Dr.WEB

for Linux

User Manual

© Doctor Web, 2023. All rights reserved

This document is intended for information and reference purposes regarding the Dr.Web software discussed herein. This document is not a basis for exhaustive conclusions about the presence or absence of any functional and/or technical features in Dr.Web software and cannot be used to determine whether Dr.Web software meets any requirements, technical specifications and/or parameters, and other third-party documents.

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

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 the property of their respective owners.

Disclaimer

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

Dr.Web for Linux
Version 11.1
User Manual
9/1/2023

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

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 UNIX convention will be used), install and use Dr.Web for Linux version 11.1.

If the previous version of Dr.Web for Linux is already installed on your computer and you wish to upgrade the product to version 11.1, follow the steps described in the upgrade procedure (see section Upgrading to a Newer Version).

Conventions and Abbreviations

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

Convention	Comment
❗	An important note or instruction.
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`/home/user`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

> Command-line commands, entered using a keyboard (in the terminal or a 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.

List of abbreviations is in section Appendix F. List of Abbreviations.

About this Product

This section contains the following information about the product:

- Function.
- Main Functions.
- Structure of Dr.Web for Linux.
- Placing in Quarantine.
- File Permissions and Privileges.
- Operation Modes.

Function

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 (scan 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 running 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), 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.

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 scan 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, and so on). 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 from virus databases.
   - *Heuristic analysis*, which allows detection of threats that are not present in virus databases.

- *Cloud-based threat detection technologies*, using the 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 on software activities which are not malicious. 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 with a graphical desktop environment, integration of file scanning with either the taskbar or a graphic file manager is available. For systems that implement mandatory access control with different access levels, files that are not available for a current level can be scanned as an offline copy.

All objects containing threats detected in the file system are registered in the permanently stored threats registry, except those threats that were detected in the autonomous copy mode.

The command-line tool included in Dr.Web for Linux, allows to scan for threats file systems of remote network hosts, that provide remote terminal access via SSH or Telnet.

> Remote scanning can only be used to detect malicious and suspicious files on a remote host. To eliminate the detected threats on the remote host, use administration tools provided directly by this host. For example, for routers and other smart devices, update the firmware; for computing machines, connect to them (using a remote terminal mode as one of the options) and perform the necessary operations with the file system (remove or move files, etc.), or run the anti-virus software installed on them.

2. **Monitoring access to files**. This mode tracks the access to data files and attempts to run executables. This allows you to detect and neutralize malware when it attempts to infect the computer. In addition to the standard monitoring mode, you can use the enhanced (or Paranoid) mode, so that the monitor blocks access to files until the scan is completed (this helps prevent access to files that contain a threat; however, the scan result only becomes known after the application manages to access the file). The enhanced monitoring mode increases security, but slows down the access to non-verified files for applications.
3. **Monitoring of network connections**. All attempts to access internet servers (web servers, file servers) via the HTTP and FTP protocols are monitored to block access to websites or hosts of the unwanted categories, and to prevent downloading malicious files.
4. **Scanning of email messages** to prevent receiving and sending emails containing infected files and unwanted links, as well as emails classified as spam.

   Scan of email messages and files downloaded for viruses and other threats from the web is performed on the fly. Depending on the distribution, Dr.Web Anti-Spam could be unavailable in Dr.Web for Linux. In this case, email messages will not be scanned for signs of spam.

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 CloudD service is also used to check whether the requested web resource is marked malicious by other anti-virus products of Dr.Web.

> If any email messages are falsely detected by the email anti-spam component Dr.Web Anti-Spam, we recommend you to forward them to special addresses for analysis and improvement of spam filter quality. To do that, save each message to a separate `.eml` file. Then attach the files to an email message and forward it to the special address.
>
> - nonspam@drweb.com—if it contains email files, *erroneously considered spam*;
> - spam@drweb.com—if it contains spam email files, *failed to be recognized as spam*.

5. **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.
6. **Automatic updating** of Dr.Web virus databases and of the scan engine to support a high level of protection against malware.
7. **Collection of statistics** on virus events, logging threat detection events (available only via command line tool), as well as the sending of statistics on virus incidents to Dr.Web Cloud service.
8. **Operation in the centralized protection mode** (when connected to the centralized protection server, such as Dr.Web Enterprise Server or as a part of Dr.Web AV-Desk service). This mode allows implementation of 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, 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.

Structure of Dr.Web for Linux

Dr.Web for Linux consists of the following components:

Component	Description
Scanner	A component which performs scanning of file system objects (files, directories, boot records) at user request or according to the schedule to detect threats. The user can start scanning both from a graphical mode or the command line.

Component	Description
SpIDer Guard	A resident mode component that tracks file operations (such as creating, opening, closing, and launching). It sends requests to the Scanner to scan the contents of new and modified files, as well as executable files when programs are launched. It works with the OS file system using the fanotify system mechanism or a special kernel module (*LKM, i.e. Linux Kernel Module*) developed by Doctor Web. When using the fanotify system mechanism, the monitor can operate in an enhanced mode, blocking access to not yet checked files (all types or executables only) until the scan is completed. By default, the enhanced monitoring mode is disabled.
SpIDer Gate	A component which works in a resident mode and monitors all network connections. • It checks whether the URL is present in databases of web resource categories or in user black lists; blocks access to the websites if URLs targeting them are included in a user black list or fall under categories marked as unwanted. • It blocks sending e-mail messages if they contain dangerous objects or unwanted links. • The component also sends Scanner files downloaded from the internet (from servers access to which is not restricted) and blocks downloading them if they contain threats. Additionally, if allowed by the user, the component sends requested URLs to Dr.Web Cloud service for a scan.
Scanning Engine	A core component of the anti-virus solution. It is used by Scanner to detect viruses and malicious programs as well as to analyze suspicious behavior.
Dr.Web Anti-Spam	A component which performs scanning of email messages for spam. This component is not included in versions for ARM64 and E2K architecture.
Virus databases	An automatically updated database containing information about known threats and used by the scanning engine to detect and cure them.
Database of web resource categories	An automatically updated database containing a list of web resources separated into categories and used by SpIDer Gate to block access to unwanted websites.
Updating component	A component which automatically downloads updates of virus databases, databases of web resource categories and scanning engine from Doctor Web update servers (both scheduled and on demand).
Graphical management interface	A component which 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, start receiving updates, and also configure Dr.Web for Linux operation.
Notification agent	A component which works in a background mode. It displays pop-up notifications on events and Dr.Web for Linux indicator in the notification area,

Component	Description
	runs scheduled scanning. By default it is launched when a user session starts in the desktop environment.
License Manager	A component which facilitates managing licenses in a graphical mode. It allows to activate a license or a demo period, view information about the current license, renew it, and install or remove a license key file.

Apart from those listed in the table, Dr.Web for Linux also includes additional service components running in background with no user interaction required.

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 UNIX kernel module developed by Doctor Web (compatible with any GNU/Linux-based OS with kernel 2.6.x and newer). Using LKM is not supported for ARM64 and E2K architectures.

By default, the file system monitor automatically chooses an appropriate operation mode according to the environment. If SpIDer Guard cannot be started, build and install a loadable kernel module from distributed source code.

Placing in Quarantine

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” (Quarantine)* 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
Listing all detected threats	Unrestricted. No special permission required.
Output of container contents (an archive, email file, and so on) (display only corrupted or malicious elements)	Unrestricted. No special permission required.
Moving to quarantine	Unrestricted. The user can quarantine all infected files regardless of read or write permissions on them.
Deleting threats	The user needs to have write permissions for the file that is being deleted. If threat is detected in a file located in a container (an archive, email message, and so on), its removal is replaced with moving of a container to quarantine.
Curing	Unrestricted. The access permissions and owner of a cured file remain the same after curing.

Action	Required rights
	The file can be removed if deletion can cure the detected threat.
Restoring a file from quarantine	The user should have permissions to read the file and to write to the restore directory.
Deleting a file from quarantine	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 the standalone mode and as a part of an *anti-virus network* managed by a *centralized protection server*. Operation in the *centralized protection mode* does not require installation of additional software or Dr.Web for Linux re-installation or uninstallation.

- *In the 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 the centralized protection mode*, protection of the computer is managed by the centralized 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 the centralized protection mode is received from the centralized protection server. The demo 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 centralized protection server. Updates to virus databases are also received from the centralized protection server.
- *In the 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 license key file is received from the centralized protection server.

When Dr.Web for Linux is operating in the centralized protection mode or the 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 centralized protection center is dependent on permissions specified on the server.

In the centralized 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 centralized protection server, the page for starting scanning and **Scanner** button of the Dr.Web for Linux window will be disabled.

Centralized Protection Concept

Doctor Web solutions for centralized 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 centralized protection server.

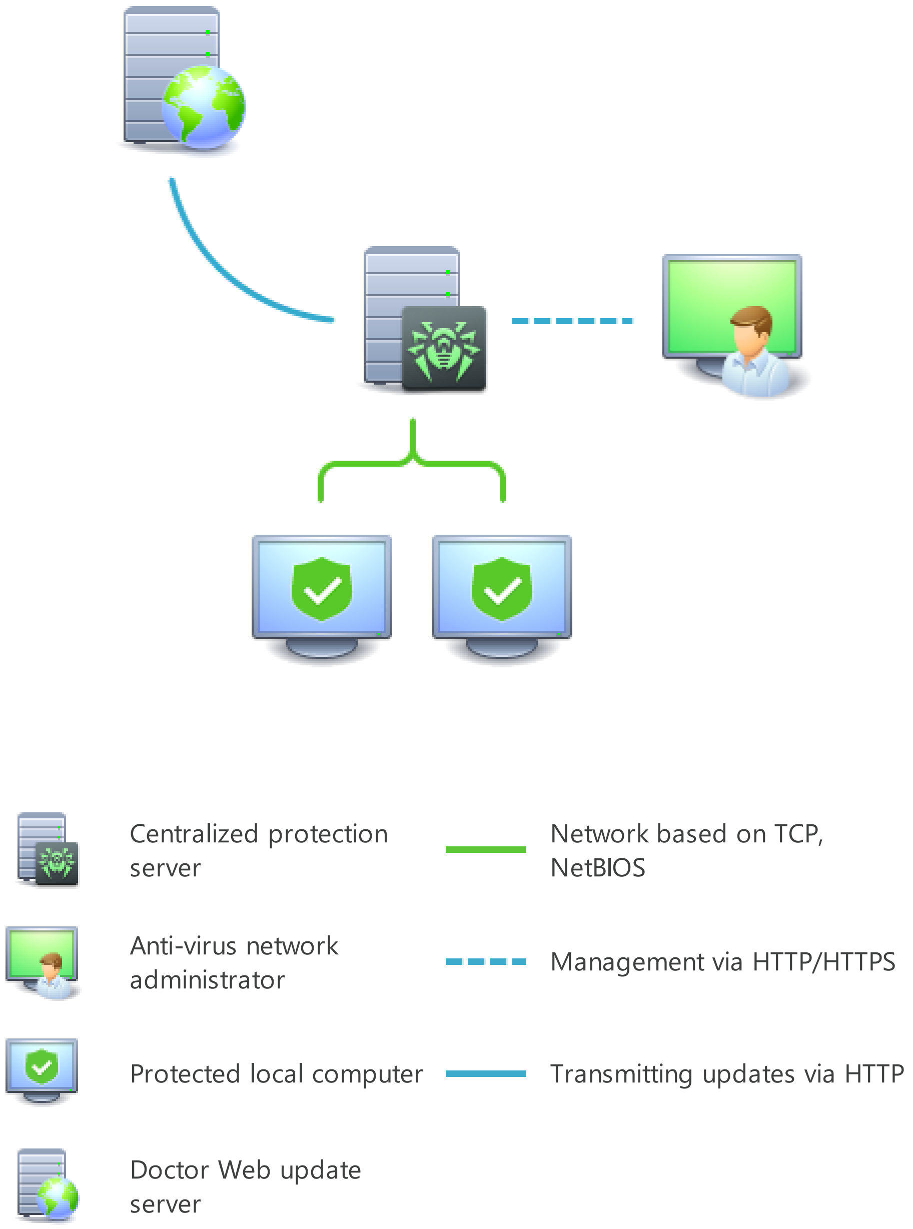

Centralized protection server
Network based on TCP, NetBIOS
Anti-virus network administrator
Management via HTTP/HTTPS
Protected local computer
Transmitting updates via HTTP
Doctor Web update server

Figure 1. Logical structure of the Anti-virus Network

Local computers are updated and configured from the *centralized protection server*. The stream of instructions, data and statistics in the anti-virus network goes also through the centralized 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 centralized protection server from Doctor Web update servers.

Local anti-virus components are configured and managed from the centralized protection server according to commands received from anti-virus network administrators. Administrators manage centralized protection servers and topology of anti-virus networks (for example, validate connections to the centralized 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 the centralized 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.

Centralized protection mode allows exporting and saving Dr.Web for Linux operation reports using the centralized protection center. Reports can be exported and saved in the following formats: HTML, CSV, PDF, and XML.

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`).

System Requirements and Compatibility

In this section:

- System Requirements.
- List of Supported Operating System Distributions.
- Required Additional Components and Packages.
- Compatibility with Components of Operating Systems.
- Compatibility with Security Subsystems.

System Requirements

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

Component	Requirement
Platform	Processors of the following architectures and command systems are supported: • Intel/AMD: 32-bit (*IA-32, x86*); 64-bit (*x86-64, x64, amd64*) • ARM64 • E2K *(Elbrus)* • IBM POWER (*ppc64el*)
Random Access Memory (RAM)	At least 500 MB of free RAM (1 GB or more recommended).
Space on hard disk	At least 2 GB of free disk space on the volume where Dr.Web for Linux directories are stored.
Operating system	UNIX based on kernel ver. 2.6.37 or later, and using PAM and `glibc` library ver. 2.13 or later, `systemd` initialization system ver. 209 or later. The supported UNIX distributions are listed below.
Other	The following valid network connections: • 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 the centralized protection mode, connection to the server on the local network is enough; connection to the internet is not required.

⚠ For the correct operation of SpIDer Gate, OS kernel must be built with inclusion of the following options:

- *CONFIG_NETLINK_DIAG, CONFIG_INET_TCP_DIAG;*
- *CONFIG_NF_CONNTRACK_IPV4, CONFIG_NF_CONNTRACK_IPV6, CONFIG_NF_CONNTRACK_EVENTS;*
- *CONFIG_NETFILTER_NETLINK_QUEUE, CONFIG_NETFILTER_NETLINK_QUEUE_CT, CONFIG_NETFILTER_XT_MARK.*

The set of required options from the specified list can depend on your distribution kit of GNU/Linux.

To ensure the correct operation of Dr.Web for Linux, open the following ports:

Purpose	Direction	Port numbers
To receive updates	outgoing	80
To connect to the Dr.Web Cloud service	outgoing	2075 (including those for UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

⚠ 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.

List of Supported Operating System Distributions

Dr.Web for Linux is supported for the following UNIX distributions:

Platform	Supported GNU/Linux versions
x86_64	• Astra Linux Special Edition 1.5 (with cumulative patch 20201201SE15), 1.6 (with cumulative patch 20200722SE16), 1.7 • Astra Linux Common Edition (Orel) 2.12 • Debian 9, 10 • Fedora 31, 32 • CentOS 7, 8 • Ubuntu 18.04, 20.04, 22.04 • ALT Workstation 9, 10 • ALT Server 9, 10 • ALT 8 SP

Platform	Supported GNU/Linux versions
	• RED OS 7.2 MUROM, RED OS 7.3 MUROM • GosLinux IC6 • SUSE Linux Enterprise Server 12 SP3 • Red Hat Enterprise Linux 7, 8
x86	• CentOS 7 • Debian 10 • ALT Workstation 9, 10 • ALT 8 SP
ARM64	• Ubuntu 18.04 • CentOS 7, 8 • ALT Workstation 9, 10 • ALT Server 9, 10 • ALT 8 SP • Astra Linux Special Edition (Novorossiysk) 4.7
E2K	• Astra Linux Special Edition (Leningrad) 8.1 (with cumulative patch 8.120200429SE81) • ALT 8 SP • Elbrus-D MCST 1.4 • GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	• CentOS 8; • Ubuntu 20.04

⚠ In ALT 8 SP and GosLinux 7.1 mandatory access control is not supported.

For other UNIX distributions that meet the abovementioned requirements full compatibility with Dr.Web for Linux is not guaranteed. If a compatibility issue occurs, contact technical support.

Required Additional Components and Packages

- To enable Dr.Web for Linux operation in graphical mode and startup of the program for 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 installer or uninstaller, designed for the command line, in graphical mode, a terminal emulator (such as xterm, xvt, and so on) 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 Dr.Web for Linux, 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 your command shell (if disabled).
>
> If you encounter any problem with installation of additional packages and components, refer to manuals for your 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 Dr.Web for Linux 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.
  For ARM 64 and E2K achitectures the work with the LKM is not supported.

> 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 Guard can operate in the enhanced (Paranoid) mode, which blocks access to the files that have not been scanned yet, only via fanotify and providing that an OS kernel is built with the enabled `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` option.

- 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 your 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 NetFilter, and looks like as follows: after disabling SpIDer Gate, the network connections are broken and cannot be re-established. If you face this problem, it is recommended that you upgrade your OS to a version that includes NetFilter 1.4.15 or above. The ways to resolve the problem are described in the section "Description of 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).

To install Dr.Web for Linux on systems with SELinux (as well as systems that use mandatory access control models), you may require to configure a security subsystem, so that Dr.Web for Linux operates in full functionality mode. For details, refer to the section Configuring Security Subsystems.

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 Dr.Web for Linux 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 you correctly activate the demo period, you gain the rights to use the installed copy of 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 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 of a demo period is expired), anti-virus functions of Dr.Web for Linux 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 centralized 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 centralized protection server.

Installing and Uninstalling

This section describes how to install and uninstall the Dr.Web for Linux version 11.1. 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 Dr.Web for Linux components (for example, to resolve errors that occurred during the program operation or to get an installation with a limited function set) and configuration of advanced security subsystems (such as SELinux) that could be necessary for installation and operation of Dr.Web for Linux.

- Installing Dr.Web for Linux.
- Upgrading Dr.Web for Linux.
- Uninstalling Dr.Web for Linux.
- Configuring Security Subsystems.
- Additional information:
  - Dr.Web for Linux Files Location.
  - Custom Component Installation and Uninstallation.

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.

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), make sure that the version of the installed product is the *same* as the version of Dr.Web for Linux you want to install. If the version that you plan on installing is newer that the installed product version, *before* installation update the installed Dr.Web 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.

> In distributions using the outdated versions of the package manager (for instance, ALT 8 SP) it is recommended to install the universal package.

> 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 centralized protection server. Anti-virus protection *will be disabled* unless you do that.
>
> ---
>
> If a mail client using IMAP for receiving messages (for instance, Mozilla Thunderbird) is running on your system, restart it after the antivirus is installed so that incoming email messages could be scanned.

After you installed Dr.Web for Linux 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 UNIX for correct operation of Dr.Web for Linux. If there is a problem with functioning of any individual components, you can perform their custom installation and uninstallation, without uninstalling Dr.Web for Linux.

Installing the Universal Package

Dr.Web for Linux is distributed as an installation file named `drweb-<`*version*`>-av-linux-<`*platform*`>.run`, where <*platfrom*> is a platform for which the product is intended (for 32-bit platforms—`x86`, for 64-bit platforms—`amd64`, `arm64` and `e2s`). For example:

```
drweb-11.1-av-linux-amd64.run
```

Then, the name of the installation file will be specified 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.

   > If you install Dr.Web for Linux on the Astra Linux SE OS of versions 1.6 and 1.7 operating in the *CSE* mode, the installer could fail to start because the Doctor Web public key is not on the list of trusted keys. In this case, configure the CSE mode (see Configuring the Launch in the CSE Mode (Astra Linux SE 1.6 and 1.7)) and start the installer again.

   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 `TMPDIR` 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 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 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 Dr.Web for Linux 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 UNIX distribution you use features the SELinux security subsystem, it can interrupt the installation process. If such situation occurs, temporarily 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 Dr.Web for Linux or its components without the need to update its 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 the graphical mode.
- **Remove Dr.Web components** item to uninstall the components.

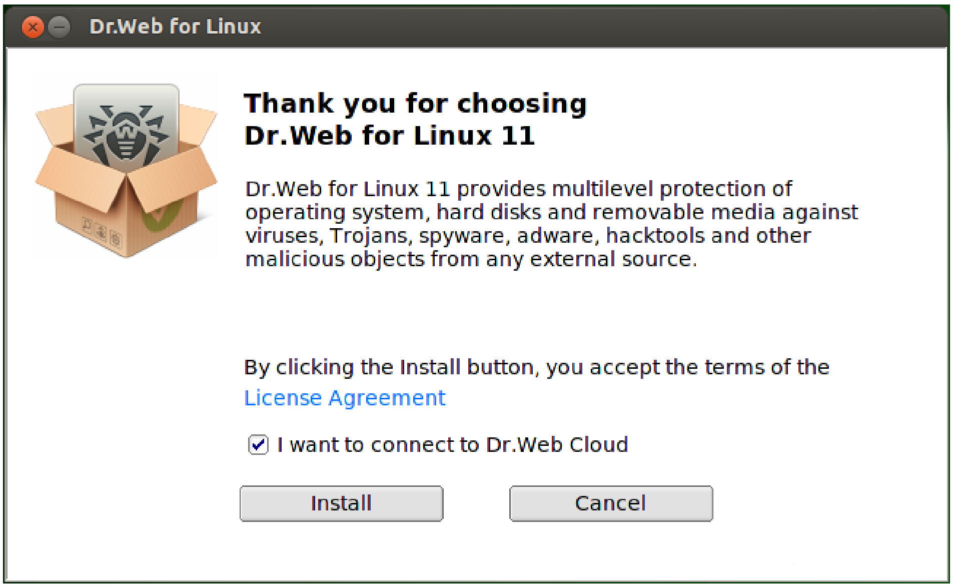
The program indicator automatically appears in the notification area after the user logs in again.

> For correct operation of Dr.Web for Linux, it may be necessary to install packages specified in the System Requirements and Compatibility 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 the 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 can 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.



Thank you for choosing Dr.Web for Linux 11

Dr.Web for Linux 11 provides multilevel protection of operating system, hard disks and removable media against viruses, Trojans, spyware, adware, hacktools and other malicious objects from any external source.

By clicking the Install button, you accept the terms of the License Agreement

☑ I want to connect to Dr.Web Cloud

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.

   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 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 **Details**.

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.

6. To exit the Installation Wizard, click **OK**. If the desktop environment you are using supports this feature, at the final installation step you will be prompted to launch Dr.Web for Linux in the graphical mode. To run the program after installation, set the **Run Dr.Web for Linux now** flag and click **OK**.

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 the 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?” request. To exit the installer, enter *No* or *N*. In this case, installation will be canceled.
2. After that, you need to review the terms of the Doctor Web License Agreement, 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 available.
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.
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.
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.
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, resolve the problems that caused this error and start an installation procedure again.

Installing from the Repository

Dr.Web for Linux 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 package manager, you can install the product from native packages as you install any other programs from the operating system 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).

See below the procedures for the following OS (package managers):

- Debian, Mint, Ubuntu (apt).
- ALT Linux, PCLinuxOS (apt-rpm).
- Mageia, OpenMandriva Lx (urpmi).
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf).
- SUSE Linux (zypper).

Debian, Mint, Ubuntu (apt)

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
8C42FC58D8752769
```

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

```
deb https://repo.drweb.com/drweb/debian 11.1 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/drweb-repo11.1.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 11.1/<arch> drweb
   ```

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

   - for the 32-bit version: `i386`;
   - for the AMD64 architecture: `x86_64`;
   - for the ARM64 architecture: `aarch64`;
   - for the E2K architecture: `e2s`.

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/linux/11.1/<arch>/
   ```

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

   - for the 32-bit version: `i386`;
   - for the 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 - 11.1
baseurl=https://repo.drweb.com/drweb/linux/11.1/$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/drweb-repo11.1.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 https://repo.drweb.com/drweb/linux/11.1/\$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

Dr.Web for Linux has two update modes:

1. Getting updates of packages and components released in the course of operation of the current Dr.Web for Linux 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 Dr.Web for Linux, and it has new features.

Getting Current Updates

In this section:

- Updating online.
- Updating offline.

Updating online

After installation of Dr.Web for Linux 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 Dr.Web for Linux 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 Dr.Web for Linux 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).

Updating offline

In highly secure environments where internet connection is blocked or limited, it is possible to update virus bases offline. You need to download updates to a computer connected to the internet, copy them to a USB drive or local network share and then install them to another computer (which is not connected to the internet).

The update procedure has to be run from the command line.

In order to get the updates:

1. Run the following command on a computer connected to the internet:

   ```
   $ drweb-ctl update --Path <a path to a directory to store updates>
   ```

2. Copy the downloaded updates to a USB drive or local network share.

3. Mount the local network share or removable drive on the computer to be updated. If the updates are from the USB drive, run the following commands:

   ```
   # mkdir /mnt/usb
   # mount <a path to the device> /mnt/usb
   ```

4. Apply the updates with the following command:

   ```
   $ drweb-ctl update --From /mnt/usb
   ```

Upgrading to a Newer Version

Introductory Remarks

The upgrade procedure for previous Dr.Web for Linux versions to version 11.1 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 Dr.Web for Linux version was installed from the repository, an upgrade requires updating program packages from the repository.
- If the current Dr.Web for Linux version was installed from the universal package, then to upgrade the product, you need to install another universal package that contains a newer version.

> 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 11.1. 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 11.1 can be performed *only* by uninstalling the outdated Dr.Web for Linux and installing the version 11.1.

