [License Manager](#) page, where you can find more detailed information on the current license as well as purchase and register a new license (if required).

Integration with Desktop Environment


Dr.Web for Linux supports the following four methods of integration with the graphic desktop environment:

- Displaying the application status indicator in the desktop notification area. The indicator allows you to show the application context menu and to view the popup notifications.
- Show the context menu containing main scan commands, when user does the mouse right-click on the application icon in the task bar.
- Start scanning of selected files and directories by the command of context menu in the graphic file manager.



- Start scanning of files and directories that the user drops on the application main window using the mouse pointer.

Status Indicator in Notification Area

After the user logs on, in the Desktop notification area (if it is supported by the used graphical environment) the notification agent displays an indicator, which looks like the Dr.Web for Linux icon . The indicator displays the application state and provides access to the Dr.Web for Linux menu. If any problem occurs (e.g., the virus databases are outdated, license is about to expire), the indicator displays an exclamation mark: .

In addition to the status indicator, the notification agent also displays pop-up notifications that inform the user on important events of Dr.Web for Linux's operation, such as:

- Detected threats (including those detected by SpIDer Guard and SpIDer Gate).
- License validity period is about to expire

Once the icon is clicked, the Dr.Web for Linux menu displays on the screen.

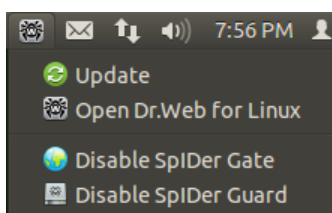




Figure 21. Dr.Web for Linux indicator context menu

When you select the **Open Dr.Web for Linux** item, [window](#) of Dr.Web for Linux's graphical management interface appears on the screen; that is, Dr.Web for Linux [operation](#) is started. Selection of **Enable SpIDer Gate/Disable SpIDer Gate** or **Enable SpIDer Guard/Disable SpIDer Guard** items starts or stops operation of the corresponding monitor. Note that you need to authenticate as a user with administrative privileges to disable operation of any monitor (refer to [Managing Application Privileges](#)). Selection of the **Update** item forces an update procedure to start.

If the indicator notifies on problems in Dr.Web for Linux operation, the icon of the component, which caused the problem, also displays an exclamation mark, for example: .

Status Indicator Issues

1. If the indicator displays a critical error mark , and drop-down menu contains only one disabled item **Loading**, it means that Dr.Web for Linux cannot start because some core components are unavailable. If this status is permanent, try to [resolve](#) this error manually or contact [technical support](#).
2. If the indicator is not displayed in the notification area after the user logged in, try to [resolve](#) this error manually or contact [technical support](#).



In different desktop environments, appearance and behavior of the indicator can differ from the ones described above; for example, icons may not display on the drop-down menu.

Context Menu on Task Bar Icon

If the desktop environment contains a task bar, such as **Unity Launcher** in **Ubuntu** OS, on the task bar appears the button with an application icon, when Dr.Web for Linux is started. It is recommended to launch the application via the **Dr.Web for Linux** item in **Applications** desktop menu. When you click on the task button by the right mouse button, the application menu is appeared. The menu looks like as follows (example for **Unity Launcher** in **Ubuntu 12.04**).

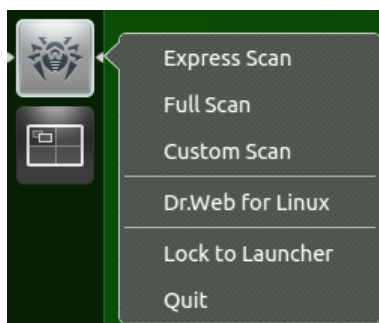


Figure 22. Context menu in task bar for Dr.Web for Linux

Selection of **Express scan**, **Full scan** and **Custom scan** items allows you to start the corresponding [scan task](#) (for **Custom scan** item, selection only opens the page on application window where you can select objects for scan). The **Dr.Web for Linux** item [launches](#) the graphical management interface (if not launched), and **Quit** item [terminates](#) it (if launched). The **Lock to Launcher** item allows you to lock the application icon on the task bar in order to provide quick access to graphical management interface and general scan tasks.

In case there are executed tasks for scanning of the file system in the [task queue](#), indicator of the total execution of active scanning tasks is displayed on top of the application icon in the task bar.



In the different desktop environments, the task bar as well as the context menu and behavior of the menu items (excluding **Express scan**, **Full scan** and **Custom scan**) may differ from described above.

Task Bar Menu Issues

If the button with application icon is displayed on the task bar but the context menu does not contain items for starting of scan tasks, try to launch the application via the **Dr.Web for Linux** item on **Applications** menu (instead of launching the application by the **drweb-gui** command in a terminal emulator or selecting of **Open Dr.Web for Linux** item in the context menu of the [status indicator](#) in the notification area).



Launching Scan from File Manager

Dr.Web for Linux allows you to scan files and directories directly from the window of graphic file manager (such as **Nautilus**). For scanning of files and directories it is necessary to select them in the file manager window and then click right mouse button. Then in the appeared context menu select the **Open With Other Application** item, and after that in the list of installed applications find and choose **Dr.Web for Linux**. Usually, after you have selected usage of Dr.Web for Linux for opening of files at first time, this association will be saved by the file manager, and in the future the context menu will contain the item **Open With Dr.Web for Linux**.



In the different graphic file managers, the item of the context menu as well as the way to choose an application for processing the selected files may differ from the ones described above.

Problems that occur when using the context menu of the file manager

Some graphical environments for **GNU/Linux** can automatically configure associations for file or directories (based on their MIME type) with **Dr.Web for Linux** that has been selected in the file manager for scanning by choosing the option **Open With Other Application**. Thus, if you then double-clicked on those files or directories, **Dr.Web for Linux** was run. To resolve this issue, [cancel configured associations](#) between files and **Dr.Web for Linux**.

Drag and Drop of files and directories onto a window of the graphical management interface

Dr.Web for Linux allows you to initiate scanning of files and directories when you drag and drop them with the mouse pointer from file manager window and directories of the graphical file manager to the window of running Dr.Web for Linux's graphical management interface. To start the scanning by dragging and dropping, it is necessary for the [main page](#) or page with [scan types](#) on the interface window to be opened. The dropped file objects will be scanned, if the page contains the area marked with a special label **Drag files here or click to select** that indicates that objects can be dropped onto this page of Dr.Web for Linux's interface window for management.

Starting and Shutting Down Graphical Interface

Launch of the Dr.Web for Linux's Graphical Management Interface

To launch the Dr.Web for Linux's graphical management interface, it is necessary to:

- Select **Dr.Web for Linux** item on the **Applications** desktop menu.

or

- Right-click the Dr.Web for Linux [status indicator](#) icon in the notification area and select **Open Dr.Web for Linux**.



You can also start Dr.Web for Linux' graphical management interface from [the command line](#) by entering the **drweb-gui** command. You can use this option only if graphical environment is accessible in the command-line mode, for example, when working in a terminal emulator window.

Termination of Dr.Web for Linux's Graphical Management Interface Operation

To shut down Dr.Web for Linux's graphical management interface, close the window using the standard close button on the title bar.



Note that service components, including the notification agent, SpIDer Guard and SpIDer Gate, continue their operation after Dr.Web for Linux graphical interface shuts down (unless they are disabled by the user).

Under normal operation, operation of all necessary service components does not require user intervention.

Threat Detection and Neutralization

Search and neutralization of threats can be started either by Scanner (on [user demand](#) or as [scheduled](#)), or by the file system monitor SpIDer Guard and the network connection monitor SpIDer Gate.

- To enable or disable SpIDer Guard and SpIDer Gate, use the [context menu](#) in the notification area or open the corresponding page with the monitor settings (refer to [File System Monitoring](#) and [Monitoring of Network Connections](#)).
- To view current tasks of Scanner or manage them, open the page for [task management](#).
- To view threats detected by Scanner or during SpIDer Guard checks, open the [page with listed threats](#).
- To manage quarantined threats, open the [Quarantine view](#) page.
- To configure Dr.Web for Linux reaction on detected threats, open the [Settings window](#). On this window, you can also set [schedule](#) to start scanning, [configure](#) monitoring of encrypted connections.



Please note that in case if the Dr.Web for Linux is operating in [Central protection mode](#) and launching of scanning by user demand is prohibited on central protection server, the **Scanner page** of the Dr.Web for Linux window will be disabled. Moreover, in this case the notification agent and the graphical interface for management will not launch scanning even if it is scheduled.



Scanning on Demand

Scanning Types

On user demand, scanning in one of the following modes can be started:

- *Express scan*—scan of critical system objects that are at high risk to be compromised (boot records, system files, etc.).
- *Full scan*—scan of all file system objects available for the user under whom Dr.Web for Linux is started.
- *Custom scan*—scan of file system objects or other special objects specified by the user.



If Dr.Web for Linux is operating in [Central protection](#) mode and launch of scanning on demand is prohibited on the Central protection server, this page is disabled.

Scanning can increase processor load, which can cause the battery to discharge faster. Thus, it is recommended to perform a scan of a portable computer when it is plugged in.

Starting Scanning

To start scanning, click the **Scanner** button on the [Main](#) page.

The page with scan types opens. To start *Express* or *Full* scan, click the corresponding button. Once one of these buttons is clicked, scanning process automatically starts.

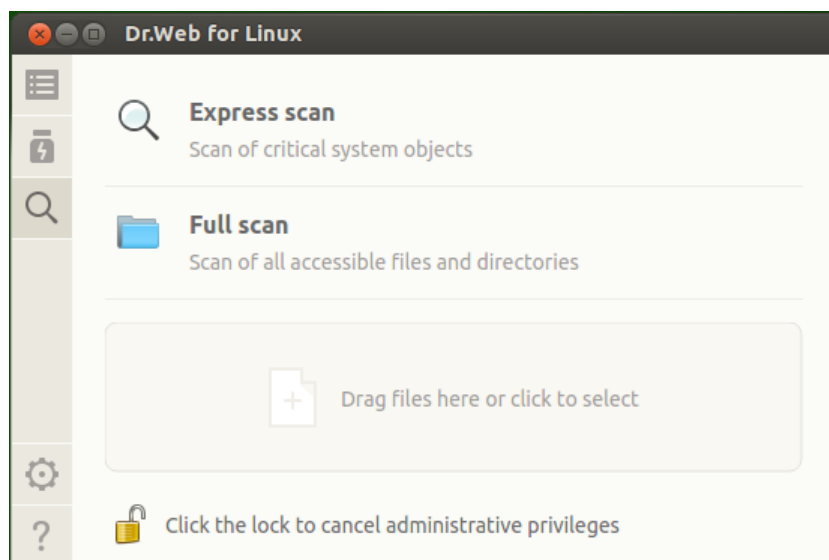


Figure 23. Select scan type page



Scanning is performed with current application privileges. If the user whose privileges are currently active does not have superuser permissions, all files and directories that are not accessible to this user cannot be scanned. To enable check of all required files on which you do not have owner permissions, elevate the application privileges before scanning starts. For details, refer to [Managing Application Privileges](#).

To start *Custom* scan of certain files and directories, do one of the following:

- **Drag and drop required objects**

Drag and drop required files and directories from the system File Manager window to the area marked with a special label **Drag files here or click to select**. You can also drag and drop the objects to the [Main page](#).

When dragging objects over the page, it changes to the pane indicated with the **Drop files here** label. To start scanning, drop the dragged objects onto the target area by releasing the mouse button.

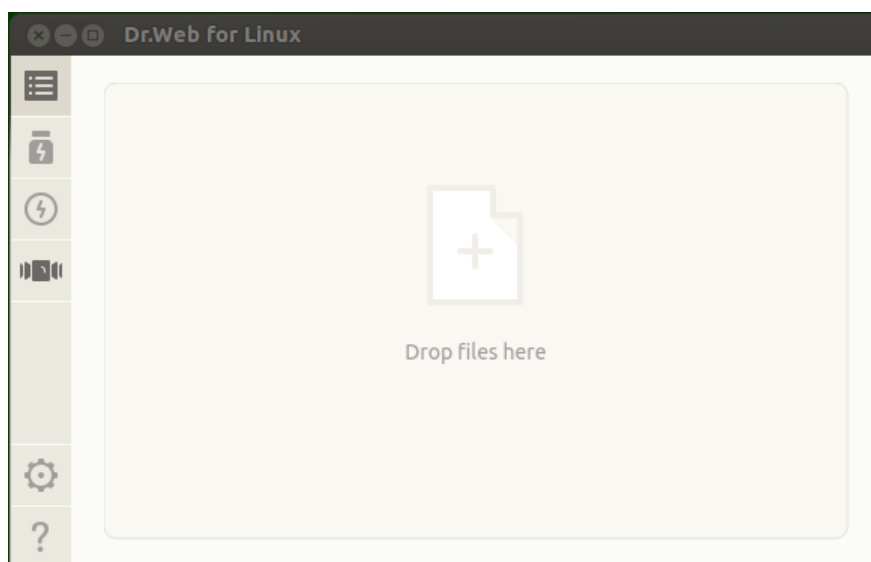


Figure 24. Target area where objects are dropped for scanning

- **List the objects to be scanned**

To select the objects for scanning, click the target area. The window where you can select system objects for Custom scan opens.

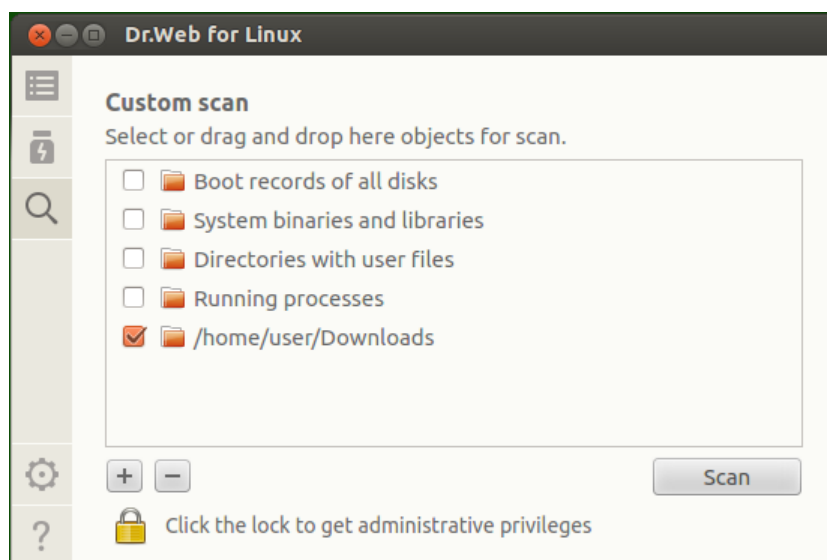


Figure 25. List of objects for scanning


The list of objects for Custom scan contains four predefined items:

- *Boot records of all disks.* If you enable this item, all boot records of all available disks are selected for scanning.
- *System binaries and libraries.* If you enable this item, all directories with system binaries are selected for scanning (`/bin`, `/sbin`, etc.)
- *Directories with user files.* If you select this item, all directories where user files and files of the current session reside are selected for scanning (`/home/<username>` (`~`), `/tmp`, `/var/mail`, `/var/tmp`).
- *Running processes.* If you select this item, binary executable files containing code of currently running processes are selected for scanning. At that, if a threat is detected, not only the malicious object is neutralized but also the active process is terminated.

Editing the List of Custom Scan Objects

If required, you can add custom paths to the list of objects for scanning. For that purpose, drag and drop necessary objects (paths to the objects are automatically added to the list) or click the **+** button below the list. In this case, a standard dialog window opens, where you can select required objects (a file or a directory). After you select an object, click **Open**.



Hidden files and directories are not displayed in the file chooser by default. To view such objects, click the  button in the file chooser.

To remove all selected paths from the list, click the **–** button. The path is selected for removal, if list item containing this path is selected. To choose several paths, select items in the list with pressed SHIFT or CTRL key. Please note that the first four items in the list are predetermined and cannot be removed.



Starting Custom Scan of Listed Objects

To start Custom scan of listed objects, select all required files or directories and click **Scan**. Once the button is clicked, scan of the selected objects starts.

After scanning starts, the task is added to the queue which contains all scanning tasks of the current session: complete tasks, tasks in progress, and pending tasks. You can view the list of tasks and manage them on the [scan task management](#) page.

Scheduled scanning

Dr.Web for Linux can perform the automatic launch of scheduled scanning of the specified list of the file system objects according to the [indicated schedule](#).



If Dr.Web for Linux is operating under server's control in [Central protection](#) mode and launch of scanning on demand is prohibited on the Central protection server, this Dr.Web for Linux's possibility is unavailable.

Scanning Types

According to schedule, it is possible to perform the following types of scanning:

- *Express scan*—scan of critical system objects that are at high risk to be compromised (boot records, system files, etc.).
- *Full scan*—scan of all file system objects available for the user under whom Dr.Web for Linux is started.
- *Custom scan*—scan of file system objects or other special objects specified by the user.

Starting Scanning

Scanning is started automatically according to the set schedule. Start of the scanning is performed by:

1. The graphical interface itself if it runs when the scanning starts.
2. The notification agent if the graphical interface is unavailable when the scanning starts.

When scheduled scanning starts, the graphical management interface automatically starts (if it is not launched yet), the created task is added to the queue which contains all scanning tasks of the current session: complete tasks, tasks in progress, and pending tasks. You can view the list of tasks and manage them on the [scan task management](#) page.



Managing Scan Tasks

You can view the list of created tasks and tasks in progress on the special Dr.Web for Linux page. If at least one task is queued, a button that opens the page with the task list becomes visible in the [navigation pane](#). Depending on the status of the queued tasks, the button has one of the following icons:

	At least one of the tasks is not complete (icon is animated).
	All scanning tasks in the list are complete or stopped by the user; no threat is detected or all detected threats are successfully neutralized.
	All scanning tasks in the list are complete or stopped by the user; some of the detected threats are not neutralized.
	All scanning tasks in the list are complete or stopped by the user. Some of the tasks failed.

Tasks are sorted by creation time (from the last to the first created task).

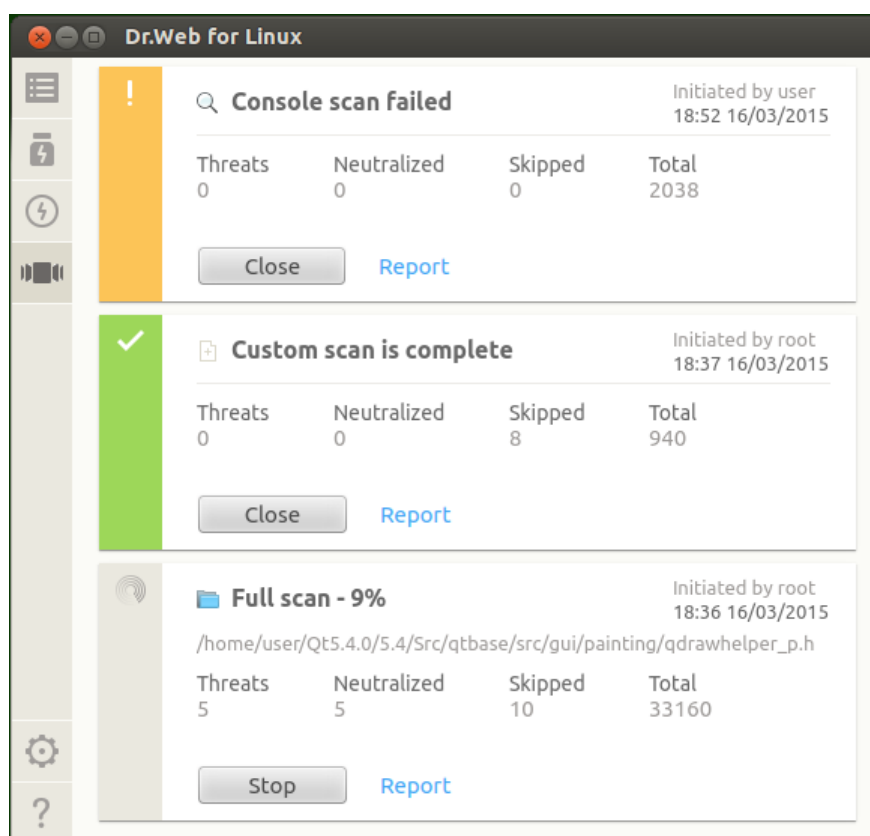


Figure 26. Task management page





For each listed task, the following information is available:

- Scanning type.



- Name of the user who started scanning (if unknown, the system identifier—*UID*—is displayed).
- Date of task creation and completion (if complete)
- Number of detected threats, neutralized threats, skipped files, and total number of scanned objects

The status of the task is indicated with the color mark assigned to the listed task. The following colors are used:

	Scanning is not complete or is pending.
	Scanning is complete or stopped by the user; no threat is detected or all detected threats are neutralized.
	Scanning is stopped due to an error.
	Scanning is complete or stopped by the user; at least one detected threat is not neutralized.

Note that the list contains scanning tasks performed by Scanner in the current session, not just the tasks [created by the user](#) in Dr.Web for Linux window. Other types of scanning can be the following:

- *Console scan*—scanning initiated by the user or an external application via the [command-line interface](#)
- *Enterprise scan*—scanning initiated by the [central protection](#) server
- *Scheduled scan*—scanning started automatically according to the specified [schedule](#) set in the application settings.

On the task description area, one of the following buttons is available:

- **Cancel**—cancel the pending task. The button is available if the task is pending. Once the button is clicked, the task completes. Information on the task remains in the list.
- **Stop**—stop the task which is in progress. After you click this button, the stopped task cannot be resumed. The button is available if the task is in progress. Information on the stopped task remains in the list.
- **Close**—close information on the complete task and delete the task from the list. The button is available if the task is not complete and if all detected threats are neutralized.
- **Neutralize**—neutralize threats. The button is available if the task is complete and some of the detected threats are not neutralized.
- **Details**—open the list with detected threats and neutralize them. The button is available if the task is complete and some of the detected threats are not neutralized.

Click **Report** to display information on scanning results including detailed information on the task and the list of detected threats, if any.

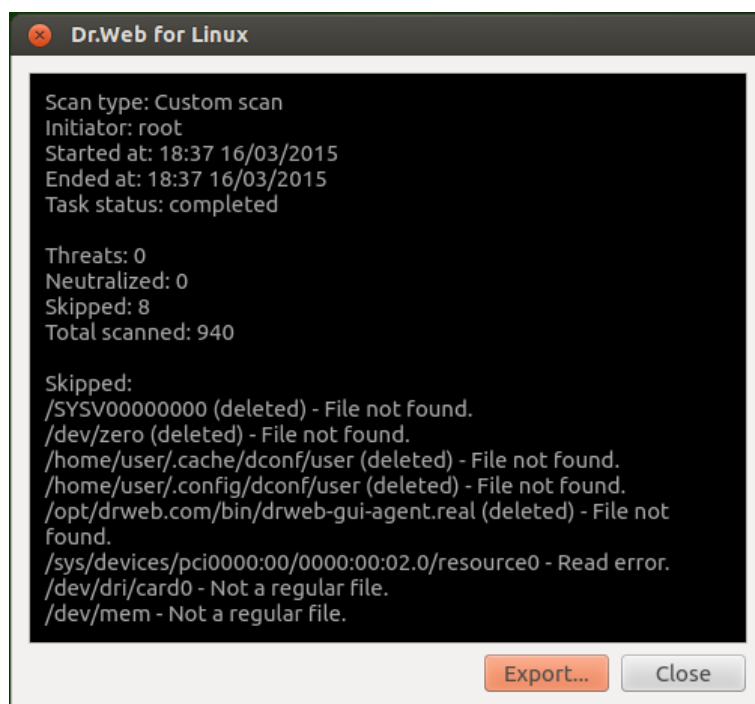


Figure 27. Detailed information on scanning results



File systems of UNIX-like operating systems, such as **GNU/Linux**, can contain special objects that appear as named files but are not actual files containing data (for example, such objects are symbolic links, sockets, named pipes, and device files). They are called *special* files as opposed to *usual* (*regular*) ones. Dr.Web for Linux *always* skips special files during scanning.

If you click the detected threat name, its description will open in the browser (a page of Doctor Web official website will open; Internet connection is required) installed in the system.

Click **Export** if you want to save the scanning report to a text file. To close the window with detailed scanning information, click **Close**.

To any threat detected during scanning which was started in graphical mode (including a scheduled scanning), Dr.Web for Linux applies [actions](#) that are specified in the settings on the **Scanner** [tab](#).



Note that threat neutralization settings specified on the **Scanner** tab are not used for *centralized* and *console* scanning.

To view all detected threats, open the [page with listed detected threats](#).

File System Monitoring

Continuous monitoring of file system objects is performed by the file system monitor SpIDer Guard.



The Dr.Web for Linux allows to configure SpIDer Guard, namely:

- Start and stop the file system monitor
- View component statistics and list of detected threats
- Configure the following parameters of the file system monitor:
 - Reaction to detected threats
 - List of objects excluded from scanning

Managing Operation of the File System Monitor

You can start and stop the file system monitor SpIDer Guard and view statistics on its operation on the special page of Dr.Web for Linux. To access the page, click the **SpIDer Guard** button on the [main page](#).

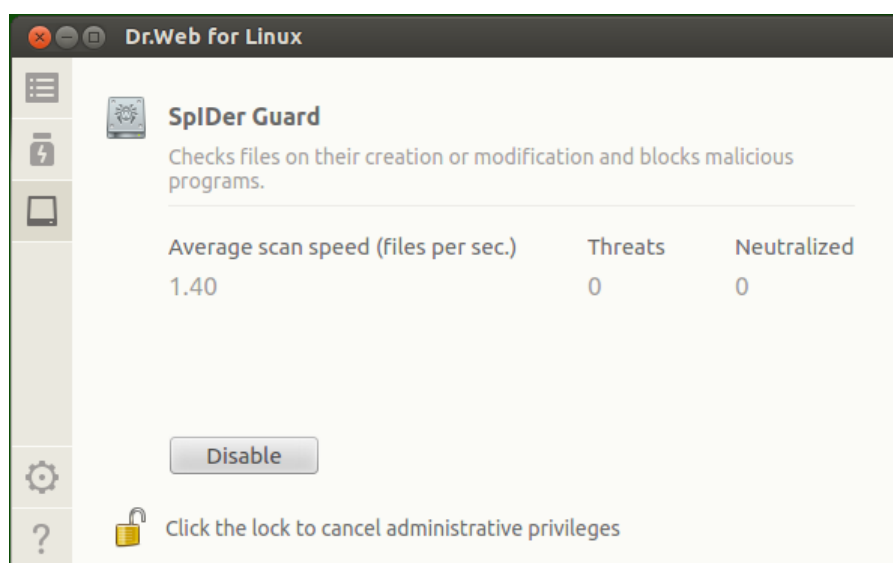


Figure 28. SpIDer Guard management page

On the page for monitoring management, the following information is displayed:

- State of the file system monitor SpIDer Guard (enabled or disabled) and details on errors if they occurred during the component operation.
- File system monitoring statistics:
 - Average file scanning speed
 - Number of detected and neutralized threats



To enable monitoring, if disabled, click the **Enable** button. To disable monitoring, if enabled, click the **Disable** button.



To disable the file system monitor, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

The option to enable and disable SpIDer Guard when Dr.Web for Linux is operating under the [central protection](#) server can be blocked if disabled by the server.

SpIDer Guard state (enabled or disabled) is shown with the indicator:

	File system monitor SpIDer Guard is enabled and is protecting the file system.
	File system monitor SpIDer Guard is not protecting the file system because either the user disabled the component, or an error occurred.

To close the page, go to another page by using the buttons in the pane.

The list of threats detected by SpIDer Guard in current Dr.Web for Linux session is displayed on the [detected threats view](#) page (available if at least one threat is detected).

Setting the File System Monitor

You can set how the file system monitor SpIDer Guard works in the [settings window](#):

- On the **SpIDer Guard** [tab](#), specify reaction to detected threats.
- On the **Exclusions** [tab](#), specify objects to be excluded from monitoring.

Problems with SpIDer Guard operation

If an error occurs in operation of SpIDer Guard, the management page displays the error message. To solve the problem, refer to the description of known errors in [Appendix D](#).