If the current version of Dr.Web for Linux is operating in the centralized protection mode, it is recommended that you record the address of the centralized 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

```
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 certificate file.

In case there are any problems with finding out the parameters of the connection that you are currently using, refer to the Administrator Manual for the Dr.Web for Linux 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 11.1 from the installation file. If necessary, during the installation 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 repository, do one of the following, depending on the required type of packages:

- **In case of using RPM packages (yum)**:
  1. Change the repository (from the package repository of your current version to the package repository 11.1).

     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 your 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 Dr.Web for Linux. If necessary, see sections Uninstallation of Dr.Web for Linux 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 repository (from the package repository of your current version to the package repository 11.1).
  2. Upgrade the Dr.Web for Linux packages by entering 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 Centralized Protection Server

If possible, after upgrading Dr.Web for Linux, if the upgraded version was connected to the centralized 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) to connect the upgraded Dr.Web for Linux version to the anti-virus network:

- Select the check box on the **Mode** tab of the Dr.Web for Linux settings window.
- Use the command:

```
$ drweb-ctl esconnect <address> --Certificate <path to the server certificate file>
```

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 using IMAP for receiving messages (for instance, Mozilla Thunderbird) is running on your system, restart it after the antivirus is installed so that incoming email messages could be scanned.

Upgrading Version 6.0.2 and Older

Upgrade of Dr.Web for Linux from version 6.0.2 and older to version 11.1 can be performed only by uninstalling the outdated Dr.Web for Linux version and installing version 11.1. 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 11.1 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 lower) uses as quarantine the following directories:

- `/var/drweb/infected`—system quarantine;
- `/home/`*<user>*`/.drweb/quarantine`—user quarantine (where *<user>* is 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 the 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 Dr.Web for Linux 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 Dr.Web for Linux via the Command Line

To uninstall Dr.Web for Linux, 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 the 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.

On ALT 8 SP you may see the following messages appear when the universal package is being uninstalled:

```
/etc/init.d/drweb-configd: No such or directory
```

These messages do not affect the functioning of the system. The uninstallation procedure is performed correctly.

Uninstalling the Product in the Graphical Mode

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

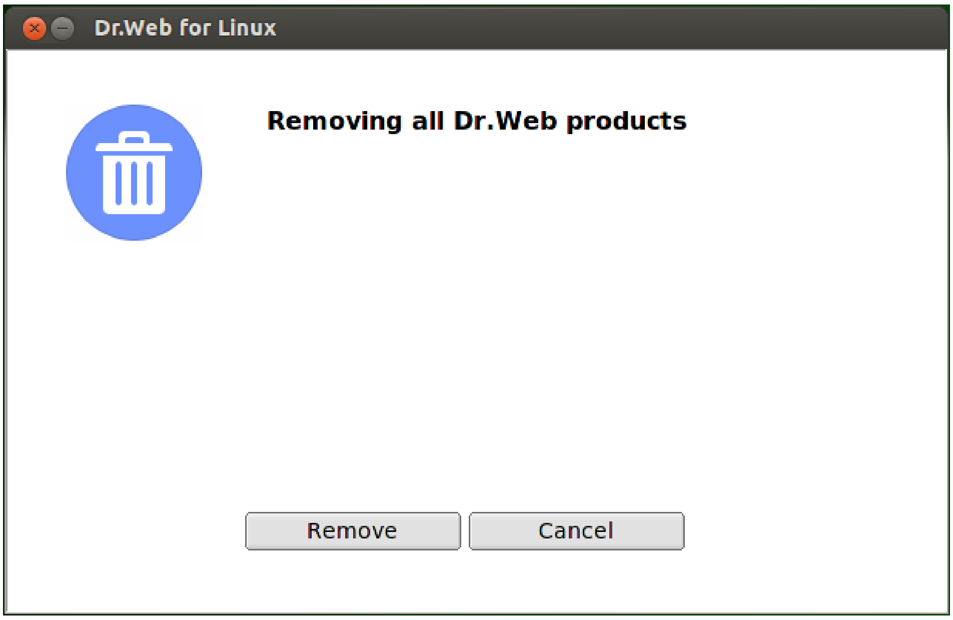


Figure 3. Welcome page

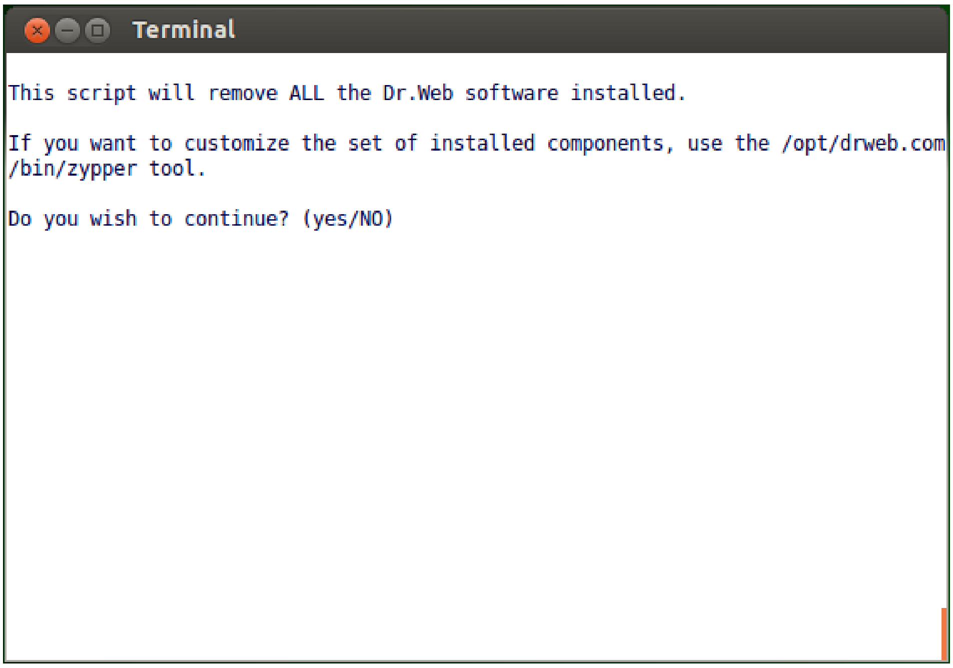
1. To uninstall Dr.Web products, click **Remove**. To close the Uninstallation Wizard and discontinue the removal of Dr.Web products from your computer, click **Cancel**.

2. After the uninstallation starts, a page with the progress bar opens. To view the log, click **Details**.
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.
4. To close the Uninstallation Wizard, click **OK**.

Uninstalling from the Command Line

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

1. To initiate the removal, enter *Yes* or *Y* in response to the "Do you want to continue?" request. To exit the uninstaller, type *No* or *N*. In this case, removal of Dr.Web products will be canceled.



```
This script will remove ALL the Dr.Web software installed.

If you want to customize the set of installed components, use the /opt/drweb.com
/bin/zypper tool.

Do you wish to continue? (yes/NO)
```

Figure 4. Offer to uninstall the product

2. An automatic uninstallation procedure of all installed Dr.Web packages will be launched after you confirm it. During this procedure, information about the removal process will be displayed on the screen and entered into the uninstallation log.
3. Once the process is completed, the uninstallation program will automatically terminate.

Uninstallation of Dr.Web for Linux 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).

See below the procedures for the following OS (package managers):

- Debian, Mint, Ubuntu (apt),
- ALT Linux, PCLinuxOS (apt-rpm),
- Mageia, OpenMandriva Lx (urpmi),
- Red Hat Enterprise Linux, Fedora, CentOS (yum, dnf),
- SUSE Linux (zypper).

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 root meta-package together with all dependencies perform the following command:

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

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 package managers (for example, Synaptic or aptitude) to uninstall the Dr.Web for Linux 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 package managers (for example, Synaptic or aptitude) to uninstall the Dr.Web for Linux packages.

On ALT 8 SP you may see the following messages appear when the universal package is being uninstalled:

```
/etc/init.d/drweb-configd: No such or directory
```

These messages do not affect the functioning of the system. The uninstallation procedure is performed correctly.

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 package managers (for example, rpmdrake) to uninstall the Dr.Web for Linux 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 specified 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 package managers (for example, PackageKit or Yumex) to uninstall the Dr.Web for Linux 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 package managers (for example, YaST) to uninstall the Dr.Web for Linux packages.

Additional Information

Dr.Web for Linux 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 directories

Directory	Contents
`/opt/drweb.com`	Executable files of components and main libraries necessary for Dr.Web for Linux operation.
`/etc/opt/drweb.com`	Component setting files (by default) and a license key file for Dr.Web for Linux operation in the standalone mode.
`/var/opt/drweb.com`	Virus databases, scan 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 Dr.Web for Linux 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.

Dr.Web for Linux Component Installation and Uninstallation:

- installed from the repository;
- installed from the universal package.

1. Installation and Uninstallation of Dr.Web for Linux Components Installed from Repository

If Dr.Web for Linux 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 Dr.Web for Linux installed on CentOS, use the command:

```
# yum remove drweb-gated
```

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

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

   If needed, use help on package manager used in your OS.

2. Installation and Uninstallation of Dr.Web for Linux Components Installed from the Universal Package

If Dr.Web for Linux 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 Dr.Web for Linux was installed. If you did not save this file, download it from the Doctor Web official website.

Unpacking the Installation File

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

`--noexec`—unpack Dr.Web for Linux 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 Dr.Web for Linux installation files and the installation log automatically after the installation completes.

`--target` *<directory>*—unpack Dr.Web for Linux 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 custom installation of Dr.Web for Linux components, you need to use the unpacked Dr.Web for Linux installation files. If there is no directory containing these files, 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>*, containing the unpacked Dr.Web for Linux files.

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 release, and *<platform>* is a platform for which Dr.Web for Linux is intended. Names of all the packages containing the components of Dr.Web for Linux start with the “drweb” prefix.

The `zypper` package manager is enabled for the installation of packages to the installation kit. For the custom installation, use a service script `installpkg.sh`. To do that, first, unpack the contents of the installation package to any 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 Dr.Web for Linux installation, launch the automatic installation script. To do that, use the following command:

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

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

```
# ./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 remove drweb-gated
```

If your OS uses DEB packages, use the package manager `zypper`, which is automatically installed within Dr.Web for Linux installation, for the custom uninstallation. 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 you need to uninstall Dr.Web for Linux, launch the automatic removal script. To do this, enter 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 Subsystems

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 following settings that ensure correct operation of Dr.Web for Linux:

- Configuring SELinux Security Policies.
- Configuring the permissions of the PARSEC mandatory access control system (the Astra Linux SE OS).
- Configuring the launch in the CSE (Closed Software Environment) mode (OS Astra Linux SE 1.6 and 1.7).

> ⚠ 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 components, 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 it as an autonomous copy, you will need a valid key file, working in Centralized protection mode is not supported (an option to install the key file, exported from the centralized protection server, is available). In this case, even if Dr.Web for Linux is connected to the centralized protection server, the autonomous copy *does not notify* the centralized 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 will be launched as the current user and will work with a configuration file, separately generated for this session.
- All 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 file scanning and quarantine management functions, supported by Scanner, are available.

- All the required paths (to virus databases, scan engine and executable files of the service components) are defined by default or retrieved from the special environment variables.
- The number of the autonomous copies working simultaneously is not limited.
- When the autonomous copy is shut down, the set of servicing components is also terminated.

Configuring SELinux Security Policies

If the UNIX distribution features SELinux (*Security-Enhanced UNIX*), you may need to configure SELinux security policies to enable correct Dr.Web for Linux component operation (for example, operation of the scan 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.

If installation of Dr.Web for Linux from the file (`.run`) fails due to inability to create the *drweb* user, check the SELinux operation mode with the `getenforce` command. The command outputs the current scanning mode:

- *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 the its settings (file with SELinux settings usually resides in the `/etc/selinux` directory).

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

```
# setenforce 1
```

2. Dr.Web for Linux 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).

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 UNIX 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 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 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 Red Hat 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 this 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 `audit2allow` 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 Red Hat Enterprise Linux and CentOS, 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.

Usage example:

```
# 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 your UNIX distribution.

Configuring the PARSEC Permissions

In Linux distributions equipped with PARSEC security subsystem, the access of all applications to files depends on their privilege level.That is why SpIDer Guard can intercept file-access events as far as its privilege level allows.

Moreover, if the user works at any privilege level other than the zero, 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; the access to the consolidated quarantine may also become unavailable.

In case if PARSEC is used in OS and user accounts working at privilege levels other than zeroth, are present, you need to customize Dr.Web for Linux in order to ensure that its components run at different privilege levels.

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

- Customizing of interaction of the components that are run at the different privilege levels.
- Customizing the automatic launch of the Dr.Web for Linux components with the user privileges.
- Configuring SpIDer Guard for file access events interception.

> 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.

Customizing of interaction of the components that are run at the different privilege levels

For OS Astra Linux SE of version 1.6

Modify the `/etc/parsec/privsock.conf` system file to authorize the Dr.Web for Linux configuration daemon (`drweb-configd`) to use the *privsock* mechanism. `drweb-configd` is Dr.Web for Linux service component that is responsible for interaction of all anti-virus components between each other. The *privsock* mechanism is designed for the operation of system network services that do not process information using the mandatory context but interact with processes that operate in the mandatory context of an access subject. To do this, proceed as follows:

1. Open the `/etc/parsec/privsock.conf` file in any text editor. Add the following lines:

   ```
   /opt/drweb.com/bin/drweb-configd
   /opt/drweb.com/bin/drweb-configd.real
   ```

2. Save the file and restart the operating system.

For OS Astra Linux SE of version 1.5 and earlier

Modify the Dr.Web for Linux (`drweb-configd`) configuration daemon launch script. 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.
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 restart the operating system.

Customizing the automatic launch of the components with user privileges

To make Dr.Web for Linux components with which the user interacts available in the user environment (when the user works at a privilege level other than zero), you need to make changes to the files containing PAM settings to ensure the automatic launch of the required Dr.Web for Linux components at the beginning of the user session and their termination at the end of the session. The module (the special `pam_drweb_session.so` PAM module by Doctor Web launches the `drweb-session` mediation component, which connects the local copies of components run in the user environment with the components operating at zero-level privilege and autorun on OS startup).

To change PAM settings, we recommend that you use the `drweb-configure` configuration utility, included in Dr.Web for Linux, or you can make manual changes to the necessary configuration files.

1. Using the drweb-configure utility

To make configuring complex parameters of Dr.Web for Linux more convenient, we have developed the special auxiliary utility `drweb-configure`.

1. To enable or disable the automated launch of the necessary Dr.Web for Linux components in the user environment when it is running at a privilege level other than zero, use the following command:

   ```
   $ sudo drweb-configure session <mode>
   ```

   where <*mode*> may have one of the following values:

   - `enable`—enables the automated launch of the necessary components during the user session with the appropate privileges.
   - `disable`—disables the automated launch of the necessary components during the user session with the appropate privileges (it will render a number of Dr.Web for Linux functions unavailable).

2. Restart the system.

   To use help on how to use `drweb-configure` for configuring PAM settings, use the following command:

   ```
   $ drweb-configure --help session
   ```

2. Manual modification of PAM configuration

For Astra Linux and other distributions using the pam_parsec_mac.so PAM module

1. To change PAM configuration, you need to modify all configuration files in `/etc/pam.d` directory which launch the `pam_parsec_mac.so` PAM module. You can get the list of such files by performing the following command:

```
# grep -R pam_parsec_mac.so /etc/pam.d
```

Add the following records of *session* type to all files from the list:

- Before the first records of *session* type:

```
session optional pam_drweb_session.so type=close
```

- After the last record of *session* type:

```
session optional pam_drweb_session.so type=open
```

2. Save the changed files.
3. Create a symbolic link to the `pam_drweb_session.so` file from the system directory containing PAM modules. The `pam_drweb_session.so` file is located in the Dr.Web for Linux library directory (`/opt/drweb.com/lib/`); in 64-bit operating systems, for instance, the path to the module is `/opt/drweb.com/lib/x86_64-linux-gnu/pam/`.
4. Reboot the operating system.

For ALT 8 SP and other distributions using the pam_namespace.so PAM module

1. To change PAM configuration, you need to modify all configuration files in `/etc/pam.d` directory which launch the `pam_namespace.so` PAM module. You can get the list of such files by performing the following command:

```
# grep -R pam_namespace.so /etc/pam.d
```

2. Add *session*-type records same as the records for distributions using the `pam_parsec_mac.so` PAM module (see the paragraph above) to each file.

Configuring SpIDer Guard for file access events interception

To give the SpIDer Guard file monitor an ability to detect the attempts of accessing files, which have any level of access privileges, you need to switch SpIDer Guard to the *Fanotify* operating mode.

To switch SpIDer Guard to the *Fanotify* operating mode, execute the following command:

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

To get additional information, use the following command:

```
$ man drweb-spider
```

Configuring the Launch in the CSE Mode (Astra Linux SE 1.6 and 1.7)

The OS Astra Linux SE supports a special *closed software environment* (CSE) mode. In the mode, applications can be launched only if their executable files are signed with the developer digital signature. The developer’s public key must be added to the OS list of trusted keys.

By default, Dr.Web for Linux components supplied for Astra Linux SE are signed with the Doctor Web digital signature and the public key for the signature is automatically added to the list of trusted keys during the application installation therefore Dr.Web for Linux should be launched correctly when activating CSE mode in Astra Linux SE 1.5 and earlier versions.

However, in Astra Linux SE 1.6, the signature mechanism has been changed. To launch Dr.Web for Linux in the CSE mode in Astra Linux SE 1.6 and 1.7, configure the OS.

Configuring Astra Linux SE 1.6 and 1.7 to Launch Dr.Web for Linux in the CSE Mode

1. Install the package `astra-digsig-oldkeys` using the OS installation disk if it is not installed yet.
2. Add the Doctor Web public key to the directory `/etc/digsig/keys/legacy/keys` (if the directory is absent, create it):

   ```
   # cp /opt/drweb.com/share/doc/digsig.gost.gpg /etc/digsig/keys/legacy/keys
   ```

3. Execute the command:

   ```
   # update-initramfs -k all -u
   ```

4. Reboot the operating system.

Getting Started

1. Activate Dr.Web for Linux.
2. Ensure its proper operation.
3. Set the file monitoring mode.
4. Specify exclusions, if any.

Registration and Activation

In this section:

- Purchasing and Registering License.
- Dr.Web for Linux Activation:
  - Demo Period.
  - Key File Installation.
  - Connection to the centralized protection server.
- Repeated Registration.

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 options, visit the Doctor Web official website at https://license.drweb.com/.

License registration is required to prove that you are a legal user of Dr.Web for Linux and activate the anti-virus functions, including the regular updates of virus databases. We recommend that you register the product and activate the license once the installation is completed.

Dr.Web for Linux Activation

A license can be activated one of the following ways:

- Via the Registration Wizard included in License Manager.
- On the Doctor Web official website at https://products.drweb.com/register/.

To activate or renew the license, you need to enter the serial number. The serial number is supplied with Dr.Web for Linux 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, all licenses will be combined and license validity period will be automatically extended.

Demo Period

Users of Dr.Web can obtain a demo period for 1 month. It can be received in the Registration wizard window of License Manager without providing personal data.

The Registration Wizard of License Manager opens upon the first Dr.Web for Linux startup (usually the Registration Wizard starts once installation of Dr.Web for Linux completes). You can start registration from the License Manager window at any time by clicking **Get new license** 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.

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 will be sent to you by email and you will need to install it manually.

If the registration wizard is unavailable (for example, if the operating system has no GUI), you can use the command for license management of the command-line interface `drweb-ctl`, which allows you to obtain the license key file corresponding to the serial number of the registered license. The description of the `drweb-ctl` utility can be found in User Manual.

> The full version of the Dr.Web for Linux User Manual is available:
>
> - On the Doctor Web official website at https://download.drweb.com/doc/ (an internet connection is required).
> - As a PDF file in the folder `/opt/drweb.com/share/doc` (a suffix in the file name indicates a language of the manual).

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
  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 the 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 to the centralized protection server

If the internet service provider or network administrator submits a file with settings for connecting to the centralized protection server, you can activate Dr.Web for Linux by specifying the file path. This can be done as follows:

- In the open program settings window, go to the **Mode** tab and select the **Enable centralized 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**.

Repeated Registration

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

A license key file can be obtained through the License Manager or the license management command a limited number of times. If that amount has been exceeded, you can confirm the registration of your serial number at https://products.drweb.com/register/ to receive the key file. The key file is sent to the email that was specified during the first registration.

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 Dr.Web for Linux 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).

Connection Settings File

The connection settings file is a special file that stores parameters that configure connection between Dr.Web for Linux and the centralized 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 centralized protection server (in this case, you cannot use Dr.Web for Linux in the standalone mode without purchasing additional license).

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 Dr.Web for Linux by means of EICAR test from the command line:

```
$ tail /opt/drweb.com/share/doc/drweb-se/readme.eicar | grep X5O > testfile
&& drweb-ctl scan testfile && rm testfile
```

This command sets off from the file `/opt/drweb.com/share/doc/drweb-se/readme.eicar` (supplied with Dr.Web for Linux) 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 directory. 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.

File Monitoring Modes

General Information

File system monitor SpIDer Guard that controls access to files may use three monitoring modes:

- *Regular* (set by default)—SpIDer Guard monitors file access (creation, opening, closing, and running) and requests the file scanning. If a threat is detected upon the scan, an action is applied to neutralize the threat. Apps are allowed to access the file until the file scanning is finished.
- *Enhanced control of executable files*—SpIDer Guard monitors files considered as non-executable like in the regular mode. Access to files that are considered as executable is blocked at the access attempt until the file scanning is finished.

> Executable files are binary files of formats PE and ELF as well as text script files containing the "`#!`" preamble.

- *"Paranoid" mode*—SpIDer Guard blocks access to a file at any access attempt until the file scanning is finished.

Scanner stores file scan results in a special cache for a certain time, so when re-accessing the same file, the file is not rescanned if there is information in the cache, and this data is displayed instead of a scan result. Despite this, the use of the Paranoid monitoring mode leads to a significant slowdown in accessing files.

Switching Between File Monitoring Modes

> The modes for enhanced monitoring of files and pre-blocking are only available if SpIDer Guard works in the `FANOTIFY` mode and the OS kernel is built with the option `CONFIG_FANOTIFY_ACCESS_PERMISSIONS` enabled.
>
> Switching between the monitoring modes for SpIDer Guard is performed using the `cfset` command of the `drweb-ctl` utility.
>
> To switch between SpIDer Guard monitoring modes, administrative (root) privileges are required. To obtain them, you can use the `su` command to switch to another user or the `sudo` command to perform the action as a different user.

- To switch SpIDer Guard into the `FANOTIFY` mode, use the following command:

```
$ sudo drweb-ctl cfset LinuxSpider.Mode FANOTIFY
```

- To change the monitoring mode, use the command:

```
$ sudo drweb-ctl cfset LinuxSpider.BlockBeforeScan <mode>
```

  where <*mode*> defines the blocking mode:

  - `Off`—access is not blocked, SpIDer Guard operates in regular (not blocking) monitoring mode.
  - `Executables`—access to executable files is blocked, SpIDer Guard enhances monitoring of executable files.
  - `All`—access to all files is blocked, SpIDer Guard monitors files in “paranoid” mode.

- To change the validity period for the file scan results in the cache, use the command:

```
$ sudo drweb-ctl cfset FileCheck.RescanInterval <period>
```

  where the <*period*> parameter determines the validity period for scan results, stored in the cache. It can have a value from `0s` through `1m`. If you set an interval smaller than 1 second, there will be no delay and files will be scanned upon any request.

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 graphical interface for management, 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 interface for management 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 arguments.
- 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 taskbar (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.
- For details on enabling enhanced file monitoring by SpIDer Guard, refer to File Monitoring Modes.

> Regardless of the selected way to install Dr.Web for Linux, after the installation you need either to activate the license or install the key file if already obtained, or connect Dr.Web for Linux to the centralized protection server (see Registration and Activation). 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 the Graphical Mode

In this section:

- General Information.
- Notification Agent.
- Graphical Management Interface.

General Information

Two components are responsible for Dr.Web for Linux 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 Dr.Web for Linux 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 it.
- 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 operation.

Notification Agent

The Dr.Web for Linux 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 are 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).

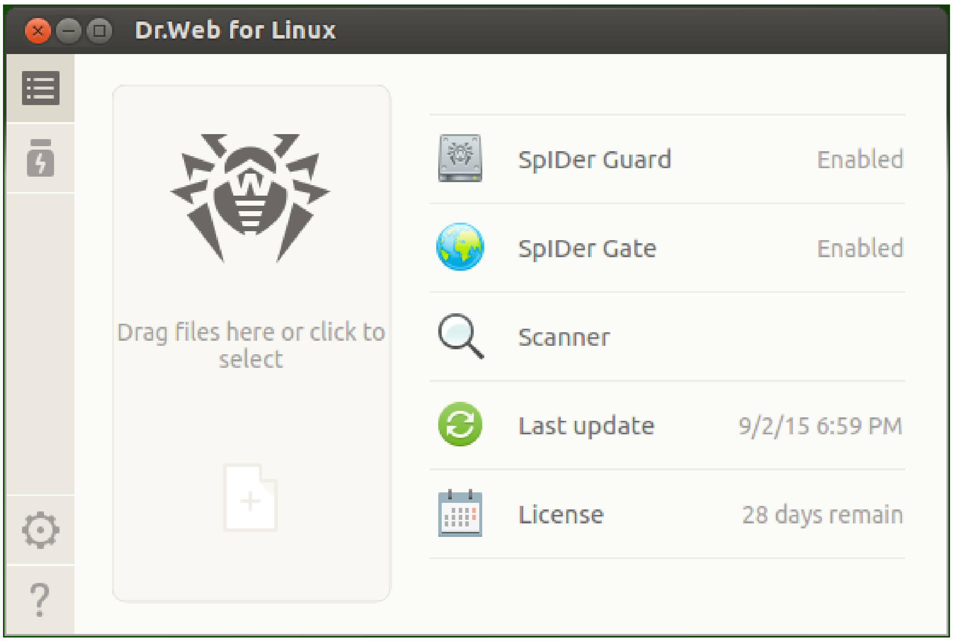
You can select the files to be scanned by specifying target directories and files before scanning and by dragging and dropping them with the mouse from the window of the file manager to the main page (see below) or to the **Scanner** page of the Dr.Web for Linux window.

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 are not scanned by the Scanner and are not 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 centralized 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).
9. Viewing messages on state of the anti-virus network that are sent by the centralized protection server (if only Dr.Web for Linux operates in the anti-virus network and your anti-virus network administrator configures the corresponding setting on the centralized protection server).

> 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 main window of the graphical management interface is shown in the figure below.



SpIDer Guard Enabled

SpIDer Gate Enabled

Scanner

Last update 9/2/15 6:59 PM

License 28 days remain

Figure 5. Dr.Web for Linux 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
1. Continuously Enabled	
☰	Opens the main page where you can • 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.
▯	Opens the quarantine page, where you can view the files moved to the quarantine and delete or restore them, if necessary.
⚙	Opens Dr.Web for Linux settings window, in particular: • Scanner of file system objects. • The file system monitor SpIDer Guard. • Monitoring of SpIDer Gate network connections.

Button	Description
	• Start scanning as scheduled. In addition, you can configure the settings of the centralized protection mode.
?	Provides access to reference materials and supportive Doctor Web resources: • Product information. • User manual. • Dr.Web Forum. • Technical support. • Personal user webpage **My Dr.Web**. All links are opened in the browser installed in your system.
2. Visible Depending on Certain Conditions	
◙	Opens the page of the scanning task list, where you can find uncompleted (running) scanning tasks. *It is situated on the navigation panel only if scanning is performed.*
✓ ⚡ !	Opens the page with the list of completed scans. The button changes its color depending on the scanning results: 1. Green—all scannings 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. *It is displayed in the navigation pane only if at least one scanning was started.*
⚡	Opens the page with threats detected by Scanner or by the file system monitor SpIDer Guard. *It is displayed in the navigation pane only if at least one threat was detected.*
🔍	It is displayed in the navigation pane only if the scanning start page is open and active. *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.*
🖵	It is displayed in the navigation pane only if the SpIDer Guard control page is open and active. *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.*
🌐	It is displayed in the navigation pane only if the SpIDer Gate control page is open and active. *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.*
🔄	It is displayed in the navigation pane only if the update control page is open and active.

Button	Description
	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.
📅	It is displayed in the navigation pane only if the License Manager control page is open and active. *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.*
💬	Opens the message view page from the centralized protection server. *It is displayed in the navigation pane only if Dr.Web for Linux operates in the centralized protection mode and the anti-virus network administrator enables message sending to the workstation.*

Main Page

On the main page of Dr.Web for Linux 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, directories, 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 icon in the desktop notification area. The indicator allows you to show the application context menu and view the popup notifications;
- Calling of the context menu with basic scan commands when user right-clicks on the application icon in the taskbar;
- Launch of scanning of selected files and directories by the context menu command in the graphic file manager;
- Launch of file and directory scanning, when the user drags and drops them on the main window of Dr.Web for Linux.

Status Indicator in Notification Area

After the user logs on, in the Desktop notification area (if it is supported by your 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 operation, such as:

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

If you click this icon, it opens the Dr.Web for Linux context menu.

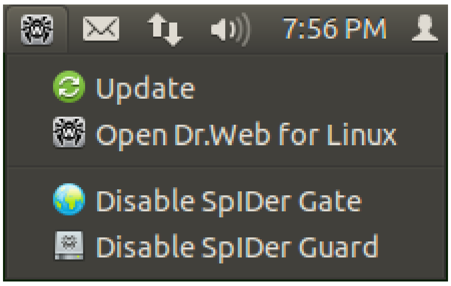


Figure 6. Dr.Web for Linux indicator context menu

When you select the **Open Dr.Web for Linux** item, window of Dr.Web for Linux graphical interface for management 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 Taskbar Icon

If the desktop environment contains a taskbar, 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. Right-click on the task button opens the application menu. The context menu looks like as follows (example for Unity Launcher in Ubuntu).

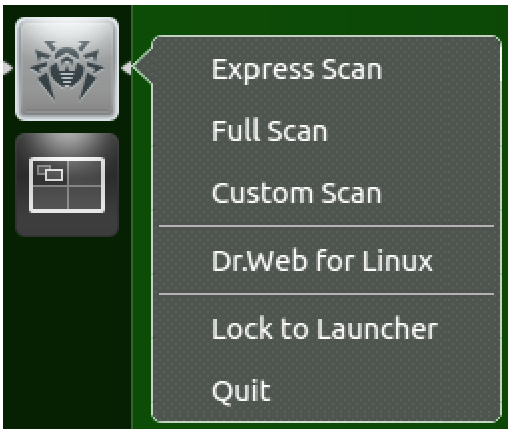


Figure 7. Dr.Web for Linux context menu on taskbar

- Selection of **Express scan** items, **Full scan** items and **Custom scan** items allows you to start the corresponding scan task (for **Custom scan** item it opens the page where you can select objects to be scanned).
- Selection of **Dr.Web for Linux** menu item launches the graphical interface (if not launched) and the selection of **Quit** item terminates it (if currently launched).
- The selection of **Lock to Launcher** item allows you to lock the application icon on the taskbar in order to provide quick access to graphical 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 the active scanning tasks is displayed on top of the application icon in the taskbar.

> In the different desktop environments, the taskbar 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.

Taskbar Icon Issues

If the button with application icon is displayed on the taskbar 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 **Dr.Web GUI for Linux** 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). To scan the files and directories:

1. Select them in the file manager window and then click right mouse button.
2. In the appeared context menu select the **Open With Other Application** item.
3. In the list of installed applications find and select **Dr.Web for Linux** item.

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, furtherly, the item **Open With Dr.Web for Linux** will be available in the context menu.

> 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 Files and Directories to 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 the Dr.Web for Linux graphical interface for management. 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 interface window for management.

Starting and Shutting Down Graphical Interface

Launch of the Dr.Web for Linux Graphical Management Interface

To launch the Dr.Web for Linux graphical management interface, do the following:

- Select in **Applications Dr.Web for Linux** item.

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 a graphical environment is accessible from the command line, for example, when working in a terminal emulator.

Termination of operation of the Dr.Web for Linux graphical interface for management

To shut down the Dr.Web for Linux 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 the centralized protection mode and launching of scanning by user demand is prohibited on the centralized 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

In this section:

- Scanning Types.
- Starting Scanning.
- Editing the List of Custom Scan Objects.
- Starting Custom Scan of Listed Objects.

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, and so on).
- *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 the centralized protection mode and launch of scanning on demand is prohibited on the Centralized 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 **Scanner** 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.

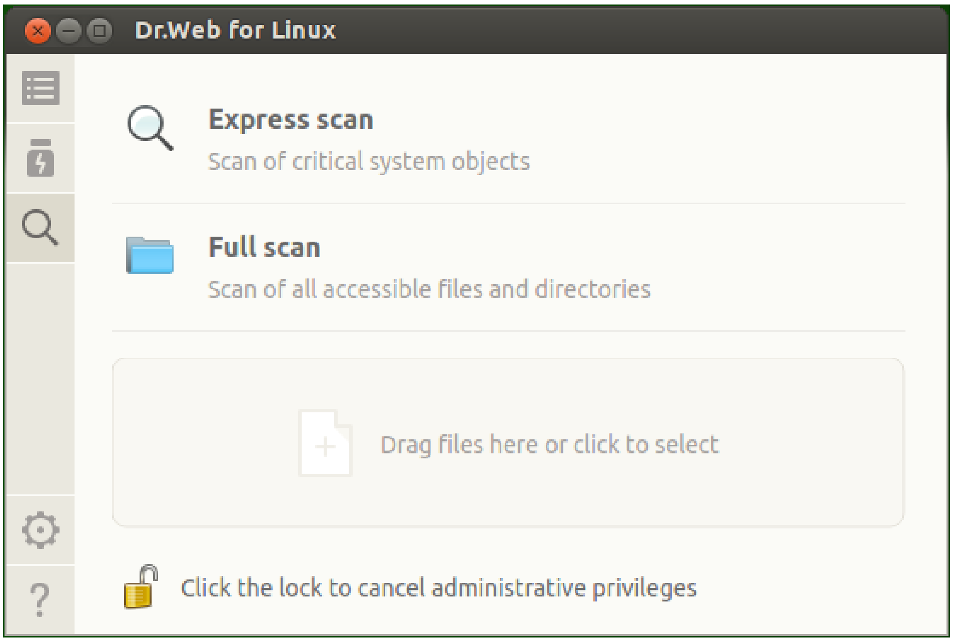

Dr.Web for Linux
Express scan
Scan of critical system objects
Full scan
Scan of all accessible files and directories
Drag files here or click to select
Click the lock to cancel administrative privileges

Figure 8. 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, elevate the application privileges before scanning starts. For details, refer to Managing Application Privileges.

To start *Custom scan* 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.

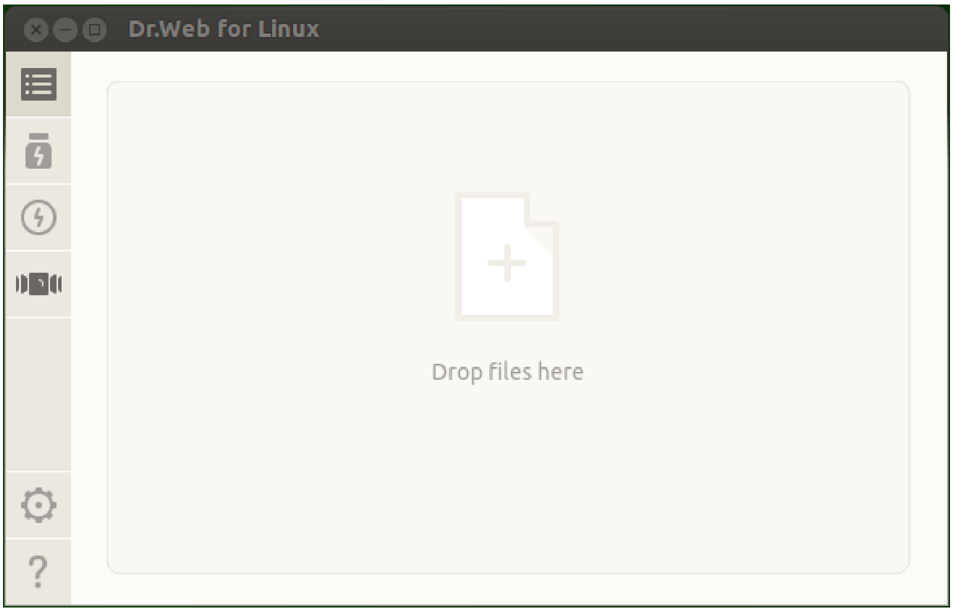
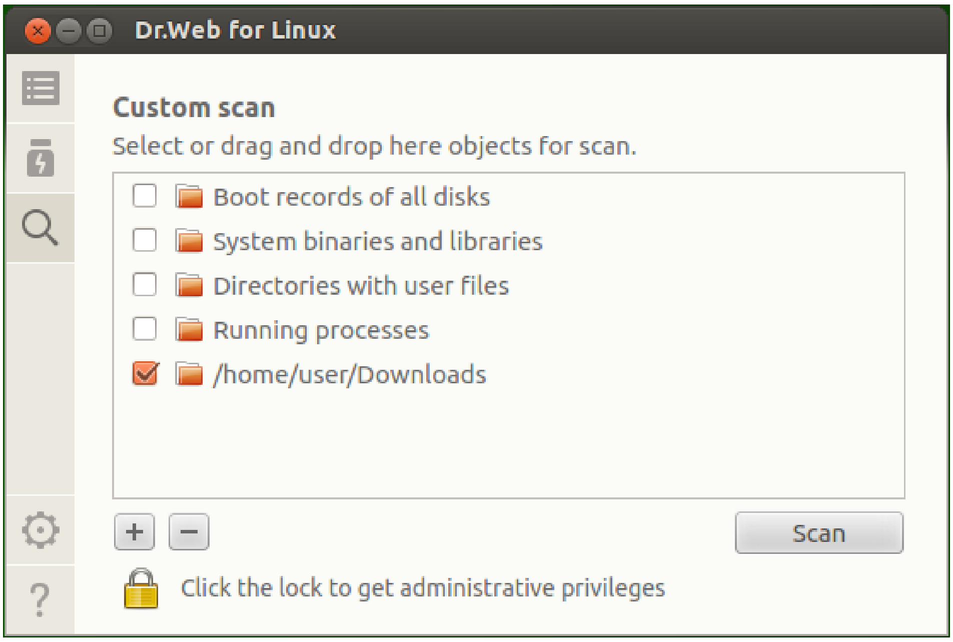


Figure 9. Target area where objects are dropped for scanning

- **List the objects for scanning**.

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



Custom scan

Select or drag and drop here objects for scan.

☐ Boot records of all disks

☐ System binaries and libraries

☐ Directories with user files

☐ Running processes

☑ /home/user/Downloads

Click the lock to get administrative privileges

Figure 10. 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`, and so on).
- *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 + 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 ✱ in the file chooser.

To remove all selected paths from the list, click –. 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, select all required check boxes of objects 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 Object 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 the server control in the centralized protection mode and launch of scanning on demand is prohibited on the centralized protection server, this Dr.Web for Linux option 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, and so on).
- *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 in unavailable when the scanning starts.

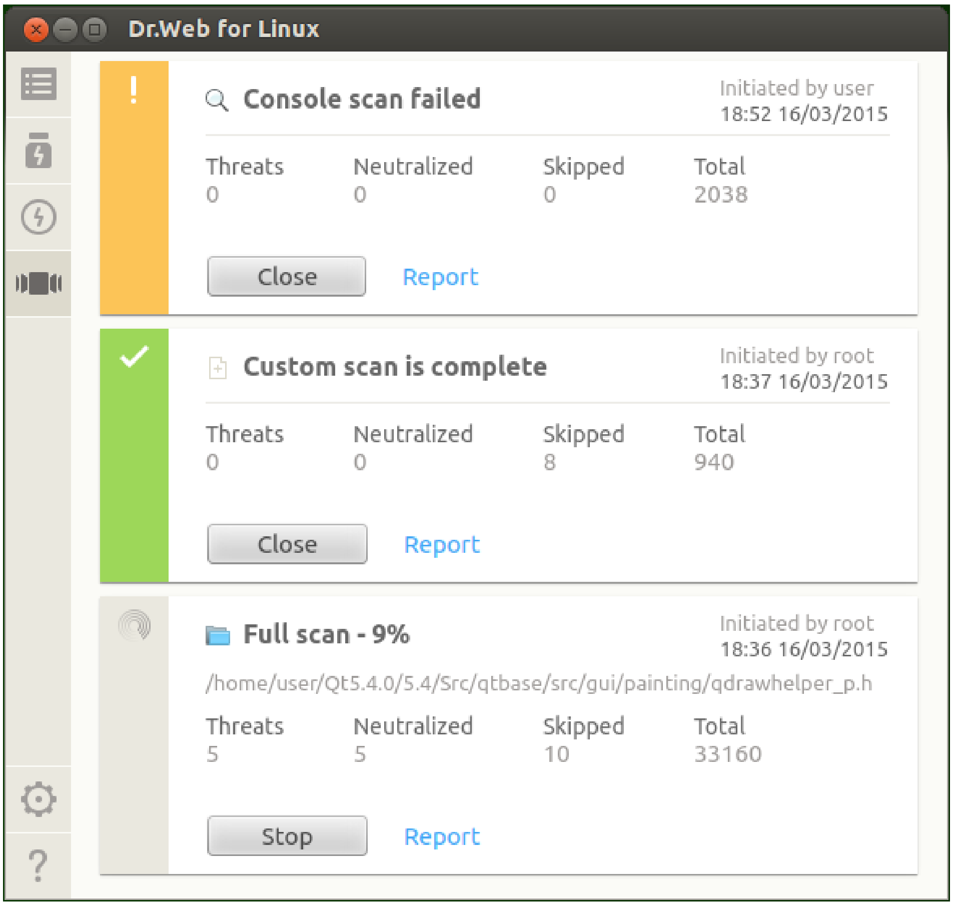
When scheduled scanning starts, the graphical interface for management automatically starts (if it is not launched yet), the created task is added to the queue which contains all scanning tasks of the current session: complete tasks, tasks in progress, and pending tasks. You can view the list of tasks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



Dr.Web for Linux

! Console scan failed

Initiated by user
18:52 16/03/2015

Threats	Neutralized	Skipped	Total
0	0	0	2038

Close Report

✓ Custom scan is complete

Initiated by root
18:37 16/03/2015

Threats	Neutralized	Skipped	Total
0	0	8	940

Close Report

Full scan - 9%

Initiated by root
18:36 16/03/2015

/home/user/Qt5.4.0/5.4/Src/qtbase/src/gui/painting/qdrawhelper_p.h

Threats	Neutralized	Skipped	Total
5	5	10	33160

Stop Report

Figure 11. Task management page

For each listed task, the following information is available:

- Scanning type (the list may contain not only *Express scan*, *Full scan*, and *Custom scan* but also scanning of additional types, see below).
- Name of the user who started scanning (if unknown, the system identifier of the user (*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:

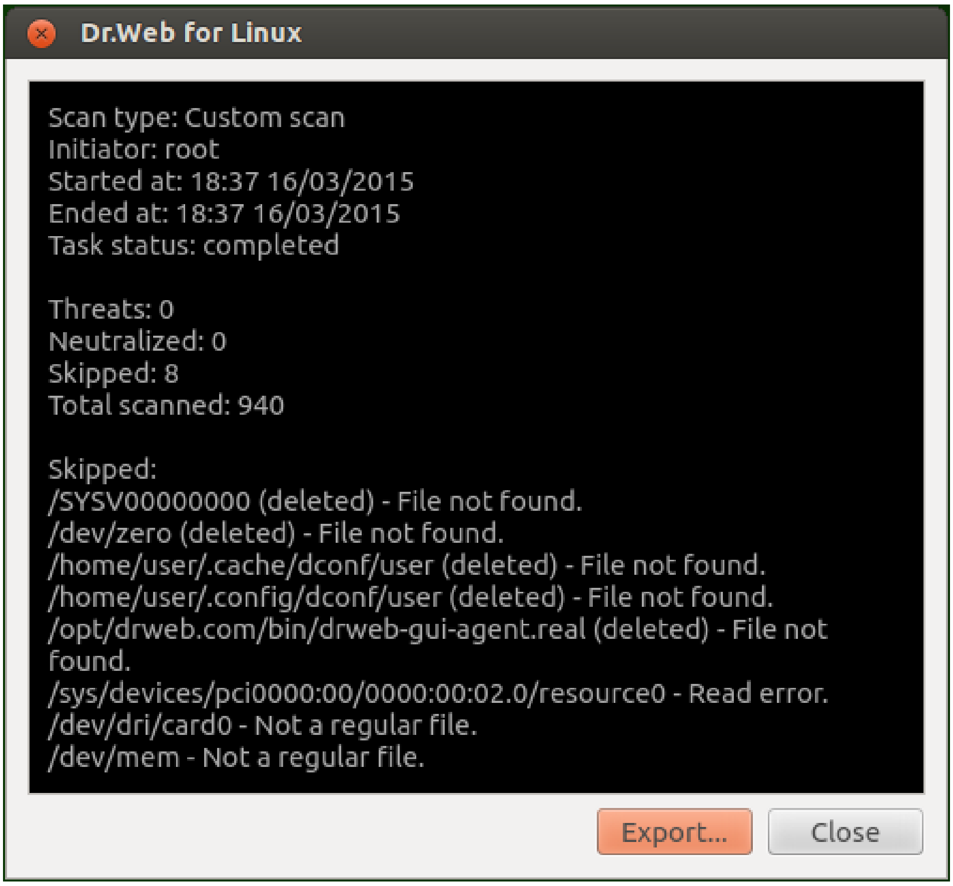
▨	Scanning is not complete or is pending.
🟩	Scanning is complete or stopped by the user; no threat is detected or all detected threats are neutralized.
🟧	Scanning is stopped due to an error.
🟥	Scanning is complete or stopped by the user; at least one detected threat is not neutralized.

Note that the list contains only those scanning tasks performed by Scanner that were directly created by the user in the Dr.Web for Linux window but also scanning tasks that were launched automatically according to the set schedule.

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.



```
Scan type: Custom scan
Initiator: root
Started at: 18:37 16/03/2015
Ended at: 18:37 16/03/2015
Task status: completed

Threats: 0
Neutralized: 0
Skipped: 8
Total scanned: 940

Skipped:
/SYSV00000000 (deleted) - File not found.
/dev/zero (deleted) - File not found.
/home/user/.cache/dconf/user (deleted) - File not found.
/home/user/.config/dconf/user (deleted) - File not found.
/opt/drweb.com/bin/drweb-gui-agent.real (deleted) - File not
found.
/sys/devices/pci0000:00/0000:00:02.0/resource0 - Read error.
/dev/dri/card0 - Not a regular file.
/dev/mem - Not a regular file.
```

Figure 12. 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

In this section:

- General Information.
- Managing Operation of the File System Monitor.
- Setting the File System Monitor.
- Problems with SpIDer Guard Operation.

General Information

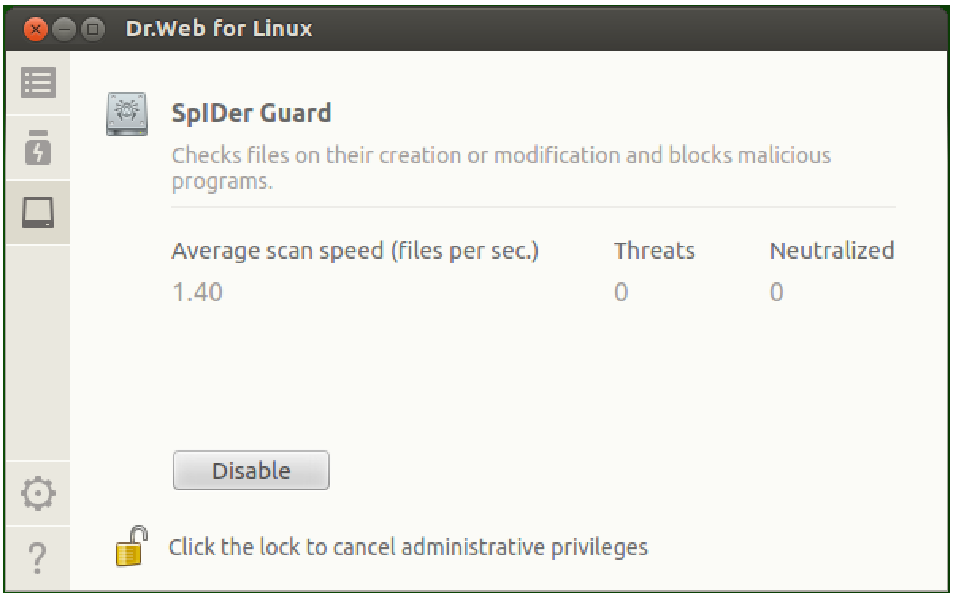
Continuous monitoring of file system objects is performed by the file system monitor SpIDer Guard.

The Dr.Web for Linux graphical management interface 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 **SpIDer Guard** on the main page.



Dr.Web for Linux

SpIDer Guard

Checks files on their creation or modification and blocks malicious programs.

Average scan speed (files per sec.)	Threats	Neutralized
1.40	0	0

Click the lock to cancel administrative privileges

Figure 13. 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 **Enable**. To disable monitoring, if enabled, click **Disable**.

> 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 centralized 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.

> For details on enabling the enhanced file monitoring mode by SpIDer Guard, refer to File Monitoring Modes.

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

In this section:

- General Information.
- Managing Operation of the Network Connection Monitor.
- Configuring SpIDer Gate.
- Problems with SpIDer Gate Operation.

General Information

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 scans:

- incoming and outgoing email messages;
- files downloaded from the internet.

If SpIDer Gate detects a threat in the scanned object, SpIDer Gate blocks its receiving or sending.

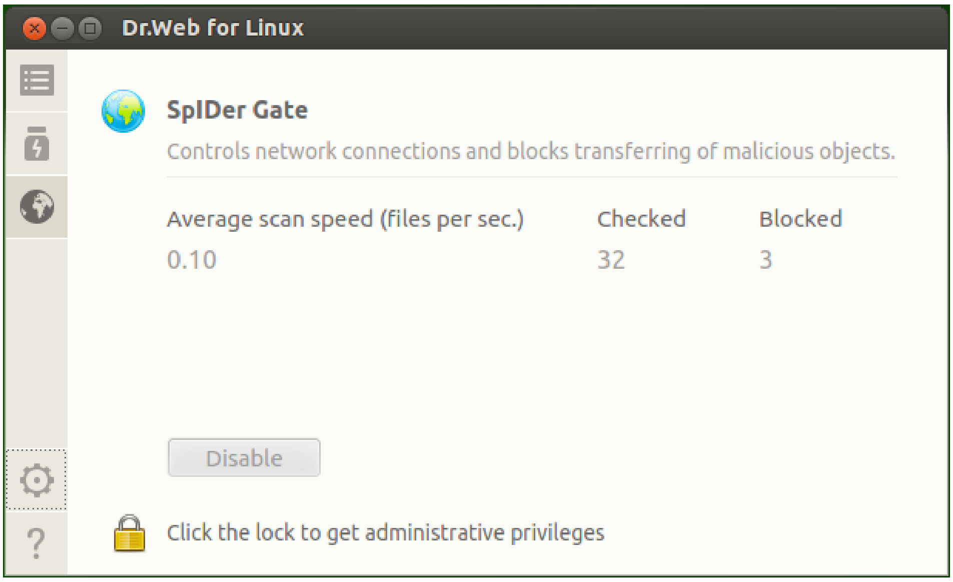
The Dr.Web for Linux graphical management interface allows you to configure the operation of SpIDer Gate:

- Start and stop the network connection monitor.
- View the number of scanned and blocked objects and attempts to access websites.
- Configure the following parameters of network connection monitoring:
  - Select a type of traffic to be scanned (web traffic, FTP traffic).
  - List of websites and hosts access to which is restricted.
  - Personal black and white lists of websites and hosts.
  - Parameters of scanning files downloaded from the internet.

The threats in email messages 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.

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 **SpIDer Gate** on the main page.



Dr.Web for Linux

SpIDer Gate

Controls network connections and blocks transferring of malicious objects.

Average scan speed (files per sec.)	Checked	Blocked
0.10	32	3

Click the lock to get administrative privileges

Figure 14. 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 scanned 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 **Enable**. To disable monitoring, if enabled, click **Disable**.

> 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 the SpIDer Gate network connection monitor when Dr.Web for Linux is operating under the centralized 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 scanned) because either the user disabled the component or an error occurred.

> If a mail client using IMAP for receiving messages (for instance, Mozilla Thunderbird) is running on your system, restart it after the antivirus is installed so that incoming email messages could be scanned.

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

Configuring SpIDer Gate

Operation setting of the network connection monitor SpIDer Gate is performed in the settings window:

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

Problems with SpIDer Gate Operation

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.

Depending on the distribution, Dr.Web Anti-Spam could be unavailable in Dr.Web for Linux. In this case, email messages will not be scanned for signs of spam.

If any email messages are falsely detected by the email anti-spam component Dr.Web Anti-Spam, we recommend you to forward them to special addresses for analysis and improvement of spam filter quality. To do that, save each message to a separate `.eml` file. Then attach the files to an email message and forward it to the special address.