Monitoring of Network Connections

Continuous control of established network connections is performed by SpIDer Gate. It restricts access to websites added to user black lists or marked as unwanted for visiting. In addition, SpIDer Gate checks sent and received email messages and files being downloaded from the Internet and blocks them if a threat is detected.

The Dr.Web for Linux allows to configure SpIDer Gate, namely:

- Start and stop the network connection monitor.
- View the number of checked and blocked objects and attempts to access websites
- Configure the following parameters of network connection monitoring:
 - List of websites access to which is restricted
 - Personal black and white lists of websites



- Parameters of checking files downloaded from the Internet or transmitted via email.

Managing Operation of the Network Connection Monitor

You can start and stop the network connection monitor SpIDer Gate and view statistics on its operation on the special page of Dr.Web for Linux. To access the page, click the **SpIDer Gate** button on the [main page](#).

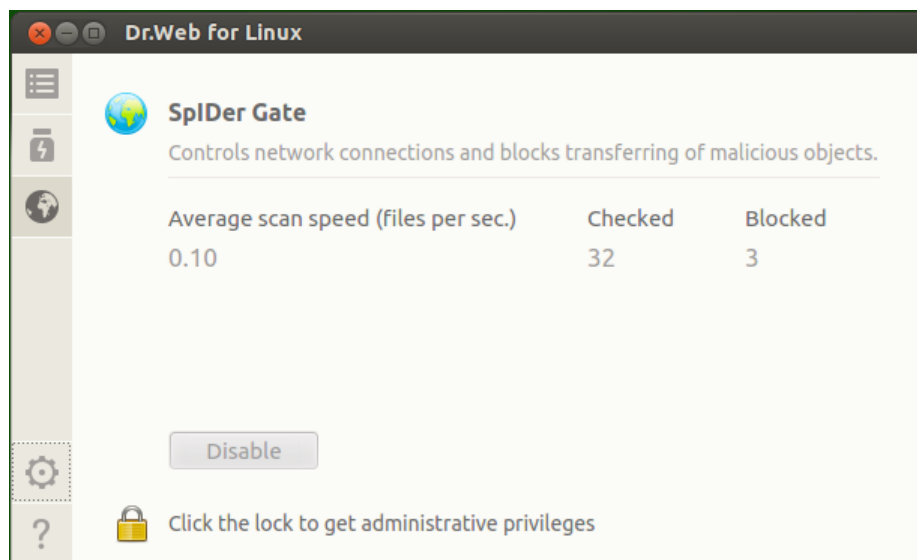


Figure 29. SpIDer Gate management page

On the page for monitoring management, the following information is displayed:

- State of the network connection monitor SpIDer Gate (enabled or disabled) and details on errors if they occurred during the component operation.
- Monitoring statistics:
 - Average speed of scanning of email messages and files downloaded from the Internet.
 - Number of checked objects (email messages, files downloaded from the Internet and URLs).
 - Number of blocked attempts to access websites and malicious objects

To enable monitoring, if disabled, click the **Enable** button. To disable monitoring, if enabled, click the **Disable** button.





To disable the monitoring of network connections, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

The option to enable and disable SpIDer Gate network connection monitor when Dr.Web for Linux is operating under the [central protection](#) server can be blocked if disabled by the server.



State of the network connection monitor SpIDer Gate (enabled or disabled) is indicated as follows:

	SpIDer Gate is enabled and is controlling network connections (and also email and Internet access).
	SpIDer Gate is not controlling network connections (access to websites is not restricted, email messages and downloaded files are not checked) because either the user disabled the component or an error occurred.



If a mail client runs in the system (such mail client as **Mozilla Thunderbird**) that uses the IMAP protocol to receive email messages, it is necessary to restart it after enabling SpIDer Gate to provide the scanning of incoming email messages.

Even if transmission of files and email messages is not controlled by SpIDer Gate, their threats can be detected by the enabled file system monitor SpIDer Guard at the moment of their saving by the mail client to the local file system.

To close the page, go to another page by using the buttons in the pane.

Operation Settings of the Network Connection Monitor

Operation setting of the network connection monitor SpIDer Gate is performed in the [settings window](#):

- On the **SpIDer Gate** [page](#), you can specify the list of blocked website categories and reaction to detected threats.
- On the **Exclusions** [page](#), configure the black and white lists of websites and exclude application network activity from monitoring.
- On the **Network** [tab](#)—managing of check of protected connections (SSL/TLS).


Issues in the Operation of the Network Connection Monitor

If an error occurs in operation of the network connection monitor, the management page displays the error message. To solve the problem, refer to the description of known errors in [Appendix D. Known Errors](#) section.

Viewing Detected Threats

The list of threats detected by Scanner and SpIDer Guard during the current Dr.Web for Linux session is displayed on the special window page which is available only if at least one threat was detected.



If threats were detected, you can open this page by clicking the  button in the GUI navigation pane.

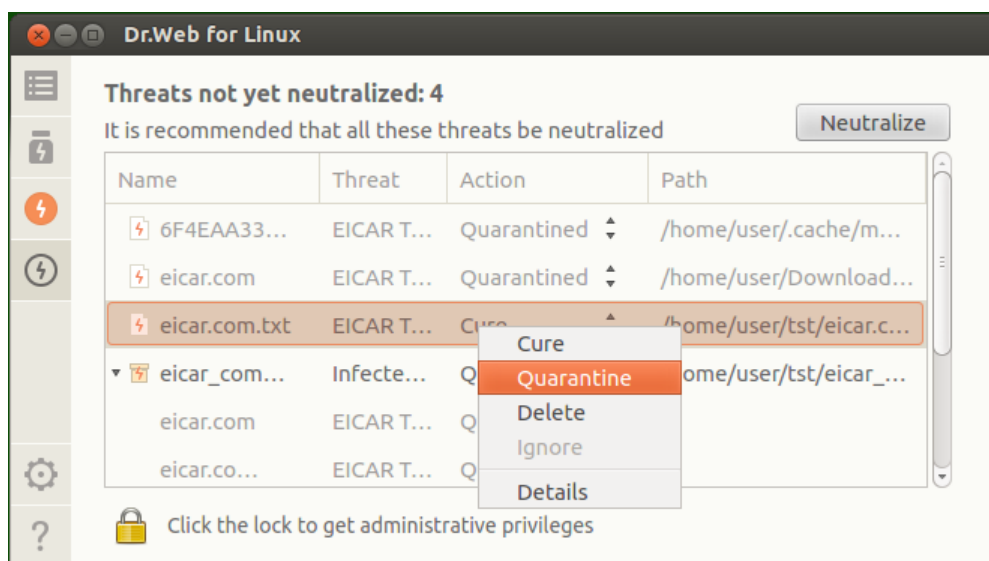


Figure 30. Page with listed threats

In the list, the following information is available for each detected threat:

- Name of the malicious object
- Name of the [threat](#) (according to the Doctor Web classification)
- [Action](#) applied (or to be applied) to the threat
- Path to the malicious object

Neutralized threats display in the list as grayed out items.

Neutralizing Detected Threats

If some of the listed threats are not neutralized, the **Neutralize** button above the list becomes available. Once the button is clicked, actions specified in the corresponding *Action* fields are applied to the threats. If an attempt to neutralize a threat fails, the listed item is displayed red and an error message appears in the *Action* field.

By default, an action to be applied to a threat is selected according to the settings of the component which detected the threat. You can configure actions applied to threats of a certain type by Scanner and SpIDer Guard. For that purpose, open the corresponding tab on the [Settings window](#) and adjust the settings.

If it is necessary to apply an action which is different from the one specified in the settings, click the *Action* field and select the required action on the menu.



If threat is detected in a file located in a container (an archive, email message, etc.), its removal is replaced with moving of a container to quarantine.

You can select multiple items in the threat list at a time. To do that, select the items with a mouse button while holding down CTRL and SHIFT keys.

- When you hold down a CTRL key, threats are selected one by one.
- When you hold down a SHIFT key, threats are selected contiguously.

After you select threats, you can apply a required action to them by right-clicking in the selected area and then clicking the required item on the displayed menu. The action selected on the menu is applied to all of the selected threats.



Note that

- If a threat is detected in a complex object (archive, email message, etc.), the selected action is applied to the container as a whole (and not to only the infected object).
- The *Cure* action can be applied not to all threat types.

If required, elevate [application privileges](#) to enable successful neutralization of threats.

Viewing Information on Threats

To receive detailed information about any detected threat, right-click the corresponding row and select **Details** in the appeared context menu. This opens the window with information on the threat and the infected object. If you need to view details on several threats, select them from the list by using the left mouse button and holding down CTRL before requesting the context menu.

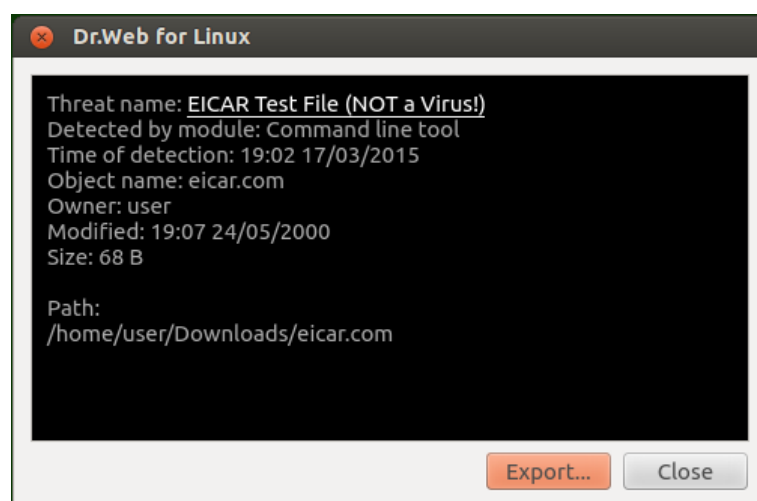


Figure 31. Information on a threat

This window contains the following information:

- Threat name (according to the Doctor Web classification)
- Name of the Dr.Web for Linux component which detected the threat



- Date and time when the threat was detected.
- Information on the file system object where the threat was detected: object name, owner, date of the latest modification and path to the object in the file system
- Last action applied to the threat and the result (if an option to apply actions to threat automatically is enabled for the component, for example – in a [corresponding tab](#) of the application settings window).

If you click the threat name, its description will open in the browser (a page of Doctor Web official website will open; Internet connection is required) installed in the system.

Click **Export** if you want to save the displayed information to a text file (once the button is clicked, the file browsing window will open). To close the window with threat and object details, click **Close**.

Managing Quarantine

The list of objects isolated by Dr.Web for Linux to quarantine is displayed on a separate page. To

open this page, click  on the [navigation pane](#).

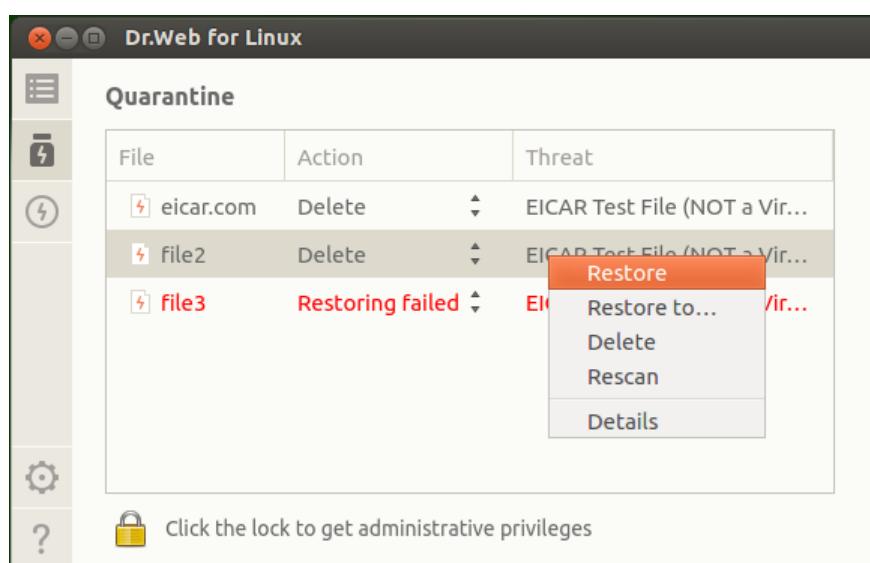


Figure 32. Quarantine management page

If quarantine is not empty, the following information is listed for every threat:

- Name of the malicious object
- [Action](#) to be applied to the object in quarantine
- Name of the [threat](#) (according to the Doctor Web classification)



Applying Actions to Quarantined Threats

To apply an action to an object isolated in quarantine, right-click anywhere in the table row, which contains the information about this object, and select the required action on the appeared shortcut menu. If you need to apply an action to several isolated objects, select the corresponding rows in the table and then right-click anywhere in the selected area. To select several rows, hold CTRL or SHIFT down:

- When you hold CTRL, rows are added to the selection one at a time.
- When you hold SHIFT, adjacent rows are added to the selection.

The menu contains the following actions:

- **Restore**—restore selected objects to its original location.
- **Restore to**—restore selected objects to the specified file system location (the window for choosing of the target location will appear).
- **Delete**—delete selected objects permanently.
- **Rescan**—scan selected objects once again and cure, if possible.

If the selected action is successfully applied to the object, the corresponding row is removed from the table automatically. If the attempt to apply the action fails, the corresponding row remains active and becomes red and the *Action* field displays details on the error.



To apply actions to isolated object, it may be necessary to elevate [application privileges](#). For example, to apply actions to objects moved to quarantine by any user.

Viewing Details on Quarantined Objects

To receive detailed information about any isolated object, right-click the corresponding row and select **Details** on the appeared menu. This opens the window with information on the object. If you need to view details on several objects, select them on the list by using the left mouse button and holding down CTRL.

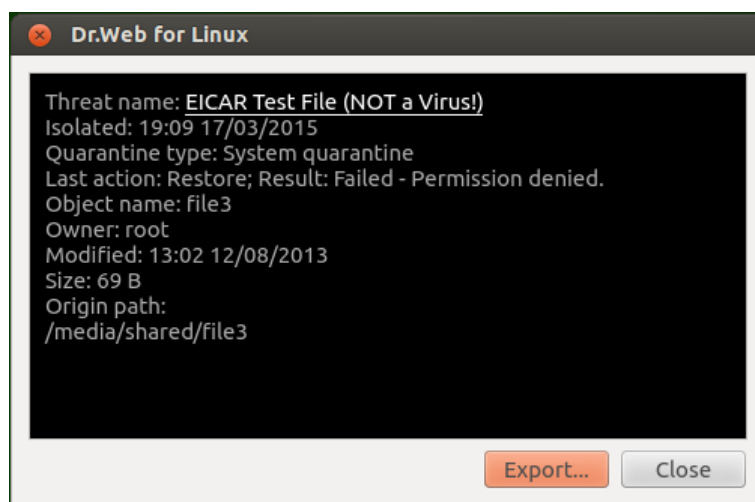


Figure 33. Isolated object details

This window contains the following information:

- Threat name (according to the Doctor Web classification)
- Date and time when the object was isolated to quarantine
- [Type](#) of the quarantine where the object is isolated.
- Name of the last applied action and its result;
- Details on the isolated file system object: name, owner, last modification date, object path in the file system.

If you click the threat name, its description will open in the browser (a page of Doctor Web official website will open; Internet connection is required) installed in the system.

Click **Export** if you want to save the displayed information to a text file (once the button is clicked, the file browsing window will open). To close the window with threat and object details, click **Close**.

Updating Antivirus Protection

Periodic updates to virus and web categories databases as well as Dr.Web for Linux anti-virus engine are downloaded and installed by Updater automatically. You can view status of databases and force an update, if required, on a special page of the window. To open the page, on the [Main page](#) click **Last update**.

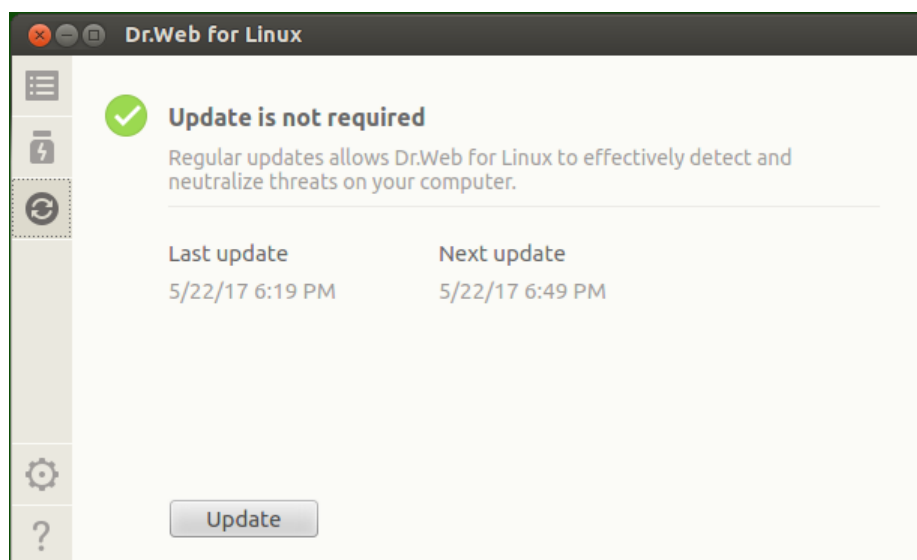


Figure 34. Update management page

The page displays the following information:

- Status of virus databases, database of web resource categories and anti-virus engine
- Information on the last update and time of the next scheduled update

To force an update, click **Update**. To close the update management page, select another main window page by clicking a corresponding button in the navigation pane.



If Dr.Web for Linux is operating in [Central protection](#) mode, the update management page can be blocked.

Configuring Updates

You can configure Dr.Web for Linux update settings in the [Settings window](#), in the **Main tab**.

Problems with Updater Operation

If Updater failure is detected, error information is displayed on the update management page. To resolve the problem, refer to [Appendix D](#), where you can find detailed description of known errors.

License Manager

In graphical mode, License Manager allows to view information on the current license issued for the Dr.Web for Linux user. License data is stored in a license key file that provides operation of Dr.Web for Linux on the user computer. If neither license key file nor demo key file is found on the computer, all Dr.Web for Linux functions (including file check, file system monitoring, virus database update) are blocked.



License Manager

License Manager page is available in the Dr.Web for Linux graphical management interface. To open the page, on the [Main page](#) click **License**.

If a demo key file or license key file for Dr.Web for Linux to use is installed, the License Manager start page displays license information including license number, license owner, and duration period. This information is retrieved from the corresponding key file.

The figure below shows appearance of the License Manager page.

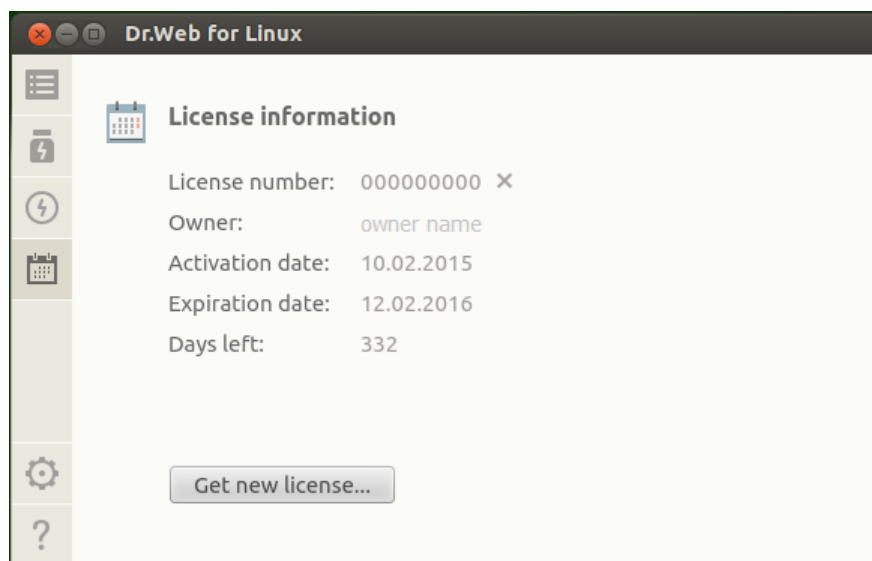


Figure 35. License information page

To [delete](#) a license key file, click  next to the license number.

To close a License Manager page, select another Main window page by clicking a corresponding button in the navigation pane.

License Activation

To activate a license via License Manager and obtain the corresponding key file providing functionality of Dr.Web for Linux (which includes purchasing a new license or renewing the current one) or to obtain a demo license, click **Get new license**. After that, the registration wizard opens. Note that the registration wizard also opens automatically when Dr.Web for Linux is first started after its installation.

On the first step, you should choose an activation type. The following three types are available:

1. [Activation](#) of license or demo period using a serial number
2. [Obtaining](#) a demo period
3. [Installation](#) of a key file obtained earlier



To register a serial number or to get a demo period, an Internet connection is required.

1. Activation of License or Demo Period Using a Serial Number

To activate a license or demo period, enter the serial number in the text field and click **Activate**.

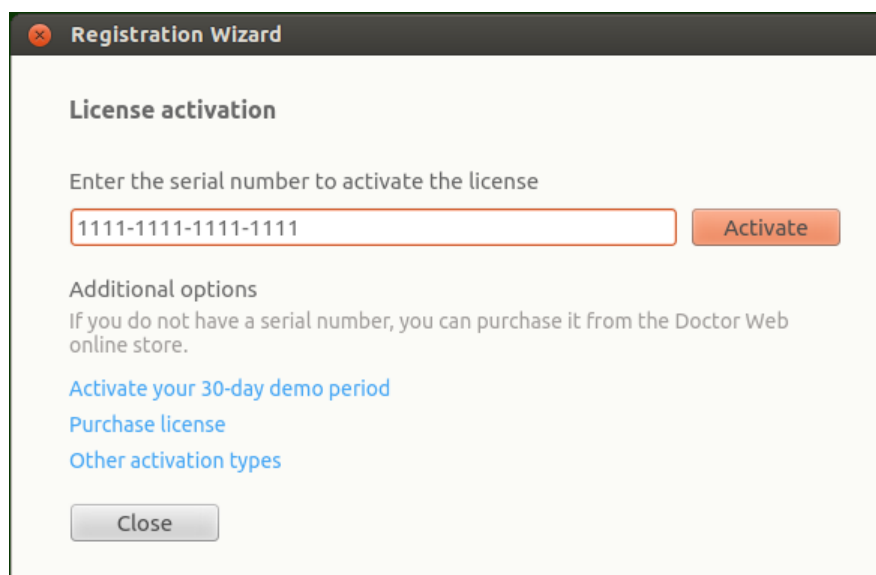


Figure 36. Registration using a serial number



If you do not have a serial number or a valid key file, you can purchase license on the Doctor Web official website. To open the online store page, click **Purchase license**.

For information on other ways to purchase the license for Dr.Web products, refer to [Licensing](#).

Once you click the **Activate** button, connection to the Doctor Web registration server is established.

If the serial number, which you specified on the first step, was obtained from the Doctor Web website and issued for a three month's demo period, further steps are not required for its activation.

If the specified serial number corresponds to the license for using the product on two computers, you need to select on how many computers you would like to use the product. If you select **On two computers**, you can activate the second serial number on another computer and receive another license key file. The registered licenses will have the same validity period (for example, one year). If you select **On one computer**, you should specify the second serial number from the purchased kit. In this case, you cannot register this serial number later on another computer (neither can you use a copy of the license key file resulting from sequential activation of the serial numbers), but the duration of the current license is doubled (for example, extended to two years if the license period is one year).

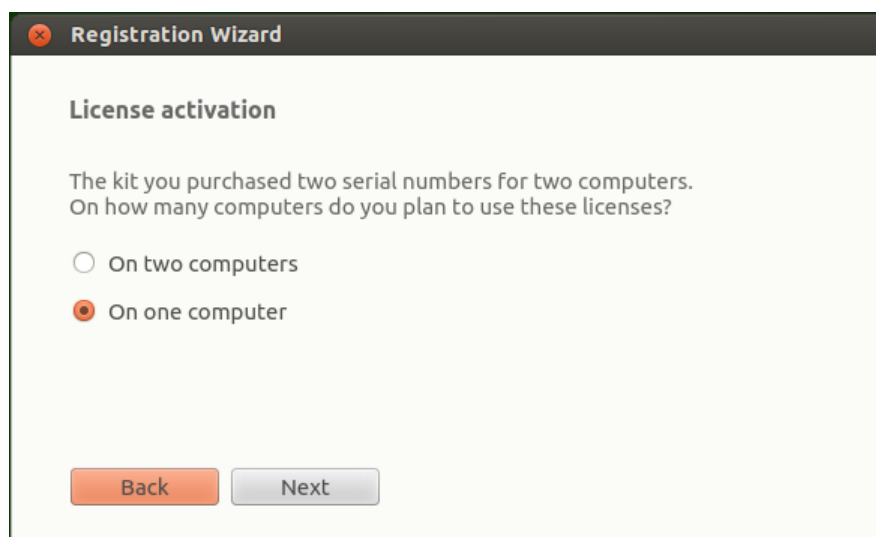


Figure 37. Selecting the number of computers

After you select the number of computers on which you would like to activate the license, click **Next**, and if you have selected **On one computer**, in the next wizard page specify the second serial number and then click **Next**.

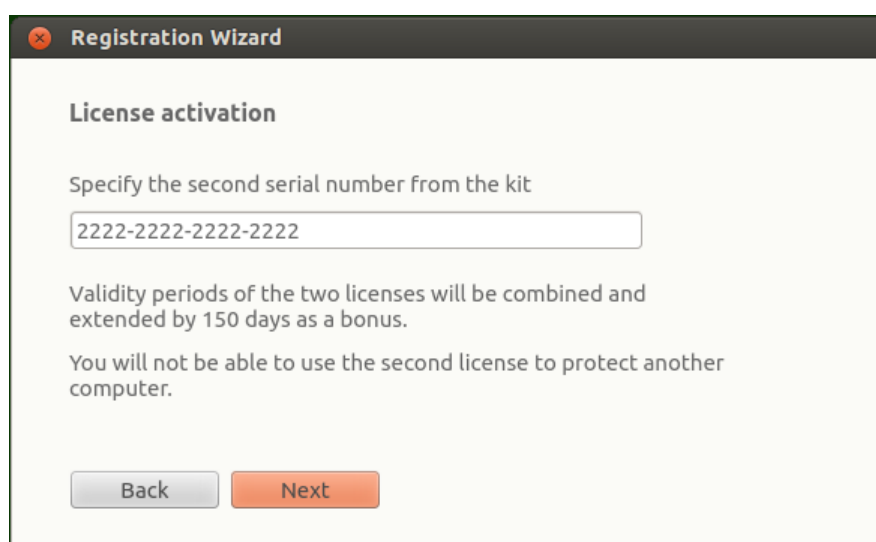


Figure 38. Specifying the second serial number from the kit

In next step, you are prompted to receive a bonus and extend the license period for 150 days. To receive the bonus, select **Specify the previous license**. If you do not want to receive the bonus or do not have a previous license, select **I do not have a previous license**. Then click **Next**.

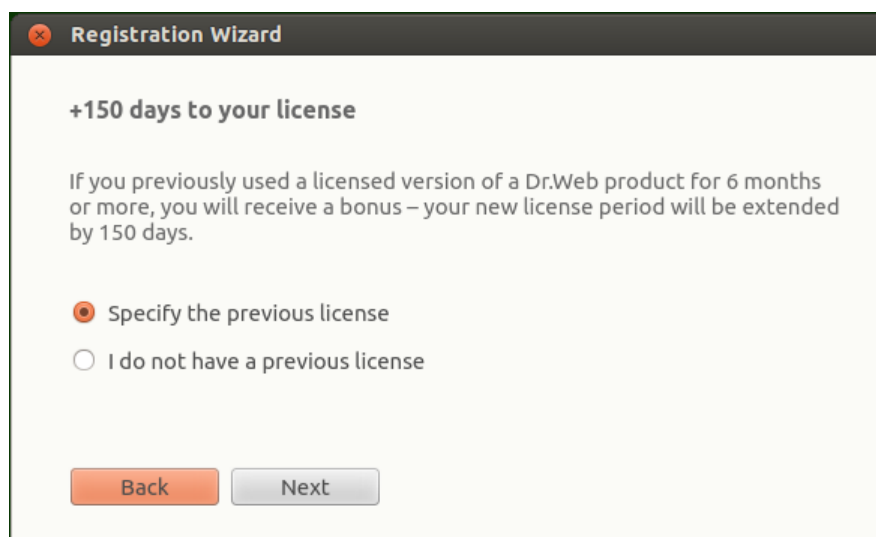


Figure 39. The bonus prompt

If in the first step you have specified a special *renewal* serial number, you will not be shown a bonus prompt in this step. Instead, you will be prompted to specify a previous license to avoid reducing the validity period of the renewal license by 150 days. If in this step you select **I do not have a previous license**, the validity period of the new license will be reduced by 150 days.