- nonspam@drweb.com—if it contains email files, *erroneously considered spam*;
- spam@drweb.com—if it contains spam email files, *failed to be recognized as spam*.

Viewing Detected Threats

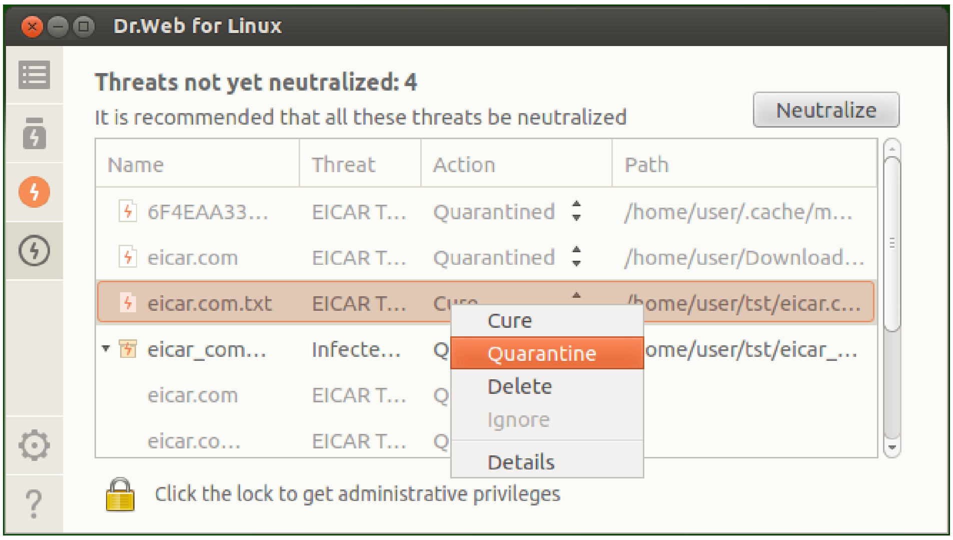
In this section:

- General Information.
- Neutralizing Detected Threats.
- Viewing Information on Threats.

General Information

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 ⚡ in the navigation pane.



Threats not yet neutralized: 4

It is recommended that all these threats be neutralized

Name	Threat	Action	Path
6F4EAA33…	EICAR T…	Quarantined	/home/user/.cache/m…
eicar.com	EICAR T…	Quarantined	/home/user/Download…
eicar.com.txt	EICAR T…	Cure	/home/user/tst/eicar.c…
eicar_com…	Infecte…	Q	ome/user/tst/eicar_…
eicar.com	EICAR T…	Q	
eicar.co…	EICAR T…	Q	

Click the lock to get administrative privileges

Figure 15. 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 you set Scanner or SpIDer Guard to perform the action *Report* for certain threat types, all threats of this type will be displayed with the action *No action* in the threat list. To neutralize such threats, indicate the action for each of them in the **Action** field.

If you need to apply an action, 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, and so on), 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

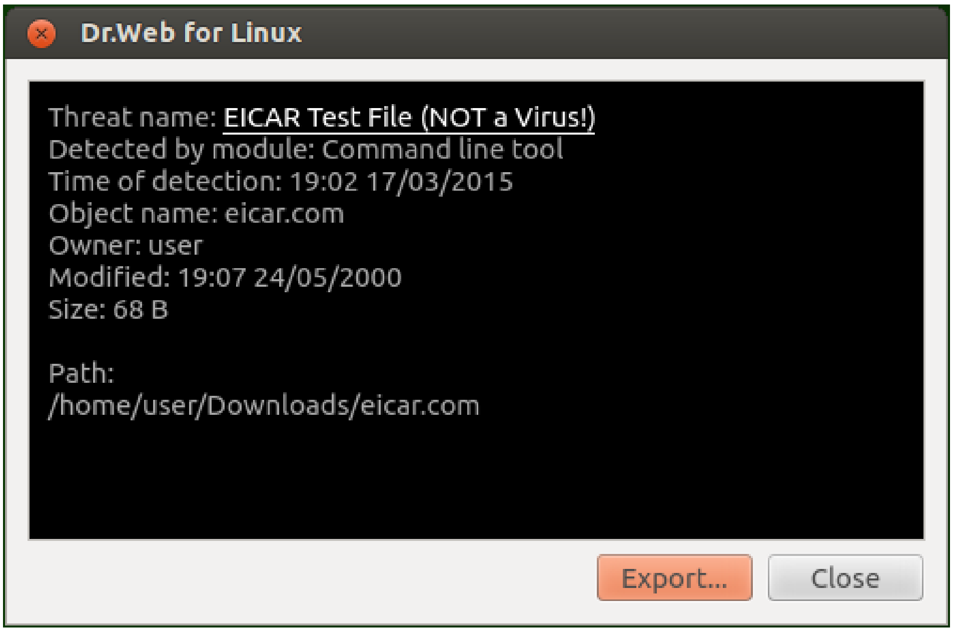
- If a threat is detected in a complex object (archive, email message, and so on), the selected action is applied to the container as a whole (and not to only the infected object).
- The *Cure* action can not be applied to certain threat types.

If required, elevate application privileges to enable successful neutralization of threats.

Threats, for which you indicate the action *Ignore*, will be displayed in the list until the graphical user interface is restarted.

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.



```
Threat name: EICAR Test File (NOT a Virus!)
Detected by module: Command line tool
Time of detection: 19:02 17/03/2015
Object name: eicar.com
Owner: user
Modified: 19:07 24/05/2000
Size: 68 B

Path:
/home/user/Downloads/eicar.com
```

Figure 16. 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, you can set it on a corresponding tab of the application settings window for Scanner).

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 (the file browsing window will open). To close the window with threat and object details, click **Close**.

Managing Quarantine

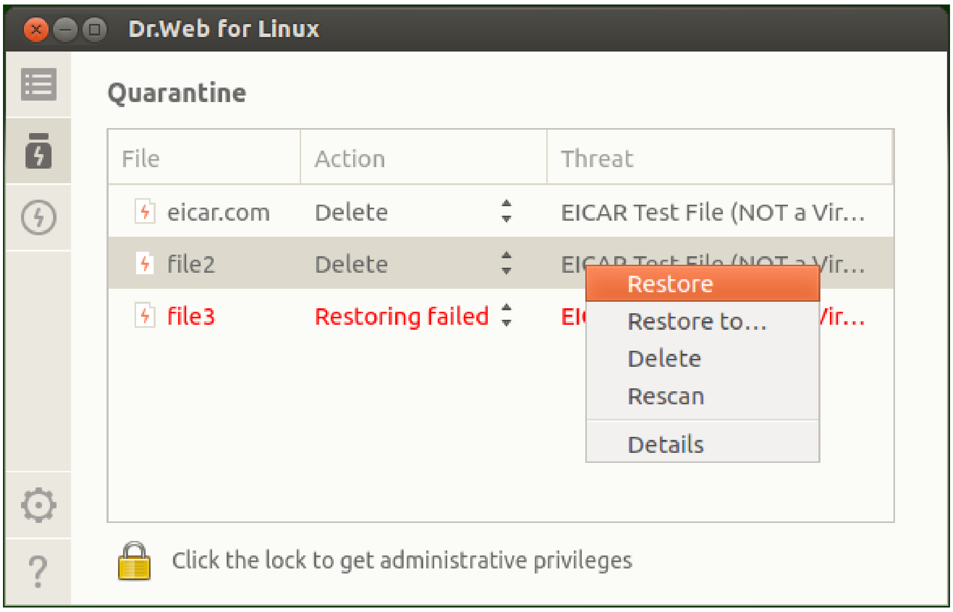
In this section:

- General Information.
- Applying Actions to Quarantined Threats.
- Viewing Details on Quarantined Objects.

General Information

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.



Dr.Web for Linux

Quarantine

File	Action	Threat
eicar.com	Delete	EICAR Test File (NOT a Vir…
file2	Delete	EICAR Test File (NOT a Vir…
file3	Restoring failed	EI… Vir…

Click the lock to get administrative privileges

Figure 17. 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:

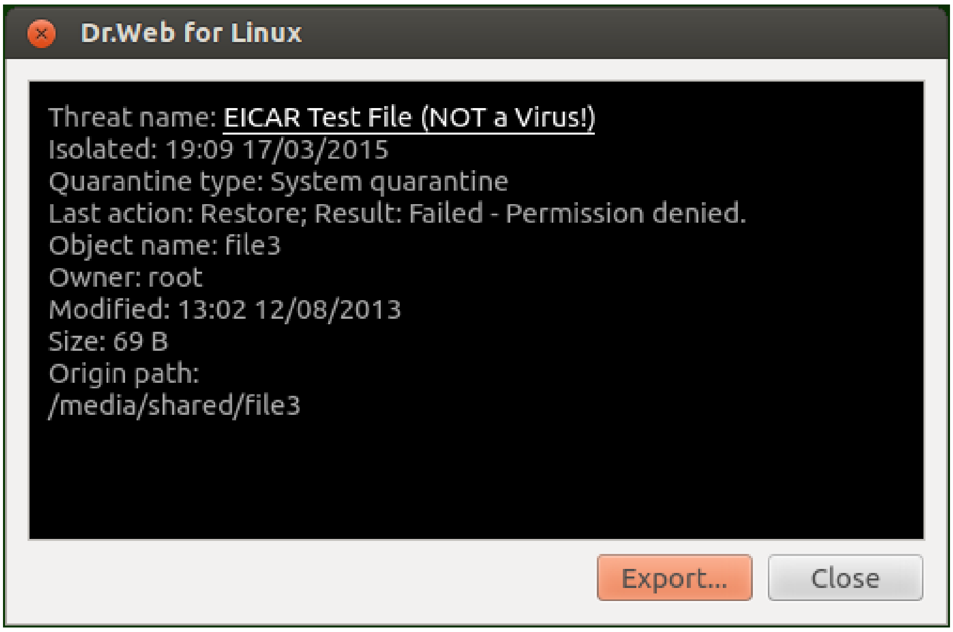
- **Restore**—restore selected objects to its original location.
- **Restore to**—restore selected objects to the specified file system location (the window for choosing of the target location will appear).
- **Delete**—delete selected objects permanently.
- **Rescan**—scan selected objects once again 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 menu. This opens the window with object details. If you need to view details on several isolated objects, select them on the list before opening the context menu.



Threat name: EICAR Test File (NOT a Virus!)
Isolated: 19:09 17/03/2015
Quarantine type: System quarantine
Last action: Restore; Result: Failed - Permission denied.
Object name: file3
Owner: root
Modified: 13:02 12/08/2013
Size: 69 B
Origin path:
/media/shared/file3

Figure 18. 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 (the file browsing window will open). To close the window with threat and object details, click **Close**.

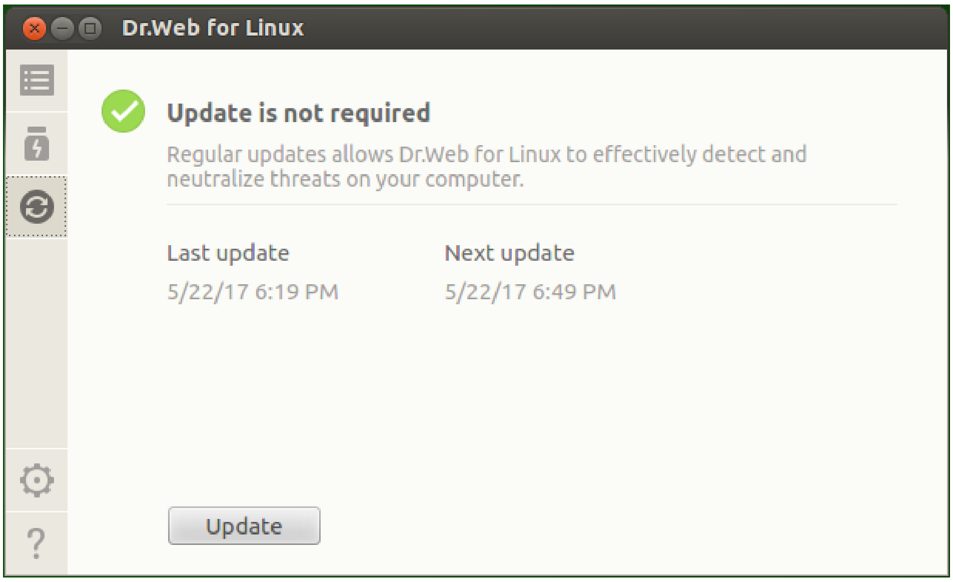
Updating Antivirus Protection

In this section:

- General Information.
- Configuring Updates.
- Problems with Updater Operation.

General Information

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**.



Update is not required

Regular updates allows Dr.Web for Linux to effectively detect and neutralize threats on your computer.

Last update: 5/22/17 6:19 PM

Next update: 5/22/17 6:49 PM

Figure 19. Update management page

The page displays the following information:

- Status of virus databases, database of web resource categories and the scan 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 the centralized 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 this section:

- General Information.
- Launching the License Manager.
- License Activation.
- Deleting License Key File.

General Information

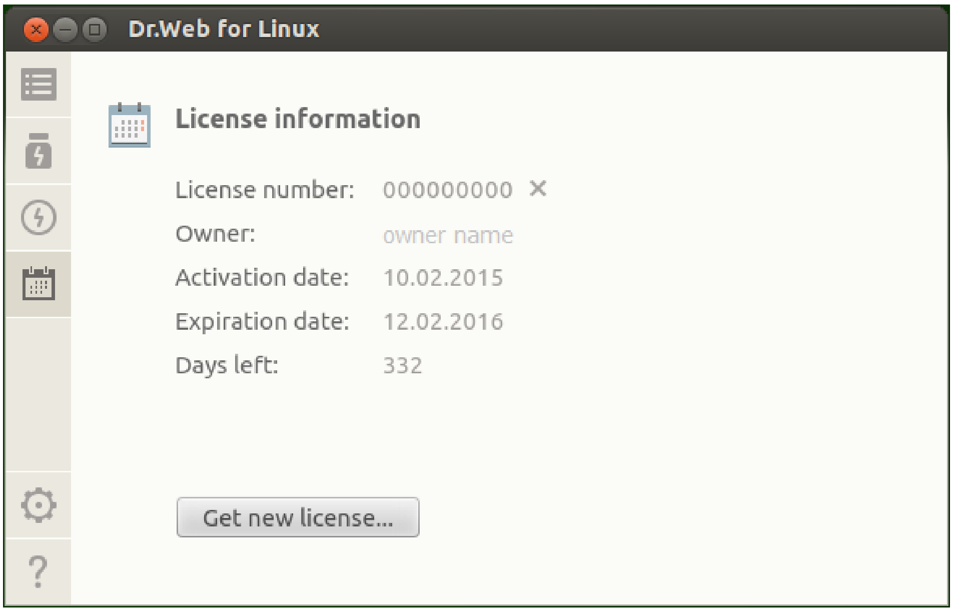
License Manager allows to view information on the current license issued for the Dr.Web for Linux user. License data is stored in a license key file that provides operation of Dr.Web for Linux on the user computer. If neither license key file nor demo key file is found on the computer, all Dr.Web for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

License Manager

License Manager page is available in the Dr.Web for Linux graphical 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 a license number, a license owner, and a duration period. This information is retrieved from the corresponding key file.

The figure below shows appearance of the License Manager page.



License number: 000000000
Owner: owner name
Activation date: 10.02.2015
Expiration date: 12.02.2016
Days left: 332

Figure 20. 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 (by purchasing a new license or renewing the current one) or to obtain a demo license, click **Get new license**. After that, the registration wizard will open. Note that the registration wizard also opens automatically when Dr.Web for Linux is first launched after installation.

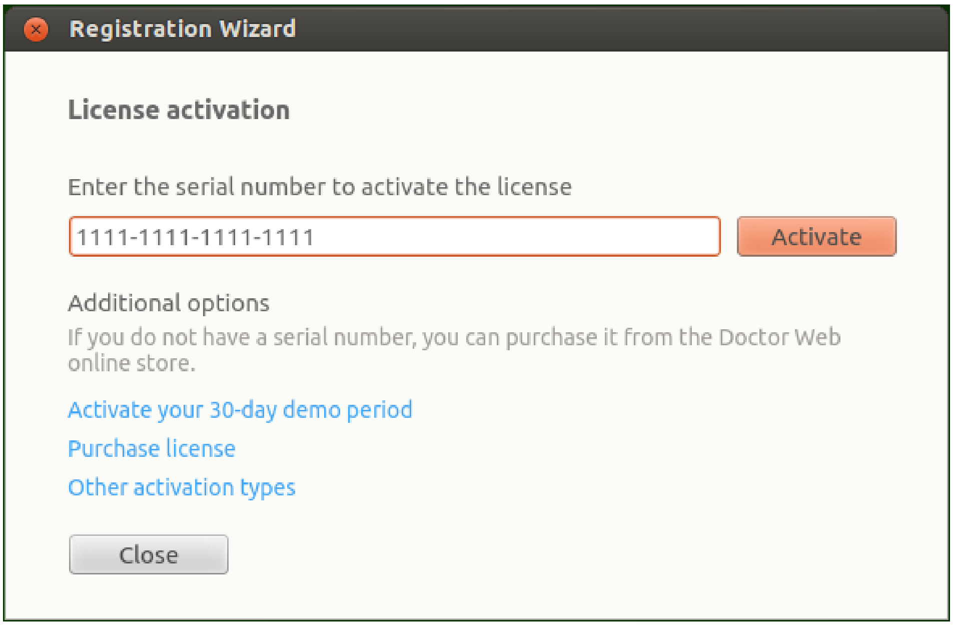
On the first step, you should choose an activation type. The following three types are available:

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 a demo period with a serial number, enter the number in the text field and click **Activate**.



Registration Wizard

License activation

Enter the serial number to activate the license

1111-1111-1111-1111

Additional options

If you do not have a serial number, you can purchase it from the Doctor Web online store.

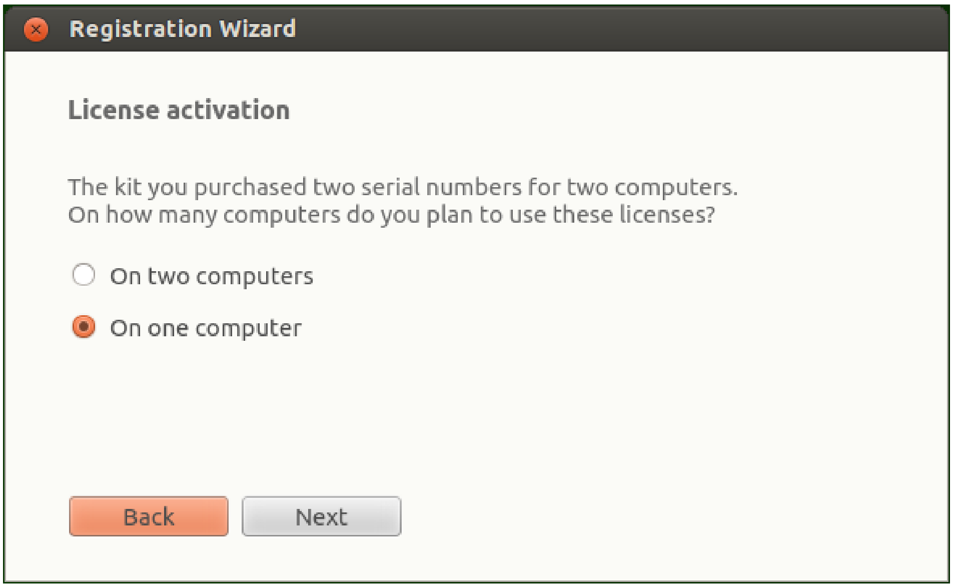
Figure 21. Registration using a serial number

If you do not have a serial number or a valid key file, you can purchase the 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 Registration and Activation.

Once you press the **Activate** button, connection to the Doctor Web registration server will be established.

If the specified serial number corresponds to a license for two computers, you need to select, how many computers you would like to use Dr.Web for Linux on. 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).


Registration Wizard

License activation

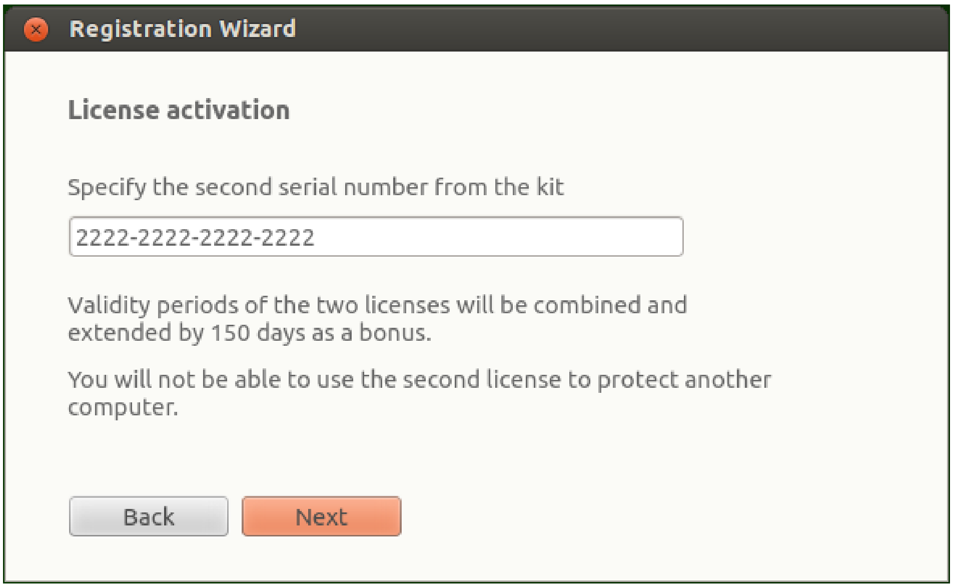
The kit you purchased two serial numbers for two computers.
On how many computers do you plan to use these licenses?

○ On two computers

● On one computer

Figure 22. Selecting the number of computers

After selecting the number of computers to activate the license on, click **Next**, and if you have selected **On one computer**, specify the second serial number on the next step of the wizard and then click **Next**.



Registration Wizard

License activation

Specify the second serial number from the kit

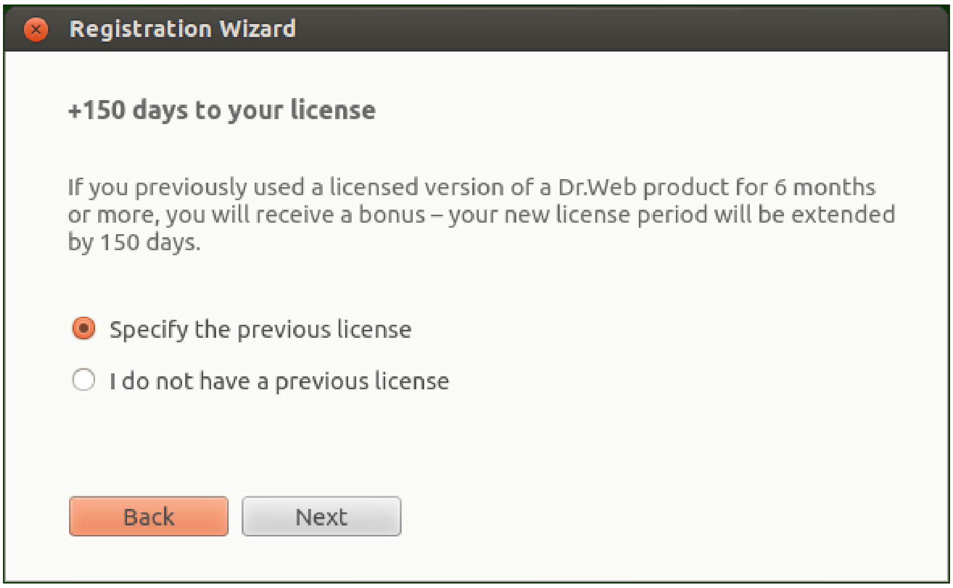
2222-2222-2222-2222

Validity periods of the two licenses will be combined and extended by 150 days as a bonus.

You will not be able to use the second license to protect another computer.

Figure 23. 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**.



Registration Wizard

+150 days to your license

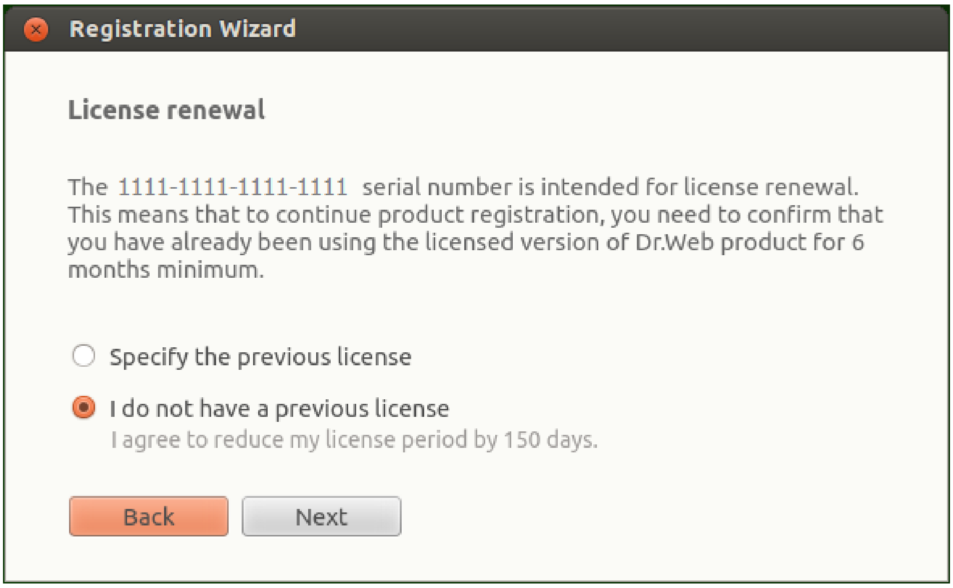
If you previously used a licensed version of a Dr.Web product for 6 months or more, you will receive a bonus – your new license period will be extended by 150 days.

● Specify the previous license

○ I do not have a previous license

Figure 24. 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.