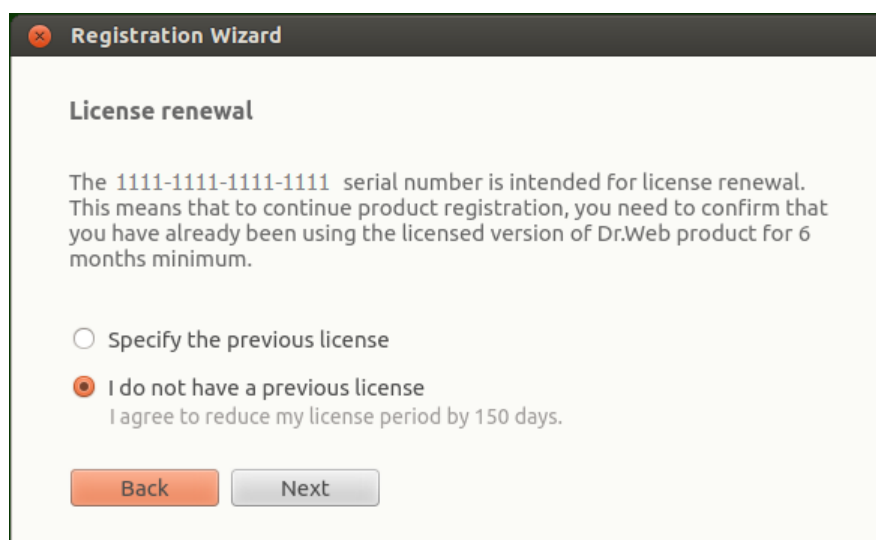


Figure 40. License renewal

If you have selected **Specify the previous license**, in the subsequent wizard page specify the previous license's serial number or its key file.



Registration Wizard

Specify the previous license

Serial number : 2222-2222-2222-2222

The license specified in this step will be blocked.
Do not specify a license that you plan to use later.

If validity period of the license is 6 or more months, you will
receive a bonus – validity period of new license will be extended
by 150 days.

Back Next

Figure 41. Specifying a previous license

If you specify a license which is not expired, the new license period will be extended by the remaining period of the previous license. If you activate a license with two serial numbers, the available bonus will depend on the option you specified in the previous step.

- **On two computers, and this computer is the first one.** To enable the bonus of 150 days for the first computer, specify the previous license issued for this computer (if any). *Do not specify the second serial number here.*
- **On two computers, and this computer is the second one.** To enable the bonus of 150 days for the second computer, specify the previous license issued for this computer (if any). *Do not specify the first serial number here.*
- **On one computer.** In this case, not only the duration of the purchased licensed is doubled, but also the license period is extended for 150 days. Moreover, if you specify the previous license issued for the second computer, the doubled period of the new license will be extended by another 150 days (and by the remaining period of the previous license).

To specify the previous license, you can either enter its serial number in the corresponding box or specify its key file. To do so, select a corresponding option in a combo box, which is placed on the left of the edit box. To specify the key file, do one of the following:

- Specify the file path in the entry filed
- Specify the file via the standard file chooser by clicking the **Browse** button.
- Drag and drop the file from the file manager window to the window of the Registration wizard



You can specify the zip archive containing the key file without unpacking it.

To continue the registration, click **Next**.

On the next step, specify registration data including the following:

- Registration name



- Your region (country), which is selected from the list
- Correct email address

All registration form fields are mandatory.

The image shows a 'Registration Wizard' dialog box with a title bar containing a close button and the text 'Registration Wizard'. The main content area is titled 'Last step' and contains the following text: 'To finish the activation, please enter the information on the license owner.' Below this text are three input fields: 'Registration name' with the placeholder 'User Name', 'Region' with a dropdown menu showing 'United States', and 'Email address' with the placeholder 'user@usermail.dom'. At the bottom of the dialog are two buttons: 'Back' and 'Finish'.

Figure 42. User information page

After all fields are filled in correctly, click the **Finish** button to establish a server connection and obtain a license key file. If necessary, you can use the license key file on another computer after you [remove](#) it from this computer.

2. Obtaining a Demo Period

If you would like to activate a demo period that provides full functionality of Dr.Web for Linux components for a period of 30 days, in the first step of activation click the link **Activate your 30-day demo period**.



When activating a demo period for 1 month, you do not need to provide your personal data. However, you can register on the official Doctor Web website and obtain a serial number for three month's demo period.

Another demo period for the same computer can be obtained after a certain time period. For details, refer to [Licensing](#).

3. Installation of a Key File Obtained Earlier

If you already have a valid license and the related key file (for example, obtained from Doctor Web or Doctor Web partners via email), you can activate Dr.Web for Linux by installing this key file. For that purpose, click **Other activation types** in the first step and specify the key file path in the displayed box.

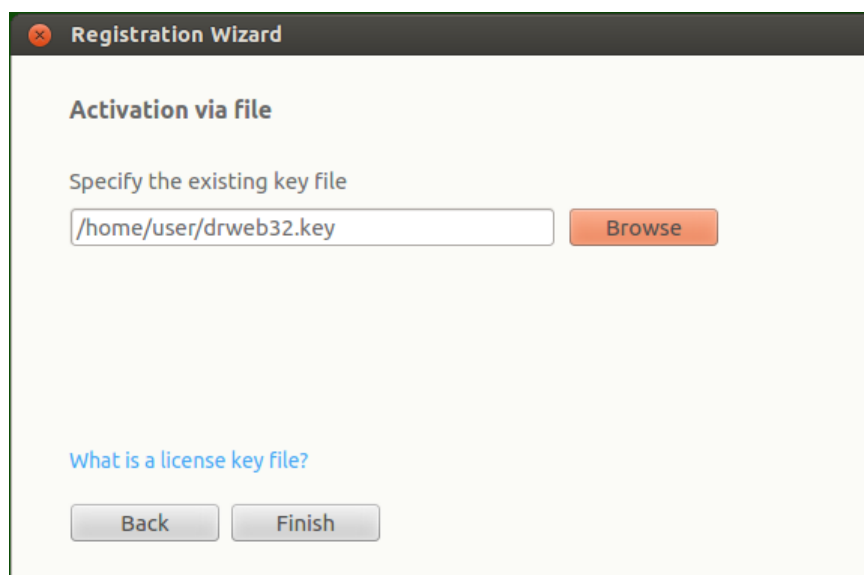


Figure 43. Activation via key file

To specify the key file, you may:

- Specify the file path in the entry field
- Specify the file via the standard file chooser by clicking the **Browse** button.
- Drag and drop the file from the file manager window to the window of the Registration wizard



You can specify the zip archive containing the key file without unpacking it.

After you specify the key file path (or the path to the archive containing the key file), click **Finish** to install the key file automatically. If required, the key file is automatically unpacked and copied to the directory with Dr.Web for Linux files. An Internet connection is not required.

After the activation procedure completes (regardless of the selected activation type), the final page of the wizard with the corresponding notification displays. Click **OK** to exit the wizard and open the [Main page](#) of the Dr.Web for Linux.



Figure 44. Successful activation notification

If an error occurs on any step of the procedure, a page with the corresponding notification and short error description is displayed. The figure below shows an example of such a page.



Figure 45. Error message

If an error occurs, you can return to the previous step and make corrections (for example, correct the serial number or specify the correct file path). To return to the previous step, click **Back**.

If the error is caused due to a temporary problem (for example, temporary network failure), you can attempt to retry the operation by clicking **Retry**. If necessary, you can click **Close** to cancel the registration and exit the wizard. In this case, you need to retry the registration procedure later. If the wizard cannot establish a connection to the Doctor Web registration server to verify the serial number, the following page is displayed.

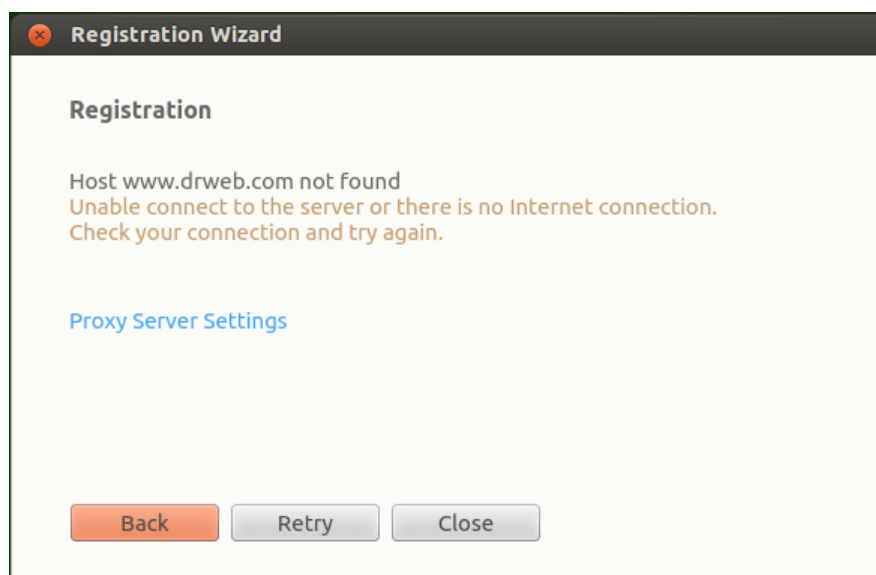


Figure 46. Registration server connection error

If the error has occurred because your computer cannot use a direct Internet connection, but you use a proxy server to access the Internet, click the link **Proxy Server Settings** to open the window containing proxy server settings:

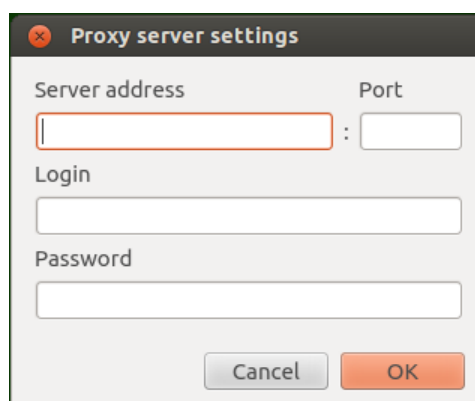



Figure 47. Proxy server settings

Specify the proxy server settings and click **OK**. After that click **Retry**.



Note that upon activation of a new license and generation of a new [key file](#), the previous key file, used by Dr.Web for Linux, is automatically saved as a backup copy to the `/etc/opt/drweb.com` directory. If required, you can use it again by [installing the key file](#).

Deleting License Key File

If necessary (for example, if you decided to use Dr.Web for Linux on another computer), you can delete an installed license key file that manages Dr.Web for Linux operation. For that purpose, open the page with [license information](#) (the start page of License manager) and click  next to the number of the current license.



After that, confirm deletion of the license key file in the appeared window by clicking **Yes**. If you want to cancel the deletion, click **No**.

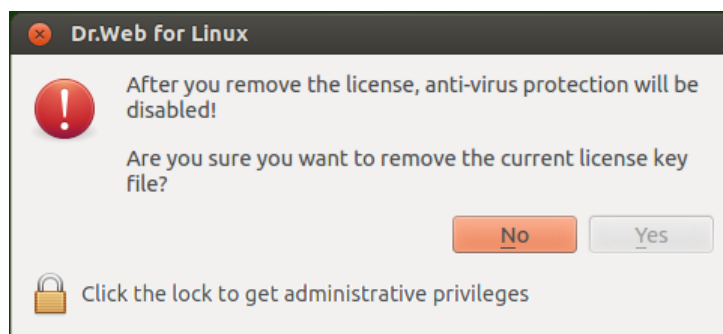


Figure 48. Confirmation dialog before deleting a license key file



To delete a license key file, the application must be started with superuser privileges. If the application does not have elevated permissions, the **Yes** button is unavailable on attempt to delete a key file. If required, you can [elevate the privileges](#) and, if the elevation succeeds, the **Yes** button becomes available.

Deletion of a license key file does not affect the license validity period. If the license is not expired, you can obtain a new key file for this license for the remaining period.

After a license key file is deleted, all anti-virus functions of Dr.Web for Linux ([file scanning](#), [updating](#) of databases and anti-virus engine, file system [monitoring](#)) are blocked until a new license or demo period is activated.

Managing Application Privileges

Some operations with Dr.Web for Linux can be performed in graphical mode only if the application has elevated privileges (*administrative privileges*) that correspond to the *superuser* (*root* user) permissions. Among such actions are the following:



1. [Management of objects](#) moved to the system quarantine (that is, to the non-user quarantine [directory](#))
2. [Check](#) of files and directories of other users (in particular, of superuser)
3. [Disabling](#) the file system monitor SpIDer Guard.
4. [Disabling](#) the network connection monitor SpIDer Gate.
5. [Removal](#) of a license key file, [connection and disconnection](#) from the central protection server



Even if the application is started by the superuser (for example, by using **su** or **sudo** commands), it is *not* granted elevated privileges by default.



All pages that provide for actions requiring elevated privileges contain a special button with a lock icon. The icon indicates whether or not the application has superuser privileges:

	Application does not have elevated privileges. Click the icon to elevate the privileges.
	Application has elevated privileges. Click the icon to lower the privileges; that is, to switch from administrative privileges to user rights.

Once you click the icon for privilege elevation, the user authentication window opens.

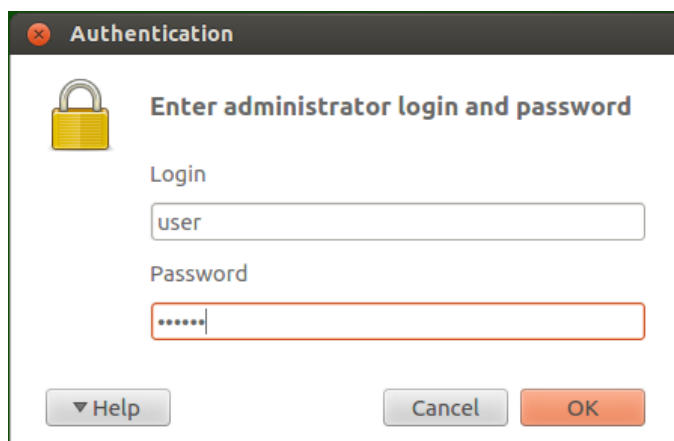


Figure 49. Authentication window

To grant the application administrative privileges, you need to authenticate as a user whose account is included in administrator group of Dr.Web for Linux, or as a superuser (system account *root*) and click **OK**. To cancel the privilege elevation, click **Cancel**. Clicking the **Help** button displays a short help text describing how to authenticate. To hide the text, click the Help button again.



During installation of Dr.Web for Linux, a group of users who can elevate their rights to superuser privileges (for example, *sudo* group) is selected as the group of administrators. If an attempt to find such a group fails, you can enter the superuser login and password (*root*) in the authentication window to elevate application rights.

Switching from administrative privileges to user rights does not require authentication.

Help and Reference



To access the Help file, click  on the [navigation pane](#).

Once you click the button, a pop-up menu with the following items appears:

- **Help**—opens the Dr.Web for Linux User manual.
- **Forum**—opens the webpage of the Doctor Web forum (requires a valid Internet connection).



- **Technical support**—opens the Doctor Web technical support webpage (requires a valid Internet connection).
- **My Doctor Web**—opens your personal webpage on the Doctor Web official website (requires a valid Internet connection).
- **About**—opens a window showing information about your version of Dr.Web for Linux.

Besides, when any page of the Dr.Web for Linux main window displays an error message, you can follow the **Details** link to get information on the error and instructions to resolve the problem.

Operation Settings

Configuration of application parameters, such as

- Update frequency
- Reactions of Dr.Web for Linux to threats detected during [scanning at request](#) by Scanner or detected by the file system monitor SpIDer Guard.
- The list of objects excluded from Scanner and SpIDer Guard checks
- Parameters of monitoring of network connections.
- Schedule of scans performed by Scanner
- Protection mode (Standalone, Central protection).
- Using Client of the Dr.Web Cloud service.

is performed in the Dr.Web for Linux settings window.




To open this window, click  on the [navigation bar](#).

In the settings window, the following pages are available:

- [Main](#)—allow to enable and configure notifications or frequency of automatic updates.
- [Scanner](#) allows to configure reaction of Dr.Web for Linux to threats detected by Scanner during scheduled scans or scans at request.
- [SpIDer Guard](#) allows to configure reaction of Dr.Web for Linux to threats detected by the file system monitor SpIDer Guard.
- [SpIDer Gate](#) allows to configure how SpIDer Gate controls network connections.
- [Exclusions](#), where you can configure the list of objects excluded from scans at request or scheduled scans, as well as from SpIDer Guard checks and SpIDer Gate monitoring.
- [Scheduler](#) allows to configure periodical scanning according to the specified schedule.
- [Network](#) allows to enable or disable protected connection check mode (based on SSL/TLS, such as HTTPS) for SpIDer Gate, to save a certificate of Dr.Web, which is used to intercept protected connections, to a file.
- [Mode](#) allows to select the [protection mode](#) (Standalone, Central protection) for operation of Dr.Web for Linux.
- [Dr.Web Cloud](#) allows or prohibits Dr.Web for Linux to use Dr.Web Cloud service.



To open the help file, click the  button on the corresponding page of the settings window.



All settings changed on these pages are applied immediately.

If Dr.Web for Linux operates in [enterprise mode](#), some settings can be blocked and unavailable for modifying.

Main Settings

On the **Main** tab, you can configure the main application settings.

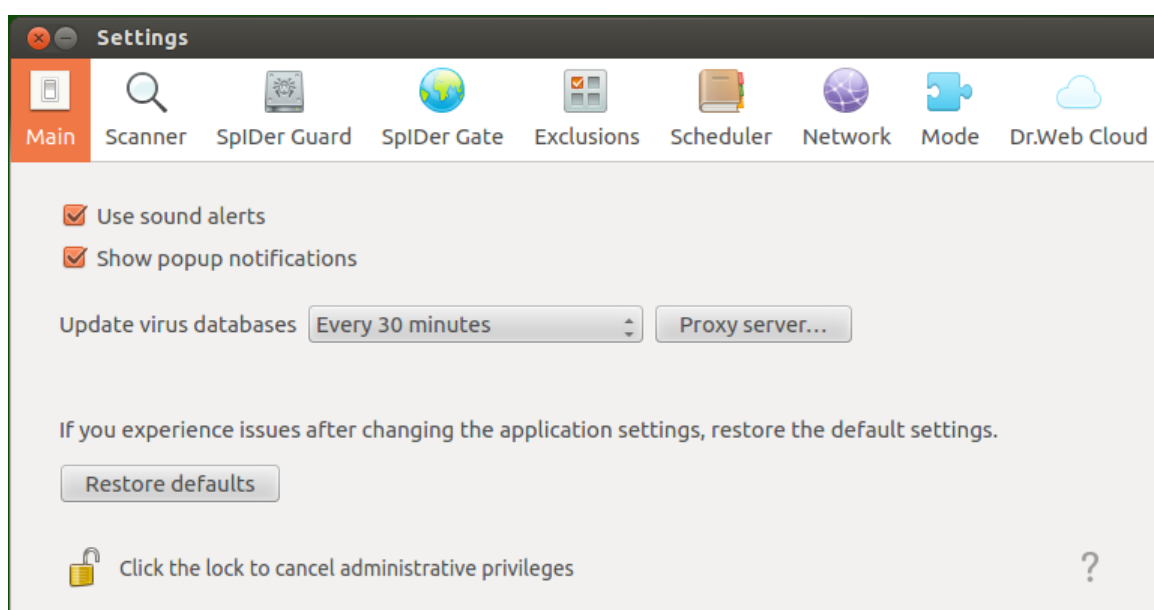


Figure 50. Main tab

Option	Action
Check box Use sound alerts	Select this check box if you want Dr.Web for Linux to use sound notifications on particular events, such as <ul style="list-style-type: none">• Detection of a threat (by both Scanner and SpIDer Guard)• Scan error• Others
Check box Show popup notifications	Select this check box if you want Dr.Web for Linux to show pop-up notifications on particular events, such as <ul style="list-style-type: none">• Threat detection• Scan error• Others



Option	Action
Drop-down list Download updates	Select the frequency at which availability of updates to virus and web resource categories databases and to Dr.Web for Linux anti-virus engine is checked by Updater.
Button Proxy server	Click to configure the proxy server settings for receiving updates (Updater uses a proxy server if contact to external servers is prevented by the network security policy).
Button Restore defaults	Click to restore default settings.

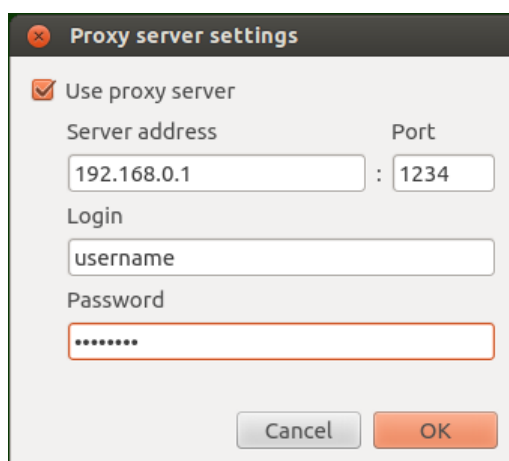


To manage update settings and restore defaults, the application must have root privileges. For details, refer to [Managing Application Privileges](#).

Configuring Proxy Server for Updates

In the window with settings that configure how Updater uses a proxy server, you can

- Enable or disable use of the proxy server for receiving updates.
- Specify address of the proxy sever used for receiving updates.
- Specify the port to connect to the proxy server.
- Specify the user name and password used for authentication on the proxy server.



The image shows a dialog box titled "Proxy server settings". It has a checkbox labeled "Use proxy server" which is checked. Below this, there are fields for "Server address" (containing "192.168.0.1") and "Port" (containing "1234"). There are also fields for "Login" (containing "username") and "Password" (containing "....."). At the bottom, there are "Cancel" and "OK" buttons.

Figure 51. Proxy server settings



As the server address, you can specify an IP address as well as FQDN of the host with the used proxy server. The server address and port are mandatory parameters. Because HTTP protocol is used for updating, an HTTP proxy server must be used. You must specify login and password only if the proxy server requires authorization for Internet access.



To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.

Scanner Settings

On the **Scanner** tab, you can configure reactions of Dr.Web for Linux to threats detected by Scanner during file scanning at user's [request](#) or as [scheduled](#).

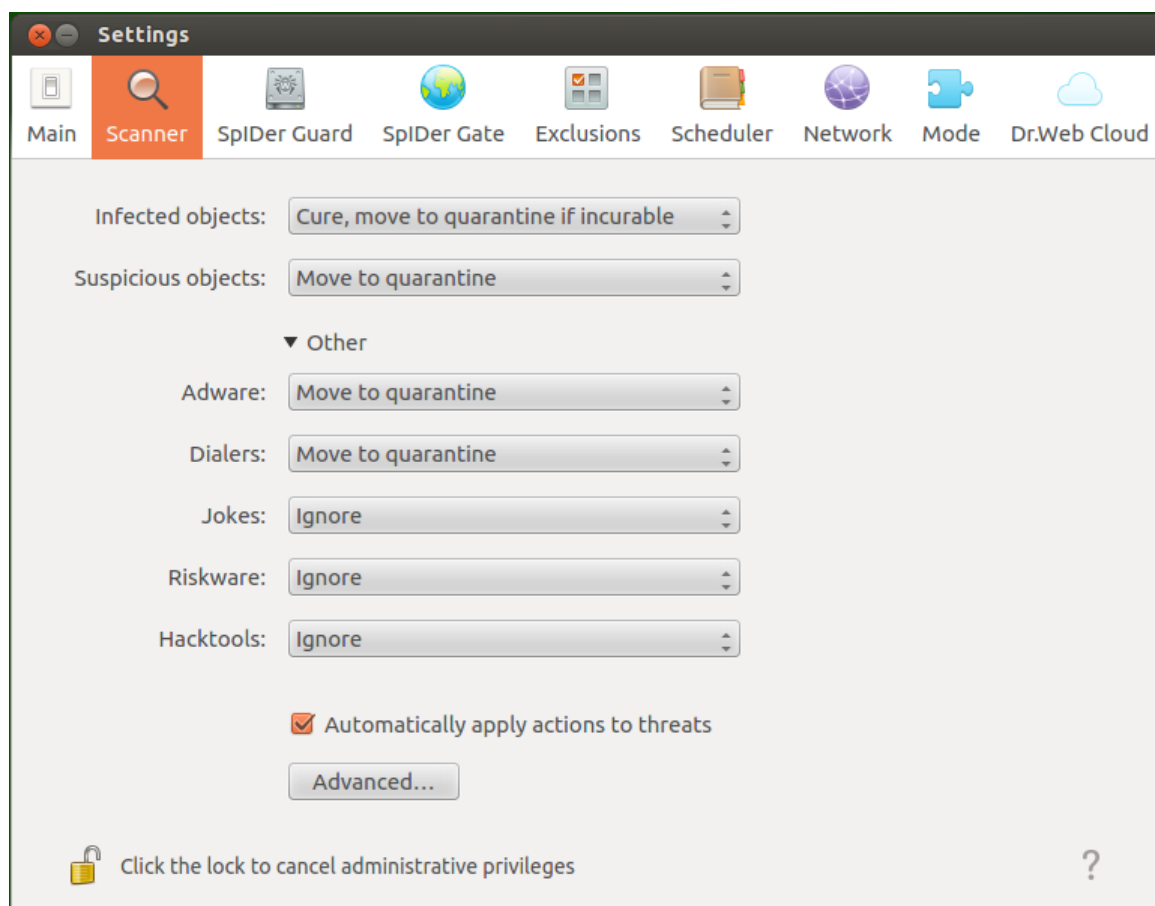


Figure 52. Scanner settings tab

On the drop-down lists, select the [action](#) to be applied by Dr.Web for Linux to an object if a threat of a [certain type](#) is detected in this object.



If threat is detected in a file located in a container (an archive, email message, etc.), its removal is replaced with moving of a container to quarantine.

By clicking the **Automatically apply actions to threats** check box, you instruct Dr.Web for Linux to apply the specified action to a threat once it is detected by Scanner during scanning at request or as scheduled (the user will be informed about threat neutralization and details on the threat will be available on the [threat list](#)). If the check box is cleared, a threat, detected by Scanner will be added to the list of detected threats and the user will need to manually select the action to be applied.



Click the **Advanced** button to open the window with advanced file scanning settings.

You can exclude files from scanning by Scanner on the **Exclusions** [tab](#).



Reactions on threat detection defined for Scanner, including them automatic applying, do not influence on behavior of SpIDer Guard. Reactions on threat detection for SpIDer Guard are specified on the [corresponding](#) tab.

To change Scanner reaction to threats and to access advanced settings, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

The option to configure Scanner when Dr.Web for Linux is operating under the [central protection](#) server can be blocked if disabled by the server.

Advanced Scanning Settings

In advanced scanning setting window, you can configure the following parameters of Scanner:

- Enable and disable scanning of containers:
 - Archives
 - Mail files
- Set a time limit for scanning of one file.