Registration Wizard

License renewal

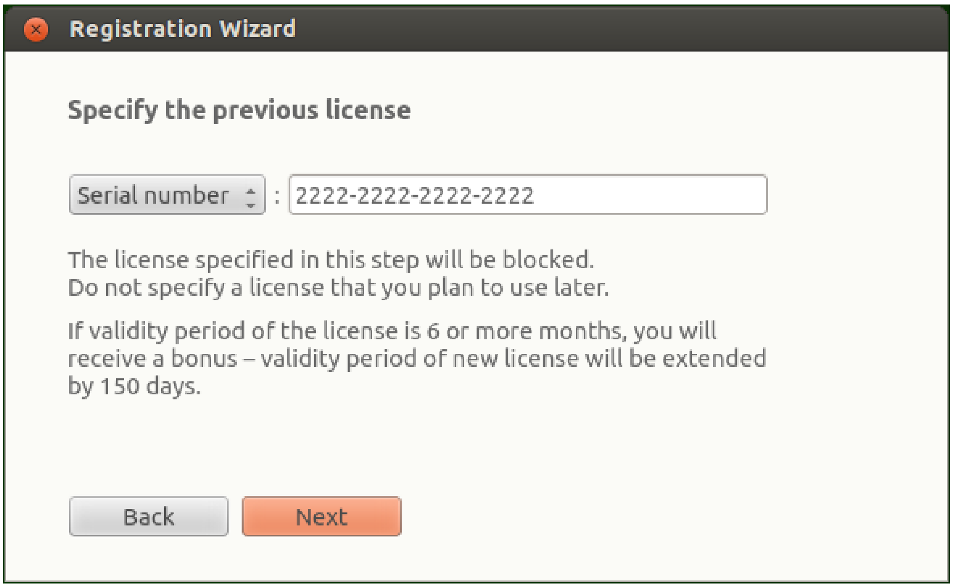
The 1111-1111-1111-1111 serial number is intended for license renewal. This means that to continue product registration, you need to confirm that you have already been using the licensed version of Dr.Web product for 6 months minimum.

○ Specify the previous license

● I do not have a previous license
I agree to reduce my license period by 150 days.

Figure 25. License renewal

If you have selected **Specify the previous license**, specify the previous license serial number or key file in the opened wizard window.



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.

Figure 26. 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 drop-down list 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 **Browse**.
- Drag and drop the file from the file manager window to the window of the Registration wizard.

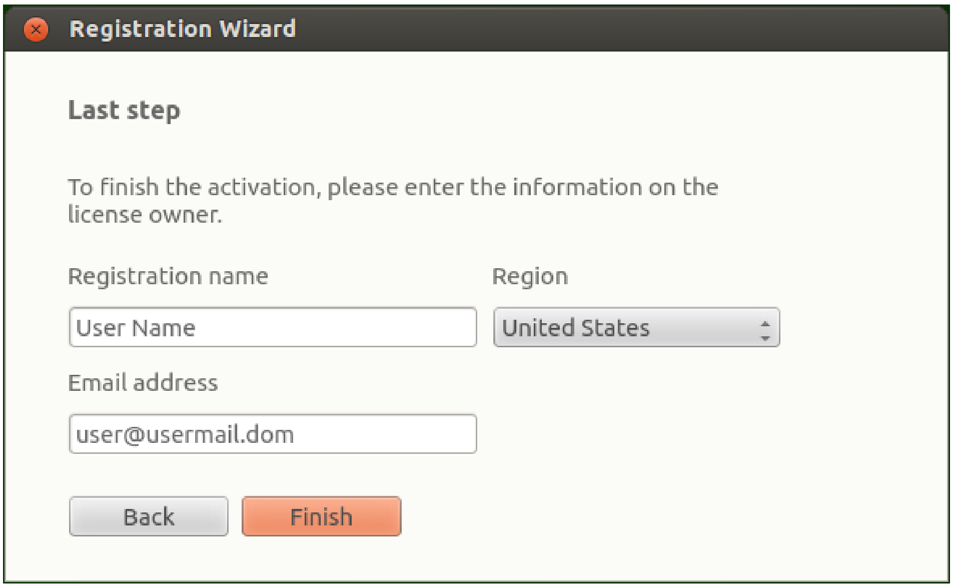
You can specify the zip archive containing the key file without unpacking it.

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.



Registration Wizard

Last step

To finish the activation, please enter the information on the license owner.

Registration name: User Name

Region: United States

Email address: user@usermail.dom

Figure 27. User information page

After all fields are filled in correctly, click **Finish** 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.

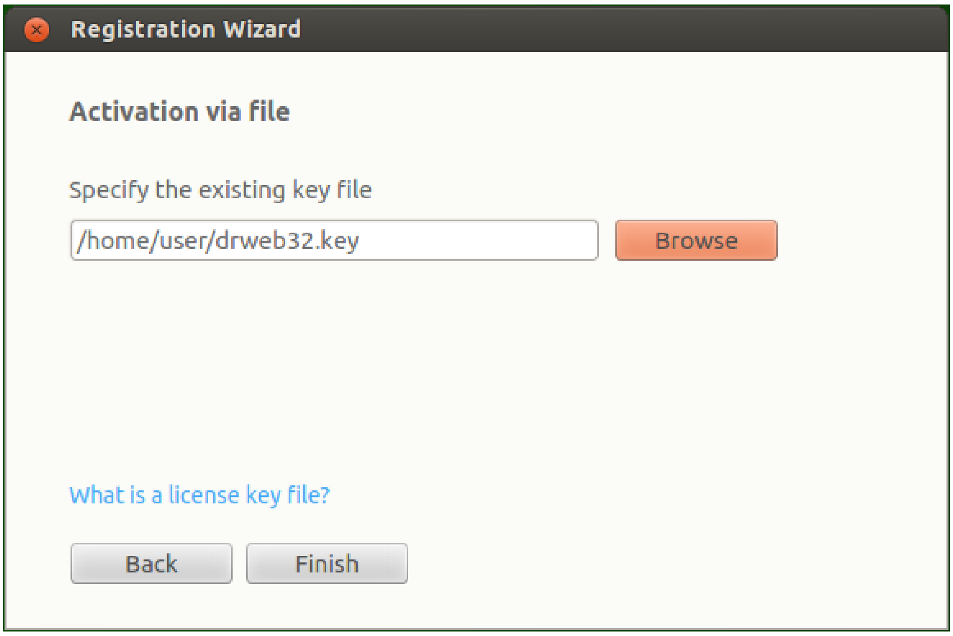
2. Obtaining a Demo Period

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 via License Manager, you do not need to provide your personal data.

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.



Registration Wizard

Activation via file

Specify the existing key file

/home/user/drweb32.key

Figure 28. Activation via key file

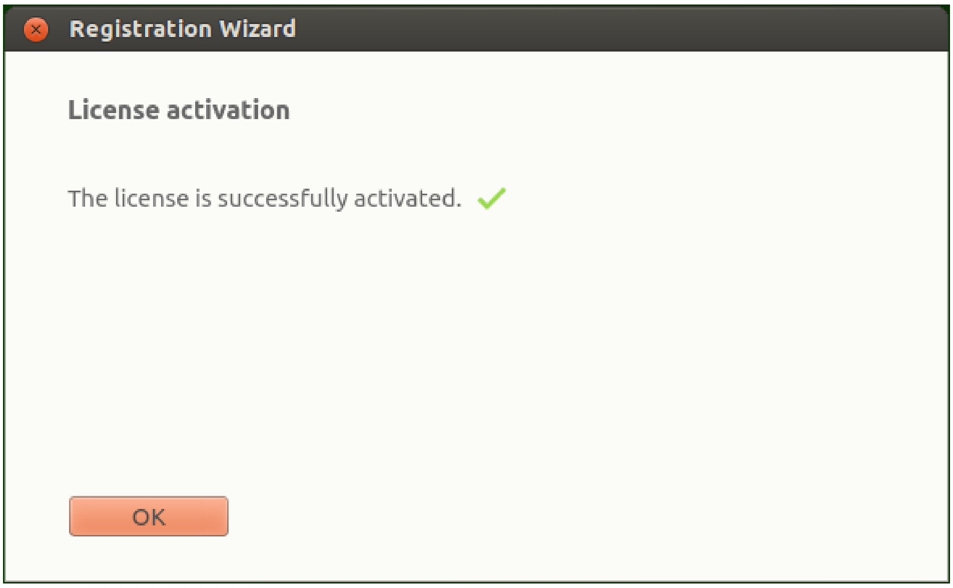
To specify the key file, you may:

- Specify the file path in the entry filed.
- Specify the file via the standard file chooser by clicking **Browse**.
- 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.

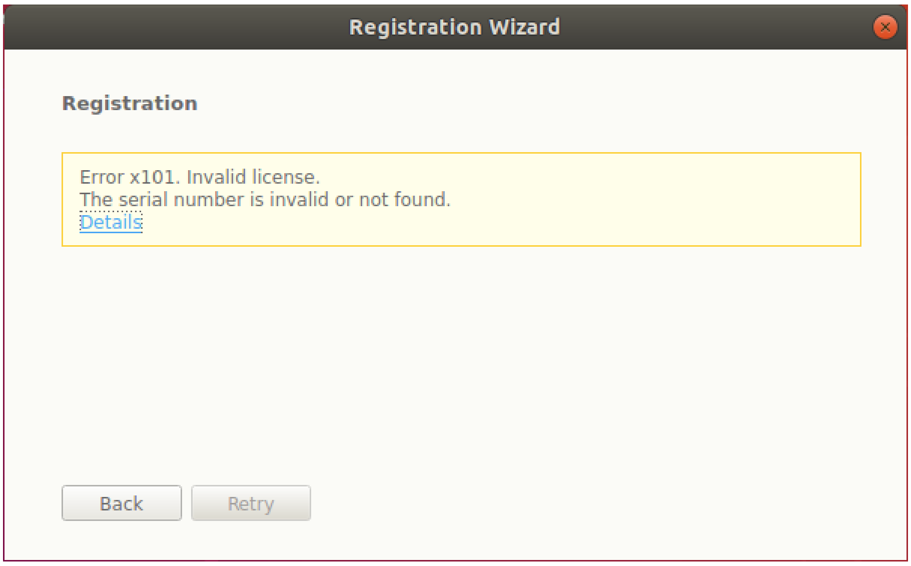


License activation

The license is successfully activated. ✓

Figure 29. 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 aexample of such a page.



Registration

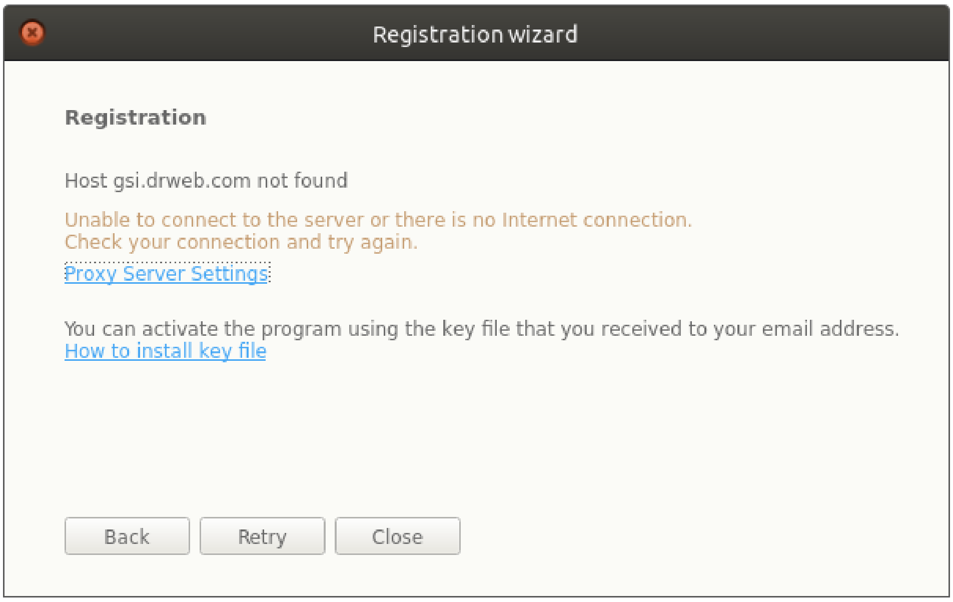
Error x101. Invalid license.
The serial number is invalid or not found.
Details

Figure 30. 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 by 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.



Registration wizard

Registration

Host gsi.drweb.com not found

Unable to connect to the server or there is no Internet connection.
Check your connection and try again.

Proxy Server Settings

You can activate the program using the key file that you received to your email address.
How to install key file

Figure 31. 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:

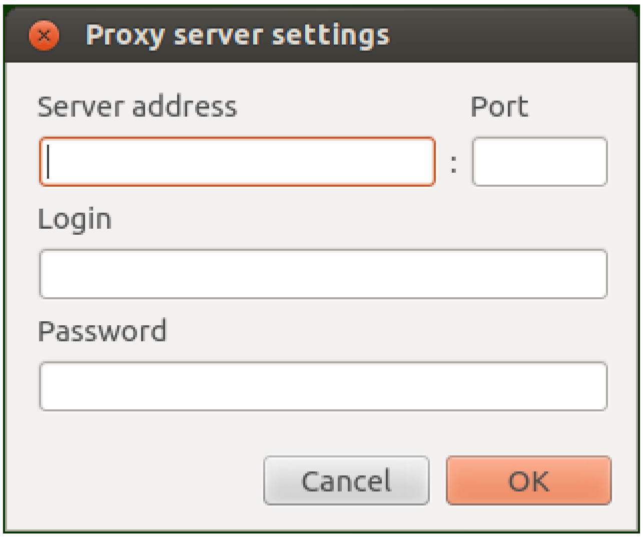


Figure 32. Proxy server settings

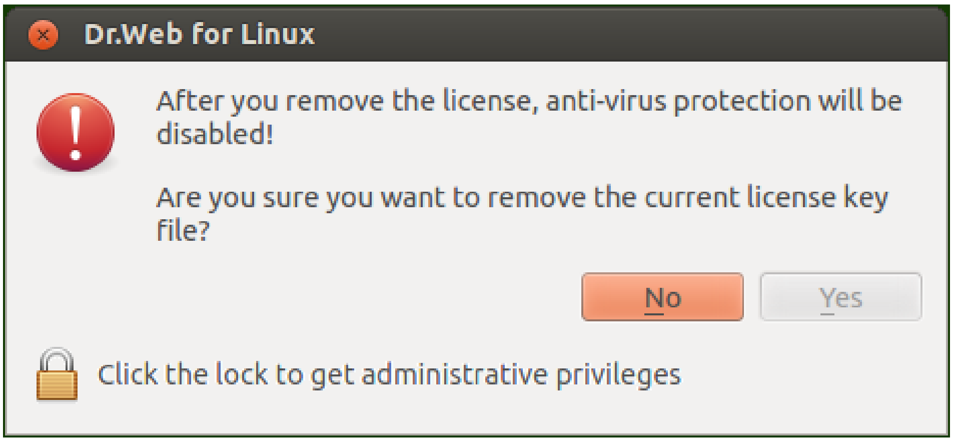
Specify the proxy server settings and click **OK**. After that retry establishing connection with the Doctor Web registration server by clicking **Retry**.

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 the ✕ symbol 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**.


Dr.Web for Linux

After you remove the license, anti-virus protection will be disabled!

Are you sure you want to remove the current license key file?

Click the lock to get administrative privileges

Figure 33. 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 virus databases, the scan engine and databases of web resource categories, file system monitoring) are blocked until a new license or demo period is activated.

Viewing messages from the centralized protection server

In this section:

- General Information.

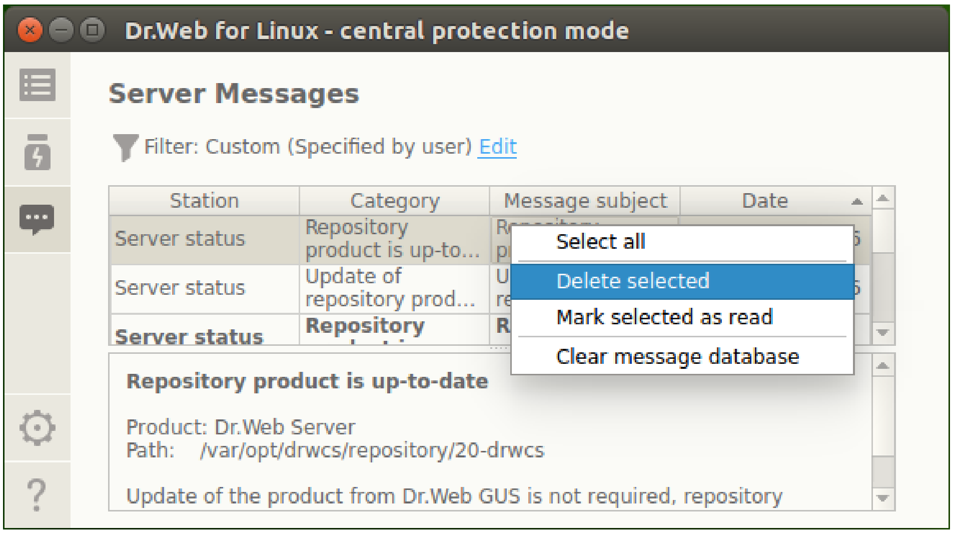
- Applying Actions to Messages.
- Filtering messages.

General Information

If Dr.Web for Linux is connected to the centralized protection server, you can view messages on state of the anti-virus network that are sent by the centralized protection server to the workstations. The anti-virus network administrator can use the tool to monitor the network state and important events of the centralized protection server.

> The messages on the network status and the network events are sent to the workstation only if the anti-virus network administrator configures the corresponding setting on the centralized protection server Dr.Web for Linux is connected to. Otherwise, the messages cannot be viewed and the corresponding page is not displayed on the Dr.Web for Linux main window.

The interface for viewing messages from the server is displayed on a separate page. To open this page, click 💬 on the navigation pane.



Server Messages

Filter: Custom (Specified by user) Edit

Station	Category	Message subject	Date
Server status	Repository product is up-to...	Re... p...	
Server status	Update of repository prod...	U... re...	
Server status	**Repository**	**R**	

Repository product is up-to-date

Product: Dr.Web Server
Path: /var/opt/drwcs/repository/20-drwcs

Update of the product from Dr.Web GUS is not required, repository

Figure 34. Centralized protection server messages page

For each message in the list, the following information is available:

- Name (address) of the workstation that is mentioned in the message.
- Message category.
- Message title (subject).
- Date and time that the message was sent by the server.

To view the message, select it from the list. The selected message body is shown on the pane under the message list. Unread messages are shown in bold.

The messages text about the status and events of the anti-virus network is in the language that is specified in the centralized protection server settings.

Applying Actions to Messages

To apply an action to a message, right-click anywhere in the table row with the information about the message, and select the required action in the drop-down menu. If you need to apply an action to several messages, 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, messages are selected one by one.
- When you hold SHIFT, messages are selected contiguously.

To select all messages, press CTRL+A.

The menu contains the following actions:

- Select all the filtered messages in the list.
- Delete the selected messages.
- Mark the selected messages as read.
- Clean up the messages database.

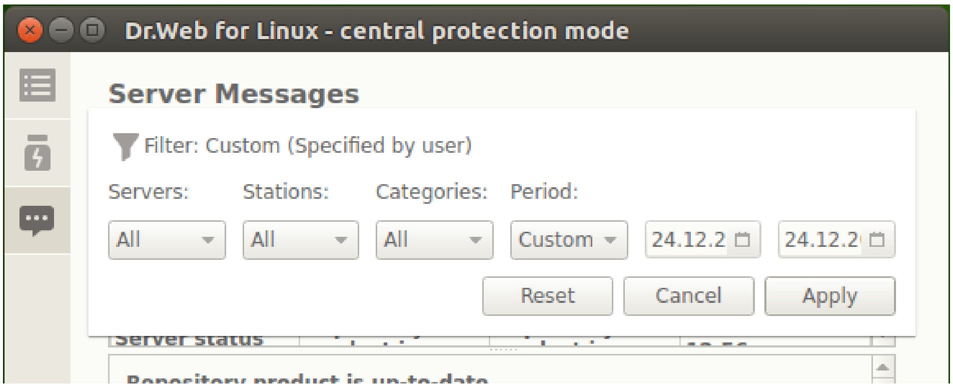
If you clean up the database, all received messages are deleted (including unread messages).

Note that messages received from the centralized protection server are automatically deleted at the end of the maximum storage time that is specified in settings.

Filtering messages

Since the server can send a significant number of messages, you can filter them by the sending server address, anti-virus network workstation name, message category, or receiving period. By default, the enabled filter shows all categories of messages received from all servers during the current day.

If necessary, you can edit the filter. For that, click the link **Edit**. After that, the filter pane opens at the top.



Dr.Web for Linux - central protection mode

Server Messages

Filter: Custom (Specified by user)

Servers: All

Stations: All

Categories: All

Period: Custom 24.12.2 24.12.2

Figure 35. Message filter pane

On the filter pane, you can specify the following filtering parameters:

- **Servers**—list of servers, from which the messages are shown.
- **Stations**—list of workstations about which the messages are shown.
- **Categories**—list of message categories to show.
- **Period**—list of generation periods of messages to show. You can select a standard period from the list or you can specify certain start and end moments of the generation period.

To save the changes, click **Apply**. To close the filter pane and discard the changes, click **Cancel**. To reset the filter to the default values, click **Reset**.

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. Scan of files and directories of other users (in particular, root).
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 centralized protection server.

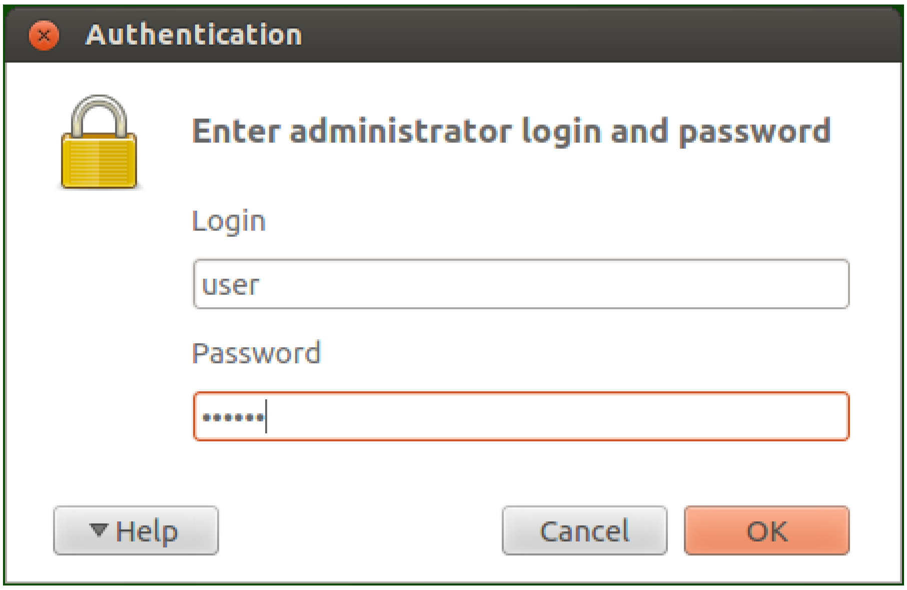
> Even if the application is started by root (for example, by using `su` or `sudo` commands), it *is not* granted elevated privileges by default.

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 to root.

🔓	Application has root 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.



Authentication

Enter administrator login and password

Login

user

Password

••••••

Figure 36. Authentication window

To grant the application administrative privileges, indicate the credentials of the user, included in *administrator group* of Dr.Web for Linux, or a superuser (system account *root*) and click **OK**. To cancel the privilege elevation, close the window by clicking **Cancel**. To view or hide a short help text describing how to authenticate, click **Help**.

> 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, press ? on the navigation pane of Dr.Web for Linux.

The following drop-down menu will appear:

- **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 Dr.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 scanning by Scanner and SpIDer Guard.
- Parameters of monitoring of network connections.
- Schedule of scans performed by Scanner.
- Protection mode (standalone, centralized 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 allows 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 scan 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, centralized 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 ? 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.

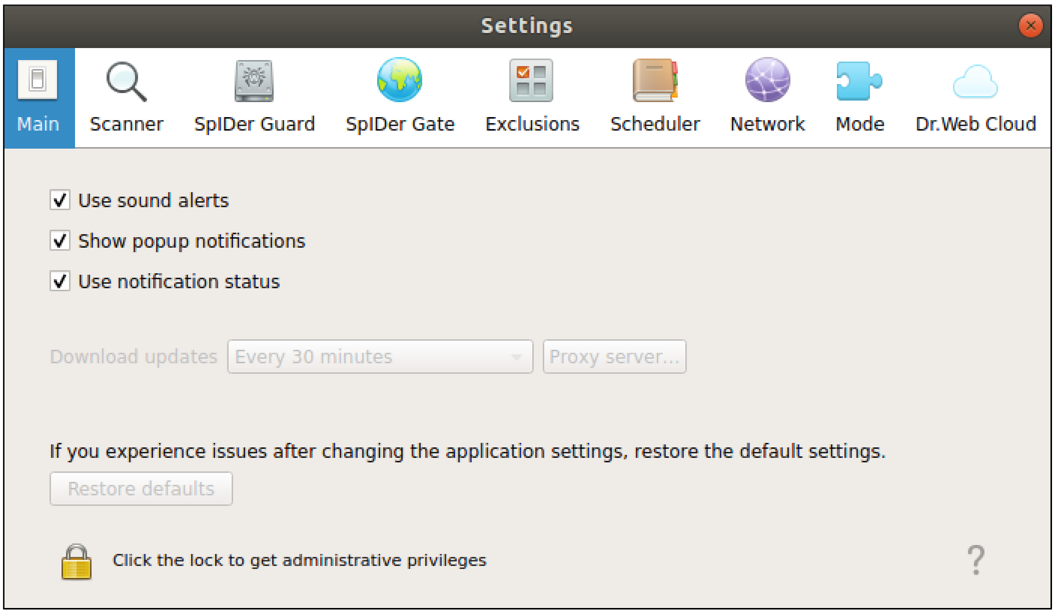
Main Settings

In this section:

- General Information.
- Configuring Proxy Server for Updates.

General Information

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



☑ Use sound alerts

☑ Show popup notifications

☑ Use notification status

Download updates Every 30 minutes Proxy server...

If you experience issues after changing the application settings, restore the default settings.

Restore defaults

Click the lock to get administrative privileges ?