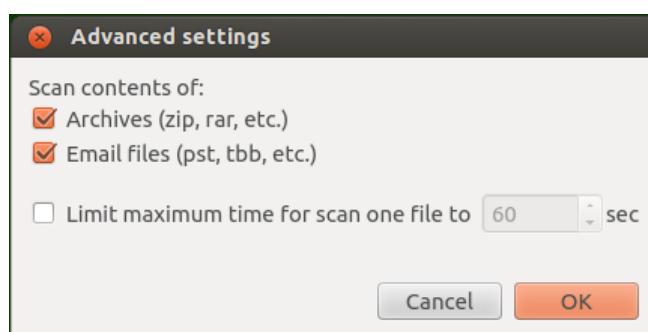


Figure 53. Advanced scanning settings



If the check boxes that turn on scanning of containers are not selected, the container file structure are scanned by Scanner anyway, but enclosed files are excluded from scanning.

To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.



File System Monitoring Settings

On the **SpIDer Guard** tab, you can configure reactions of Dr.Web for Linux to threats detected by the file system monitor SpIDer Guard.

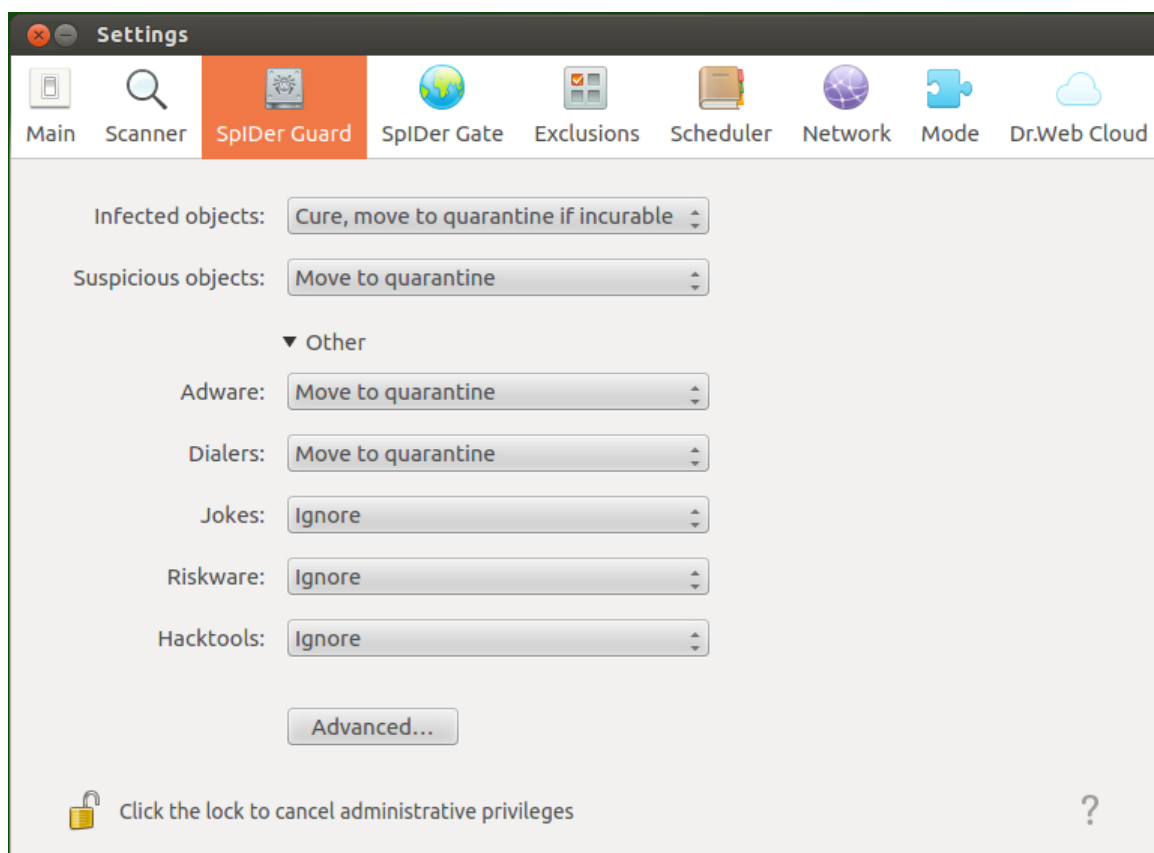


Figure 54. File system monitoring settings page

This page, including the window with advanced settings, is the same as the page with [Scanning settings](#) (**Scanner** tab).

You can exclude files from monitoring by SpIDer Guard on the **Exclusions** [tab](#).



If threat is detected in a file located in a container (an archive, email message, etc.), its removal is replaced with moving of a container to quarantine.

Reactions to threat detection defined for SpIDer Guard do not influence on behavior of Scanner. Reactions to threat detection for Scanner are specified on the [corresponding](#) page.

To change the settings of the SpIDer Guard file system monitor, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

The option to configure SpIDer Guard when Dr.Web for Linux is operating under the [central protection](#) server can be blocked if disabled by the server.

Monitoring Settings of Network Connections

On the **SpIDer Gate** tab, you can configure security policies used by SpIDer Gate upon an attempt to check sent and received mail and also to access the Internet.

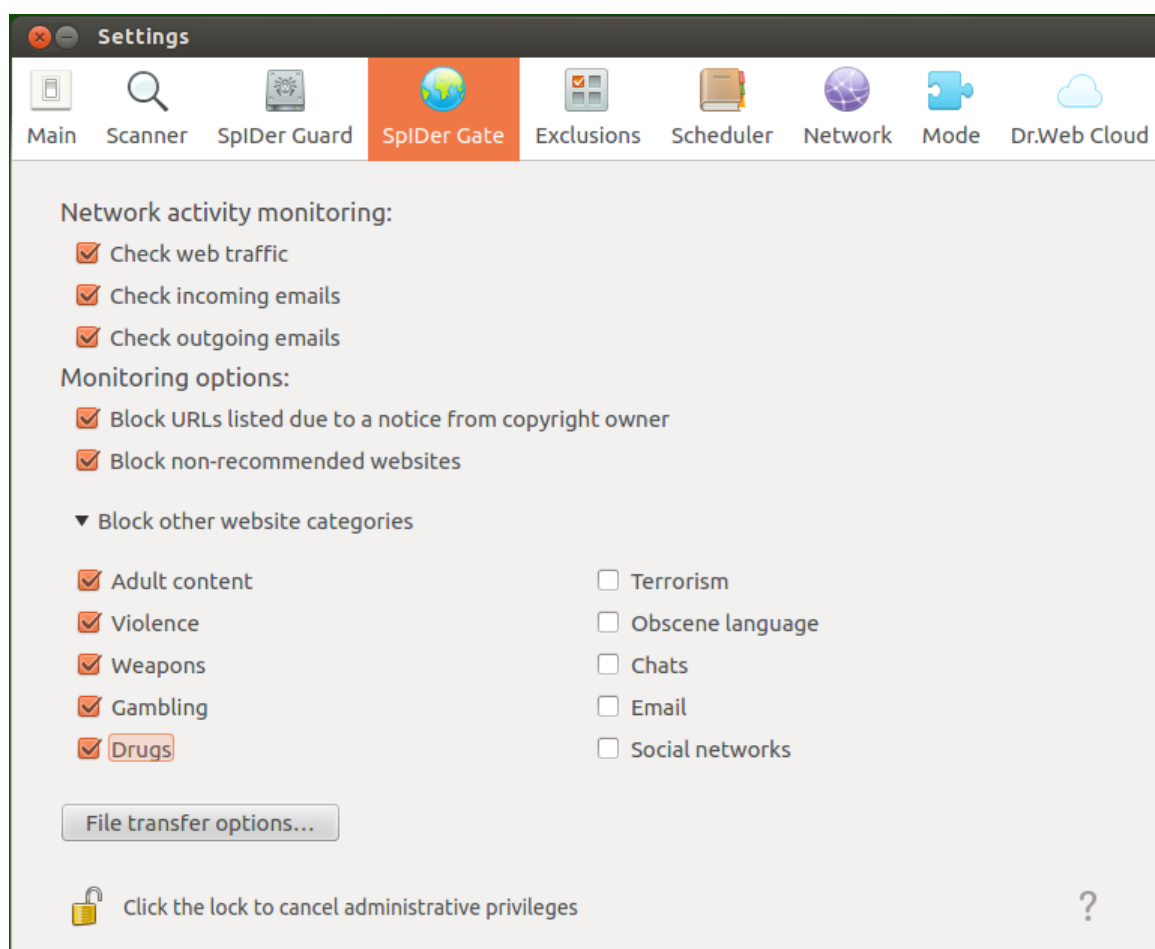


Figure 55. Internet access control settings



By selecting or clearing switches in the **Network activity monitoring** section, you can define the types of network activity that the monitor controls, if it is [enabled](#).

Switches in the **Monitoring options** section define website categories with restricted access (it applies not only to attempts to access such websites via browser but also to the blocking of email messages that contain links to such websites). By selecting or clearing switches, you can respectively allow or restrict access to websites of the following categories:

Category	Description
<i>URL added due to a notice from copyright owner</i>	Websites with content that infringes copyright (according to the copyright holder of this content). Among such websites are pirated sites, file reference directories, file hosting services, and others.
<i>Non-recommended sites</i>	Websites with unreliable content (suspected of phishing, password theft, and so on).
<i>Adult content</i>	Websites with adult content
<i>Violence</i>	Websites that contain violent material (for example, war scenes, acts of terrorism, and so on)
<i>Weapons</i>	Websites that contain information on weapons and explosives
<i>Gambling</i>	Internet casinos, gambling and bookmaking websites
<i>Drugs</i>	Websites that contain information on drug production, distribution, and use
<i>Obscene language</i>	Websites with obscene language
<i>Chats</i>	Chat websites
<i>Terrorism</i>	Websites that contain information about terrorism
<i>Email</i>	Websites that offer free email registration.
<i>Social networks</i>	Social networking websites



Database of web resource categories is provided with Dr.Web for Linux and is updated automatically upon virus database update. Users do not have permissions to edit the database.

The same web resource can fall into several categories. If so, SpIDer Gate blocks access to it if the URL is included at least in one of the selected categories. Click on the **Block other website categories** label allows to display either a compact or an extended version of the list of available categories.

If you need to block access to a website which does not fall into any of these categories, add it to the user black list. If, alternatively, you need to allow access to a website which is included in any



of the above mentioned categories and marked as unwanted, add it to the user white list. If necessary, you can also configure the list of applications which network connections will not be controlled by SpIDer Gate.

You can configure black and white lists of websites and applications excluded from SpIDer Gate monitoring on the **Exclusions** [tab](#).



As for a special website category *Websites known as infection sources*, access to these websites is always disabled even if they are added to the white list.

Managing File Scanning Parameters

To manage parameters that SpIDer Gate uses when checking files downloaded from the Internet or sent via email messages, click the **File transfer options** button.

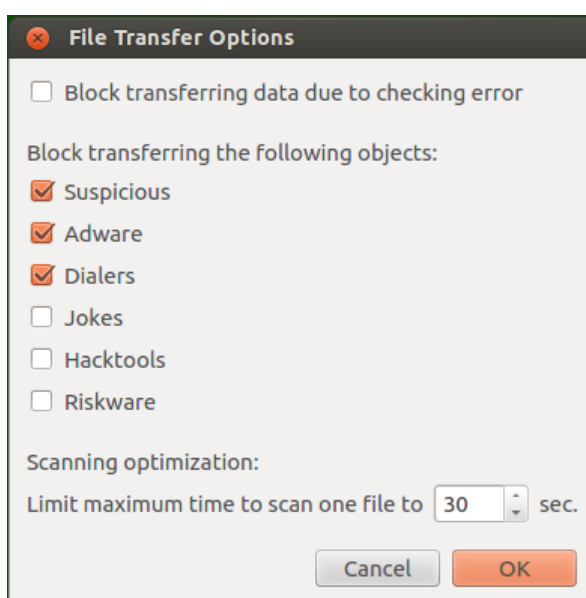


Figure 56. File check settings window

In the appeared window, you can specify the categories of malicious objects to be blocked on attempt to transmit them (including email message attachments). If a check box is selected, files that fall into the corresponding category are rejected on attempt to download them or transmit via email. If the check box is cleared, files that fall into this category are allowed for downloading. You can also set the maximum time to scan downloaded files (and email messages). If the **Block transferring data due to checking error** check box is selected, files and email messages that were not checked due to an error are blocked and cannot be downloaded. To allow downloading of such files and email messages, clear this check box (not recommended).



If scanning of a downloaded file or a transmitted email message failed because the interval for performing this operation expired, such file or message *will not* be treated as unchecked and will not be blocked even if the **Block transferring data due to checking error** check box is selected.



To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.



To change the SpIDer Gate settings, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

Configuring Exclusions

On the **Exclusions** page, you can see the following buttons for configuration of exclusions:

- **Files and directories**—opens the window where you can [specify paths](#) to file system objects that are excluded from checks of Scanner and the file system monitor SpIDer Guard.
- **Websites**—opens the window where you can manage [black and white lists](#) of websites, access to which is regulated regardless of policies applied by the SpIDer Guard network connection monitor.
- **Applications**—opens the window where you can [specify applications](#), whose network connections will not be controlled by the SpIDer Gate network connection monitor.

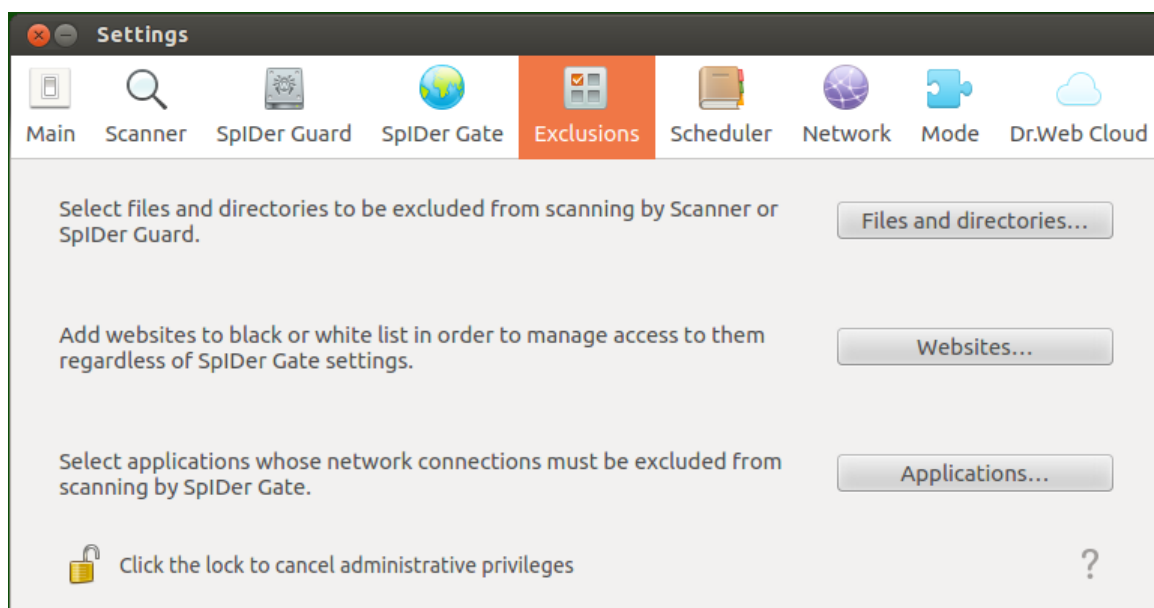


Figure 57. Exclusion configuration page



To add or remove objects from the exclusion list, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

Excluding Files and Directories

You can manage the list of files and folders to be excluded from scanning in the **Files and directories** window. To open it, click the **Files and directories** button on the **Exclusions** [tab](#).



In this window, you can list paths to objects that you want to exclude from scanning by Scanner at user [request](#) and/or as [scheduled](#) and from [monitoring](#) performed by SpIDer Guard.

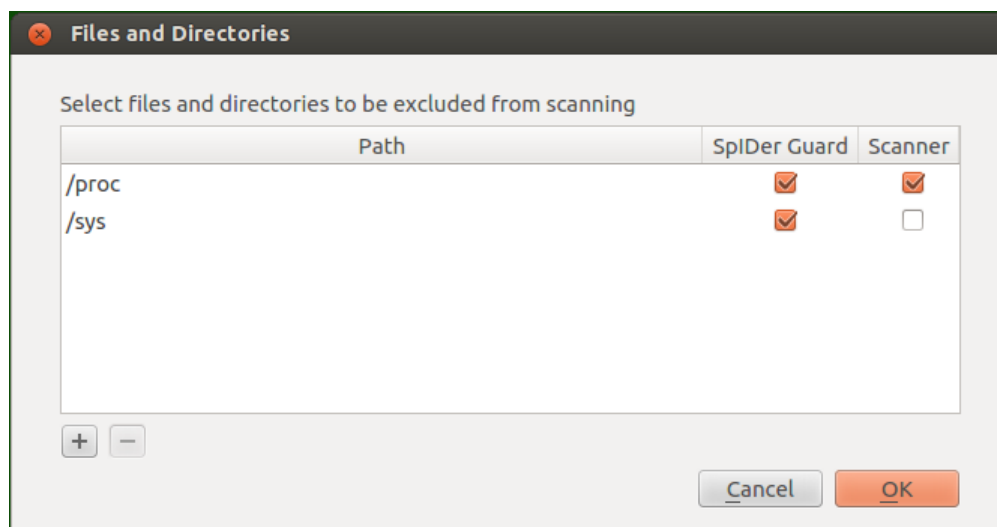


Figure 58. Configuring file and folder exclusions

The same object can be excluded from scanning by Scanner (at request or as scheduled) and from monitoring by the file system monitor SpIDer Guard. The check box in the corresponding column indicates what group of exclusions the object is added to.

Adding and Removing Objects From Exclusions

- To add an object to the group of exclusions for Scanner or for SpIDer Guard, select the corresponding check box in the row of the object. To remove it from the list, clear the corresponding check box.
- To add a new object to the list, click the **+** button below the list and select the required object in the appeared window. Moreover, you can add objects to this list by dragging them from the file manager window.
- To remove the object from the list, select the corresponding line in the text and click the **-** button below the list.

To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.

Exclusion of Applications

You can exclude application's network connections from monitoring by SpIDer Gate network connection monitor. To do it, open the **Applications** window by clicking the **Applications** button located on the **Exclusions** [tab](#).

This window allows you to list paths to the application executable files, which network connections should not be [controlled](#) by SpIDer Gate network connection monitor.

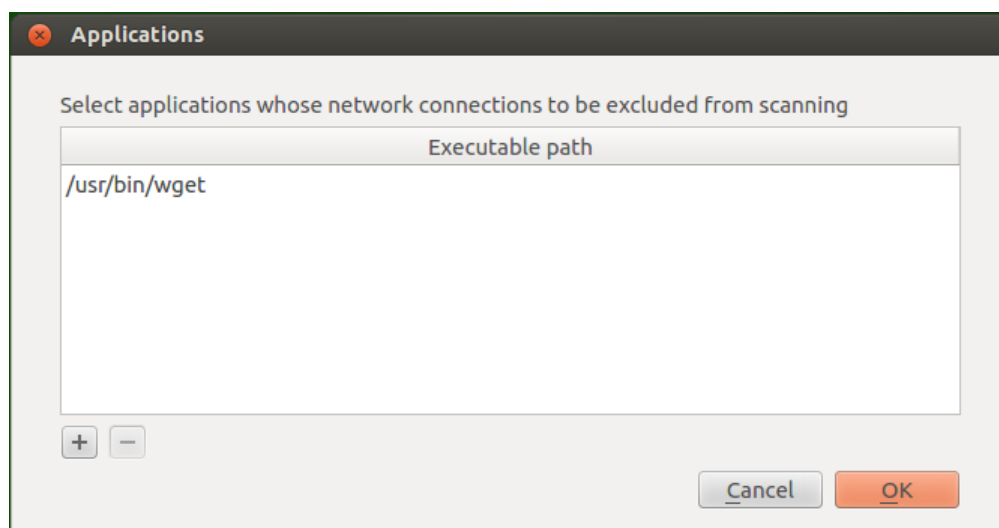


Figure 59. Configuring exclusions for network applications

Adding and Removing Applications From the List of Exclusions

- To add a new application to the list, click the **+** button below the list and select the application executable file in the appeared window. In addition, you can add applications to this list by dragging the executable files from the file manager window.
- To remove the application from the list, select the corresponding line in the text and click the **-** button below the list.

To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.

Black and white Lists of Websites

You can manage black and white lists of web sites in the **List Management** window. To open it, click the **Websites** button on the **Exclusions** [tab](#).

In this window you may list the websites, access to which will be always disabled or, on the contrary, always enabled by the SpIDer Gate network connection monitor.

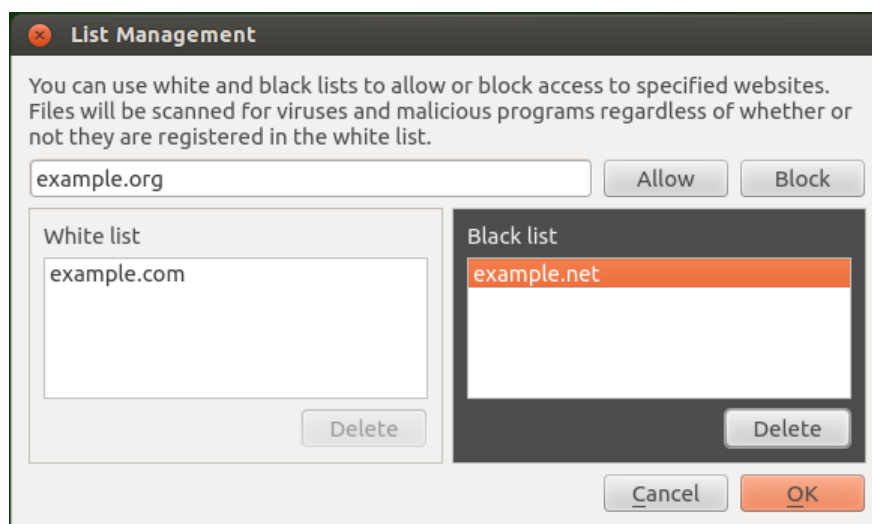


Figure 60. Black and white list management window



As for a special website category *Websites known as infection sources*, access to these websites is always disabled even if they are added to the white list.

Adding and Removing Websites From the Black and White Lists

- To add a website to the black or to the white list, type its domain in the edit box and click the respective button.
 - By clicking the **Allow** button, you add the required address to the *white* list.
 - By clicking the **Block** button, you add the required address to the *black* list.
- Adding a domain address to the white or to the black list allows or, respectively, denies access to all resources within the domain.
- To remove the website from white or black list, select it on the list and click the **Delete** button.

To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.

Scheduler Settings

On the **Scheduler** tab, you can enable an option to scan objects automatically according to the schedule as well as specify this schedule and select the type.

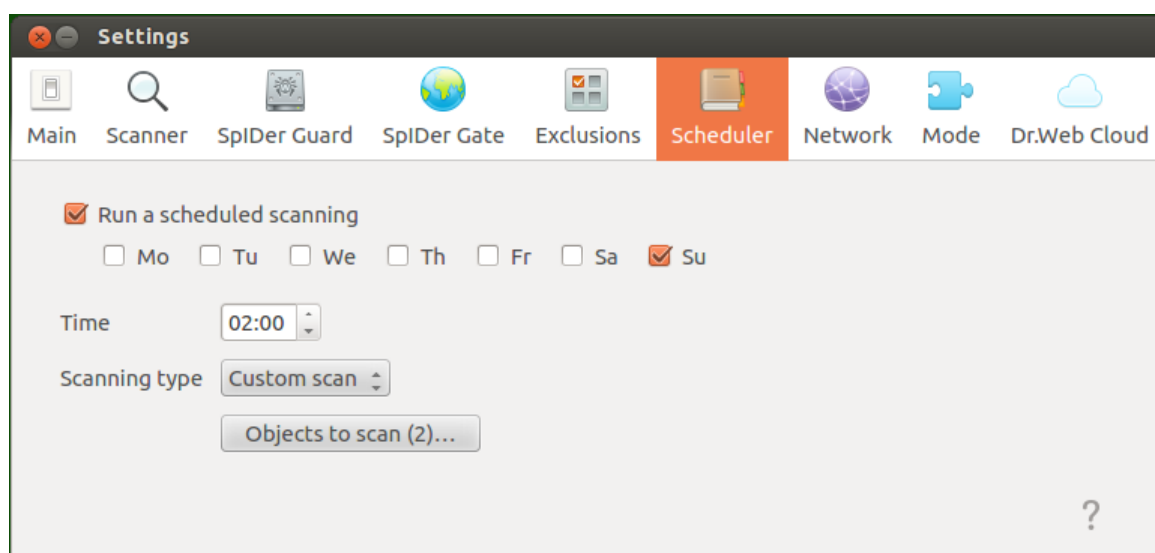


Figure 61. Schedule configuration page

To enable automatic scheduled scans, select the **Run a scheduled scanning** check box. In this case, Dr.Web for Linux generates a schedule to periodically start certain type o scanning.



The scheduled scanning will start at the specified intervals by the notification agent or directly by the graphical management interface if it is launched when the scanning starts. Scheduled scanning is not launched if Dr.Web for Linux operates under control of the [central protection](#) server, or if an active [license](#) is not available.

Scanning started according to the schedule as well as scanning [on demand](#) is configured with the settings specified on the **Scanner** [tab](#).

Scheduler Settings

If scheduled scanning is enabled, you can configure the following parameters:

- Days of week when scanning is to be started (by selecting the corresponding check boxes)
- Time (hours and minutes) when scanning is to be started
- Indicate the [scanning type](#) (*Express scan*, *Full scan*, or *Custom scan*).
- If you select *Custom scan*, you should also specify the list of objects for scanning. For that purpose, click the **Objects to scan** button (number of objects for scanning is indicated within the brackets).

After that, select the necessary object in the appeared window which is similar to the [file chooser](#) for custom scanning on demand. You can add objects to the list either by clicking the [+](#) button or by dragging and dropping them from the File manager window.

To disable scheduled scanning, clear the **Run a scheduled scanning** check box. The respective task for the notification agent will be automatically removed.



Preventing Threats Distributing over Network

On the **Network** tab, you can enable the network connection monitor SpIDer Gate to check traffic transmitted via secure connections that use SSL- and TLS-based protocols.

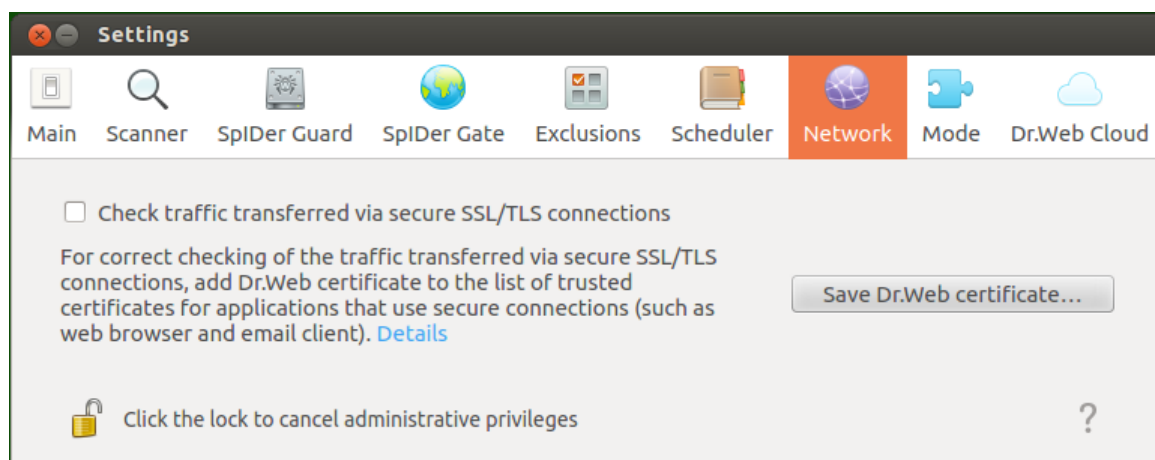


Figure 62. Secure connections checking configuration tab

Configuring Check of Protected Connections

To allow SpIDer Gate scan traffic sent via protected network connections that use SSL and TLS protocols, select the **Check traffic transferred via secure SSL/TLS connections** check box. To disable checks of protected traffic, clear the check box.