Figure 37. 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 • threat detected (by both Scanner and SpIDer Guard); • object scan error; • and so on

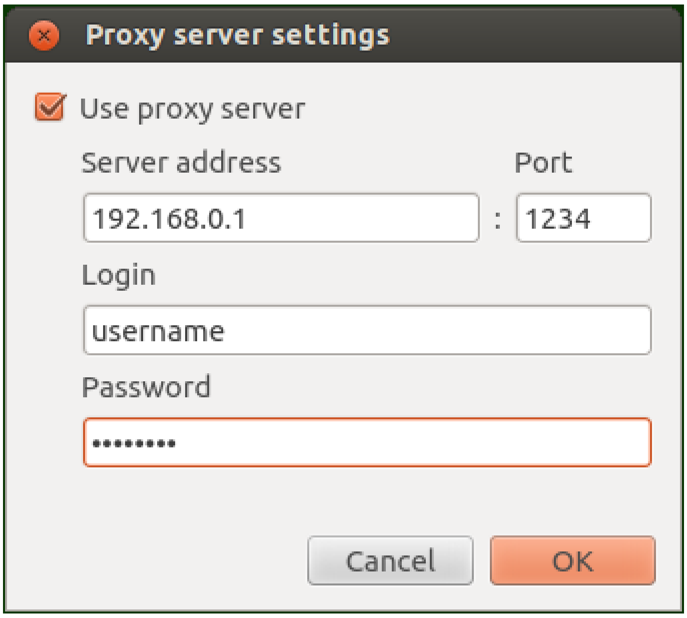
Option	Action
Check box **Show popup notifications**	Select this check box if you want Dr.Web for Linux to show pop-up notifications on particular events, such as • threat detected; • scan error; • and so on
Check box **Use notification status**	Select this check box if you want Dr.Web for Linux to show pop-up notifications on changing the state of the components.
Drop-down list **Download updates**	Select the frequency at which availability of updates to virus and web resource categories databases and to the Dr.Web for Linux scan 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.



Proxy server settings

☑ Use proxy server

Server address: 192.168.0.1

Port: 1234

Login: username

Password: •••••••••

Figure 38. Proxy server settings

As the server address, you can specify an IP address as well as FQDN of the host with your 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**.

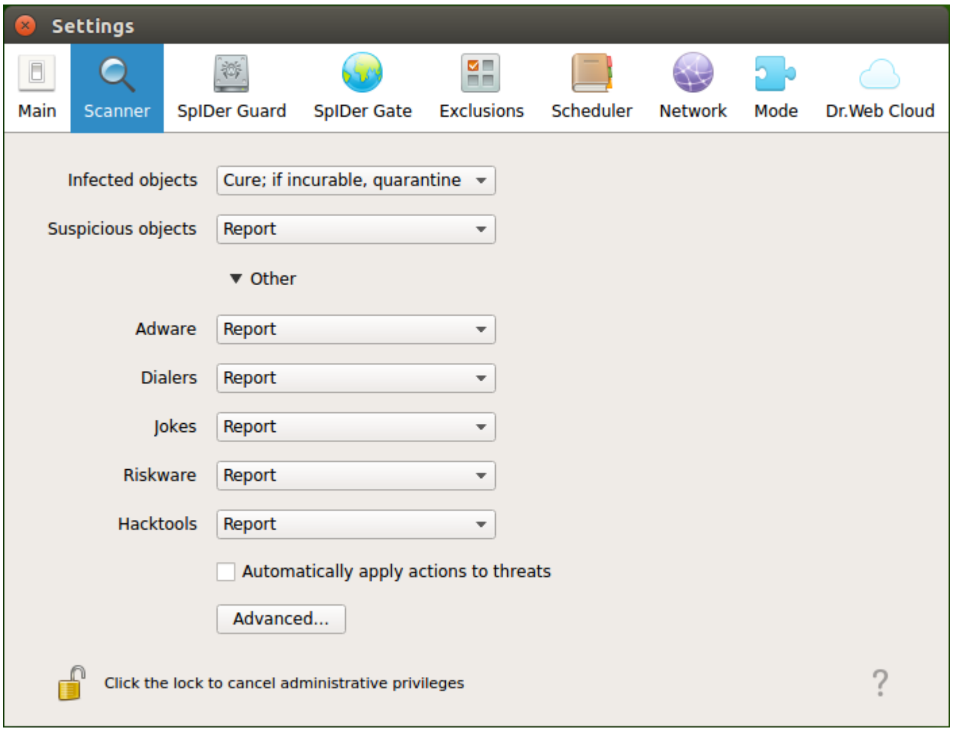
File Scan Settings

In this section:

- General Information.
- Advanced Scanning Settings.

General Information

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.



Infected objects: Cure; if incurable, quarantine

Suspicious objects: Report

▼ Other

Adware: Report

Dialers: Report

Jokes: Report

Riskware: Report

Hacktools: Report

□ Automatically apply actions to threats

Click the lock to cancel administrative privileges

Figure 39. Scanner settings tab

Select actions in the drop-down menu, that Dr.Web for Linux will apply to objects upon detection of any threat of the corresponding type.

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

By selecting 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 threat details 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 **Advanced** to open the window with advanced file scanning settings.

Notes:

- You can exclude files and directories 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.

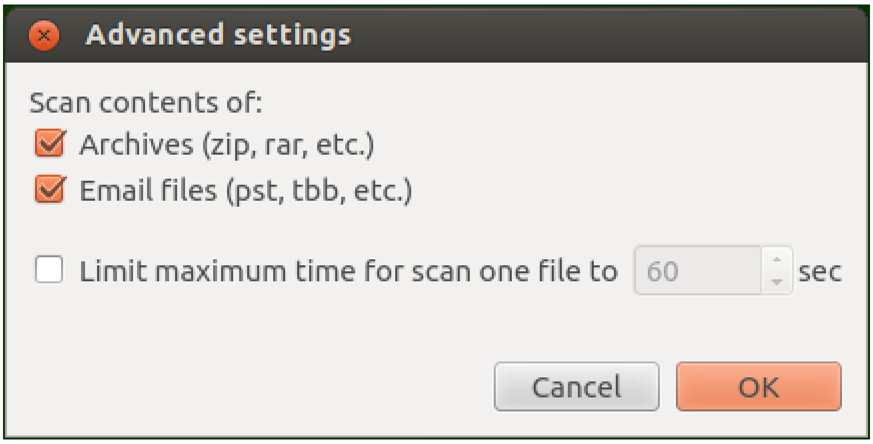
To change Scanner reaction to threats and to access advanced settings, the application must operate with elevated permissions. Refer to Managing Application Privileges section.

The option to configure Scanner when Dr.Web for Linux is operating under the centralized 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.



Advanced settings

Scan contents of:

☑ Archives (zip, rar, etc.)

☑ Email files (pst, tbb, etc.)

□ Limit maximum time for scan one file to 60 sec

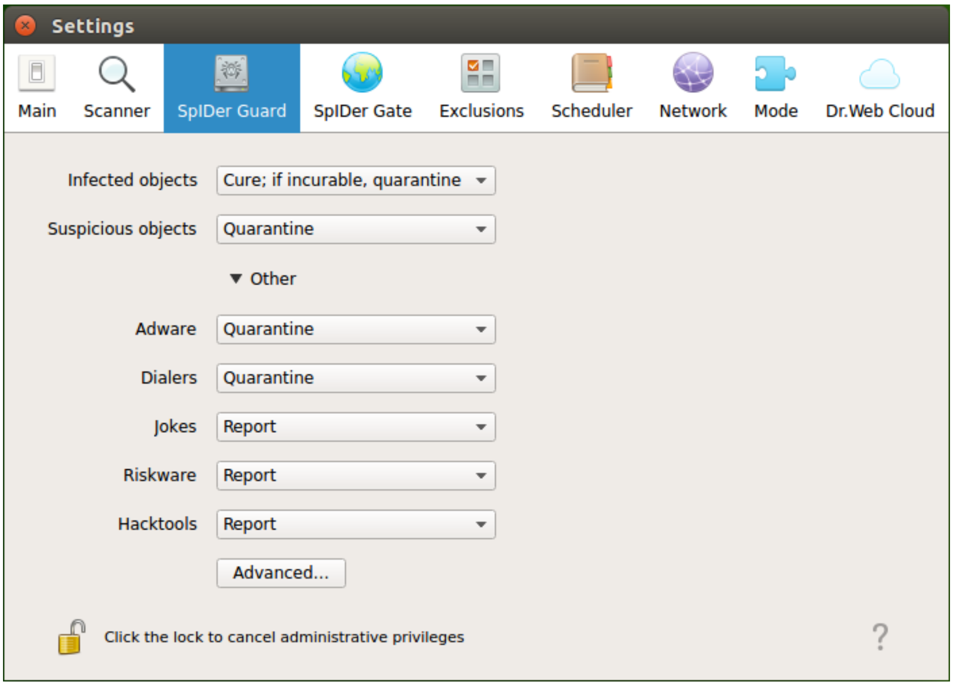
Figure 40. Advanced scanning settings

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.



Infected objects: Cure; if incurable, quarantine

Suspicious objects: Quarantine

Adware: Quarantine

Dialers: Quarantine

Jokes: Report

Riskware: Report

Hacktools: Report

Figure 41. File system monitoring settings page

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

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

Notes:

- You can exclude files from monitoring by SpIDer Guard on the **Exclusions** tab.
- For details on enabling the enhanced file monitoring mode by SpIDer Guard, refer to File Monitoring Modes.
- 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 centralized protection server can be blocked if disabled by the server.

Monitoring Settings of Network Connections

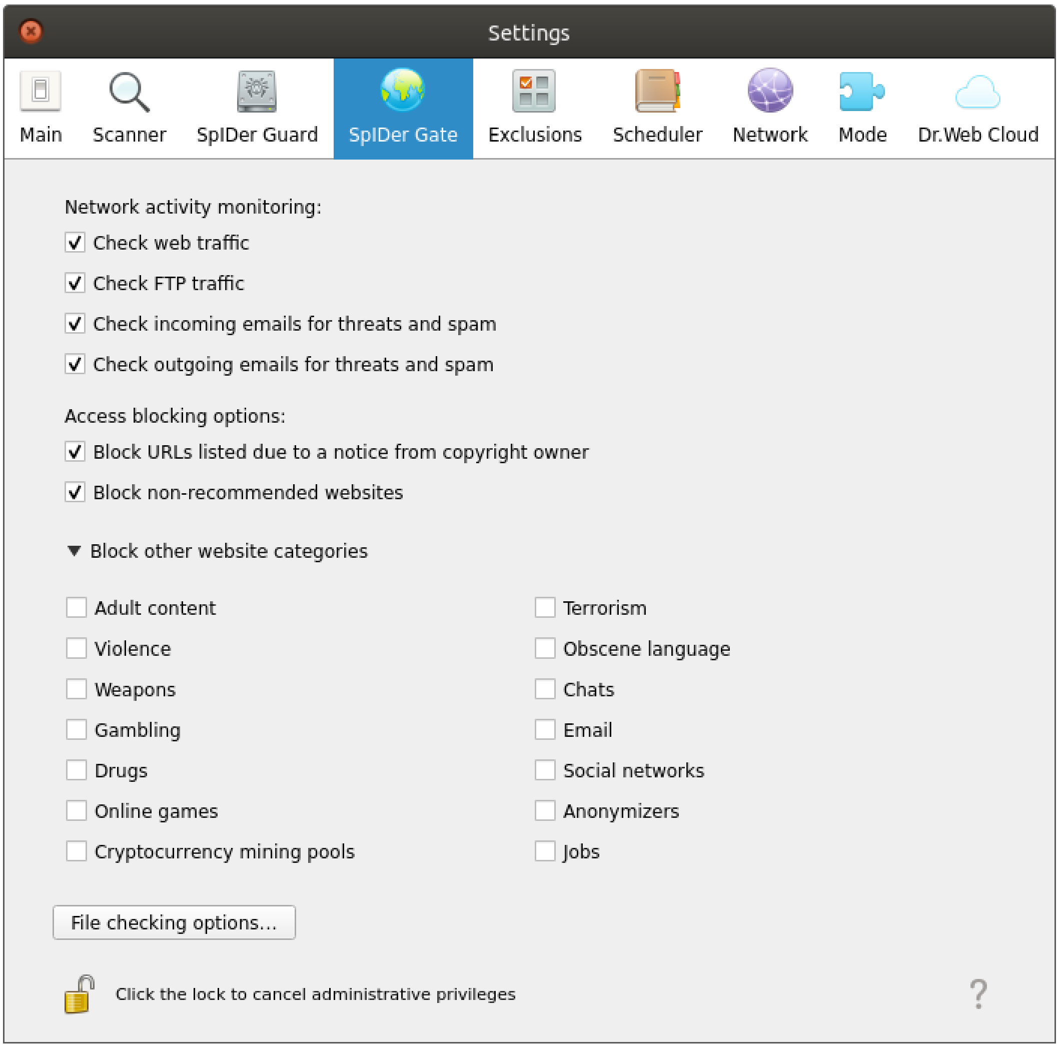
In this section:

- General Information.
- Website Category Selection.

- Managing File Scanning Parameters.

General Information

On the **SpIDer Gate** tab, you can configure security policies used by SpIDer Gate upon an attempt to access the internet.



Network activity monitoring:

☑ Check web traffic

☑ Check FTP traffic

☑ Check incoming emails for threats and spam

☑ Check outgoing emails for threats and spam

Access blocking options:

☑ Block URLs listed due to a notice from copyright owner

☑ Block non-recommended websites

▼ Block other website categories

□ Adult content	□ Terrorism
□ Violence	□ Obscene language
□ Weapons	□ Chats
□ Gambling	□ Email
□ Drugs	□ Social networks
□ Online games	□ Anonymizers
□ Cryptocurrency mining pools	□ Jobs

File checking options...

Click the lock to cancel administrative privileges

?

Figure 42. 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.

Website Category Selection

Switchers in the **Monitoring options** section define categories of websites and hosts with restricted access (it applies not only to attempts to access such websites via a browser but also to attempts to access FTP servers). By enabling or disabling corresponding switchers, you can allow or restrict access to websites and hosts from the following categories:

Category	Description
URL added due to a notice from copyright owner	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.
Non-recommended websites	Websites with unreliable content (suspected of phishing, password theft, and so on).
Adult content	Websites with adult content
Violence	Websites that contain violent material (for example, war scenes, acts of terrorism, and so on)
Weapons	Websites that contain information on weapons and explosives
Gambling	Internet casinos, gambling and bookmaking websites
Drugs	Websites that contain information on drug production, distribution, and use
Obscene language	Websites with obscene language
Chats	Chat websites
Terrorism	Websites that contain information about terrorism
Email	Websites that offer free email registration
Social networks	Social networking websites
Online games	Websites that provide access to games using the permanent internet connection.
Anonymizers	Websites that allow the user to hide personal information and that provide access to the blocked web resources.
Cryptocurrency mining pools	Websites that provide access to common services for cryptocurrencies mining.
Jobs	Job search 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 to expand or collapse the list of available categories.

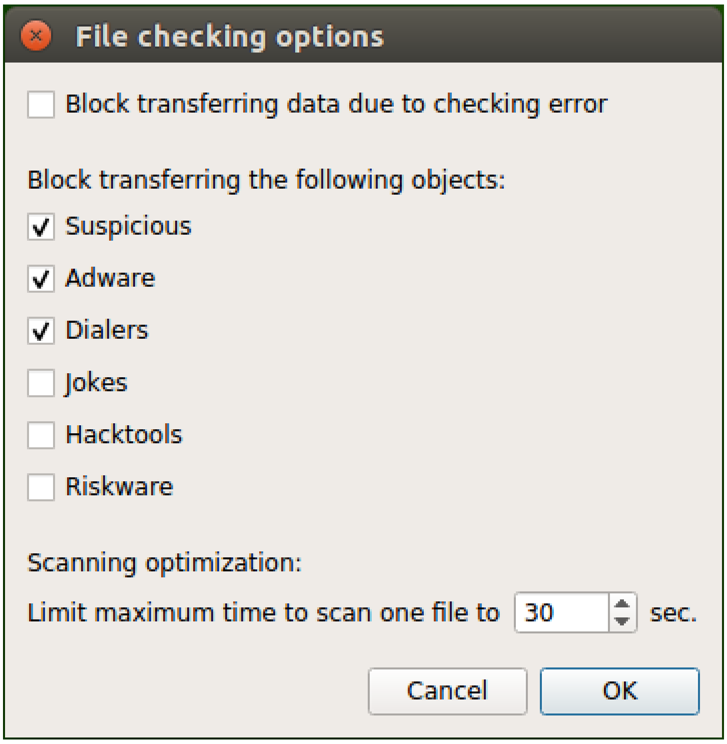
If you need to block access to a website or to a host which does not fall into any of these categories, add it to the user black list. If otherwise, you need to allow access to a website or to a host which is included in any of the above categories and marked as unwanted, add it to the user white list. You can also configure the list of applications which network connections will not be monitored 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 category *Websites known as infection sources*, access to these websites and hosts is always disabled even if they are added to the white list.

Managing File Scanning Parameters

To configure parameters used by SpIDer Gate for scanning files downloaded from the internet, click **File checking options**.



File checking options

□ Block transferring data due to checking error

Block transferring the following objects:

☑ Suspicious

☑ Adware

☑ Dialers

□ Jokes

□ Hacktools

□ Riskware

Scanning optimization:

Limit maximum time to scan one file to 30 sec.

Figure 43. File scan settings window

In the appeared window, you can specify the categories of malicious objects to be blocked on attempt to transmit them. If a check box is selected, files that fall into the corresponding category are rejected on attempt to download them. 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. If the **Block transferring data due to checking error** check box is selected, files that were not scanned due to an error are blocked and cannot be downloaded. To allow downloading of such files, clear this check box (not recommended).

If scanning of a downloaded file failed because the interval for performing this operation expired, such file *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.

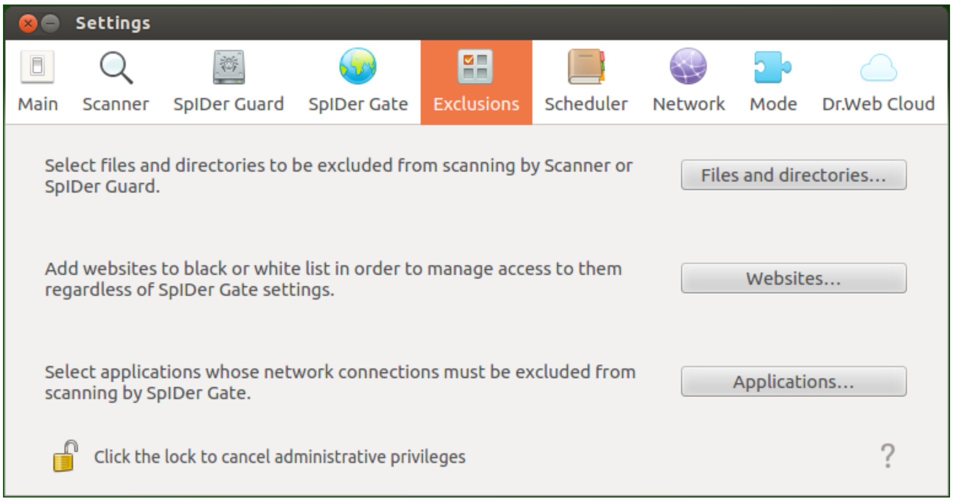
To close the window and save the changes, click **OK**. To discard the changes and close the window, click **Cancel**.

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 scanning by 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 Gate 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.



Select files and directories to be excluded from scanning by Scanner or SpIDer Guard.

Add websites to black or white list in order to manage access to them regardless of SpIDer Gate settings.

Select applications whose network connections must be excluded from scanning by SpIDer Gate.

Click the lock to cancel administrative privileges

Figure 44. 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

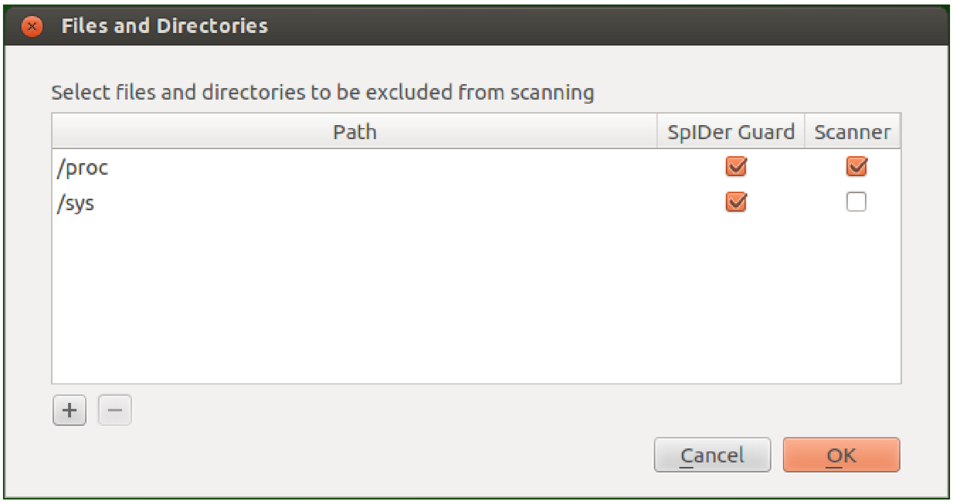
In this section:

- General Information.
- Adding and Removing Objects From the List of Exclusions.

General Information

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

Here 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.



Files and Directories

Select files and directories to be excluded from scanning

Path	SpIDer Guard	Scanner
/proc	☑	☑
/sys	☑	□

Figure 45. 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 the List of 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 + below the list and select the required object in the appeared window. You can also 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 – 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

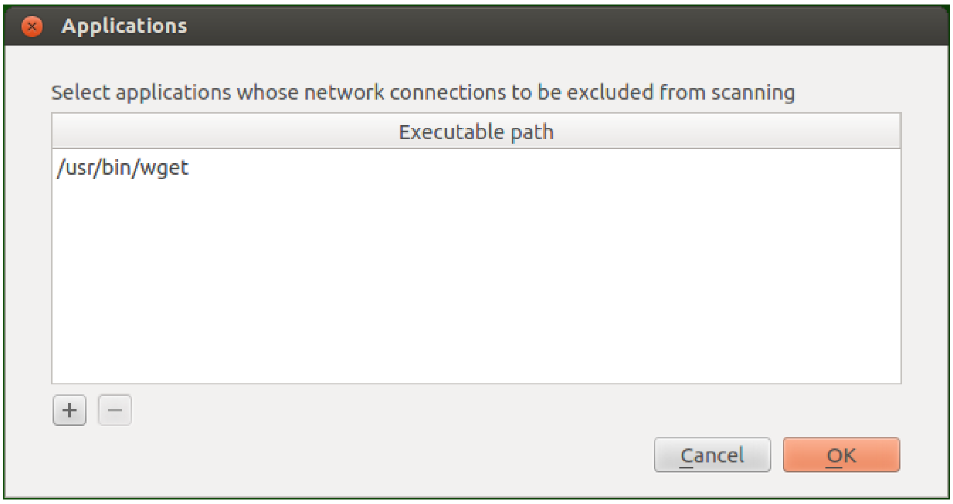
In this section:

- General Information.
- Adding and Removing Applications From the List of Exclusions.

General Information

You can exclude application 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.

Here you can list paths to the application executable files, which network connections should not be controlled by SpIDer Gate network connection monitor.


Applications
Select applications whose network connections to be excluded from scanning
Executable path
+
−
Cancel
OK

/usr/bin/wget

Figure 46. Configuring exclusions for network applications

Adding and Removing Applications From the List of Exclusions

- To add a new application to the list, click + 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 – 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

In this section:

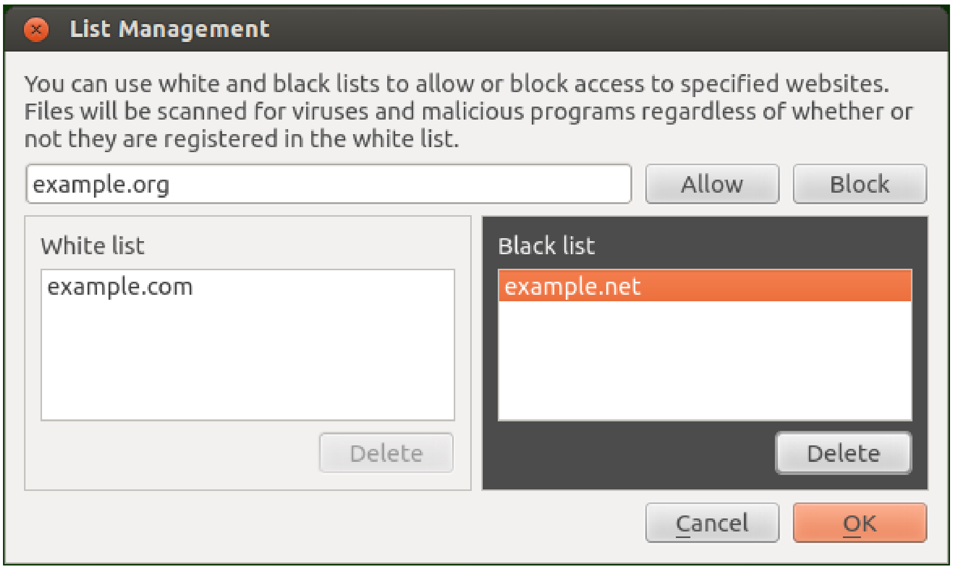
- General Information.

- Adding and Removing Websites From the Black and White Lists.

General Information

You can manage black and white lists of websites in the **List Management** window. To open it, click **Websites** on the **Exclusions** tab.

Here you can list the websites, access to which will be always disabled or, on the contrary, always enabled by the SpIDer Gate network connection monitor.



You can use white and black lists to allow or block access to specified websites. Files will be scanned for viruses and malicious programs regardless of whether or not they are registered in the white list.

Figure 47. 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, otherwise, denies access to all resources within the domain.
- To remove the website from white or black list, select it on the list and click **Delete**.