To manage the check of protected traffic, the application must operate with elevated permissions. Refer to [Managing Application Privileges](#) section.

If a mail client runs in the system (such mail client as **Mozilla Thunderbird**) that uses the IMAP protocol to receive email messages, it is necessary to restart it after the mode **Check traffic transferred via secure SSL/TLS connections** is enabled.

To ensure correct check of the traffic, transmitted via protected network connections, export the special Dr.Web certificate to a file and then manually add it to the list of trusted application certificates that use protected connections. Such applications are primarily web browsers and mail clients. Otherwise, if Dr.Web certificate is not added to the trusted list, data will be displayed incorrectly if received from the website accessible via HTTPS (for example, from online banking websites, web interfaces of mail servers). If the certificate of Dr.Web is not added to the trusted certificate list of the mail client, authorization on mail servers that use protected protocols (such as SMTPS) for data transfer will fail.

To export Dr.Web certificate to the file, click the **Save Dr.Web certificate** button and in the appeared window specify where to save the file. Its default name is `SpIDer Gate Trusted Root Certificate.pem`, but you can change it if required.



Then the saved file of the Dr.Web certificate is manually added to the trusted certificate lists of those applications which fail when trying to establish protected connections. You need to add the certificate only once for an application. If you clear and then select the **Check traffic transferred via secure SSL/TLS connections** check box again on the **Network** setting page, you will not need to save Dr.Web certificate once again and add it to the list of trusted certificates.

To Add Dr.Web Certificate to the Trusted Certificate List

Mozilla Firefox browser

- 1) Select **Preferences** item of main menu and then (on the appeared settings page) select **Advanced**. Another page opens, where you need to select **Certificates**.
- 2) Click the **View Certificates** button. In the appeared window, open the **Authorities** tab and click **Import**.
- 3) In the appeared window, specify the path to the Dr.Web certificate (by default, its file name is `SpIDer Gate Trusted Root Certificate.pem`) and click **Open**.
- 4) In the appeared window use the check boxes to specify the required trust level to the certificate. It is recommended to select all three check boxes (for identification of websites, identification of email users, and for identification of software). After that, click **OK**.
- 5) In the trusted certificate list, a new section, *DrWeb* will appear. This section contains the added certificate (*SpIDer Gate Trusted Root Certificate* by default).
- 6) Close the window with the list of certificates by clicking **OK** and then close the page with browser settings (by closing the corresponding tab on the browser tab bar).

Mozilla Thunderbird mail client

- 1) Select **Preferences** item of main menu and then in the settings window click **Advanced**. In the appeared page, select **Certificates**.
- 2) Click the **View Certificates** button. In the appeared window, open the **Authorities** tab and click **Import**.
- 3) In the appeared window, specify the path to the Dr.Web certificate (by default, its file name is `SpIDer Gate Trusted Root Certificate.pem`) and click **Open**.
- 4) In the appeared window use the check boxes to specify the required trust level to the certificate. It is recommended to select all three check boxes (for identification of websites, identification of email users, and for identification of software). After that, click **OK**.
- 5) In the trusted certificate list, a new section, *DrWeb* will appear. This section contains the added certificate (*SpIDer Gate Trusted Root Certificate* by default).
- 6) Close the window with the list of certificates by clicking **OK** and then close the page with mail client settings by clicking **Close**.
- 7) Restart the mail client.



Mode Settings

On the **Mode** tab, you can connect Dr.Web for Linux to the central protection server (by enabling Central protection [mode](#)) as well as disconnect from the central protection server (if so, Dr.Web for Linux is operating in Standalone mode).

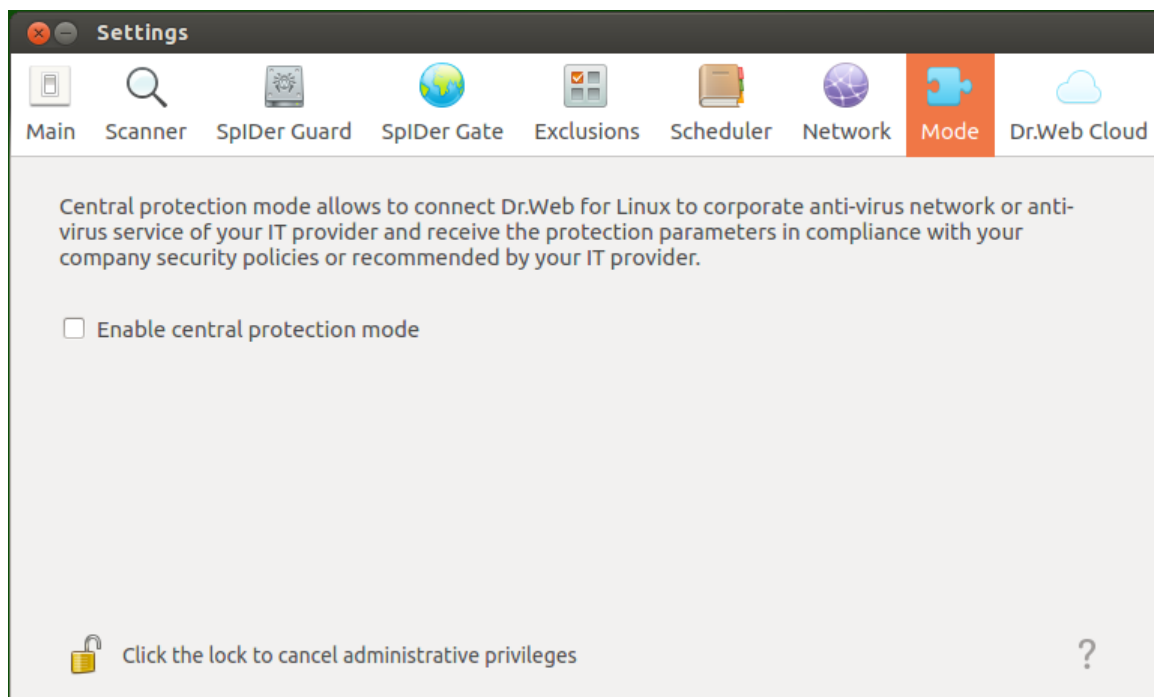


Figure 63. Mode tab

To connect Dr.Web for Linux to the central protection server or disconnect from that, use the corresponding check box.



To connect Dr.Web for Linux to the central protection server or disconnect from it, the application must have elevated privileges. Refer to [Managing Application Privileges](#).

Connecting to an Anti-Virus Network

On attempt to establish connection to the central protection server, a window with connection parameters appears.

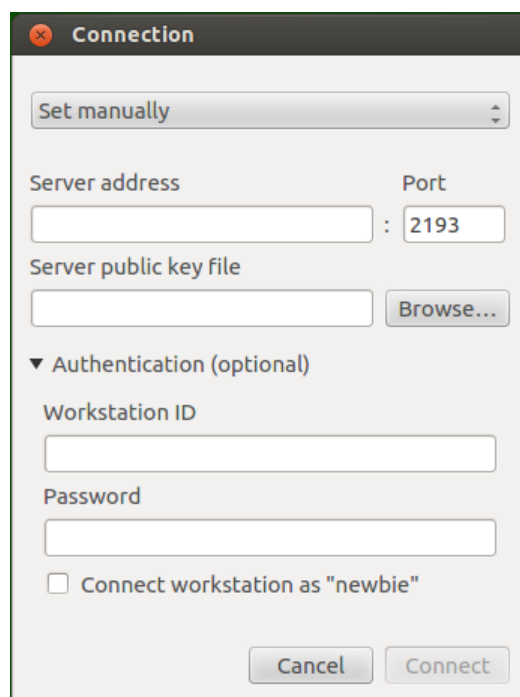


Figure 64. Connection to the central protection server

In the drop-down list located at the top of the window chose one of the methods for connecting to a central protection server. Three methods are available:

- *Load from file.*
- *Set manually.*
- *Detect automatically.*

If you select the *Load from file* item, specify the path to the connection settings file in the corresponding box. The file is provided by the anti-virus network administrator. If you select *Set manually* item, specify the address and the port of the central protection server. For *Set manually* or *Detect automatically* items, you can also specify the path to the public key file (provided by your network administrator or Internet service provider).

Additionally, in the **Authentication** section you can specify your login (workstation identifier) and password for authentication on the central protection server, if you know them. If these fields are filled in, then your connection to the central protection server will succeed only if a correct identifier/password pair was entered. If you leave these fields empty, connection to the central protection server is established only if it is approved by the central protection server (either automatically or by the anti-virus network administrator, depending on the server settings).

Moreover, you can use the **Connect workstation as "newbie"** option (to connect as a new user). If the option is allowed on the central protection server and after approving the connection, the server automatically generates a unique identifier/password pair, which is then used for connecting your computer to the server. Note that, in this mode, the central protection server generates a new account for the host even if this host has a previously created account on the server.



Connection parameters must be specified in strict accordance with the instructions provided by the administrator of your anti-virus network or service provider.

To connect to the server, specify all of the parameters, click **Connect** and wait for connection to be established. To close the window without establishing a server connection, click **Cancel**.



After you connected Dr.Web for Linux to the central protection server, the program is administered by the server until the operation mode is switched to Standalone. In Central protection mode, a server connection is automatically established on every operating system startup. For details, refer to [Operation Modes](#).

Note that if launch of scanning on demand is prohibited on the used central protection server, the [page for starting scanning](#) and **Scanner** button of the Dr.Web for Linux window will be disabled. Moreover, in this case Scanner will not launch scheduled scans.

Configuring Dr.Web Cloud

On the **Dr.Web Cloud** tab, you can allow or prohibit Dr.Web for Linux to use Dr.Web Cloud service.

Dr.Web Cloud provides most recent information on threats which is updated on Doctor Web servers in real-time mode and used for anti-virus protection. Depending on [update settings](#), information on threats used by anti-virus components may become out of date. Using of Dr.Web Cloud can reliably prevent users from viewing unwanted websites and protect your system from infected files.

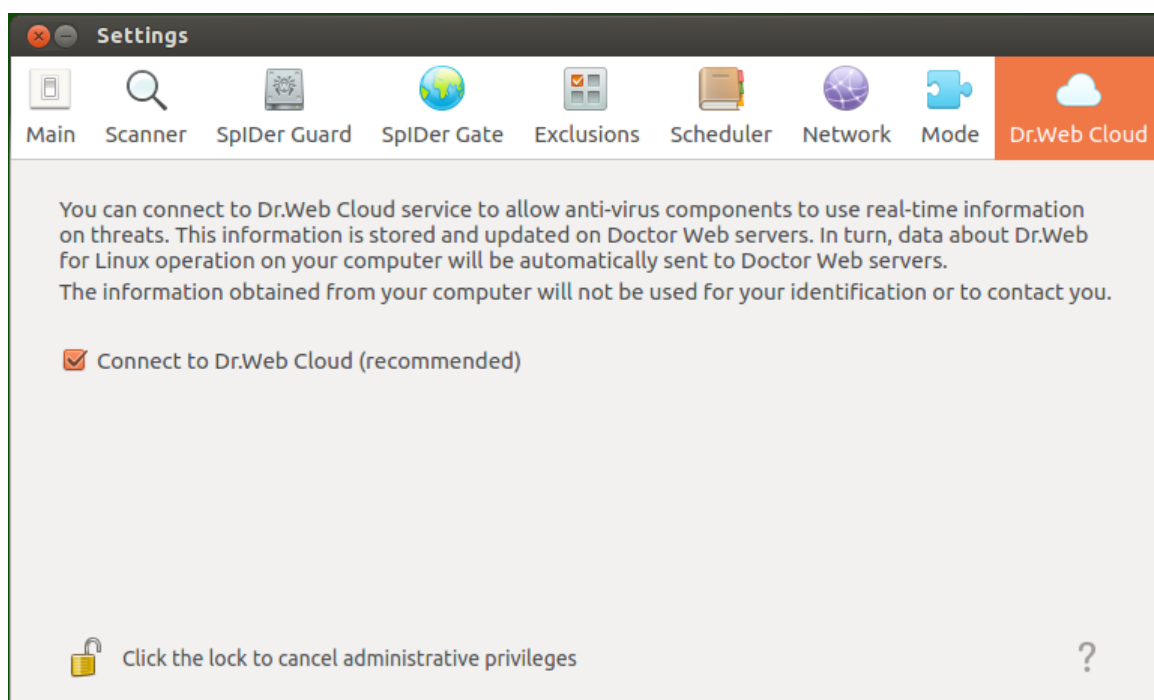


Figure 65. Dr.Web Cloud tab



To allow or prohibit Dr.Web for Linux to use Dr.Web Cloud service, select the corresponding check box.



For interaction with Dr.Web Cloud service, it is necessary to have an active Internet connection.

To allow or prohibit Dr.Web for Linux using of Dr.Web Cloud, the application must have elevated privileges. Refer to [Managing Application Privileges](#).

Additional Information

Command Line Parameters

To start Dr.Web for Linux graphical management interface from the command line, the following command is used:

```
$ drweb-gui [<path>[ <path> ...] | <parameters>]
```

where *<path>* is the path to be scanned. You can specify several paths to scan, delimited by whitespaces.

You can also specify the following parameters (*<parameters>*):

- `--help (-h)`—Show information about supported command-line parameters and terminate operation of the graphical management interface.
- `--version (-v)`—Show information on the graphical management interface version and terminate the operation.
- `--Autonomous (-a)`—Run the [autonomous copy](#) of the Dr.Web for Linux graphical management interface.
- `--FullScan`—Start the full scan task upon Dr.Web for Linux graphical management interface startup.
- `--ExpressScan`—Start the express scan task upon Dr.Web for Linux graphical management interface startup.
- `--CustomScan`—Start the custom scan task upon Dr.Web for Linux graphical management interface startup (page for selection of objects to scan will open).

Example:

```
$ drweb-gui /home/user/
```

This command instructs Dr.Web for Linux graphical management interface to run and then Scanner starts scanning the files in the specified directory (the corresponding task will be appear in the [list of current scans](#)).



Starting the Autonomous Copy

Dr.Web for Linux supports running in a special mode—as an *autonomous copy*.

If the Graphical management interface of Dr.Web for Linux is [run](#) as autonomous copy, then it will work with a separate set of service components (background working *configuration daemon* of Dr.Web for Linux (**drweb-configd**), Scanner and Scanning engine), run for supporting the running instance of the software.

Features of the Dr.Web for Linux graphical management interface run as an autonomous copy:

- To run Graphical management interface of Dr.Web for Linux as an autonomous copy, you will need a valid [key file](#), working in [Central protection](#) mode is not supported (an option to [install](#) the key file, exported from central protection server, is available). In this case, even if Dr.Web for Linux is connected to the central protection server, the autonomous copy *does not notify* the central protection server of the threats detected in the autonomous copy mode.
- All additional components, that are run to serve the work of the autonomous copy of the Graphical management interface, will be launched as the current user and will work with a configuration file, separately generated for this session.
- All the used temporary files and UNIX sockets are created only in the directory with an unique name, which is created when the autonomous copy is launched. The unique temporary directory is created in the system directory for temporary files (path to this directory is available in the `TMPDIR` environment variable).
- The autonomous copy of the Graphical management interface *does not launch* SpIDer Guard and SpIDer Gate monitors, only [files checking](#) and [quarantine management](#) functions, supported by Scanner, are available.
- All the required paths (to virus databases, anti-virus engine and executable files of the service components) are defined by default or retrieved from the special environment variables.
- The number of simultaneously running autonomous copies of the Graphical management interface is unlimited.
- When the autonomous copy of the Graphical management interface is shut down, the set of servicing components is also terminated.

Working from Command Line

You can manage operation of Dr.Web for Linux from the command line with the help of a special command-line tool—**drweb-ctl**.

You can do the following actions from the command line:

- Start scanning file system objects including boot records
- Launch of scanning of files on remote network hosts (see note [below](#)).
- Start updating virus databases
- View and change parameters of Dr.Web for Linux configuration



- View the status of the product's components and statistics on detected threats
- View quarantine and manage quarantined objects
- Connect to the central protection server or disconnect from it

User [commands](#) for Dr.Web for Linux management can have an effect only if Dr.Web for Linux service components are running (by default, they are automatically run on system startup).



Note that some control commands require superuser privileges. To elevate privileges, use the **su** command (change the current user) or the **sudo** command (execute the specified command with other user privileges).

The **drweb-ctl** tool supports auto-completion of commands for managing Dr.Web for Linux operation if this option is enabled in the used command shell. If the command shell does not allow auto-completion, you can configure this option. For that purpose, refer to the instruction manual for the used OS distribution.



When shutting down, the tool returns the exit code according to convention for the POSIX compliant systems: 0 (zero)—if an operation is successfully completed, non-zero—if otherwise.

Note that the tool returns a non-null exit code only in case of internal error (for example, the tool could not connect to a component, a requested operation could not be executed, etc.). If the tool detects (and possibly) neutralizes a threat, it returns the null exit code, because the requested operation (such as `scan`, etc.) is successfully completed. If it is necessary to define the list of detected threats and applied actions, analyze the messages displayed on the console.

Remote host scanning

Dr.Web for Linux allows to perform scanning for threats of files located on remote network hosts. Such hosts can be not only full computing machines (workstations and servers) but also routers, set-top boxes and other “smart” devices that form the so-called Internet of things. To perform the remote scanning, it is necessary for the remote host to provide a remote terminal access via SSH (Secure Shell). Besides, it is required to know an IP address and a domain name of the remote host, name and password of the user, who could remotely access the system via SSH. The indicated user must have access rights to the scanned files (at least the reading rights).

This function can be used only for detection of malicious and suspicious files on a remote host. Elimination of threats (i.e. isolation in the quarantine, removal and curing of malicious objects) using means of the remote scanning is impossible. To eliminate detected threats on the remote host, it is necessary to use administration tools provided directly by this host. For example, for routers and other “smart” devices, a mechanism for a firmware update can be used; for computing machines, it can be done via a connection to them (as an option, using a remote terminal mode) and respective operations in their file system (removal or moving of files, etc.), or via running an anti-virus software installed on them.



Remote scanning is performed only via the command-line tool **drweb-ctl** (the `remotescan` [command](#) is used).

Call Format

1. Command Format for Calling the Command-Line Utility to Manage the Product

The call format for the command-line tool which manages Dr.Web for Linux operation is as follows:

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

Where:

- *<general options>*—options that can be applied on startup when the command is not specified or can be applied for any command. Not mandatory for startup.
- *<command>*—command to be performed by Dr.Web for Linux (for example, start scanning, output the list of quarantined objects, and other commands).
- *<argument>*—command argument. Depends on the specified command. It can be missing for certain commands.
- *<command options>*—options for managing the operation of the specified command. They can be omitted for some commands.

2. General Options

The following general options are available:

Option	Description
-h, --help	Show general help information and exit. To display the help information on any command, use the following call: <pre>\$ drweb-ctl <i><command></i> -h</pre>
-v, --version	Show information on the module version and exit
-d, --debug	Instructs to show debug information upon execution of the specified command. It cannot be executed if a command is not specified. Use the call <pre>\$ drweb-ctl <i><command></i> -d</pre>




3. Commands

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

- Anti-virus scanning commands.
- Commands to manage updates and operation in Central protection mode
- Configuration management commands.
- Commands to manage detected threats and quarantine.
- Information commands.

3.1. Anti-virus Scanning Commands


The following commands to manage anti-virus scanning are available:

Command	Description
<code>scan <path></code>	<p>Purpose: Start checking the specified file or directory with the Scanner.</p> <p>Arguments:</p> <p><code><path></code>—path to the file or directory which is selected to be scanned.</p> <p><i>This argument may be omitted, if you use the <code>--stdin</code> or the <code>--stdin0</code> option. To specify several files that satisfy a certain criterion, use the find utility (see the Usage Examples) and the <code>--stdin</code> or <code>--stdin0</code> option.</i></p> <p>Options:</p> <p><code>-a [--Autonomous]</code>—run a specified scanning by a separate instance of Scanning Engine and the Scanner, then terminate their operation after the scanning task is completed. Note that threats detected during an autonomous scanning are not displayed in the common threat list that is displayed using the <code>threats</code> command (see below).</p> <p><code>--stdin</code>—get the list of paths to scan from the standard input string (<i>stdin</i>). Paths in the list need to be separated by the next line character (<code>'\n'</code>).</p> <p><code>--stdin0</code>—get the list of paths to scan from the standard input string (<i>stdin</i>). Paths in the list need to be separated by the zero character NUL (<code>'\0'</code>).</p> <div> When using <code>--stdin</code> and <code>--stdin0</code> options, the paths in the list should not contain patterns or regular expressions for a search. Recommended usage of the <code>--stdin</code> and <code>--stdin0</code> options is processing a path list (generated by an external utility, for example, <code>find</code>) in the scan command (see Usage Examples).</div>



Command	Description
	<p><code>--Report <BRIEF DEBUG></code>—specify the type of the report with scanning results.</p> <p>Allowed values:</p> <ul style="list-style-type: none">• BRIEF—brief report.• DEBUG—detailed report. <p>Default value: <i>BRIEF</i></p> <p><code>--ScanTimeout <number></code>—specify timeout to scan one file, in ms.</p> <p>If the value is set to <i>0</i>, time on scanning is not limited.</p> <p>Default value: <i>0</i></p> <p><code>--PackerMaxLevel <number></code>—set the maximum nesting level when scanning packed objects.</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--ArchiveMaxLevel <number></code>—set the maximum nesting level when scanning archives (zip, rar, etc.).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--MailMaxLevel <number></code>—set the maximum nesting level when scanning email messages (pst, tbb, etc.).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--ContainerMaxLevel <number></code>—set the maximum nesting level when scanning other containers (HTML and so on).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--MaxCompressionRatio <ratio></code>—set the maximum compression ratio of scanned objects.</p> <p>The ratio must be at least equal to 2.</p> <p>Default value: <i>3000</i></p> <p><code>--HeuristicAnalysis <On Off></code>—enable or disable heuristic analysis during the scanning.</p> <p>Default value: <i>On</i></p> <p><code>--OnKnownVirus <action></code>—action applied to a threat detected by using signature-based analysis.</p> <p>Allowed values: <i>REPORT, CURE, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnIncurable <action></code>—action applied on failure to cure a detected threat or if a threat is incurable.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p>



Command	Description
	<p>Default value: <i>REPORT</i></p> <p><code>--OnSuspicious <action></code>—action applied to a suspicious object detected by heuristic analysis.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnAdware <action></code>—action applied to detected adware programs.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnDialers <action></code>—action applied to dialers.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnJokes <action></code>—action applied to joke programs.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnRiskware <action></code>—action applied to potentially dangerous programs (riskware).</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <p><code>--OnHacktools <action></code>—action applied to hacktools.</p> <p>Allowed values: <i>REPORT, QUARANTINE, DELETE.</i></p> <p>Default value: <i>REPORT</i></p> <div> If threat is detected in a file located in a container (an archive, email message, etc.), its removal (<i>DELETE</i>) is replaced with moving of a container to quarantine (<i>QUARANTINE</i>).</div>
<code>bootscan</code> <code><disk drive> ALL</code>	<p>Purpose: Run checking boot records on the specified disks by the Scanner. Both MBR and VBR records are scanned.</p> <p>Arguments:</p> <p><code><disk drive></code>—path to the block file of a disk device whose boot record you want to scan. You can specify several disk devices separated by spaces. The argument is mandatory. If <code>ALL</code> is specified instead of the device file, all boot records on all available disk devices will be checked.</p> <p>Options:</p> <p><code>-a [--Autonomous]</code>—run a specified scanning by a separate instance of Scanning Engine and the Scanner, then terminate their operation after the scanning task is completed. Note that threats detected during an</p>




Command	Description
	<p>autonomous scanning are not displayed in the common threat list that is displayed using the <code>threats</code> command (see below).</p> <p><code>--Report <BRIEF DEBUG></code>—specify the type of the report with scanning results.</p> <p>Allowed values:</p> <ul style="list-style-type: none">• <i>BRIEF</i>—brief report.• <i>DEBUG</i>—detailed report. <p>Default value: <i>BRIEF</i></p> <p><code>--ScanTimeout <number></code>—specify timeout to scan one file, in ms.</p> <p>If the value is set to <i>0</i>, time on scanning is not limited.</p> <p>Default value: <i>0</i></p> <p><code>--HeuristicAnalysis <On Off></code>—enable or disable heuristic analysis during the scanning.</p> <p>Default value: <i>On</i></p> <p><code>--Cure <Yes No></code>—enable or disable attempts to cure detected threats.</p> <p>If the value is set to <i>No</i>, only a notification about a detected threat is displayed.</p> <p>Default value: <i>No</i></p> <p><code>--ShellTrace</code>—enable display of additional debug information when scanning a boot record.</p>
<code>proscan</code>	<p>Purpose: Start checking executable files containing code of currently running processes with the Scanner. If a malicious executable file is detected, it is neutralized, and all processes run by this file are forced to terminate.</p> <p>Arguments: None.</p> <p>Options:</p> <p><code>-a [--Autonomous]</code>—run a specified scanning by a separate instance of Scanning Engine and the Scanner, then terminate their operation after the scanning task is completed. Note that threats detected during an autonomous scanning are not displayed in the common threat list that is displayed using the <code>threats</code> command (see below).</p> <p><code>--Report <BRIEF DEBUG></code>—specify the type of the report with scanning results.</p> <p>Allowed values:</p> <ul style="list-style-type: none">• <i>BRIEF</i>—brief report.• <i>DEBUG</i>—detailed report. <p>Default value: <i>BRIEF</i></p> <p><code>--ScanTimeout <number></code>—specify timeout to scan one file, in ms.</p> <p>If the value is set to <i>0</i>, time on scanning is not limited.</p>



Command	Description
	<p>Default value: 0</p> <p>--HeuristicAnalysis <On Off>—enable or disable heuristic analysis during the scanning.</p> <p>Default value: On</p> <p>--PackerMaxLevel <number>—set the maximum nesting level when scanning packed objects.</p> <p>If the value is set to 0, nested objects will be skipped during scanning.</p> <p>Default value: 8</p> <p>--OnKnownVirus <action>—action applied to a threat detected by using signature-based analysis.</p> <p>Allowed values: REPORT, CURE, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnIncurable <action>—action applied on failure to cure a detected threat or if a threat is incurable.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnSuspicious <action>—action applied to a suspicious object detected by heuristic analysis.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnAdware <action>—action applied to detected adware programs.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnDialers <action>—action applied to dialers.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnJokes <action>—action applied to joke programs.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnRiskware <action>—action applied to potentially dangerous programs (riskware).</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p> <p>--OnHacktools <action>—action applied to hacktools.</p> <p>Allowed values: REPORT, QUARANTINE, DELETE.</p> <p>Default value: REPORT</p>
remotescan <host> <path>	<p>Purpose: Connect to the specified remote host and start scanning the specified file or directory using SSH.</p>



Command	Description
	<div><p>Note that threats detected by remote scanning will not be neutralized and also will not be included into the list of detected threats that is displayed by the <code>threats</code> command (see below).</p></div> <div><p>This function can be used only for detection of malicious and suspicious files on a remote host. To eliminate detected threats on the remote host, it is necessary to use administration tools provided directly by this host. For example, for routers, set-top boxes, and other “smart” devices, a mechanism for a firmware update can be used; for computing machines, it can be done via a connection to them (as an option, using a remote terminal mode) and respective operations in their file system (removal or moving of files, etc.), or via running an anti-virus software installed on them.</p></div> <p>Arguments:</p> <p><code><host></code>—IP address or a domain name of the remote host.</p> <p><code><path></code>—path to the file or directory which is selected to be scanned.</p> <p>Options:</p> <p><code>-l [--Login] <name></code>—login (user name) used for authorization on the remote host via SSH.</p> <p><i>If a user name is not specified, there will be an attempt to connect to a remote host on behalf of the user who has launched the command.</i></p> <p><code>-i [--Identity] <path to file></code>—path to the file containing a private key used for authentication of the specified user via SSH.</p> <p><code>-p [--Port] <number></code>—number of the port on the remote host for connecting via SSH.</p> <p>Default value: 22</p> <p><code>--Password <password></code>—password used for authentication of a user via SSH.</p> <p><i>Please note that the password is transferred as a plain text.</i></p> <p><code>--Report <BRIEF DEBUG></code>—specify the type of the report with scanning results.</p> <p>Allowed values:</p> <ul style="list-style-type: none">• <code>BRIEF</code>—brief report.• <code>DEBUG</code>—detailed report. <p>Default value: <code>BRIEF</code></p> <p><code>--ScanTimeout <number></code>—specify timeout to scan one file, in ms.</p>



Command	Description
	<p>If the value is set to <i>0</i>, time on scanning is not limited.</p> <p>Default value: <i>0</i></p> <p><code>--PackerMaxLevel <number></code>—set the maximum nesting level when scanning packed objects.</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--ArchiveMaxLevel <number></code>—set the maximum nesting level when scanning archives (zip, rar, etc.).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--MailMaxLevel <number></code>—set the maximum nesting level when scanning email messages (pst, tbb, etc.).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--ContainerMaxLevel <number></code>—set the maximum nesting level when scanning other containers (HTML and so on).</p> <p>If the value is set to <i>0</i>, nested objects will be skipped during scanning.</p> <p>Default value: <i>8</i></p> <p><code>--MaxCompressionRatio <ratio></code>—set the maximum compression ratio of scanned objects.</p> <p>The ratio must be at least equal to 2.</p> <p>Default value: <i>3000</i></p> <p><code>--HeuristicAnalysis <On Off></code>—enable or disable heuristic analysis during the scanning.</p> <p>Default value: <i>On</i></p>
<code>checkmail</code> <code><path to file></code>	<p>Purpose: To perform scanning of a mail message, which is saved to a file, for threats, signs of spam, or non-compliance with rules of mail processing. The console output thread (stdout) will display the results of the message scanning and the action applied to this message in the course of scanning.</p> <p>Arguments:</p> <p><code><path to file></code> – path to file of the mail message that requires scanning. Mandatory argument.</p> <p>Options:</p> <p><code>--Report <BRIEF DEBUG></code>—specify the type of the report with scanning results.</p> <p>Allowed values:</p> <ul style="list-style-type: none">• <i>BRIEF</i>—brief report.• <i>DEBUG</i>—detailed report.