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

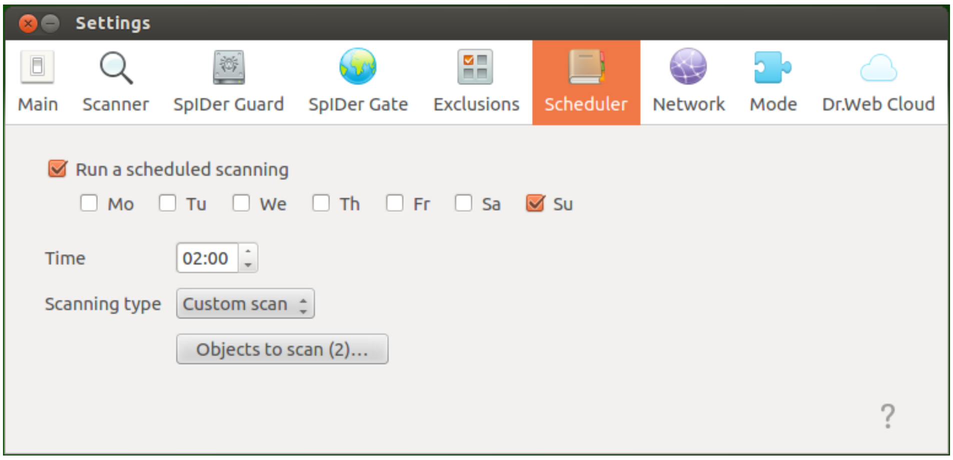
Scheduler Settings

In this section:

- General Information.
- Scheduler Settings.

General Information

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.



☑ Run a scheduled scanning

□ Mo □ Tu □ We □ Th □ Fr □ Sa ☑ Su

Time 02:00

Scanning type Custom scan

Figure 48. 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 interface for management if it is launched when the scanning starts. Scheduled scanning is not launched if Dr.Web for Linux operates under control of the centralized 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:

- Select the days of the week to start the scan (to do this, check the appropriate boxes).
- Set the time (hours and minutes) to start the scan.
- Select 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 **Objects to scan** (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 + 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.

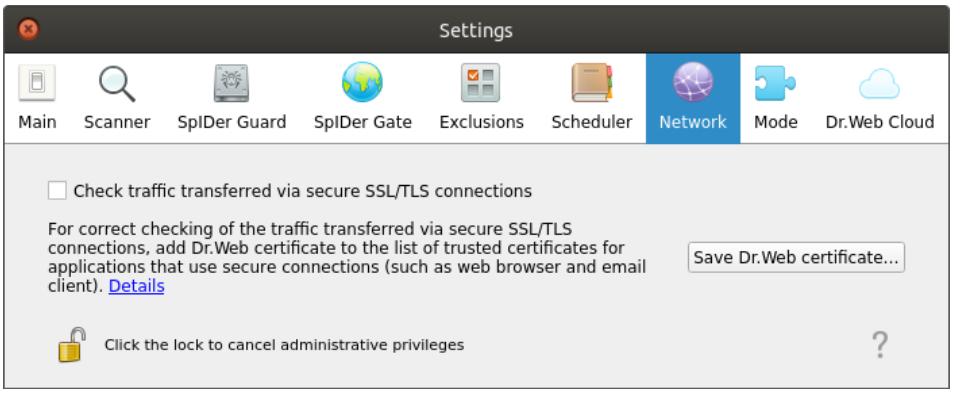
Protection Against Threats Distributed over Network

In this section:

- General Information.
- Configuring Scan of Protected Connections.
- Adding a Dr.Web Certificate to the Trusted Certificate List.
- Adding a Dr.Web Certificate to the Trusted Certificate via the Command Line.

General Information

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



□ Check traffic transferred via secure SSL/TLS connections

For correct checking of the traffic transferred via secure SSL/TLS connections, add Dr.Web certificate to the list of trusted certificates for applications that use secure connections (such as web browser and email client). Details

Click the lock to cancel administrative privileges

Figure 49. Secure connections checking configuration tab

Configuring Scan of Protected Connections

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

To manage the scan of protected traffic, the application must operate with elevated permissions. Refer to Managing Application Privileges section.

If a mail client using IMAP for receiving messages (for instance, Mozilla Thunderbird) is running on your system, restart it after the mode **Check traffic transferred via secure SSL/TLS connections** is enabled.

To ensure correct scan 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 **Save Dr.Web certificate** 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 manually add the saved file of the Dr.Web certificate 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.

Adding a 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.

Adding a Dr.Web Certificate to the Trusted Certificate List via the Command Line

Besides the graphical user interface, you can use the command line to add Dr. Web Certificate. To generate a certificate, perform the following command (you need to specify the name under which the certificate in PEM format will be saved):

```
$ drweb-ctl certificate > <cert_name>.pem
```

After that add the certificate to the system storage. This operation is performed by means of different commands in different Linux distributions. In Ubuntu, Debian, Mint:

```
# cp <cert_name>.pem /etc/ssl/certs/
# c_rehash
```

In CentOS and Fedora:

```
# cp <cert_name>.pem /etc/pki/ca-trust/source/anchors/
# update-ca-trust extract
```

Mode Settings

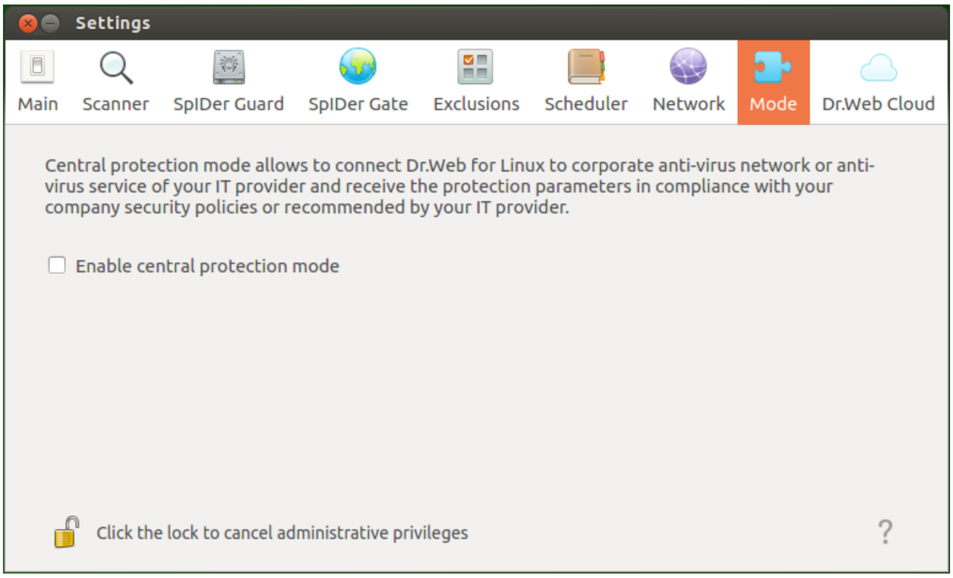
In this section:

- General Information.

- Connection to the centralized protection server.
- Advanced Settings.

General Information

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



Central protection mode allows to connect Dr.Web for Linux to corporate anti-virus network or anti-virus service of your IT provider and receive the protection parameters in compliance with your company security policies or recommended by your IT provider.

□ Enable central protection mode

Click the lock to cancel administrative privileges

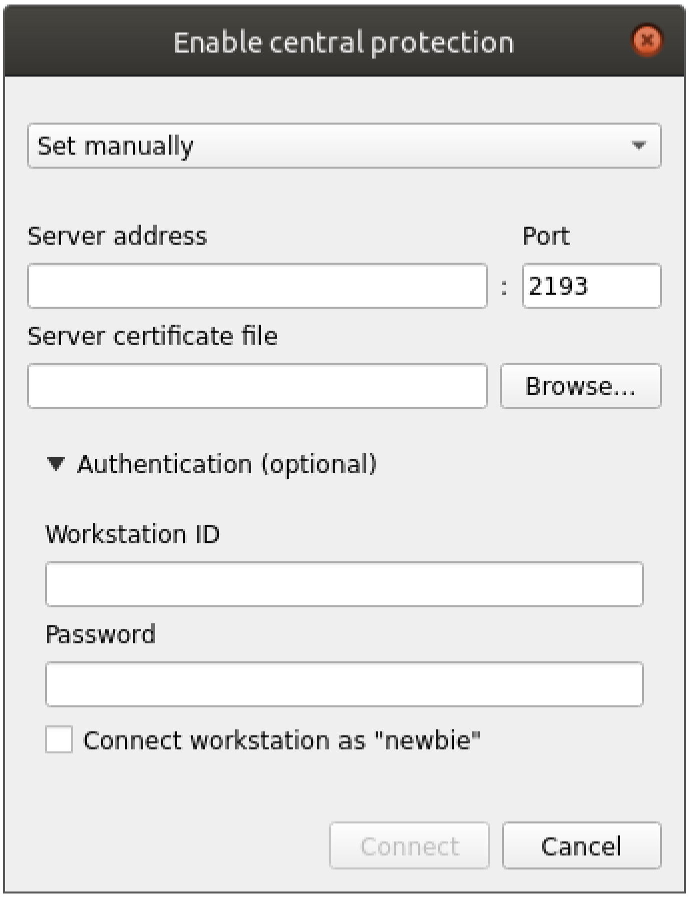
Figure 50. Mode tab

To connect Dr.Web for Linux to the centralized protection server or disconnect from that, select or clear the corresponding check box.

> To connect Dr.Web for Linux to the centralized protection server or disconnect from it, the application must have elevated privileges. Refer to Managing Application Privileges.

Connection to the Centralized Protection Server

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



Enable central protection

Set manually

Server address : Port

2193

Server certificate file

Browse...

▼ Authentication (optional)

Workstation ID

Password

□ Connect workstation as "newbie"

Connect Cancel

Figure 51. Connection to the centralized protection server

In the drop-down list located at the top of the window chose one of the methods for connecting to the centralized 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. If you select *Set manually* item, specify the address and the port of the centralized protection server. For *Set manually* or *Detect automatically* items, you should specify the path to the certificate 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 centralized protection server, if you know them. If these fields are filled in, then your connection to the centralized protection server will succeed only if a correct identifier/password pair was entered. If you leave these fields empty, connection to the centralized protection server is established only if it is approved by the centralized protection server (either automatically or by the anti-virus network administrator, depending on the server settings).

Moreover, you can use the **Connect to workstation as newbie** option (to connect as a newbie). If the option is allowed on the centralized 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 centralized protection server generates a new account for the host even if this host has a previously created account on the server.

> Specify connection parameters 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 centralized protection server, the program is administered by the server until the operation mode is switched to the standalone mode. In Centralized 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 your centralized 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.

Advanced Settings

From the **Maximum storage time for server messages** drop-down list, you can select the maximum storage time for messages about anti-virus network status and events that are received on your workstation from the centralized protection server. The messages will be automatically deleted at the end of the retention period even if they are not read.

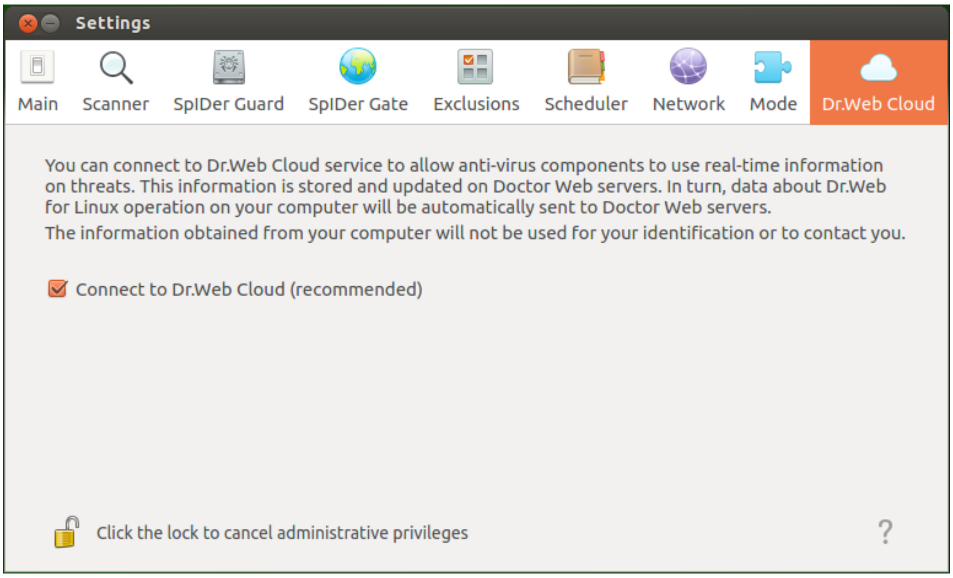
> The messages on the status and events of the anti-virus network will be received only if the anti-virus network administrator has configured messages delivery to your workstation on the centralized protection server Dr.Web for Linux is connected to. Otherwise, messages viewing will not be available and the **Maximum storage time for server messages** drop-down list will be not displayed on the protection mode settings page.

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.



You can connect to Dr.Web Cloud service to allow anti-virus components to use real-time information on threats. This information is stored and updated on Doctor Web servers. In turn, data about Dr.Web for Linux operation on your computer will be automatically sent to Doctor Web servers.
The information obtained from your computer will not be used for your identification or to contact you.

☑ Connect to Dr.Web Cloud (recommended)

Click the lock to cancel administrative privileges ?

Figure 52. Dr.Web Cloud tab

To allow or prohibit Dr.Web for Linux to use Dr.Web Cloud service, select or clear 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 Arguments

To launch Dr.Web for Linux GUI from the command line of the operating system, 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)` displays the information about supported command-line parameters and terminates operation of the GUI.
- `--version (-v)` displays the information on the GUI version.

- `--Autonomous (-a)` runs the autonomous copy of the Dr.Web for Linux GUI.
- `--FullScan` starts the full scan task upon Dr.Web for Linux GUI startup.
- `--ExpressScan` starts the express scan task upon Dr.Web for Linux GUI startup.
- `--CustomScan` starts the custom scan task upon Dr.Web for Linux GUI startup (opens page for selection of objects to scan).

Example:

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

This command launches Dr.Web for Linux GUI, 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 the scan 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 the Dr.Web for Linux graphical user interface as an autonomous copy, you will need a valid key file. Working in the centralized protection mode is not supported (you can install the key file, exported from the centralized protection server). In this case, even if Dr.Web for Linux is connected to the centralized protection server, the autonomous copy *does not notify* the centralized 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 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 scanning and quarantine management functions, supported by Scanner, are available.
- All the required paths (to virus databases, scan 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

In this section:

- General Information.
- Remote host scanning.

General Information

You can manage operation of Dr.Web for Linux from the command line of the operating system. For that, you can use the special Dr.Web Ctl utility (`drweb-ctl`). You can use it to perform the following operations:

- Start scanning file system objects including boot records.
- Launch of scanning of files on remote network hosts (see note below).
- Start updating anti-virus components (virus databases, the scan engine, and so on depending on the distribution).
- View and change parameters of the Dr.Web for Linux configuration.
- View the status of the Dr.Web for Linux components and statistics on detected threats.
- View quarantine and manage quarantined objects.
- Connect to the centralized protection server or disconnect from it.

User commands to control Dr.Web for Linux will only take effect 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 your 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 your 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 only returns a non-null exit code in the case of internal error (for example, the tool could not connect to a component, the requested operation could not be executed, and so on). If the tool detects and possibly neutralizes a threat, it returns the null exit code, because the requested operation (such as `scan`, and so on) is successfully completed. If you need to define the list of the detected threats and applied actions, analyze the messages displayed on the console.

Codes of all errors are listed in the Appendix D. Known Errors section.

Remote host scanning

Dr.Web for Linux allows you to scan files located on remote network hosts for threats. Such hosts can be not only fully-featured computing machines, such as workstations and servers, but also routers, set-top boxes, and other smart devices of the Internet of Things. To perform the remote scanning, the remote host has to provide a remote terminal access via *SSH* (*Secure Shell*) or *Telnet*. To access the device, you need to know an IP address and a domain name of the remote host, as well as the credentials of the user that can remotely access the system via *SSH* or *Telnet*. This 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 cure of malicious objects) using remote scanning is impossible. To eliminate the detected threats on the remote host, use administration tools provided directly by this host. For example, for routers and other smart devices, update the firmware; for computing machines, establish a connection (in a remote terminal mode, as one of the options) and perform the respective operations in the file system (remove or move files, etc.), or run the anti-virus software installed on them.

Remote scanning is only performed via the command-line tool `drweb-ctl` (using the command `remotescan`).

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: `$ drweb-ctl <command> -h`
`-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 `$ drweb-ctl <command> -d`

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 the centralized protection mode.
- Configuration management commands.
- Commands to manage detected threats and quarantine.
- Information commands.

> To request help about this component of the product from the command line, use the following command `man 1 drweb-ctl`

3.1. Anti-virus Scanning Commands

The following commands to manage anti-virus scanning are available:

Command	Description
`scan` *<path>*	Purpose: To initiate the scan of the specified file or directory by Scanner. Arguments: *<path>*—path to the file or directory to be scanned (the path can be relative). *This argument may be omitted if you use the* `--stdin` *or the* `--stdin0` *option. To specify several files that satisfy a certain criterion, use the* `find` *utility (see Usage Examples) and the* `--stdin` *or* `--stdin0` *option.* Options: `-a [--Autonomous]` runs an autonomous copy of scan engine and Scanner to perform the specified scan, terminating them after it is over. Note that threats detected during autonomous scanning will not be added to the common list of threats detected displayed by `threats` command (see below), and information on them will not be sent to the centralized protection server, if Dr.Web for Linux is controlled by it. `--stdin`—get the list of paths to scan from the standard input string (*stdin*). Paths in the list need to be separated by the next line character ('`\n`'). `--stdin0`—get the list of paths to scan from the standard input string (*stdin*). Paths in the list need to be separated by the zero character NUL ('`\0`'). When using `--stdin` and `--stdin0` options, the paths on the list should not contain patterns or regular expressions for a search. We recomment that you use the `--stdin` and `--stdin0` options to process a paths list generated by an external utility, for example, `find` in the `scan` command (see Usage Examples).

Command	Description
	--Exclude *<path>*—an excluded path. The path can be relative and contains a file mask (with the following wildcards: '?' and '*', as well as symbol classes '[ ]', '[!]', '[^]'). *Facultative option; can be set more than once.* --Report *<type>*—specifies the type of scan report. Allowed values: • BRIEF—brief report. • DEBUG—detailed report. • JSON—a serialized report in JSON format. Default value: *BRIEF* --ScanTimeout *<number>*—specify time-out to scan one file, in ms. If the value is set to *0*, time on scanning is not limited. Default value: *0* --PackerMaxLevel *<number>*—set the maximum nesting level when scanning packed objects. If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* --ArchiveMaxLevel *<number>*—set the maximum nesting level when scanning archives (zip, rar, and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* --MailMaxLevel *<number>*—set the maximum nesting level when scanning email messages (pst, tbb, and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* --ContainerMaxLevel *<number>*—set the maximum nesting level when scanning other containers (HTML and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* --MaxCompressionRatio *<ratio>*—set the maximum compression ratio of scanned objects. The ratio must be at least equal to *2*. Default value: *3000* --MaxSizeToExtract *<size>*—specify the maximum size for files enclosed in archives. Files whose size is greater than the value of this parameter will be skipped when scanning. There is no size limit for files in archives by default. The size is specified as a number with a suffix (b, kb, mb, gb). If no suffix is specified, the value is treated as size in bytes. --HeuristicAnalysis *<On|Off>*—enable or disable heuristic analysis during the scanning. Default value: *On*

Command	Description
	`--OnKnownVirus` *<action>*—an action to perform upon detection of a known threat by using signature-based analysis. *Possible actions: Report, Cure, Quarantine, Delete.* Default value: *Report* `--OnIncurable` *<action>*—an action to perform upon detection an incurable threat or when curing action (`Cure`) failed. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnSuspicious` *<action>*—an action to perform upon detection of a suspicious object by heuristic analysis. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnAdware` *<action>*—an action to perform upon detection of adware programs. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnDialers` *<action>*—an action to perform upon detection of a dialer. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnJokes` *<action>*—an action to perform upon detection of joke software. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnRiskware` *<action>*—an action to perform upon detection of riskware. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnHacktools` *<action>*—an action to perform upon detection of a hacktool. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* If threat is detected in a file placed in a container (an archive, an email message, and so on), instead of removing the file (*Delete*), the tool moves the container to the quarantine (*Quarantine*). `--FollowSymlinks`—resolve symlinks automatically
`bootscan` *<disk drive>* `| ALL`	Purpose: Start scanning boot records on the specified disks via the Scanner. Both MBR and VBR records are scanned.

Command	Description
	Arguments: <*disk drive*>—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 `ALL` is specified instead of the device file, all boot records on all available disk devices will be checked. Options: `-a [--Autonomous]` runs an autonomous copy of the scan engine and the Scanner to perform the specified scan, terminating them after it is over. Note that threats detected during autonomous scanning will not be added to the common list of detected threats displayed by `threats` command (see below), and information on them will not be sent to the centralized protection server, if Dr.Web for Linux is controlled by it. `--Report` <*type*>—specifies the type of scan report. Allowed values: • `BRIEF`—brief report. • `DEBUG`—detailed report. • `JSON`—a serialized report in JSON format. Default value: *BRIEF* `--ScanTimeout` <*number*>—specify time-out to scan one file, in ms. If the value is set to *0*, time on scanning is not limited. Default value: *0* `--HeuristicAnalysis` <*On|Off*>—enable or disable heuristic analysis during the scanning. Default value: *On* `--Cure` <*Yes|No*>—enable or disable attempts to cure detected threats. If the value is set to *No*, only a notification about a detected threat is displayed. Default value: *No* `--ShellTrace`—enable display of additional debug information when scanning a boot record.
`procscan`	Purpose: Initiates scanning of executables containing the code of currently running system 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. Arguments: None. Options: `-a [--Autonomous]` runs an autonomous copy of the scan engine and the Scanner to perform the specified scan, terminating them after it is over. Note that threats detected during autonomous scanning will not be added to the common list of detected threats displayed by `threats` command

Command	Description
	(see below), and information on them will not be sent to the centralized protection server, if Dr.Web for Linux is controlled by it. `--Report` <*type*>—specifies the type of scan report. Allowed values: • `BRIEF`—brief report. • `DEBUG`—detailed report. • `JSON`—a serialized report in JSON format. Default value: *BRIEF* `--ScanTimeout` <*number*>—specify time-out to scan one file, in ms. If the value is set to *0*, time on scanning is not limited. Default value: *0* `--HeuristicAnalysis` <*On*|*Off*>—enable or disable heuristic analysis during the scanning. Default value: *On* `--PackerMaxLevel` <*number*>—set the maximum nesting level when scanning packed objects. If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* `--OnKnownVirus` <*action*>—an action to perform upon detection of a known threat by using signature-based analysis. Possible actions: *Report, Cure, Quarantine, Delete*. Default value: *Report* `--OnIncurable` <*action*>—an action to perform upon detection an incurable threat or when curing action (`Cure`) failed. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnSuspicious` <*action*>—an action to perform upon detection of a suspicious object by heuristic analysis. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnAdware` <*action*>—an action to perform upon detection of adware programs. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnDialers` <action>—an action to perform upon detection of a dialer. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnJokes` <*action*>—an action to perform upon detection of joke software.

Command	Description
	Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnRiskware` <*action*>—an action to perform upon detection of riskware. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* `--OnHacktools` <*action*>—an action to perform upon detection of a hacktool. Possible actions: *Report, Quarantine, Delete*. Default value: *Report* Note that if a threat is detected in an executable file, Dr.Web for Linux terminates all processes started by the file.
`remotescan` <*host*> <*path*>	Purpose: Initiates scanning of the specified file or directory on the specified remote host by connecting to it via *SSH* or *Telnet*. 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 `threats` command (see below). 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, and so on), or via running an anti-virus software installed on them. Arguments: <*host*>—IP address or a domain name of the remote host. <*path*>—path to the file or directory to be scanned (the path must be absolute). Options: `-m [--Method]` <*SSH|Telnet*>—remote host connection method (protocol). *If method is not specified, SSH is used.*

Command	Description
	`-l [--Login]` <*name*>—login (user name) used for authorization on the remote host via the selected protocol. *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 [--Identity]` <*path to file*>—path to the file containing a private key used for authentication of the specified user via the selected protocol. `-p [--Port]` <*number*>—number of the port on the remote host for connecting via the selected protocol. Default value: *default port for the selected protocol (22 for SSH, 23 for Telnet).* `--ForceInteractive`—use the SSH interactive session (only for *SSH* connections). *Optional feature.* `--TransferListenAddress` <*address*>—an address, listened to receive files transferred from the remote device for scanning. *Optional feature. If not indicated, an arbitrary address is used.* `--TransferListenPort` <*port*>—a port, listened to receive files transferred from the remote device for scanning. *Optional feature. If not indicated, an arbitrary port is used.* `--TransferExternalAddress` <*address*>—an address specified to the remote device to send files for scanning. *Optional feature. If not indicated, use the* `--TransferListenAddress` *value, or the outgoing address of the already established session.* `--TransferExternalPort` <*port*>—a port to transfer files for scanning, specified for the remote device. *Optional feature. If not indicated, an automatically determined port is used.* `--Password` <*password*>—password used for authentication of a user via the selected protocol. *Please note that the password is transferred as a plain text.* `--Exclude` <*path*>—the path to be excluded from scanning. The path can contain a file mask with the following allowed symbols: '`?`' and '`*`', as well as the symbol classes '`[ ]`', '`[! ]`', '`[^ ]`'. The path (including the path with the file mask) mast be absolute. *Facultative option; can be set more than once.* `--Report` <*type*>—specifies the type of scan report. Allowed values: • `BRIEF`—brief report. • `DEBUG`—detailed report. • `JSON`—a serialized report in JSON format. Default value: *BRIEF* `--ScanTimeout` <*number*>—specify time-out to scan one file, in ms. If the value is set to *0*, time on scanning is not limited.