Command	Description
	<p>Default value: <i>BRIEF</i></p> <p><code>-r [--Rules] <list of rules></code>—indicate a list of rules to follow during an email message scanning.</p> <p><i>If the rules are not indicated, the set of rules used by default will be used.</i></p> <p><code>-c [--Connect] <IP>:<port></code> – indicate a network socket that will be used as an address for connection by a sender of the scanned message.</p> <p><code>-e [--Helo] <name></code>—indicate an identifier of a client that sent a message (IP address or FQDN host, as for the SMTP command HELO/EHLO).</p> <p><code>-f [--From] <email></code>—indicate an email address of a sender (as for the SMTP command MAIL FROM).</p> <p><i>If the address is not indicated, the respective address from an email will be used.</i></p> <p><code>-t [--Rcpt] <email></code>—indicate an email address of a recipient (as for the SMTP command RCPT TO).</p> <p><i>If the address is not indicated, the respective address from an email will be used.</i></p>




Except above-mentioned commands, the **drweb-ctl** tool supports additional scanning parameters. To read their descriptions, refer to the **man 1 drweb-ctl** documentation.

3.2. Commands to manage updates and operation in Central protection mode


The following commands for managing updates and operation in Central protection mode are available:

Command	Description
update	<p>Purpose: Instruct the updating Component to download and install updates to virus databases and components from Doctor Web update servers or terminate a running update process.</p> <p><i>The command is not executed if Dr.Web for Linux is connected to the central protection server.</i></p> <p>Arguments: None.</p> <p>Options:</p> <p><code>--Stop</code>—terminate the running updating process.</p>
esconnect <server> [: <port>]	<p>Purpose: Connect Dr.Web for Linux to the specified central protection server (for example, Dr.Web Enterprise Server).</p>



Command	Description
	<p>For details on Dr.Web for Linux operation modes, refer to the Operation Modes section.</p> <p>Arguments:</p> <ul style="list-style-type: none">• <code><server></code>—IP address or network name of the host on which the central protection server is operating. This argument is mandatory.• <code><port></code>—port number used by the central protection server. The argument is optional and should be specified only if the central protection server uses a non-standard port. <p>Options:</p> <p><code>--Key <path></code>—path to the public key file of the central protection server to which connection is performed.</p> <p><code>--Login <ID></code>—login (workstation identifier) used for connection to the central protection server.</p> <p><code>--Password <password></code>—password for connection to the central protection server.</p> <p><code>--Group <ID></code>—identifier of the group to which the workstation is added on connection.</p> <p><code>--Rate <ID></code>—identifier of the tariff group applied to your workstation when it is included in one of the central protection server groups (can be specified only together with the <code>--Group</code> option).</p> <p><code>--Compress <On Off></code>—enables (<i>On</i>) or disables (<i>Off</i>) forced compression of transmitted data. If not specified, usage of compression is determined by the server.</p> <p><code>--Encrypt <On Off></code>—enables (<i>On</i>) or disables (<i>Off</i>) forced encryption of transmitted data. If not specified, usage of encryption is determined by the server.</p> <p><code>--Newbie</code>—connect as a “newbie” (get a new account on the server).</p> <div> This command requires drweb-ctl to be started with root privileges. If necessary, use the su or sudo commands.</div>
esdisconnect	<p>Purpose: Disconnect Dr.Web for Linux from the central protection server and switch its operation to <i>Standalone</i> mode.</p> <p><i>The command has no effect if Dr.Web for Linux is in Standalone mode.</i></p> <p>Arguments: None.</p> <p>Options: None.</p>




Command	Description
	<div> This command requires drweb-ctl to be started with root privileges. If necessary, use the su or sudo commands.</div>

3.3. Configuration Management Commands

The following commands to manage configuration are available:

Command	Description
<code>cfset</code> <code><section> . <parameter></code> <code><value></code>	<p>Purpose: to change the active value of the specified parameter in the current configuration.</p> <p><i>Note that an equals sign is not allowed.</i></p> <p>Arguments:</p> <ul style="list-style-type: none">• <code><section></code>—name of the configuration file's section where the parameter resides. This argument is mandatory.• <code><parameter></code>—name of the parameter. The argument is mandatory.• <code><value></code>—new value that is to be assigned to the parameter. The argument is mandatory. <p>The following format is used to specify the parameter value <code><section>.<parameter> <value></code>.</p> <p><i>For description of the configuration file, refer to the documentation man: <code>drweb.ini(5)</code>.</i></p> <p>Options:</p> <p><code>-a [--Add]</code>—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 when adding a new parameter group identified by a tag.</p> <p><code>-e [--Erase]</code>—do not substitute the current parameter value but remove the specified value from the list (allowed only for parameters that can have several values, specified as a list).</p> <p><code>-r [--Reset]</code>—reset the parameter value to the default. At that, <code><value></code> is not required in the command and is ignored if specified.</p> <p>Options are not mandatory. If they are not specified, then the current parameter value (the entire list of values, if the parameter currently holds several values) are substituted with the specified value.</p>



Command	Description
	<div> This command requires drweb-ctl to be started with root privileges. If necessary, use the su or sudo commands.</div>
<code>cfshow</code> <code>[<section> [. <parameter>]</code> <code>]</code>	<p>Purpose: Display parameters of the current configuration.</p> <p>The command to display parameters is specified as follows <code><section>.<parameter> = <value></code>. Sections and parameters of non-installed components are not displayed.</p> <p>Arguments:</p> <ul style="list-style-type: none">• <code><section></code>—name of the configuration file section parameters of which are to be displayed. The argument is optional. If not specified, parameters of all configuration file sections are displayed.• <code><parameter></code>—name of the displayed parameter. 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. <p>Options:</p> <p><code>--Uncut</code>—display all configuration parameters (not only those used with the currently installed set of components). If the option is not specified, only parameters used for configuration of the installed components are displayed.</p> <p><code>--Changed</code>—display only those parameters whose values differ from the default ones.</p> <p><code>--Ini</code>—display parameter values in the INI file format: at first, the section name is specified in square brackets, then the section parameters listed as <code><parameter> = <value></code> pairs (one pair per line).</p> <p><code>--Value</code>—display only value of the specified parameter (the <code><parameter></code> argument is mandatory in this case).</p>
<code>reload</code>	<p>Purpose: Restart Dr.Web for Linux service components. At that, logs are opened, the configuration file is reread, and the attempt to restart abnormally terminated components is then performed.</p> <p>Arguments: None.</p> <p>Options: None.</p>



3.4. Commands to Manage Detected Threats and Quarantine

The following commands for managing threats and quarantine are available:

Command	Description
<code>threats</code> <code>[<action> <object>]</code>	<p>Purpose: Apply the specified action to detected threats, selected by their identifiers. Type of the action is specified by the command's option.</p> <p>If the action is not specified, displays information on detected but not neutralized threats. For each threat the following information is displayed:</p> <ul style="list-style-type: none">• Identifier assigned to the threat (its ordinal number)• The full path to the infected file• Information about the threat (name of the threat, threat type according to the classification used by the Doctor Web company)• Information about the file: size, the file owner's user name, the time of last modification• History of operations applied to the threat: detection, applied actions etc. <p>Arguments: None.</p> <p>Options:</p> <p><code>-f [--Follow]</code>—wait for new messages about new threats and display them once they are received (CTRL+C interrupts the waiting).</p> <p><i>If this option is applied along with any options mentioned below, it is ignored.</i></p> <p><code>--Cure <threat list></code>—attempt to cure the listed threats (list threat identifiers separating them with commas).</p> <p><code>--Quarantine <threat list></code>—move the listed threats to quarantine (list threat identifiers separating them with commas).</p> <p><code>--Delete <threat list></code>—delete the listed threats (list threat identifiers separating them with commas).</p> <p><code>--Ignore <threat list></code>—ignore the listed threats (list threat identifiers separating them with commas).</p> <p>If it is required to apply the command to all detected threats, specify <code>All</code> instead of <code><threat list></code>. For example:</p> <pre>\$ drweb-ctl threats --Quarantine All</pre> <p>moves all detected malicious objects to quarantine.</p>
<code>quarantine</code> <code>[<action> <object>]</code>	<p>Purpose: Apply an action to the specified object in quarantine.</p> <p>If an action is not specified, information on quarantined objects and their identifiers together with brief information on the original files moved to</p>



Command	Description
	<p>quarantine is displayed. For every isolated (quarantined) object the following information is displayed:</p> <ul style="list-style-type: none">• Identifier assigned to the quarantined object• The original path to the file, before it was moved to quarantine.• The date when the file was put in quarantine• Information about the file: size, the file owner's user name, the time of last modification• Information about the threat (name of the threat, threat type according to the classification used by the Doctor Web company) <p>Arguments: None.</p> <p>Options:</p> <p><code>-a [--Autonomous]</code>—start a separate copy of Scanner to perform the specified quarantine command and shut it down after the command is executed.</p> <p><i>This option can be applied along with any options mentioned below.</i></p> <p><code>--Delete <object></code>—delete the specified object from quarantine.</p> <p><i>Note that objects are deleted from quarantine permanently—this action is irreversible.</i></p> <p><code>--Cure <object></code>—try to cure the specified object in the quarantine.</p> <p><i>Note that even if the object is successfully cured, it will remain in quarantine. To restore the cured object from quarantine, use the <code>--Restore</code> command.</i></p> <p><code>--Restore <object></code>—restore the specified object from the quarantine to its original location.</p> <p><i>Note that this command may require drweb-ctl to be started with root privileges. You can restore the file from quarantine even if it is infected.</i></p> <p><code>--TargetPath <path></code>—restore an object from the quarantine to the specified location: either as a file with the name specified here (if the <code><path></code> is a path to a file), or just to the specified directory (if the <code><path></code> is a path to a directory).</p> <p><i>Note that this option can be used only in combination with the <code>--Restore</code> command.</i></p> <p>As an <code><object></code> specify the object identifier in quarantine. To apply the command to all quarantined objects, specify <code>All</code> instead of <code><object></code>. For example,</p> <div><pre>\$ drweb-ctl quarantine --Restore All</pre></div> <p>restores all quarantined objects.</p> <p><i>Note that for the <code>--Restore All</code> variant the additional option <code>--TargetPath</code>, if specified, must set a path to a directory, not a path to a file.</i></p>




3.5. Information Commands

The following information commands are available:

Command	Description
appinfo	<p>Purpose: Display information on active Dr.Web for Linux modules.</p> <p>The following information is displayed for every module:</p> <ul style="list-style-type: none">• Internally-used name• Process identifier GNU/Linux (PID).• State (running, stopped etc.)• Error code, if the work of the component has been terminated because of an error• Additional information (optionally). <p>For the configuration daemon (drweb-configd) the following is displayed as additional information:</p> <ul style="list-style-type: none">• The list of installed components—<i>Installed</i>• The list of components which must be launched by the configuration daemon—<i>Should run</i>. <p>Arguments: None.</p> <p>Options:</p> <p><code>-f [--Follow]</code>—wait for new messages on module status change and display them once such a message is received (CTRL+C interrupts the waiting).</p>
baseinfo	<p>Purpose: Display the information on the current version of the Virus-Finding Engine and status of virus databases.</p> <p>The following information is displayed:</p> <ul style="list-style-type: none">• Version of the anti-virus engine• Date and time when the virus databases that are currently used were issued.• The number of available virus records (in the virus databases)• The time of the last successful update of the virus databases and of the anti-virus engine• The time of the next scheduled automatic update <p>Arguments: None.</p> <p>Options: None.</p>
certificate	<p>Purpose: Display contents of the trusted Dr.Web certificate used by Dr.Web for Linux to check protected connections if this option is enabled</p>



Command	Description
	<p>on the settings page. To save the certificate to the <code><cert_name>.pem</code> file, you can use the following command:</p> <pre>\$ drweb-ctl certificate > <cert_name>.pem</pre> <p>Arguments: None.</p> <p>Options: None.</p>
license	<p>Purpose: Show the information about the currently active license, or get a demo-version license, or get the key file for a license that has already been registered (for example, that has been registered on the company's website).</p> <p>If no options are specified, then the following information is displayed (if you are using a license for the Standalone mode):</p> <ul style="list-style-type: none">• License number• Date and time when the license will expire <p>If you are using a license provided to you by a central protection server (for the use of the product in the Central protection mode or in the Mobile mode), then the following information will be displayed:</p> <p>Arguments: None.</p> <p>Options:</p> <p><code>--GetDemo</code>—request a demo key that is valid for one month, and receive this key, if the conditions for the provision of a demo period have not been breached.</p> <p><code>--GetRegistered <serial number></code>—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, breached by using the product not in the Central protection mode, when the license is managed by a central protection server).</p> <p><i>If the serial number is not the one provided for the demo period, you must first register it at the company's website.</i></p> <p>For further information about the licensing of Dr.Web products, refer to the Licensing section.</p> <div> To register a serial number or to get a demo period, an Internet connection is required.</div>



Usage Examples

Example usage of the **drweb-ctl** command:

1. Object scanning

1.1. Simple Scanning Commands

1. Perform scanning of the `/home` directory with default parameters:

```
$ drweb-ctl scan /home
```

2. Scan paths listed in the `daily_scan` file (one path per line):

```
$ drweb-ctl scan --stdin < daily_scan
```

3. Perform scanning of the boot record on the `sda` drive:

```
$ drweb-ctl bootscan /dev/sda
```

4. Perform scanning of the running processes:

```
$ drweb-ctl procsan
```

1.2. Scanning of Files Selected by Criteria

Examples for selection of files for scanning are listed below and use the result of the operation of the utility **find**. The obtained list of files is sent to the command **drweb-ctl scan** with the parameter `--stdin` or `--stdin0`.

1. Scan listed files returned by the utility **find** and separated with the NUL (`'\0'`) character:

```
$ find -print0 | drweb-ctl scan --stdin0
```

2. Scan all files in all directories, starting from the root directory, on one partition of the file system:

```
$ find / -xdev -type f | drweb-ctl scan --stdin
```

3. Scan all files in all directories, starting from the root directory, with the exception of the `/var/log/messages` and `/var/log/syslog` files:

```
$ find / -type f ! -path /var/log/messages ! -path /var/log/syslog |  
drweb-ctl scan -stdin
```

4. Scan all files of the `root` user in all directories, starting from the root directory:

```
$ find / -type f -user root | drweb-ctl scan --stdin
```

5. Scan files of the `root` and `admin` users in all directories, starting from the root directory:



```
$ find / -type f \( -user root -o -user admin \) | drweb-ctl scan --stdin
```

6. Scan files of users with UID in the range 1000–1005 in all directories, starting from the root directory:

```
$ find / -type f -uid +999 -uid -1006 | drweb-ctl scan --stdin
```

7. Scan files in all directories, starting from the root directory, with a nesting level not more than five:

```
$ find / -maxdepth 5 -type f | drweb-ctl scan --stdin
```

8. Scan files in a root directory ignoring files in subdirectories:

```
$ find / -maxdepth 1 -type f | drweb-ctl scan --stdin
```

9. Scan files in all directories, starting from the root directory, with following all symbolic links:

```
$ find -L / -type f | drweb-ctl scan --stdin
```

10. Scan files in all directories, starting from the root directory, without following symbolic links:

```
$ find -P / -type f | drweb-ctl scan --stdin
```

11. Scan files created not later than May 1, 2017 in all directories, starting with the root directory:

```
$ find / -type f -newermt 2017-05-01 | drweb-ctl scan --stdin
```

1.3. Scanning of Additional Objects

1. Scanning of objects located in the directory `/tmp` on the remote server `192.168.0.1` by connecting to it via SSH as a user `user` with the password `passw`:

```
$ drweb-ctl remotescan 192.168.0.1 /tmp --Login user --Password passw
```

2. Scanning of a mail message saved in the file `email.eml`, using the default set of rules:

```
$ drweb-ctl checkmail email.eml
```

2. Configuration management

1. Display information on a current program package, including information about running processes:

```
$ drweb-ctl appinfo
```

2. Output all parameters from the `[Root]` section of the active configuration:

```
$ drweb-ctl cfshow Root
```



3. Set 'No' as the value of the **Start parameter in the** [LinuxSpider] section of the active configuration (this will disable [the file system monitor](#) SpIDer Guard):

```
# drweb-ctl cfset LinuxSpider.Start No
```

Note that superuser privileges are required to perform this action. To elevate the privileges, you can use the **sudo** command, as shown in the following example:

```
$ sudo drweb-ctl cfset LinuxSpider.Start No
```

4. Perform force update of anti-virus components of the product:

```
$ drweb-ctl update
```

5. Restart the configuration of components of the installed Dr.Web program package:

```
# drweb-ctl reload
```

Note that superuser privileges are required to perform this action. To elevate the privileges, you can use the **sudo** command, as shown in the following example:

```
$ sudo drweb-ctl reload
```

6. Connect the product to the server of [central protection](#), operating on server *192.168.0.1* under the condition that a public key of the server is located in file */home/user/cskey.pub*:

```
$ drweb-ctl esconnect 192.168.0.1 --Key /home/user/cskey.pub
```

7. Disconnect the product from Anti-Virus Network:

```
# drweb-ctl esdisconnect
```

Note that superuser privileges are required to perform this action. To elevate the privileges, you can use the **sudo** command, as shown in the following example:

```
$ sudo drweb-ctl esdisconnect
```

3. Threats management

1. Display information on detected threats:

```
$ drweb-ctl threats
```

2. Move all files containing threats which were not neutralized to quarantine:

```
$ drweb-ctl threats --Quarantine All
```

3. Display list of files moved to quarantine:

```
$ drweb-ctl quarantine
```



4. Restore all files from quarantine:

```
$ drweb-ctl quarantine --Restore All
```

4. An example of operation in the autonomous copy mode

1. Scan files and process quarantine in the autonomous copy mode:

```
$ drweb-ctl scan /home/user -a --OnKnownVirus=Quarantine  
$ drweb-ctl quarantine -a --Delete All
```

The first command will check files in the `/home/user` directory in the autonomous copy mode. Files containing known viruses will be moved to quarantine. The second command will process quarantine content (in the autonomous copy mode as well) and remove all the objects.



Appendices

Appendix A. Types of Computer Threats

Herein, the term “*threat*” is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user’s information or rights (that is, malicious and other unwanted software). In a wider sense, the term “*threat*” may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger user data or confidentiality. Programs that do not conceal their presence in the system (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

Computer Viruses

This type of computer threats is characterized by the ability to embed its code into other programs. Such implementation is called *infection*. In most cases, an infected file becomes a virus carrier and the embedded code does not necessarily match the original one. Most viruses are intended to damage or destroy data in the system.

In Doctor Web classification, viruses are divided by the type of objects they infect:

- *File viruses* infect files of the operating system (usually executable files and dynamic libraries) and are activated when the infected file is launched.
- *Macro-viruses* are viruses that infect documents used by **Microsoft® Office** and some other applications supporting macro commands (for example, written in **Visual Basic**). *Macro commands* are a type of implemented programs (macros) written in a fully functional programming language. For instance, in **Microsoft® Word**, macros can be automatically initiated upon opening (closing, saving, etc.) a document.
- *Script viruses* are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and, thus, take advantage of script vulnerabilities in web applications.
- *Boot viruses* infect boot records of disks and partitions or master boot records of hard drives. They do not require much memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down is performed.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved, and ways to overcome them are constantly being developed. All viruses may also be classified according to protection type they use:

- *Encrypted viruses* encrypt their code upon every infection to hinder their detection in a file, a boot sector or a memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.



- *Polymorphic viruses* not only encrypt their code, but they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.
- *Stealth viruses* (invisible viruses) perform certain actions to disguise their activity and to conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these “dummy” characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, and others) or according to affected operating systems.

Computer Worms

Recently, malicious programs of the “computer worm” type have become much more common than viruses and other types of malware. Just like viruses, such programs can make copies of themselves, however they do not infect other objects. A worm gets into a computer from a network (most frequently as an attachment to an email or from the Internet) and sends the functioning copies of itself to other computers. To start their spread, worms can either rely on the computer user’s actions or can select and attack computers in an automatic mode.

Worms do not necessarily consist of only one file (the worm’s body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm’s body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm’s body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

In Doctor Web classification, worms are divided by distribution method:

- *Network worms* distribute their copies via various network and file sharing protocols.
- *Mail worms* spread themselves using email protocols (POP3, SMTP, etc.)
- *Chat worms* use protocols of popular instant messengers and chat programs (ICQ, IM, IRC, etc.)

Trojan Programs (Trojans)

This type of threats cannot reproduce itself. A Trojan substitutes a frequently-used program and performs its functions (or imitates its operation). Meanwhile, it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for hackers to access the computer without permission, for example, to harm the computer of a third party.

A Trojan’s masking and malicious facilities are similar to those of a virus. A Trojan may even be a component of a virus. However, most Trojans are distributed as separate executable files



(through file exchange servers, removable data carriers or email attachments) that are launched by users or system tasks.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are attributed to Trojans only. Here are some Trojan types which are distinguished as separate classes in Doctor Web:

- *Backdoors* are Trojans that log on into the system and obtain privileged functions, bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.
- *Rootkits* are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: *User Mode Rootkits (UMR)* that operate in user mode (intercept functions of the user mode libraries) and *Kernel Mode Rootkits (KMR)* that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).
- *Keyloggers* are used to log data that users enter by means of a keyboard in order to steal personal information (i.e. network passwords, logins, credit card data, etc.).
- *Clickers* redirect hyperlinks to certain addresses (sometimes malicious) in order to increase traffic of websites or perform DDoS attacks.
- *Proxy Trojans* provide anonymous Internet access through a victim's computer.

In addition, Trojans can also change the start page in a web browser or delete certain files. However, these actions can also be performed by other types of threats (viruses and worms).

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in web browsers. Many adware programs operate with data collected by spyware.



Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These software applications were not created for malicious purposes, but due to their characteristics can pose a threat to the computer's security. Riskware programs can not only damage or delete data, but they are also used by crackers (i.e. malevolent hackers) or by some malicious programs to harm the system. Among such programs, there are various remote chat and administrative tools, FTP-servers, etc.

Suspicious objects

These are possible computer threats detected by the heuristic analyzer. Such objects can potentially be any type of threat (even unknown to IT security specialists) or turn out to be safe in case of false detection. It is recommended to move files containing suspicious objects to the quarantine, they also should be sent to Doctor Web anti-virus laboratory for analysis.



Appendix B. Neutralizing Computer Threats

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

Detection Methods

Signature Analysis

Signature analysis is the first stage of detection procedure and is used to check file code segments for the presence of known virus signatures. A *signature* is a finite continuous sequence of bytes 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. The Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing™

On completion of signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing™ method to detect new and modified viruses which use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as the notorious **Trojan.Encoder.18** ransomware (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 positives of the heuristics analyzer. Objects detected using the Origins Tracing™ algorithm are indicated with the `.Origin` extension added to their names.

Execution Emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses when a search by 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. An 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 code, which is then easily determined by searching against signature checksums.



Heuristic Analysis

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

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

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

While performing any of the checks previously mentioned, Dr.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 signatures, 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 resident guards and penetrates the system, then after an update the malicious program is detected in the list of processes and neutralized.

Actions

To avert computer threats, Dr.Web products use a number of actions that can be applied to malicious objects. A user can leave the default settings, configure which actions to apply automatically, or choose actions manually upon every detection. Below, you can see a list of available actions:

- **Ignore**—instructs to skip the detected threat without performing any other action.
- **Report**—instructs to inform on the detected threat without performing any other action.
- **Cure**—instructs to cure the infected object by removing only malicious content from its body. Note that this action cannot be applied to all types of threats.
- **Quarantine** (*Move to Quarantine, Isolate*)—instructs to move the detected threat to a special directory and isolate it from the rest of the system.
- **Delete**—instructs to remove the infected object permanently.



If threat is detected in a file located in a container (an archive, email message, etc.), its removal is replaced with moving of a container to quarantine.



Appendix C. 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.



Appendix D. Known Errors



If the occurred error is not present in this section, it is recommended that you contact [technical support](#). Be ready to name the error code and describe steps to reproduce the issue.

Recommendations for Identification of Errors

- To figure out the place and the cause of the error, read the contents of the program complex log (by default, it is located in `/var/log/syslog` file or `/var/log/messages` file, depending on the OS installed).
- To identify the error, we recommend you to configure logging to a separate file and enable output of extended information to the log. For that, execute the following [commands](#):

```
# drweb-ctl cfset Root.Log <path to log file>
# drweb-ctl cfset Root.DefaultLogLevel DEBUG
```

- To return to the default logging method and verbosity level, execute the following commands:

```
# drweb-ctl cfset Root.Log -r
# drweb-ctl cfset Root.DefaultLogLevel -r
```

Errors Determined by Code

Error message	Error on monitor channel
Error code	x1
Description	One of the components cannot connect with the configuration daemon Dr.Web ConfigD.
Resolving the error: <ol style="list-style-type: none">1. Restart the configuration daemon by executing the command<pre># service drweb-configd restart</pre>2. Check whether the authentication mechanism for PAM is installed, configured and operates correctly. If not so, install and configure it (for details refer to administration guides and manuals for your OS distribution).3. If PAM is configured correctly and restart of the configuration daemon does not help, restore program settings to the defaults. To do it, clear the contents of the <code><etc_dir>/drweb.ini</code> file (it is recommended that you make a backup of the configuration file), for example, by executing the following commands:	



```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Restart the configuration daemon after clearing the contents of the configuration file.

4. If it is not possible to start the configuration daemon, reinstall the `drweb-configd` package.

For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Operation is already in progress</i>
Error code	x2
Description	Operation requested by the user is already in progress.
Resolving the error:	
1. Wait until operation is finished. If necessary, repeat the required action after some time.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Operation is in pending state</i>
Error code	x3
Description	An operation requested by the user is in pending state (possibly, a network connection is currently establishing or one of the program components is loading or initializing, which takes a long time).
Resolving the error:	
1. Wait for the operation to start. If necessary, repeat the required action after some time.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Interrupted by user</i>
Error code	x4
Description	The action is terminated by the user (possibly, it takes a long time).
Resolving the error:	
1. Repeat the required action after some time.	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Operation canceled</i>
Error code	x5
Description	The action is cancelled (possibly, it takes a long time).
Resolving the error: 1. Repeat the required action again. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>IPC connection terminated</i>
Error code	x6
Description	An interprocess communication (IPC) connection with one of the components is terminated (most likely, the component shuts down because of the user command or being idle).
Resolving the error: 1. If the operation is not finished, start it again. Otherwise, the termination is not an error. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid IPC message size</i>
Error code	x7
Description	A message of invalid size is received during component inter-process communication (IPC).
Resolving the error: 1. Restart the program by executing the following command: <pre># service drweb-configd restart</pre> If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid IPC message format.</i>
Error code	x8
Description	A message of invalid format is received during component inter-process communication (IPC).

**Resolving the error:**

1. Restart the program by executing the following command:

```
# service drweb-configd restart
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Not ready</i>
Error code	x9
Description	The required action cannot be performed because the necessary component or device is not initialized yet.

Resolving the error:

1. Repeat the required action after some time.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>The component is not installed.</i>
Error code	x10
Description	Some function of Dr.Web for Linux is not available because the corresponding component (performing this function) is not installed in the system.

Resolving the error:

1. Install or reinstall the package with the necessary component:
 - drweb-filecheck, if Scanner is not installed
 - drweb-spider, if SpIDer Guard is not installed
 - drweb-gated, if SpIDer Guard is not installed
 - drweb-update, if Updater is not installed
2. If the error persists, or you cannot detect which component is not installed, uninstall Dr.Web for Linux and then install it again on the system.

For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Unexpected IPC message</i>
Error code	x11



Description	An unexpected message is received during component inter-process communication (IPC).
Resolving the error: <ol style="list-style-type: none">Restart the program by executing the following command: <pre># service drweb-configd restart</pre>	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>IPC protocol violation</i>
Error code	x12
Description	Protocol violation happens during component inter-process communication (IPC).
Resolving the error: <ol style="list-style-type: none">Restart the program by executing the following command: <pre># service drweb-configd restart</pre>	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Subsystem state is unknown</i>
Error code	x13
Description	It was discovered that the current state is not known for a certain subsystem that is part of this software and is needed for carrying out the requested operation.
Resolving the error: <ol style="list-style-type: none">Repeat the operation.If the error persists, restart the program by executing the command <pre># service drweb-configd restart</pre> <p>and then repeat the operation.</p>	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Path must be absolute</i>
Error code	x20



Description	Absolute path to file or directory is required (beginning with the root directory of the file system). Relative path is used now.
Resolving the error:	
1. Change the path to the file or the directory so as to make the path absolute.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Not enough memory</i>
Error code	x21
Description	Not enough memory to complete the required operation (for example, an attempt to open a large file).
Resolving the error:	
1. Increase size of available memory for program processes (for example, by changing the limits with the ulimit command), restart the program and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>IO error</i>
Error code	x22
Description	An input/output (I/O) error occurs (for example, the drive is not initialized yet or the partition of the file system is not available anymore).
Resolving the error:	
1. Check whether the required I/O device or the partition of the file system is available. If necessary, mount it and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>No such file or directory</i>
Error code	x23
Description	A specified object of the file system (file or directory) is missing. Possibly, it is removed.
Resolving the error:	
1. Check the path. If necessary, change it and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Permission denied</i>
Error code	x24
Description	There are not enough permissions to access the specified object of the file system (file or directory).
Resolving the error: 1. Check whether the path is correct and whether the component has required permissions. If it is necessary to access the object, change access permissions or elevate component's permissions. Repeat the operation. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Not a directory</i>
Error code	x25
Description	A specified object of the file system is not a directory. Enter the path to the directory.
Resolving the error: 1. Check the path. Change it and repeat the operation. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Data file corrupted</i>
Error code	x26
Description	Requested data is corrupted.
Resolving the error: 1. Repeat the operation. 2. If the error persists, restart the program by executing the command <div># service drweb-configd restart</div> and then repeat the operation. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>File already exists</i>
Error code	x27
Description	On attempt to create a file, another file with the same name is detected.

**Resolving the error:**

1. Check the path. Change it and repeat the operation.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Read-only file system</i>
Error code	x28
Description	On attempt to create or change an object of the file system (directory, file or socket), it is detected that the file system is read-only.
Resolving the error:	
<ol style="list-style-type: none">1. Check the path. Change it so that the path indicates the writable partition of the file system and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Network error</i>
Error code	x29
Description	A network error occurs (possibly, a remote node stops responding unexpectedly or the required connection fails).
Resolving the error:	
<ol style="list-style-type: none">1. Check whether the network is available and network settings are correct. If necessary, change network settings and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Not a drive</i>
Error code	x30
Description	An accessed input/output (I/O) device is not a drive.
Resolving the error:	
<ol style="list-style-type: none">1. Check the device name. Change the path so that it indicates to the drive and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Unexpected EOF</i>
Error code	x31



Description	During data reading, the end of the file is reached unexpectedly.
Resolving the error: 1. Check the name of the file. If necessary, change the path so that it indicates the correct file and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>File was changed</i>
Error code	x32
Description	During scanning the file, it is detected that the file was changed.
Resolving the error: 1. Repeat scanning.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Not a regular file</i>
Error code	x33
Description	During accessing an object of the file system. it is detected that it is not a regular file (that is, it is a directory, socket or other object of the file system).
Resolving the error: 1. Check the name of the file. If necessary, change the path so that it indicates the regular file and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Name already in use</i>
Error code	x34
Description	On attempt to create an object of the file system (directory, file or socket), another object with the same name is detected.
Resolving the error: 1. Check the path. Change it and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Host is offline</i>
Error code	x35
Description	A remote node is not available through the network.
Resolving the error: 1. Check whether the required node is available. If necessary, change the node address and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Resource limit reached</i>
Error code	x36
Description	The limit defined for the use of a certain resource has been reached.
Resolving the error: 1. Check the availability of the required resource. If necessary, raise the limit on the use of this resource and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Different mount points</i>
Error code	x37
Description	Attempt to restore a file which requires its movement between the file system directories, which belong to different mounting points.
Resolving the error: 1. Choose another path for the file restoration and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Unpacking error</i>
Error code	x38
Description	Archive unpacking unsuccessful (it is possibly password protected or corrupted)
Resolving the error: 1. Make sure that file is not corrupted. If the archive is protected with password, remove the protection by entering the correct password and repeat the operation.	



If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Virus database corrupted</i>
Error code	x40
Description	Virus databases are corrupted.

Resolving the error:

1. Check the path to the virus database directory. Change the path, if necessary (the **VirusBaseDir** parameter in the [Root] section of the configuration file).

To view and correct the path, use the [commands](#) of the command-line management tool:

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Non-supported virus database version</i>
Error code	x41
Description	Current virus databases are meant for earlier program version.

Resolving the error:

1. Check the path to the virus database directory. Change the path, if necessary (the **VirusBaseDir** parameter in the [Root] section of the configuration file).

To view and correct the path, use the [commands](#) of the command-line management tool:

- To view current parameter value, execute the following command:



```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Empty virus database</i>
Error code	x42
Description	Virus databases are empty.

Resolving the error:

1. Check the path to the virus database directory. Change the path, if necessary (the **VirusBaseDir** parameter in the [Root] section of the configuration file).

To view and correct the path, use the [commands](#) of the command-line management tool:

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```



If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Object cannot be cured</i>
Error code	x43
Description	An attempt to apply the Cure action to an incurable object during threat neutralization.
Resolving the error:	
1. Select an action that can be applied to the object and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Non-supported virus database combination</i>
Error code	x44
Description	The current virus database combination cannot be supported.
Resolving the error:	
1. Check the path to the virus database directory. Change the path, if necessary (the VirusBaseDir parameter in the [Root] section of the configuration file).	
To view and correct the path, use the commands of the command-line management tool:	
<ul style="list-style-type: none">• To view current parameter value, execute the following command:	
<pre>\$ drweb-ctl cfshow Root.VirusBaseDir</pre>	
<ul style="list-style-type: none">• To set a new parameter value, execute the command	
<pre># drweb-ctl cfset Root.VirusBaseDir <new path></pre>	
<ul style="list-style-type: none">• To restore the parameter value to the default, execute the command	
<pre># drweb-ctl cfset Root.VirusBaseDir -r</pre>	
2. Update virus databases in one of the following ways:	
<ul style="list-style-type: none">• Click Update on the update control page of the main window of the application.• Click Update in the context menu of the status indicator in the notification area.• Execute the command:	
<pre>\$ drweb-ctl update</pre>	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Scan limit reached</i>
Error code	x45
Description	When scanning an object, the specified limits have been reached (for example, the limit on the size of an unpacked file, on the nesting depth and others).
Resolving the error: <ol style="list-style-type: none">1. Change limits for scanning (in the component settings) by any of the following methods:<ul style="list-style-type: none">• On the page with the component settings in the application settings window.• Use the drweb-ctl <code>cfshow</code> and drweb-ctl <code>cfset</code> commands.2. After changing the settings, repeat the previously attempted operation. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Authentication failed</i>
Error code	x47
Description	Invalid user credentials are used for authentication.
Resolving the error: <ol style="list-style-type: none">1. Enter valid credentials of the user with the necessary privileges. Try to complete authentication again. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Authorization failed</i>
Error code	x48
Description	A user whose credentials are used for authorization does not have enough privileges.
Resolving the error: <ol style="list-style-type: none">1. Enter valid credentials of the user with the necessary privileges. Try to complete authentication again. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Access token is invalid</i>
Error code	x49



Description	One of the program components provides invalid authorization token on attempt to access the operation, requiring elevated privileges.
Resolving the error: 1. Enter valid credentials of the user with the necessary privileges. Try to complete authentication again.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid argument</i>
Error code	x60
Description	An invalid argument is used on attempt to run a command.
Resolving the error: 1. Repeat the required action again using valid argument.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid operation</i>
Error code	x61
Description	An attempt to run an invalid command is detected.
Resolving the error: 1. Repeat the required action again using valid command.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Superuser privileges required</i>
Error code	x62
Description	Only a user with root privileges can perform this action.
Resolving the error: 1. Elevate your privileges to root privileges and repeat the required action. To elevate privileges, you can use the commands su and sudo .	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Not allowed in central protection mode</i>
----------------------	---



Error code	x63
Description	The required action can be performed only if the program operates in Standalone mode .
Resolving the error: <ol style="list-style-type: none">1. Change product's operation mode to Standalone mode and repeat the operation.2. To change the mode<ul style="list-style-type: none">• Clear the Enable the central protection mode check box on the Mode settings page.• Or execute the command <pre># drweb-ctl esdisconnect</pre>	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Non-supported OS</i>
Error code	x64
Description	The program does not support operating system installed on the host.
Resolving the error: <ol style="list-style-type: none">1. Install the operating system from the list mentioned in system requirements.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Feature not implemented</i>
Error code	x65
Description	Required features of one of the components are not implemented in the current version of the program.
Resolving the error: <ol style="list-style-type: none">1. Restore software defaults by clearing the contents of the configuration file <code>/etc/opt/drweb.com/drweb.ini</code>. It is recommended to back up the file before the procedure. For example:<pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save</pre><pre># echo "" > /etc/opt/drweb.com/drweb.ini</pre>2. Restart the program after clearing the contents of the configuration file by executing the command<pre># service drweb-configd restart</pre>	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Unknown option</i>
Error code	x66
Description	The configuration file contains parameters unknown or non-supported in the current version of the program.
Resolving the error:	
1. Open the <code>/etc/opt/drweb.com/drweb.ini</code> file in any text editor, remove the line, containing invalid parameter. Save the file and restart the program by executing the command:	
<pre># service drweb-configd restart</pre>	
2. If it does not help, restore program's settings to the defaults. To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:	
<pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre>	
Restart the program after clearing the contents of the configuration file.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Unknown section</i>
Error code	x67
Description	The configuration file contains sections unknown or non-supported in the current version of the program.
Resolving the error:	
1. Open the <code>/etc/opt/drweb.com/drweb.ini</code> file in any text editor, remove the unknown section. Save the file and restart the program by executing the command:	
<pre># service drweb-configd restart</pre>	
2. If it does not help, restore program's settings to the defaults. To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:	
<pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre>	
Restart the program after clearing the contents of the configuration file.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid option value</i>
----------------------	-----------------------------



Error code	x68
Description	One of the parameters in the configuration file contains invalid value for the parameter.
Resolving the error: <ol style="list-style-type: none">Set the valid parameter value by any of the following methods:<ul style="list-style-type: none">On the page with the component settings in the application settings window.Use the drweb-ctl cfshow and drweb-ctl cfset commands.If you do not know which value is valid for the parameter, refer to the help file of the component which uses this parameter. You may also restore parameter value to the default.You may also directly edit the configuration file <code>/etc/opt/drweb.com/drweb.ini</code>. To do this, open the configuration file in any text editor, find the line containing invalid parameter value, set valid value, then save the file and restart the program by executing the command:<pre># service drweb-configd restart</pre> <p>If the previous steps do not help, restore program's settings to the defaults.</p> <p>To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:<pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre><p>Restart the program after clearing the contents of the configuration file.</p><p>If the error persists, contact technical support and be ready to name the error code.</p></p>	

Error message	<i>Invalid state</i>
Error code	x69
Description	The program or one of the components is in invalid state to complete the required operation.
Resolving the error: <ol style="list-style-type: none">Repeat the required action after some time.If the error persists, restart the program by executing the command<pre># service drweb-configd restart</pre> <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Only one value allowed</i>
Error code	x70



Description	One of the parameters in the configuration file contains a list of values; while it is allowed to contain only a single value.
Resolving the error:	
<ol style="list-style-type: none">Set the valid parameter value by any of the following methods:<ul style="list-style-type: none">On the page with the component settings in the application settings window.Use the drweb-ctl <code>cfshow</code> and drweb-ctl <code>cfset</code> commands.If you do not know which value is valid for the parameter, refer to the help file of the component which uses this parameter. You may also restore parameter value to the default.You may also directly edit the configuration file <code>/etc/opt/drweb.com/drweb.ini</code>. To do this, open the configuration file in any text editor, find the line containing invalid parameter value, set valid value, then save the file and restart the program by executing the command:<pre># service drweb-configd restart</pre>If the previous steps do not help, restore program's settings to the defaults. To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:<pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre>Restart the program after clearing the contents of the configuration file. If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Tag value is invalid</i>
Error code	x71
Description	One of the sections in the configuration file with a name containing a unique tag identifier has an invalid tag identifier.
Resolving the error:	
<ol style="list-style-type: none">If the error occurs on attempt to use the command<pre># drweb-ctl cfset <section>.<parameter> <new value></pre>set valid value for the tag and save the section again.If the section is saved directly in the configuration file <code>/etc/opt/drweb.com/drweb.ini</code>, edit the file. To do this, open the configuration file in any text editor, find the section name containing invalid tag value and set valid value for the tag. Save the file and restart the program by executing the command:<pre># service drweb-configd restart</pre>If the previous steps do not help, restore program's settings to the defaults.	



To do this, clear the contents of the file `/etc/opt/drweb.com/drweb.ini` (it is recommended to back up the configuration file), for example, by executing the following commands:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Restart the program after clearing the contents of the configuration file.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Record not found</i>
Error code	x80
Description	On attempt to access a threat record, it is found out that the record is missing (possibly, another program component processed the threat).
Resolving the error: 1. Update the threat list after some time.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Record is in process now</i>
Error code	x81
Description	On attempt to access a threat record, it is found out that another program component is processing the record now.
Resolving the error: 1. Update the threat list after some time.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>File has already been quarantined</i>
Error code	x82
Description	On attempt to move the file with the detected threat to quarantine, it is found out that the file is already in quarantine (most likely, another program component processed the threat).
Resolving the error: 1. Update the threat list after some time.	
If the error persists, contact technical support and be ready to name the error code.	



Error message	<i>Cannot backup before update.</i>
Error code	x89
Description	Prior to downloading the updates from the updates server, an attempt to make a backup copy of the files to be updated failed.
Resolving the error:	
<ol style="list-style-type: none">1. Check the path to the directory that stores backup copies of the files that are updated. Change the path, if necessary (the BackupDir parameter in the [Update] section of the configuration file). In order to view and correct the path, you may use the commands of the command line management tool.<ul style="list-style-type: none">• To view current parameter value, execute the following command:<pre>\$ drweb-ctl cfshow Update.BackupDir</pre>• To set a new parameter value, execute the command<pre># drweb-ctl cfset Update.BackupDir <new path></pre>• To restore the parameter value to the default, execute the command<pre># drweb-ctl cfset Update.BackupDir -r</pre>2. Update virus databases in one of the following ways:<ul style="list-style-type: none">• Click Update on the update control page of the main window of the application.• Click Update in the context menu of the status indicator in the notification area.• Execute the command:<pre>\$ drweb-ctl update</pre>3. If the error persists, check whether the user under whose account the Update component is running has a write permission to the directory specified in the BackupDir. The name of this user is specified in the RunAsUser parameter. If necessary, change the user name specified in the RunAsUser parameter or grant the missing permissions in the directory's properties.4. If the error persists, reinstall the drweb-update package. For details on how to install and uninstall the product or product components, refer to sections Installing Dr.Web for Linux and Uninstalling Dr.Web for Linux. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Invalid DRL file</i>
Error code	x90
Description	An integrity violation of one of the files with the list of update servers is detected.

**Resolving the error:**

1. Check the path to the file with the list of servers. Change the path, if necessary (parameters with ***DrlPath** in [Update] section of the config file. To do this, use [commands](#) of the command line management tool.
 - To view current parameter value, execute the command (<**DrlPath*> should be changed for a name of the parameter. If you do not know the parameter name, review values of all parameters in the section omitting the part specified in square brackets):

```
$ drweb-ctl cfshow Update[.<*DrlPath>]
```

- To set new parameter value, execute the command (<**DrlPath*> should be changed for a name of the parameter):

```
# drweb-ctl cfset Update.<*DrlPath> <new path>
```

- To restore parameter value to the default, execute the command (<**DrlPath*> should be changed for a name of the parameter)

```
# drweb-ctl cfset Update.<*DrlPath> -r
```

2. Update virus databases in one of the following ways:
 - Click **Update** on the update control [page](#) of the [main window](#) of the application.
 - Click **Update** in the [context menu](#) of the status indicator in the notification area.
 - Execute the [command](#):
3. If the error persists, install drweb-bases and drweb-dws components (packages) separately and then start an update.
4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.
For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid LST file</i>
Error code	x91
Description	An integrity violation of the file containing the list of updated virus databases is detected.

Resolving the error:

1. Update virus databases in one of the following ways:
 - Click **Update** on the update control [page](#) of the [main window](#) of the application.
 - Click **Update** in the [context menu](#) of the status indicator in the notification area.



- Execute the [command](#):

```
$ drweb-ctl update
```

2. If the error persists, reinstall the `drweb-update` package.
3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.
For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid compressed file</i>
Error code	x92
Description	An integrity violation of the downloaded file containing updates is detected.
Resolving the error:	
<ol style="list-style-type: none">1. Update virus databases in one of the following ways:<ul style="list-style-type: none">• Click Update on the update control page of the main window of the application.• Click Update in the context menu of the status indicator in the notification area.• Execute the command:	
<pre>\$ drweb-ctl update</pre>	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Proxy authentication error</i>
Error code	x93
Description	The program fails to connect to update servers using the proxy server specified in the settings.
Resolving the error:	
<ol style="list-style-type: none">1. Check the parameters used to connect to a proxy server (they are set in the Proxy parameter in the [Update] section of the configuration file). If necessary, change the proxy server or do not use proxy for connections. To view and set the connection parameters, go to the main settings page. You also may use the commands of the command-line management tool.<ul style="list-style-type: none">• To view current parameter value, execute the following command:	
<pre>\$ drweb-ctl cfshow Update.Proxy</pre>	
<ul style="list-style-type: none">• To set a new parameter value, execute the command	



```
# drweb-ctl cfset Update.Proxy <new parameters>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Update.Proxy -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>No update servers available</i>
Error code	x94
Description	The program fails to connect to any of the update servers.

Resolving the error:

1. Check whether the network is available. Change network settings, if necessary.
2. If the network access is available only via a proxy server, specify the parameters of connection to the proxy server (they are set in the **Proxy** parameter in the [Update] section of the configuration file). If necessary, change the proxy server or do not use proxy for connections.

To view and set the connection parameters, go to the [main settings](#) page.

You also may use the [commands](#) of the command-line management tool.

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow Update.Proxy
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Update.Proxy <new parameters>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Update.Proxy -r
```

3. If the network connection settings (including the proxy server ones) are correct, but the error occurs, make sure you are using an available list of update servers. The list of update servers used is indicated in the view parameters ***Dr1Path** in [Update] section of the configuration file. Note that if the parameters ***CustomDr1Path** indicate on the existing correct file of the server list, the servers specified there will be used instead of the servers of the standard update zone (the value specified in the corresponding ***Dr1Path** parameter, is ignored).



In order to view and configure connection settings, you may use the [commands](#) of the command line management tool.

To view current parameter value, execute the command (<*DrlPath> should be changed for a name of the parameter. If you do not know the parameter name, review values of all parameters in the section omitting the part specified in square brackets):

```
$ <%CTL_MODULE%> cfshow Update[.<*DrlPath>]
```

To set new parameter value, execute the command (<*DrlPath> should be changed for a name of the parameter):

```
# <%CTL_MODULE%> cfset <%UPDATE_SECTION%>.<*DrlPath> <new path>
```

To restore parameter value to the default, execute the command (<*DrlPath> should be changed for a name of the parameter)

```
# <%CTL_MODULE%> cfset <%UPDATE_SECTION%>.<*DrlPath> -r
```

4. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid key file format</i>
Error code	x95
Description	The key file format is violated.

Resolving the error:

1. Check whether you have the key file and the path to it. You can specify the path to the key file in the **KeyPath** parameter in the [Root] section of the configuration file.

To view the license parameters and set the path to the key file, go to the [License Manager](#) page of the [main page](#) of the application.

You also may use the [commands](#) of the command-line management tool.

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow Root.KeyPath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.KeyPath <path to file>
```

- To restore the parameter value to the default, execute the command



```
# drweb-ctl cfset Root.KeyPath -r
```

2. If you do not have the key file or the used key file is corrupted, purchase and install it. For more details on the key file, purchase and installation refer to the [Licensing](#) section.
3. To install the key file, you may use the [License Manager](#).
4. You can also view current license options in user's webpage **My Dr.Web** at <https://support.drweb.com/get+cabinet+link/>.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>License is expired</i>
Error code	x96
Description	The used license is expired.

Resolving the error:

1. Purchase a new license and install a key file that you will receive. For more details on ways to purchase the license and installation of the key file refer to the [Licensing](#) section.
2. To install the purchased key file, you may use the [License Manager](#).
3. You can also view current license options in user's webpage **My Dr.Web** at <https://support.drweb.com/get+cabinet+link/>.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Network operation timed out.</i>
Error code	x97
Description	

Resolving the error:

1. Check whether the network is available and network settings are correct. If necessary, change network settings and repeat the operation.
2. If an error persists during the update, additionally check [parameters](#) of the proxy server usage, and if necessary, change the used proxy server or do not use it at all.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid checksum</i>
Error code	x98
Description	A checksum of the downloaded file containing updates is detected.

Resolving the error:



1. Restart the update after some time in one of the following ways:
 - Click **Update** on the update control [page](#) of the [main window](#) of the application.
 - Click **Update** in the [context menu](#) of the status indicator in the notification area.
 - Execute the [command](#):

```
$ drweb-ctl update
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid demo key file</i>
Error code	x99
Description	The used demo key file is invalid (for example, it was received from another computer).
Resolving the error:	
<ol style="list-style-type: none">1. Send a request for a new demo period for this computer or purchase a new license and install a key file that you will receive. For more details on ways to purchase the license and installation of the key file refer to the Licensing section.2. To install the purchased key file, you may use the License Manager.3. You can also view current license options in user's webpage My Dr.Web at https://support.drweb.com/get+cabinet+link/.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Key file is blocked</i>
Error code	x100
Description	The used license is blocked (probably, the license agreement conditions on using the Dr.Web program are broken).
Resolving the error:	
<ol style="list-style-type: none">1. Purchase a new license and install a key file that you will receive. For more details on ways to purchase the license and installation of the key file refer to the Licensing section.2. To install the purchased key file, you may use the License Manager.3. You can also view current license options in user's webpage My Dr.Web at https://support.drweb.com/get+cabinet+link/.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	<i>Invalid license</i>
Error code	x101



Description	The used license is meant for other product or does not allow operation of the installed product components.
Resolving the error: <ol style="list-style-type: none">1. Purchase a new license and install a key file that you will receive. For more details on ways to purchase the license and installation of the key file refer to the Licensing section.2. To install the purchased key file, you may use the License Manager.3. You can also view current license options in user's webpage My Dr.Web at https://support.drweb.com/get+cabinet+link/. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Invalid configuration</i>
Error code	x102
Description	One of the program components cannot be in operation because of incorrect configuration settings.

Resolving the error:

1. If you do not know the name of the component which causes the error, try to determine it reviewing the log file.
2. If the error is produced by the SpIDer Guard component, most likely that the mode which is selected for the component operation is not supported by OS. Check the selected mode and change it, if necessary. You can do it by setting the value `AUTO` (the **Mode** parameter in the `[LinuxSpider]` section of the configuration file).

In order to view and correct the mode, you may use the [commands](#) of the command line management tool.

- To set the value to `AUTO`, execute the command

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

If the error persists, [manually build and install](#) the loadable kernel module for SpIDer Guard



Note that operation of SpIDer Guard and of the loadable kernel module is guaranteed only on the tested **Linux** distributives (see [System Requirements](#)).

3. If this error is produced by SpIDer Gate, most likely that there is a conflict with another firewall. For example, it is known that SpIDer Gate conflicts with **Firewalld** in **Fedora**, **CentOS**, **Red Hat Enterprise Linux** (on every launch, **Firewalld** corrupts traffic routing rules indicated by SpIDer Gate). To resolve this error, restart the program by executing the command

```
# service drweb-configd restart
```



or

```
# drweb-ctl reload
```



Note that if you allow **Firewalld** to operate, the noted SpIDer Gate error can repeatedly occur on every restart of **Firewalld**, including a restart of an OS. You can resolve this error by disabling **Firewalld** (refer to the manual of **Firewalld** included in the manual of your OS).

4. If the error is produced by another component, restore the component settings to the defaults by any of the following methods:

- Use the **drweb-ctl** cfshow and **drweb-ctl** cfset [commands](#).
- Edit the configuration file manually by deleting all parameters from the component section.

5. If the previous steps do not help, restore program's settings to the defaults.

To do this, clear the contents of the file `/etc/opt/drweb.com/drweb.ini` (it is recommended to back up the configuration file), for example, by executing the following commands:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save  
# echo "" > /etc/opt/drweb.com/drweb.ini
```

Restart the program after clearing the contents of the configuration file by executing the command

```
# service drweb-configd restart
```

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid executable file</i>
Error code	x104
Description	One of the program components cannot run due to incorrect path or corrupted execution file contents.

Resolving the error:

1. If you do not know the name of the component which causes the error, try to determine it reviewing the log file.
2. Check the path to the executable file of the component in the program configuration file (the **ExePath** parameter in the component section), by executing the following [command](#) (change `<component section>` for the name of the corresponding section of the configuration file):

```
$ drweb-ctl cfshow <component section>.ExePath
```

3. Restore the path to the default by executing the following command (change `<component section>` for the name of the corresponding section of the configuration file):

```
# drweb-ctl cfset <component section>.ExePath -r
```



4. If the previous steps do not help, reinstall the package of the corresponding component.
 - `drweb-filecheck`, if the executable file of Scanner is corrupted
 - `drweb-spider`, if the executable file of SpIDer Gate is corrupted.
 - `drweb-gated`, if the executable file of SpIDer Gate is corrupted
 - `drweb-update`, if the executable file of Updater is corrupted
5. If the error persists, or you cannot detect which executable file is invalid, uninstall Dr.Web for Linux and then install it again on the system.

For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Virus-Finding Engine is not available</i>
Error code	x105
Description	The file of anti-virus engine Dr.Web Virus-Finding Engine is missing or unavailable (it is necessary for threat detection).

Resolving the error:

1. Check the path to the **drweb32.dll** anti-virus engine file. Change the path, if necessary (the **CoreEnginePath** parameter in the [Root] section of the configuration file).

In order to view and correct the path, you may use the [commands](#) of the command line management tool.

- To view current parameter value, execute the command

```
$ drweb-ctl cfshow Root.CoreEnginePath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.CoreEnginePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.CoreEnginePath -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

3. If the path is correct and the error persists after updating virus databases, reinstall the `drweb-bases` package.
4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.



For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>No virus databases</i>
Error code	x106
Description	Virus databases are not found.

Resolving the error:

1. Check the path to the virus database directory. Change the path, if necessary (the **VirusBaseDir** parameter in the [Root] section of the configuration file).

In order to view and correct the path, you may use the [commands](#) of the command line management tool.

- To view current parameter value, execute the command

```
$ drweb-ctl cfshow Root.VirusBaseDir
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.VirusBaseDir -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

3. If the error persists, install the `drweb-bases` package containing virus databases and anti-virus engine executable file.
4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.
For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Process terminated by signal</i>
Error code	x107



Description	A component shuts down (possibly, because of the user command or being idle).
Resolving the error: <ol style="list-style-type: none">1. If the operation is not finished, start it again. Otherwise, the shutdown is not an error.2. If a component shuts down constantly, restore its settings to the defaults by any of the following methods:<ul style="list-style-type: none">• Use the drweb-ctl <code>cfshow</code> and drweb-ctl <code>cfset</code> commands.• Edit the configuration file manually (by deleting all parameters from the component section).3. If it does not help, restore program's settings to the defaults.<p>To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:</p><pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre><p>Restart the program after clearing the contents of the configuration file by executing the command</p><pre># service drweb-configd restart</pre> <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Unexpected process termination</i>
Error code	x108
Description	A component unexpectedly shuts down because of a failure.
Resolving the error: <ol style="list-style-type: none">1. Repeat the terminated operation.2. If the component constantly shuts down abnormally, restore its settings to the defaults by any of the following methods:<ul style="list-style-type: none">• Use the drweb-ctl <code>cfshow</code> and drweb-ctl <code>cfset</code> commands.• Edit the configuration file manually (by deleting all parameters from the component section).3. If it does not help, restore program's settings to the defaults.<p>To do this, clear the contents of the file <code>/etc/opt/drweb.com/drweb.ini</code> (it is recommended to back up the configuration file), for example, by executing the following commands:</p><pre># cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save # echo "" > /etc/opt/drweb.com/drweb.ini</pre><p>Restart the program after clearing the contents of the configuration file by executing the command</p><pre># service drweb-configd restart</pre>4. If the error persists after restoring program settings, reinstall the component package.	



5. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Incompatible software detected</i>
Error code	x109
Description	A program component cannot be in operation because an incompatible software is detected. This software interrupts correct component operation.

Resolving the error:

1. If this error is produced by SpIDer Gate, most likely that there is an incompatible software in operating system. This software generates rules for the **NetFilter** system firewall, which prevents SpIDer Gate from correct operation. Probably, you have **Shorewall** or **SuseFirewall2** installed in the system (in **SUSE Linux OS**). The application that configure the **NetFilter system firewall** **sometimes check the integrity of the specified rule system and rewrite it. This is the main reason of** SpIDer Gate conflict with such applications.

Reconfigure incompatible software so as it does not interfere in SpIDer Gate operation. If it is not possible, disable the software so as it does not load at the operating system startup any more. You can try to configure the **SuseFirewall2** application (in **SUSE Linux OS**), following the steps:

- 1) Open the configuration file of **SuseFirewall2** (by default, this is the `/etc/sysconfig/SuSEfirewall2` file).
- 2) Find the following text block:

```
# Type: yesno
#
# Install NOTRACK target for interface lo in the raw table. Doing so
# speeds up packet processing on the loopback interface. This breaks
# certain firewall setups that need to e.g. redirect outgoing
# packets via custom rules on the local machine.
#
# Defaults to "yes" if not set
#
FW_LO_NOTRACK=""
```

- 3) Set the parameter value to "no":

```
FW_LO_NOTRACK="no"
```

- 4) Restart **SuseFirewall2** by executing the following command:

```
# rcSuSEfirewall12 restart
```



Note that if **SuseFirewall2** does not have the `FW_LO_NOTRACK` option in its settings, to resolve the conflict, disable the application so that it does not load at the system



startups any more (for example, it is necessary for OS **SUSE Linux Enterprise Server 11**).

- 5) After reconfiguring or disabling the conflict application, restart SpIDer Gate (disable it and enable again on the relevant [page](#)):
2. If the error is produced by another component, disable or reconfigure the incompatible software so as to prevent any interference with the Dr.Web for Linux operation.

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Invalid VadeRetro library</i>
Error code	x110
Description	A file of VadeRetro anti-spam library is missing, unavailable or corrupted (it is necessary for email scanning)

Resolving the error:

1. Check the path to the **vaderetro.so** library file. Change the path, if necessary (the **VaderetroLibPath** parameter in the [Root] section of the configuration file).
In order to view and correct the path, you may use the [commands](#) of the command line management tool.

- To view current parameter value, execute the command

```
$ drweb-ctl cfshow Root.VaderetroLibPath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.VaderetroLibPath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.VaderetroLibPath -r
```

2. Update virus databases in one of the following ways:
 - Click **Update** on the update control [page](#) of the [main window](#) of the application.
 - Click **Update** in the [context menu](#) of the status indicator in the notification area.
 - Execute the [command](#):

```
$ drweb-ctl update
```



If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Databases of web resource categories</i>
Error code	x112
Description	Databases of web resource categories are missing.

Resolving the error:

1. Check the path to the database of web resource categories directory. Change the path, if necessary (the **DwsDir** parameter in the [Root] section of the configuration file).

- In order to view and correct the path, you may use the [commands](#) of the command line management tool.

To view current parameter value, execute the command

```
$ drweb-ctl cfshow Root.DwsDir
```

To set a new parameter value, execute the command

```
# drweb-ctl cfset Root.DwsDir <new path>
```

To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Root.DwsDir -r
```

2. Update virus databases in one of the following ways:

- Click **Update** on the update control [page](#) of the [main window](#) of the application.
- Click **Update** in the [context menu](#) of the status indicator in the notification area.
- Execute the [command](#):

```
$ drweb-ctl update
```

3. If an error persists, install the package `drweb-dws` separately. This package contains databases of web resource categories.
4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Linux kernel module for SpIDer Gate is unavailable</i>
Error code	x113
Description	SpIDer Gate requires a Linux kernel module which is missing.

Resolving the error:



1. Check which operating mode of the component was selected and change it—if necessary—by setting the value to `Auto` (for the `Mode` parameter in the `[LinuxSpider]` section of the configuration file).

In order to view and correct the mode, you may use the [commands](#) of the command line management tool.

- To set the value to `AUTO`, execute the command

```
# drweb-ctl cfset LinuxSpider.Mode AUTO
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset LinuxSpider.Mode -r
```

2. If the error persists, [manually build and install](#) the loadable kernel module for SpIDer Guard



Note that operation of SpIDer Guard and of the loadable kernel module is guaranteed only on the tested **Linux** distributives (see [System Requirements](#)).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>SpIDer Gate is unavailable</i>
Error code	x117
Description	SpIDer Gate component is missing (required for scanning network connections).

Resolving the error:

1. Check the path to the **drweb-gated** executable file. Change the path, if necessary (the `ExePath` parameter in the `[GateD]` section of the configuration file).

You may use the [commands](#) of the command-line management tool.

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow GateD.ExePath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset GateD.ExePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset GateD.ExePath -r
```

2. If the configuration does not contain settings for SpIDer Gate component or if the error persists after entering the correct path, install or reinstall the `drweb-gated` package.
3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.



For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>MailD is not available</i>
Error code	x118
Description	Dr.Web MailD component is missing (it is necessary for scanning email).

Resolving the error:

1. Check the path to the **drweb-maild** executable file. Change the path, if necessary (the **ExePath** parameter in the [MailD] section of the configuration file).

You may use the [commands](#) of the command-line management tool.

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow MailD.ExePath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset MailD.ExePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset MailD.ExePath -r
```

2. If the configuration does not contain settings for Dr.Web MailD component or if the error persists after entering the correct path, install or reinstall the **drweb-maild** package.
3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.

For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Scanning Engine is not available</i>
Error code	x119
Description	Cannot check files as ScanEngine component (drweb-se) is missing or failed to start. This module is used for searching malicious objects. Failed to start: Scanner , SpIDer Guard , SpIDer Gate (partially).

Resolving the error:

1. Check the path to the **drweb-se** executable file. Change the path, if necessary (the **ExePath** parameter in the [ScanEngine] section of the configuration file).

You may use the [commands](#) of the command-line management tool.



- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow ScanEngine.ExePath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset ScanEngine.ExePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset ScanEngine.ExePath -r
```

2. If the error persists after entering the correct path

- Execute the command

```
$ drweb-ctl rawscan /
```

If the line `Error: No valid license provided`, is output, a valid key file is missing. Register the program and receive a license. After receiving the license, check whether the [key file](#) is available and install it, if necessary.

- If you use 64-bit version of the operating system, make sure that 32-bit application support libraries are installed (see [System Requirements](#)) and, if necessary, install them.

To check that the 32-bit application support library is installed, use the following command:

```
$ dpkg -l | grep <libname>
```

where `<libname>` is name of the library (**libc6-i386** or **glibc.i686**, depending on your system). If the command does not output any result to screen, you should install the library, using the system package manager. In other case, the library is already installed and **drweb-se** module unavailable due to other reasons.

After you install the library, restart Dr.Web for Linux by the following command:

```
# service drweb-configd restart
```

- If your operating system uses **SELinux**, configure the security policy for the **drweb-se** module (see section [Configuring SELinux Security Policies](#)).
3. If the configuration does not contain the component settings or if the steps previously mentioned do not help, install or reinstall the `drweb-se` package.
 4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	Scanner is unavailable
Error code	x120



Description	Cannot check files as a Scanner component drweb-filecheck , used for this function, is missing. Failed to start: Scanner, SpIDer Guard .
Resolving the error:	
<ol style="list-style-type: none">1. Check the path to the drweb-filecheck executable file. Change the path, if necessary (the ExePath parameter in the [FileCheck] section of the configuration file). You may use the commands of the command-line management tool. To view current parameter value, execute the following command: <pre>\$ drweb-ctl cfshow FileCheck.ExePath</pre> To set a new parameter value, execute the command <pre># drweb-ctl cfset FileCheck.ExePath <new path></pre> To restore the parameter value to the default, execute the command <pre># drweb-ctl cfset FileCheck.ExePath -r</pre>2. If the error persists after entering the correct path<ul style="list-style-type: none">• If you use 64-bit version of the operating system, make sure that 32-bit application support libraries are installed (see System Requirements) and, if necessary, install them. To check that the 32-bit application support library is installed, use the following command: <pre>\$ dpkg -l grep <libname></pre> where <i><libname></i> is name of the library (libc6-i386 or glibc.i686, depending on your system). If the command does not output any result to screen, you should install the library, using the system package manager. In other case, the library is already installed and drweb-filecheck module unavailable due to other reasons. After you install the library, restart Dr.Web for Linux by the following command: <pre># service drweb-configd restart</pre>• If your operating system uses SELinux, configure the security policy for the drweb-filecheck module (see section Configuring SELinux Security Policies).3. If the configuration does not contain the component settings or if the steps previously mentioned do not help, install or reinstall the drweb-filecheck package.4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections Installing Dr.Web for Linux and Uninstalling Dr.Web for Linux.	
If the error persists, contact technical support and be ready to name the error code.	
Error message	<i>ES Agent is not available</i>



Error code	x121
Description	Dr.Web ES Agent component is missing (it is necessary to connect to the central protection server).
Resolving the error:	
<ol style="list-style-type: none">1. Check the path to the drweb-esagent executable file. Change the path, if necessary (the ExePath parameter in the [ESAgent] section of the configuration file). You may use the commands of the command-line management tool.<ul style="list-style-type: none">• To view current parameter value, execute the following command:<pre>\$ drweb-ctl cfshow ESAgent.ExePath</pre>• To set a new parameter value, execute the command<pre># drweb-ctl cfset ESAgent.ExePath <new path></pre>• To restore the parameter value to the default, execute the command<pre># drweb-ctl cfset ESAgent.ExePath -r</pre>2. If the configuration does not contain settings for the component or if the error persists after entering the correct path, install or reinstall the <code>drweb-esagent</code> package.3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections Installing Dr.Web for Linux and Uninstalling Dr.Web for Linux. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Firewall for Linux is not available</i>
Error code	x122
Description	Cannot control network connections as drweb-firewall is missing or failed to start. The module is used to divert connections. Failed to start: SpIDer Gate .
Resolving the error:	
<ol style="list-style-type: none">1. Check the path to the drweb-firewall executable file. Change the path, if necessary (the ExePath parameter in the [LinuxFirewall] section of the configuration file). You may use the commands of the command-line management tool.<ul style="list-style-type: none">• To view current parameter value, execute the following command:<pre>\$ drweb-ctl cfshow LinuxFirewall.ExePath</pre>• To set a new parameter value, execute the command	



```
# drweb-ctl cfset LinuxFirewall.ExePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset LinuxFirewall.ExePath -r
```

2. If the configuration does not contain settings for Dr.Web Firewall for **Linux** or if the error persists after entering the correct path, install or reinstall the `drweb-firewall` package.
3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>Network Checker is not available</i>
Error code	x123
Description	Cannot control network connections as drweb-netcheck is missing or failed to start. The module is used to check the downloaded files. Failed to start: SpIDer Gate (partially).

Resolving the error:

1. Check the path to the **drweb-netcheck** executable file. Change the path, if necessary (the **ExePath** parameter in the [Netcheck] section of the configuration file).

You may use the [commands](#) of the command-line management tool.

- To view current parameter value, execute the following command:

```
$ drweb-ctl cfshow Netcheck.ExePath
```

- To set a new parameter value, execute the command

```
# drweb-ctl cfset Netcheck.ExePath <new path>
```

- To restore the parameter value to the default, execute the command

```
# drweb-ctl cfset Netcheck.ExePath -r
```

2. If the configuration does not contain settings for the component or if the error persists after entering the correct path, install or reinstall the `drweb-netcheck` package.
3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#) and be ready to name the error code.

Error message	<i>CloudD is not available</i>
----------------------	--------------------------------



Error code	x124
Description	The Dr.Web CloudD component (required to request to the Dr.Web Cloud service) is missing.
Resolving the error:	
<ol style="list-style-type: none">1. Check the path to the drweb-cloudd executable file. Change the path, if necessary (the ExePath parameter in the [CloudD] section of the configuration file). You may use the commands of the command-line management tool.<ul style="list-style-type: none">• To view current parameter value, execute the following command: <pre>\$ drweb-ctl cfshow CloudD.ExePath</pre>• To set a new parameter value, execute the command <pre># drweb-ctl cfset CloudD.ExePath <new path></pre>• To restore the parameter value to the default, execute the command <pre># drweb-ctl cfset CloudD.ExePath -r</pre>2. If the configuration does not contain settings for the component or if the error persists after entering the correct path, install or reinstall the drweb-cloudd package.3. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system. For details on how to install and uninstall the product or product components, refer to sections Installing Dr.Web for Linux and Uninstalling Dr.Web for Linux. <p>If the error persists, contact technical support and be ready to name the error code.</p>	

Error message	<i>Unexpected error</i>
Error code	x125
Description	Unexpected error occurs in operation of one of the components.
Resolving the error:	
<ol style="list-style-type: none">1. Try restart the program by executing the command <pre># service drweb-configd restart</pre> <p>If the error persists, contact technical support and be ready to name the error code.</p>	



Errors Without Codes

Symptoms	After installation of the kernel module of SpIDer Guard, operating system abnormally shuts down with a kernel error « <i>Kernel panic</i> »
Description	SpIDer Guard kernel module cannot operate in the operating system kernel environment (for example, when OS operates in the Xen hypervisor environment).
Resolving the error: <ol style="list-style-type: none">1. Cancel the load of the SpIDer Guard LKM module (the module name is <code>drweb</code>) by adding to the grub loader the following string<div><pre>drweb.blacklist=yes</pre></div>to the load settings string of the operating system kernel.2. When the OS is loaded, uninstall the <code>drweb PSB.Ko</code> kernel module from the <code>/lib/'`uname-r`'/extra</code> directory of additional kernel modules.3. Set operation mode for SpIDer Guard to <i>AUTO</i> by executing the following commands:<div><pre># drweb-ctl cfset LinuxSpider.Mode AUTO # drweb-ctl reload</pre></div>4. Do not use the Xen hypervisor, in case your operating system does not support the fanotify interface or this mode does not allow using SpIDer Guard for the full file system monitoring (relevant for GNU/Linux with mandatory access models, for example, for Astra Linux), making the use of the <i>LKM</i> mode mandatory for the file system monitoring. If the error persists, contact technical support .	

Symptoms	Main window of Dr.Web for Linux is disabled, status indicator in notification area of desktop displays an critical error mark, and drop-down menu contains only one disabled item Loading
Description	Dr.Web for Linux cannot start because core component drweb-configd is not available.
Resolving the error: <ol style="list-style-type: none">1. Uninstall Dr.Web for Linux by entering the following command:<div><pre># service drweb-configd restart</pre></div>2. If this command returns error message, or has no any effect, install <code>drweb-configd</code> component (package) separately.3. Also note that this may mean, that PAM authentication is not used in the system. If so, please install and configure it.4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.	



For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#).

Symptoms

1. The [status indicator](#) is not displayed in the notification area after the user logged in
2. When trying to execute the command

```
$ drweb-gui
```

opens the Dr.Web for Linux [main window](#).

Description

The problem could mean that necessary additional library **libappindicator1** is not installed in your system.

Resolving the error:

1. Make sure that the package `libappindicator1` is installed in your system by the following command:

```
# dpkg -l | grep libappindicator1
```

2. If the command does not output any result to screen, you should install the package, using any available system package manager. After that, log out and then log in again (*log in*).
3. Also note that this may mean, that **PAM** authentication is not used in the system. If so, please install and configure it.
4. If the previous actions do not help, uninstall Dr.Web for Linux and then install it again on the system.
For details on how to install and uninstall the product or product components, refer to sections [Installing Dr.Web for Linux](#) and [Uninstalling Dr.Web for Linux](#).

If the error persists, contact [technical support](#).

Symptoms

1. After disabling SpIDer Guard, all network connections are broken (outgoing and, may be, incoming via SSH and FTP protocols) and cannot be re-established
2. Search through the **NetFilter (iptables)** rules using the following command

```
# iptables-save | grep "comment --comment --comment"
```

returns non-empty result.

Description

This error is related to the incorrect **NetFilter (iptables)** operation, which version is earlier than 1.4.15. Because of this internal error, when SpIDer Guard adds the rules with a unique label (comment) to the list of rules, the rules are added incorrectly. As a result, on shutting down, SpIDer Guard cannot delete its rules of diverting connections.

Resolving the error:



1. Enable the SpIDer Guard monitor again
2. If you need SpIDer Guard disabled, remove the incorrect rules of **NetFilter (iptables)** by the following command

```
# iptables-save | grep -v "comment --comment --comment" | iptables-restore
```

Note that the **iptables-save** and **iptables-restore** commands require the superuser privileges. To elevate your privileges, you can use the **su** and **sudo** commands. Note also that this command removes all rules with the incorrect comments, for example, added by other applications that also perform routing traffic.

Additional information:

- To prevent this problem, it is recommended to upgrade your OS (or, at least, only **NetFilter** to version 1.4.15 or later one).
- You can also switch the diversion of connections towards SpIDer Guard into the Manual mode in the Dr.Web Firewall's settings if you want to manually divert connections towards SpIDer Guard by specifying the required rules with the help of the **iptables** utility (this way is not recommended).
- For details, refer to documentation **man: drweb-firewall(1), drweb-gated(1), iptables(8)**.

If the error persists, contact [technical support](#).

Symptoms	Double click on an icon of a file or a catalog runs the scanning in Dr.Web for Linux .
Description	The graphical shell executed an automatic association of files or catalogs after you selected the action <i>Scan</i> in Dr.Web for Linux .

Resolving the error:

1. Cancel the association between files of one type and **Dr.Web for Linux**. The associations are registered in the file `mimeapps.list` or in `defaults.list`. Files with local settings which were changed in a user profile are stored in the directory `~/.local/share/applications/` or `~/.config/` (these directories are usually appended with the attribute "hidden").
2. Open the file `mimeapps.list` or `defaults.list` with any text editor (note that to edit the files, superuser privileges are required. If necessary, use the command **su** or **sudo**).
3. In the file, find the section [Default Applications] and association strings that look as `<MIME-type>=drweb-gui.desktop`. For example,

```
[Default Applications]
inode/directory=drweb-gui.desktop
text/plain=drweb-gui.desktop;gedit.desktop
```

4. If the right part (of the equality) of the association string contains links to other applications except `drweb-gui.desktop`, remove only the following link from the line: `drweb-gui.desktop`. If the association contains link only to the application **drweb-gui**, remove the whole association line.
5. Save the changed file.

Additional information:



- To check the current associations, use the utilities **xdg-mime**, **xdg-open** , and **xdg-settings** (included in the package `xdg-utils`).
- To read more about the **xdg** utilities, refer to the documentation **man: xdg-mime(1)**, **xdg-open(1)**, **xdg-settings(1)**.

If the error persists, contact [technical support](#).



Appendix E. Building Kernel Module for SpIDer Guard

If the operating system does not support the **fanotify** monitoring interface, SpIDer Guard uses a special loadable module operating in kernel space (Linux kernel module, LKM module).

By default, SpIDer Guard is supplied with a completely built loadable kernel module for the operating systems which do not support the **fanotify** service. In addition, you can build a loadable kernel module manually using the source codes supplied in a `tar.bz2` archive.



The LKM module, used by SpIDer Guard, is intended for operation with **GNU/Linux** kernels 2.6 and newer.

The archive with source codes is located in the `share/drweb-spider-kmod/src` subdirectory of the Dr.Web for Linux base directory (by default, `/opt/drweb.com`). The archive's name is as follows: `drweb-spider-kmod-<version>-<date>.tar.bz2`. The `drweb-spider-kmod` directory also contains the `check-kmod-install.sh` test script. Run the script to check whether the used OS supports kernel module versions included in the product. If not, a message prompting to manually build the module displays on the screen.

If the specified directory `drweb-spider-kmod` is absent, [install](#) the package `drweb-spider-kmod`.



To build the LKM module manually from the source codes, administrative (root) privileges are required. For that purpose, you can use the **su** command to switch to another user or the **sudo** command to build the module as a different user.

Building the Kernel Module

1. Unpack the archive with source codes to any directory. For example, the following command

```
# tar -xvf drweb-spider-kmod-<version>-<date>.tar.bz2
```

unpacks the source codes to the created directory. This directory has the archive's name and is created in the same location where the archive resides.

2. Go to the created directory and execute the following command:

```
# make
```

If an error occurs during the `make` command execution, resolve the issue (see [below](#)) and restart compilation.

3. After successful execution of the `make` command, enter the following commands:

```
# make install  
# depmod
```



4. After the kernel module is successfully compiled and registered on the system, perform additional configuration of SpIDer Guard. Set the component to operate with the kernel module by executing the following command:

```
# drweb-ctl cfset LinuxSpider.Mode LKM
```

It is also possible to specify `AUTO` instead of `LKM`. In the latter case, SpIDer Guard will attempt to use kernel module and the monitoring interface **fanotify**. For details, refer to the documentation **man: drweb-spider(1)**.

Possible Build Errors

While the *make* command is being executed, errors may occur. If so, check the following:

- To ensure successful building of the module, **Perl** and **GCC** are required. If they are missing on the system, install them.
- On certain OSes, you may need to install the `kernel-devel` package before starting the procedure.
- On certain operating systems, the procedure can fail because the path to the directory with source codes was incorrectly defined. If so, specify the **make** command with the `KDIR=<path to kernel source codes>` parameter. Typically, the source codes are located in the `/usr/src/kernels/<kernel version>` directory.



Note that the kernel version returned by the **uname -r** command can differ from the directory name `<kernel version>`.



Index

A

About the anti-virus 9
Activation of anti-virus 91
Appendices 145
appendix
 computer threat types 145
 fighting computer threats 149
Autonomous operation of graphical interface 123

B

Black and white Lists of Websites 114
Building kernel module 199

C

Central protection 14, 119
Check of protected connections 117
Check of SSL/TLS, HTTPS 117
Command Line Parameters 122
Command-line management 123
Components 11
computer threats 145
Configuring PARSEC 63
Configuring Security Systems 59
Configuring SELinux 60
Connecting to an Anti-Virus Network 27, 119
Connecting to Dr.Web CloudD 121
Connection Settings File 27
Console uninstaller 50
Console-based installer 36
Context menu of the application 70
Conventions 7
Custom Installation of the Components 55
Custom scan 75

D

Disconnecting from Dr.Web CloudD 121
Dr.Web CloudD 121

E

EICAR 17
Elevate privileges 101
Entering serial number 91
Examples of command-line calls 141
Excluding Files and Directories 112
Exclusion from scanning 112

Exclusion of Applications 113
Exclusions 112
Express scan 75

F

fighting computer threats 149
File permissions 13
File scanning 75
File System Monitoring 81
File System Monitoring Settings 108
Files' permissions 13
Full scan 75
Functions 9

G

Get new version 90
Graphical installer 31
Graphical interface for management 66
Graphical uninstaller 48

H

Help 102
Help file 102

I

Indicator in notification area 70
Installation from .run package 29
Installation from distribution 29
Installation from native packages 38
Installation from universal packages 29
Installing Dr.Web for Linux 28, 29
Installing from the Repository 38
Introduction 8
Isolation 12

K

Key File 25, 91
Known errors 153

L

License key file 25
License Manager 91
List of exclusions 112
List of threats 85
Lower privileges 101



Index

M

Main Settings 104
Management interface 65
Managing key files 23
Managing licenses 23
Managing privileges 101
Managing Quarantine 88
Methods of Dr.Web for Linux installation 29
Mobile mode 14
Modules 11
Monitoring of network connections 83
Monitoring Settings of Network Connections 109

N

neutralizing a threat 85
Notifications 70

O

Obtaining license 91
Open Help 102
Operating systems 19
Operation mode 119
Operation modes 14

P

Parameters 103
Problems with SELinux 60
Product files 55

Q

Quarantine 12, 88
Quarantine Directories 12

R

Registration 23
Registration of license 91
Root privileges 101

S

Scan list 79
Scan tasks 79
Scanner settings 106
Scanning files from the file manager 70
Scanning settings 106
Schedule 115

Scheduled scanning 78
Scheduler scanning 115
Scheduler Settings 115
Security in SELinux 60
Settings 103
Shutting Down Graphical Interface 73
SpIDer Gate 83
SpIDer Gate settings 109
SpIDer Guard 81
SpIDer Guard settings 108
Standalone mode 14
Start updating 90
Starting command-line tool 125
Starting Graphical Interface 73
Starting uninstaller 47
Structure of the product 11
Subsequent Registration 23
System Requirements 19

T

Tasks 9
Technical support 152
Testing the Anti-virus 17
Threat detection 75
Threats 85

U

Uninstallation methods for Dr.Web for Linux 47
Uninstalling distribution 47
Uninstalling Dr.Web for Linux 28, 29, 47
Uninstalling from repository 52
Uninstalling native packages 52
Update virus databases 90
Upgrading components 42
Upgrading the Product 42
Upgrading to a Newer Version 43
Using Dr.Web CloudD 121

V

View Help 102
Viewing Quarantine 88

W

Working with Dr.Web for Linux 65