Command	Description
	Default value: *0* `--PackerMaxLevel` <*number*>—set the maximum nesting level when scanning packed objects. If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* `--ArchiveMaxLevel` <*number*>—set the maximum nesting level when scanning archives (zip, rar, and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* `--MailMaxLevel` <*number*>—set the maximum nesting level when scanning email messages (pst, tbb, and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* `--ContainerMaxLevel` <*number*>—set the maximum nesting level when scanning other containers (HTML and so on). If the value is set to *0*, nested objects will be skipped during scanning. Default value: *8* `--MaxCompressionRatio` <*ratio*>—set the maximum compression ratio of scanned objects. The ratio must be at least equal to *2*. `--MaxSizeToExtract` <*size*>—specify the maximum size for files enclosed in archives. Files whose size is greater than the value of this parameter will be skipped when scanning. There is no size limit for files in archives by default. The size is specified as a number with a suffix (b, kb, mb, gb). If no suffix is specified, the value is treated as size in bytes. Default value: *3000* `--HeuristicAnalysis` <*On*|*Off*>—enable or disable heuristic analysis during the scanning. Default value: `On`
`checkmail` <*path to file*>	Purpose: Performs scan of an email message saved to a file for threats, signs of spam, malicious links, or non-compliance with rules of mail processing (using the emails processing component). The console output thread (*stdout*) will display the message scanning results and the action applied to this message while scanning by the email processing component. Arguments: <*path to file*>—path to file of the email message that requires scanning. Mandatory argument. Options: `--Report` <*type*>—specifies the type of scan report. Allowed values:

Command	Description

	• *BRIEF*—brief report.
	• *DEBUG*—detailed report.
	• *JSON*—a serialized report in JSON format.
	Default value: *BRIEF*
	`-r [--Rules]` *<list of rules>*—indicate a list of rules to follow during an email message scanning.
	If the rules are not indicated, the following set of rules used by default will be applied:
	`threat_category in (KnownVirus, VirusModification,`
	`UnknownVirus, Adware, Dialer) : REJECT`
	`total_spam_score gt 0.80 : REJECT`
	`url_category in (InfectionSource, NotRecommended,`
	`CopyrightNotice) : REJECT`
	If Dr.Web Anti-Spam is not installed, the scanning rule for spam (the second string) will be automatically excluded from the set.
	`-c [--Connect]` *<IP>:<port>*—indicate a network socket that will be used as an address for connection by a sender of the scanned message.
	`-e [--Helo]` *<name>*—indicate an identifier of a client that sent a message (IP address or FQDN host, as for the SMTP command HELO/EHLO).
	`-f [--From]` *<email>*—indicate an email address of a sender (as for the SMTP command MAIL FROM).
	If the address is not indicated, the respective address from an email will be used.
	`-t [--Rcpt]` *<email>*—indicate an email address of a recipient (as for the SMTP command RCPT TO).
	If the address is not indicated, the respective address from an email will be used.
	If emails processing component is not installed, calling this command will return an error.

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 the centralized protection mode

The following commands for managing updates are available, as well as commands for operation in the centralized protection mode:

Command	Description
`update`	Purpose: Initiates updates of anti-virus components (virus databases, the scan engine, etc., depending on the distribution) from the Doctor Web update servers or the local cloud, terminates the updating process if already running, or performs rollback of the latest update to previous versions of the updated files. The command has no effect if Dr.Web for Linux is connected to the centralized protection server. Arguments: None. Options: `-l [--local-cloud]` uses the local cloud connected to Dr.Web for Linux to download the updates. If the option is not specified, the updates are downloaded from the Doctor Web update servers (default behavior). `--From` *<path>*—apply updates from a specified directory offline. `--Path` *<path>*—store files for updating offline in a specified directory; if this directory already has files, then they will be updated. `--Rollback`—rollback the last update, and restore the previous version of files that have been updated during the last update. `--Stop`—terminate the running updating process.
`esconnect` *<server>*`[:`*<port>*`]`	Purpose: Connects Dr.Web for Linux to the specified centralized protection server (for example, Dr.Web Enterprise Server). For details on the operation modes, refer to the Operation Modes. Arguments: • *<server>*—IP address or network name of the host on which the centralized protection server is operating. This argument is mandatory. • *<port>*—port number used by the centralized protection server. The argument is optional and should be specified only if the centralized protection server uses a non-standard port. Options: `--Certificate` *<path>*—a file path to a certificate of the centralized protection server, the connection to which will be established.

Command	Description
	`--Login` <*ID*>—login (workstation identifier) used for connection to the centralized protection server. `--Password` <*password*>—password for connection to the centralized protection server. `--Group` <*ID*>—identifier of the group to which the workstation is added on connection. `--Rate` <*ID*>—identifier of the tariff group applied to your workstation when it is included in one of the centralized protection server groups (can be specified only together with the `--Group` option). `--Compress` <*On*|*Off*>—enables (*On*) or disables (*Off*) forced compression of transmitted data. If not specified, usage of compression is determined by the server. `--Encrypt` <*On*|*Off*>—enables (*On*) or disables (*Off*) forced encryption of transmitted data. If not specified, usage of encryption is determined by the server. `--Newbie`—connect as a "newbie" (get a new account on the server). This command requires `drweb-ctl` to be started with *root* privileges. If necessary, use the `su` or `sudo` commands.
`esdisconnect`	Purpose: Disconnect Dr.Web for Linux from the centralized protection server and switch its operation to standalone mode. The command has no effect if Dr.Web for Linux already operates in standalone mode. Arguments: None. Options: None. This command requires `drweb-ctl` to be started with *root* privileges. If necessary, use the `su` or `sudo` commands.

3.3. Configuration Management Commands

The following commands to manage configuration are available:

Command	Description
`cfset` <*section*>`.`<*parameter*>	Purpose: To change the active value of the specified parameter in the current configuration of Dr.Web for Linux.

Command	Description
<value>	Arguments: • *<section>*—name of the configuration file section where the parameter resides. This argument is mandatory. • *<parameter>*—name of the parameter. The argument is mandatory. • *<value>*—new parameter value. This argument is mandatory. To specify the parameter value, we use the format *<section>*.*<parameter>* *<value>*. Assignment character '=' is not used here. Note that if you want to indicate several parameter values, you need to repeatedly call the `cfset` command, as many times as the number of parameter values you want to add. To add a new value to the list of parameter values, you need to use the `-a` option (see below). You cannot specify the string *<parameter>* *<value 1>*, *<value 2>* as an argument, because the string "*<value 1>*, *<value 2>*" will be considered one value of the *<parameter>*. For description of the configuration file, refer to the documentation page displayed by `man 5 drweb.ini`. **Options:** `-a [--Add]`—do not substitute the current parameter value but add the specified value to the list (allowed only for parameters that can have several values, specified as a list). You should also use this option to when adding a new parameter group identified by a tag. `-e [--Erase]`—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). `-r [--Reset]`—reset the parameter value to the default. At that, *<value>* is not required in the command and is ignored if specified. 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. This command requires `drweb-ctl` to be started with root privileges. If necessary, use the `su` or `sudo` commands.
`cfshow [`*<section>*`[.`*<parameter>*`]]`	**Purpose:** Displays parameters of the current configuration of Dr.Web for Linux.

Command	Description
	The command to display parameters is specified as follows *<section>*.*<parameter>* = *<value>*. Sections and parameters of non-installed components are not displayed. **Arguments:** • *<section>*—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. • *<parameter>*—name of the displayed parameter. Optional argument. If not specified, all parameters of the section are displayed. Otherwise, only this parameter is displayed. If a parameter is specified without the section name, all parameters with this name from all of the configuration file sections are displayed. **Options:** `--Uncut`—display all configuration parameters (not only those 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. `--Changed`—display only those parameters whose values differ from the default ones. `--Ini`—display parameter values in the INI file format: at first, the section name is specified in square brackets, then the section parameters listed as *<parameter>* = *<value>* pairs (one pair per line). `--Value`—display only value of the specified parameter (the *<parameter>* argument is mandatory in this case).
`reload`	Purpose: Restarts Dr.Web for Linux service components. During the procedure, logs are reopened, the configuration file is reread, and the attempt to restart abnormally terminated components is performed. Arguments: None. Options: None.

3.4. Commands to Manage Detected Threats and Quarantine

The following commands for managing threats and quarantine are available:

Command	Description
`threats [`*<action> <object>*`]`	Purpose: Apply the specified action to detected threats, selected by their identifiers. Type of the action is specified by the command option. If the action is not specified, displays information on detected but not neutralized threats. The information on threats is displayed according the format, specified using the optional `--Format` option. If the `--Format`

Command	Description
	option is not specified, for each threat the following information is displayed: • 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, and so on. Arguments: None. Options: `--Format "`<*format string*>`"`—displays information on threats in the specified format. The description of format string is below. *If this option is specified along with any action options, it is ignored.* `-f [--Follow]`—wait for new messages about new threats and display them once they are received (CTRL+C interrupts the waiting). *If this option is specified along with any action options, it is ignored.* `--Directory` <*list of directories*>—displays only threats detected in files in directories from <*list of directories*>. *If this option is applied along with any options mentioned below, it is ignored.* `--Cure` <*threat list*>—attempt to cure the listed threats (list threat identifiers separating them with commas). `--Quarantine` <*threat list*> moves the listed threats to quarantine (list threat identifiers are separated with commas). `--Delete` <*threat list*>—delete the listed threats (list threat identifiers separating them with commas). `--Ignore` <*threat list*>—ignore the listed threats (list threat identifiers separating them with commas). If you need to apply the action to all detected threats, specify `All` instead of <*threat list*>. For example, the command: `$ drweb-ctl threats --Quarantine All` moves all detected malicious objects to quarantine.

`quarantine`
`[`<*action*> <*object*>`]`
	Purpose: Applies an action to the specified object in quarantine.
	If an action is not specified, information on quarantined objects and their identifiers together with brief information on original files moved to quarantine is displayed. Information on isolated objects is displayed according a format, specified with optional `--Format` argument. If the `--`

Command	Description
	`Format` argument is not specified, for every isolated (quarantined) object the following information is displayed: • 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). Arguments: None. Options: `-a [--Autonomous]` starts a separate instance of the Scanner to perform the specified quarantine command and terminate it upon completion. *This option can be applied along with any options mentioned below.* `--Format "`*<format string>*`"`—displays information on quarantined objects in the specified format. The description of format string is below. *If this option is specified along with any action options, it is ignored.* `-f [--Follow]`—wait for new messages about new threats and display them once they are received (CTRL+C interrupts the waiting). *If this option is specified along with any action options, it is ignored.* `--Discovery [`*<list of directories>*`,]` searches for quarantine directories in the specified list of directories and add them to the consolidated quarantine upon detecting a threat. If the *<list of directories>* is not specified, it searches for quarantine directories in the common locations of the file system (volume mounting points and user home directories). *This option can be specified not only with the* `-a` *(*`--Autonomous`*) option (see above), but also with any options/actions listed below. Moreover, if the* `quarantine` *command is launched as an autonomous copy, that is, with the* `-a` *(*`--Autonomous`*) option but without the* `--Discovery` *option, then it is equivalent to the call of:* `quarantine --Autonomous --Discovery` `--Delete` *<object>*—delete the specified object from quarantine. *Note that objects are deleted from quarantine permanently—this action is irreversible.* `--Cure` *<object>*—try to cure the specified object in the quarantine. *Note that even if the object was successfully cured, it will remain in quarantine. To restore the cured object from quarantine, use the* `--Restore` *option.* `--Restore` *<object>*—restore the specified object from the quarantine to its original location.

Command	Description
	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.* `--TargetPath` <*path*>—restores an object from the quarantine to the specified location: either as a file with the name specified here (if the <*path*> is a path to a file), or just to the specified directory (if the <*path*> is a path to a directory). A path can be an absolute as well as relative (referring to a current directory). *Note that this option can only be used in combination with the* `--Restore` option. As an <*object*>, specify the object identifier in quarantine. To apply the action to all quarantined objects, specify `All` instead of <*object*>. For example, the command: `$ drweb-ctl quarantine --Restore All --TargetPath test` restores all quarantined objects and puts them in `test` subdirectory, located in a current directory, from which `drweb-ctl` command was launched. *Note that for the* `--Restore All` *variant the additional option* `--TargetPath`*, if specified, must set a path to a directory, not a path to a file.*

Formatted output for threats and quarantine commands

The output format is defined using the format string, specified as the optional argument `--Format`. The format string must be specified in quotes. The format string can include common symbols (displayed “as is”), as well as special markers, output as certain information. The following markers are available:

1. Common for `threats` and `quarantine` commands:

Marker	Description
`%{n}`	New string
`%{t}`	Tabulation
`%{threat_name}`	The name of detected threat (virus) according Doctor Web classification
`%{threat_type}`	Threat Type (“known virus”, and so on) according Doctor Web classification
`%{size}`	Original file size
`%{origin}`	The full name of the original file with path
`%{path}`	Synonym for `%{origin}`

Marker	Description
`%{ctime}`	Date/time of original file modifying in "*%Y-%b-%d %H:%M:%S*" format (for example, "`2018-Jul-20 15:58:01`")
`%{timestamp}`	Similar to `%{ctime}`, but in the *UNIX timestamp* format
`%{owner}`	Username of the original file owner
`%{rowner}`	The remote user owner of the original file (if not applicable or value is unknown it is replaced with `?`)

2. Specific for `threats` command:

Marker	Description
`%{hid}`	The identifier of the threat record in the history of events associated with the threat
`%{tid}`	The threat identifier
`%{htime}`	Date/time of the event related to a threat
`%{app}`	The identifier of the Dr.Web for Linux component which processed a threat
`%{event}`	The latest event related to a threat: • `FOUND`—a threat was detected; • `Cure`—a threat was cured; • `Quarantine`—a file with threat was moved to quarantine; • `Delete`—a file with threat was deleted; • `Ignore`—a threat was ignored; • `RECAPTURED`—a threat was detected again by an other component.
`%{err}`	Error message text (if no error is replaced with an empty string)

3. Specific for `quarantine` command:

Marker	Description
`%{qid}`	The identifier of quarantined object
`%{qtime}`	Date/time of moving the object to quarantine
`%{curetime}`	Date/time of curing attempt of the object moved to quarantine (if not applicable or value is unknown it is replaced with `?`)
`%{cureres}`	The result of the quarantined object curing attempt: • `cured`—a threat is cured; • `not cured`—a threat was not cured or no curing attempts were performed.

Example

```
$ drweb-ctl quarantine --Format "{%{n} %{origin}: %{threat_name} - %{qtime}%
{n}}"
```

This command displays quarantine contents as records of the following type:

```
{
 <path to file>: <threat name> - <date of moving to quarantine>
}
...
```

3.5. Information Commands

The following information commands are available:

Command	Description
`appinfo`	Purpose: Output information on the active Dr.Web for Linux components. The following information is displayed about each component that is currently running: • Internally-used name. • Process identifier GNU/Linux (PID). • State (running, stopped, and so on). • Error code, if the work of the component has been terminated because of an error. • Additional information (optional). For the configuration daemon (`drweb-configd`) the following is displayed as additional information: • The list of installed components—*Installed*. • The list of components which must be launched by the configuration daemon—*Should run*. Arguments: None. Options: `-f [--Follow]`—waits for new messages on module status change and display them once such a message is received (CTRL+C interrupts the waiting).
`baseinfo`	Purpose: Display the information on the current version of the scan engine and status of virus databases. The following information is displayed: • Version of the scan engine. • Date and time when the virus databases that are currently used were issued.

Command	Description
	• The number of available virus records (in the virus databases). • The time of the last successful update of the virus databases and of the scan engine. • The time of the next scheduled automatic update. Arguments: None. Options: `-l [--List]`—displays the full list of downloaded files of virus databases and number of virus records in each file.
`certificate`	Purpose: Displays contents of the trusted Dr.Web certificate used by Dr.Web for Linux to scan protected connections if this option is enabled on the settings page. To save the certificate to the <*cert_name*>`.pem` file, you can use the following command: `$ drweb-ctl certificate > <cert_name>.pem` Arguments: None. Options: None.
`events`	Purpose: Viewing the Dr.Web for Linux events. Apart from that, the command allows you to manage events (mark as read, remove). Arguments: None. Options: `--Report` <*type*>—specify the type of event report. Allowed values: • `BRIEF`—brief report. • `DEBUG`—detailed report. • `JSON`—a serialized report in JSON format. `-f [--Follow]`—waits for new events and displays them upon emergence (CTRL + C interrupts the standby). `-s [--Since]` <*date, time*>—shows the events that occurred before the specified timestamp (<*date, time*> is specified as `YYYY-MM-DD hh:mm:ss`). `-u [--Until]` <*date, time*>—shows the events that occurred no later than the specified timestamp (<*date, time*> is specified as `YYYY-MM-DD hh:mm:ss`). `-t [--Types]` <*type list*>—shows only events of the specified types (separated by commas). The following event types are available: • `Mail`—indicates that a threat has been detected in an email;

Command	Description
	• `UnexpectedAppTermination`—unexpected shutdown of a component. To view all types of events, use `All`. `--ShowSeen`—displays of already read events as well. `--Show` <*list of events*>—displays the listed events (event identifiers are separated by commas). `--Delete` <*list of events*>—removal of listed events (event identifiers are separated by commas). `--MarkAsSeen` <*list of events*>—marks the listed events as read (event identifiers are separated with a comma). If you want to mark as “read” or delete all events, specify `All` instead of <*events list*>. For example, the command: `$ drweb-ctl events --MarkAsSeen All` will mark as “read” all existing events.
`report` <*type*>	Purpose: Create a report on Dr.Web for Linux events in the HTML format (the page body is output to the specified file). Arguments: <*type*>—event type that required reporting (indicate one type). See possible values in the `--Types` option description of the `events` command above. A mandatory argument. Options: `-o [--Output]` <*path to file*>—save the report to the specified file. The option is mandatory. `-s [--Since]` <*date, time*>—reports events that occurred no earlier than the specified timestamp (<*date, time*> is specified as `YYYY-MM-DD hh:mm:ss`). `-u [--Until]` <*date, time*>—reports the events that occurred no later than the specified timestamp (<*date, time*> is specified as `YYYY-MM-DD hh:mm:ss`). `--TemplateDir` <*path to directory*>—a path to the directory that contains HTML report templates. Options `-s`, `-u`, and `--TemplateDir` are not mandatory. For example, the following command `$ drweb-ctl report Mail -o report.html` generates a report on all existing email message threat detection events, based on the default template, and saves the result in the `report.html` file in the current directory.

Command	**Description**
`license`	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 website). If no options are specified, then the following information is displayed (if you are using a license for the standalone mode): • License number. • Date and time when the license expires. If you are using a license provided to you by the centralized protection server (for the use of the product in the centralized protection mode or in the mobile mode), then the appropriate message will be displayed. Arguments: None. Options: `--GetDemo` requests a demo key that is valid for one month. You receive the key if you meet the conditions for the provision of a demo period. `--GetRegistered` <*serial number*>—get a license key file for the specified serial number, if the conditions for the provision of a new key file have not been breached (for example, breached by using the product not in the centralized protection mode, when the license is managed by a centralized protection server). `--Proxy http://`<*username*>`:`<*password*>`@`<*server address*>`:`<*port*>—get a license key via the proxy server (used only with one of the previously mentioned options) — `--GetDemo` or `--GetRegistered).` *If the serial number is not the one provided for the demo period, you must first register it at the company website.* For further information on licensing of Dr.Web products, refer to the Licensing section. To register a serial number or to get a demo period, an internet connection is required.
`log`	Purpose: Displays the latest log records of Dr.Web for Linux on console screen (in the *stdout* thread), similar to `tail` command. Arguments: None. Options: `-s [--Size]` <*number*>—the number of the last log records that are to be displayed on a screen. `-c [--Components]` <*components list*>—the list of component identifiers, which records are displayed. Identifiers are defined with comma separation. If the argument is not defined, all available records logged by all components are displayed.

Command	Description
	Actual identifiers of the components installed (e.g. internal components names, displayed in log) you can define by using the `appinfo` *command (see above).* `-f [--Follow]`—waits for new messages in log and display them once such a message is received (interrupt waiting by pressing CTRL+C).

Usage Examples

This section contains examples of using the Dr.Web Ctl (`drweb-ctl`) utility:

- Object Scanning:
    - Simple Scanning Commands.
    - Scanning of Files Selected by Criteria.
    - Scanning of Additional Objects.
- Configuration Management.
- Threats Management.
- An Example of Operation in the Autonomous Copy Mode.

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 procscan
```

1.2. Scanning of Files Selected by Criteria

Examples for file selection for scanning are listed below and use the result of the `find` utility operation. The obtained list of files is sent to the `drweb-ctl scan` command with the `--stdin` or `--stdin0` parameter.

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 host *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 Dr.Web for Linux package, including information about running components:

```
$ 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 SpIDer Guard file system monitor):

```
# 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. Force update of anti-virus components of Dr.Web for Linux:

```
$ drweb-ctl update
```

5. Restart the component configuration of Dr.Web for Linux:

```
# 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 Dr.Web for Linux to the centralized protection server operating on host *192.168.0.1* if the server certificate is located in the file `/home/user/cscert.pem`:

```
$ drweb-ctl esconnect 192.168.0.1 --Certificate /home/user/cscert.pem
```

7. Connect Dr.Web for Linux to the centralized protection server using the `settings.cfg` configuration file:

   ```
   $ drweb-ctl esconnect --cfg <path to the settings.cfg file>
   ```

8. Disconnecting Dr.Web for Linux from the centralized protection server:

   ```
   # 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
   ```

9. View the last log records made by the `drweb-update` and `drweb-configd` components in the Dr.Web for Linux log:

   ```
   # drweb-ctl log -c Update,ConfigD
   ```

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 scan 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, and so on) 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* nit only encrypt there 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 so on) 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, and so on).
- *Chat worms* use protocols of popular messengers and chat programs (ICQ, IM, IRC, and so on).

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, and so on) or makes it possible for hackers to access the computer without permission, for example, to harm the computer of a third party.

Trojan 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. The aim of this is to steal personal information (i.e. network passwords, logins, credit card data, and so on).
- *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 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, and so on.

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 positives. 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. It allows to thoroughly scan for suspicious files and control software behavior.

- Detection Methods.
- Threat-related Actions.

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 scanning 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 scans 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.

Cloud-based Threat Detection Technologies

Cloud-based detection methods allow to scan any object (file, application, browser extension, etc.) by its hash value. Hash is a unique sequence of numbers and letters of a given length. When analyzed by a hash value, objects are scanned using the existing database and then classified into categories: clean, suspicious, malicious, etc.

This technology optimizes the time of file scanning and saves device resources. The decision on whether the object is malicious is made almost instantly, because it is not the object that is analyzed, but its unique hash value. If there is no connection to the Dr.Web Cloud servers, the files are scanned locally, and the cloud scan resumes when the connection is restored.

Thus, the Dr.Web Cloud service collects information from numerous users and quickly updates data on previously unknown threats increasing the effectiveness of device protection.

Actions

To avert computer threats, Dr.Web anti-virus 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** *(Ignore)*—instructs to skip the detected threat without performing any other action.
- **Report** *(Report)*—instructs to inform on the detected threat without performing any other action.
- **Cure** *(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** *(Quarantine)*—instructs to move the detected threat to a special directory and isolate it from the rest of the system.
- **Delete** *(Delete)*—instructs to remove the infected object permanently.

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

Appendix C. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
- Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

- Fill out a web form in the appropriate section at https://support.drweb.com/.
- Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.

To facilitate processing of your issue, we recommend that you generate a data set for the installed product, its configuration, and system environment before contacting the technical support. To do that, you can use a special utility included in the Dr.Web for Linux distribution.

To collect the data for technical support, use the following command:

```
# /opt/drweb.com/bin/support-report.sh
```

> To collect all data required for technical support, we recommend that you launch the utility with superuser privileges (i.e. privileges of the *root* user). To elevate your privileges, log in as a different user with the `su` command or use the `sudo` command to execute the command on behalf of another user.

During operation, the utility collects and archives the following information:

- OS data (name, architecture, result of the `uname -a` command);
- List of packages installed to your system, including Doctor Web packages;
- Log contents:
  - Dr.Web for Linux logs (if configured for separate components);
  - log of the `syslog` system daemon (`/var/log/syslog`, `/var/log/messages`);
  - log of a system package manager (`apt`, `yum`, etc.);
  - the `dmesg` log;
- Output of the following commands: `df`, `ip a` (`ifconfig -a`), `ldconfig -p`, `iptables-save`, `nft export xml`.
- Information on settings and configuration of Dr.Web for Linux:
  - list of downloaded virus databases (`drweb-ctl baseinfo -l`);
  - list of files from Dr.Web for Linux directories and MD5 hash values of these files;
  - Dr.Web Virus-Finding Engine scan engine version and MD5 hash value;
  - configuration parameters of Dr.Web for Linux (including contents of `drweb.ini`, rules, value files used in rules, Lua procedures, etc.);
  - user information and permissions retrieved from the key file, if Dr.Web for Linux is running in the standalone mode.

An archive containing information on the product and its system environment will be saved to the home directory of the user that launched the utility. The file will be named as follows:

```
drweb.report.<timestamp>.tgz
```

where <*timestamp*> is a full timestamp of creating the report, down to milliseconds, for example: `20190618151718.23625`.

Appendix D. Known Errors

Here we can find:

- Recommendations for Error Identification
- Errors Codes
- Errors without Code

> If the occurred error is not present, contact technical support. Be ready to name the error code and describe steps to reproduce the issue.

Recommendations for Error Identification

- To identify a possible cause and background of the error, refer to the Dr.Web for Linux log (by default, it is located in the `/var/log/syslog` file or the `/var/log/messages` file, depending on OS). Also, you can use the command `drweb-ctl log`.
- 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 Codes

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:

1. Restart the configuration daemon by executing the command

```
# service drweb-configd restart
```

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 Dr.Web for Linux settings to the defaults.

   To do it, clear the contents of the <*etc_dir*>`/drweb.ini` 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 Dr.Web for Linux or its 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	*Operation is already in progress*
Error code	`x2`
Description	Operation requested by the user is already in progress.

Resolving the error:

1. Wait until the 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	*Operation is in pending state*
Error code	`x3`
Description	The operation requested by the user is in pending state (possibly, a network connection is currently establishing or one of Dr.Web for Linux 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	*Interrupted by user*
Error code	`x4`
Description	The action has been 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	*Operation canceled*
Error code	`x5`
Description	The action has been canceled (the execution of the action may have timed out).

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	*IPC connection terminated*
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	*Invalid IPC message size*
Error code	`x7`
Description	A message of invalid size has been received during component interprocess communication (IPC).

Resolving the error:

1. Uninstall Dr.Web for Linux by entering the following command:

   ```
   # service drweb-configd restart
   ```

If the error persists, contact technical support and be ready to name the error code.

Error message	*Invalid IPC message format*
Error code	`x8`

Description	A message of invalid format has been received during component inter-process communication (IPC).

Resolving the error:

1. Uninstall Dr.Web for Linux by entering the following command:

```
# service drweb-configd restart
```

If the error persists, contact technical support and be ready to name the error code.

Error message	*Not ready*
Error code	`x9`
Description	The required action cannot be performed because the necessary component or device has not been 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	*The component is not installed*
Error code	`x10`
Description	The required operation cannot be performend because the necessary component has not been installed yet.

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 Gate 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 Dr.Web for Linux or its 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	*Unexpected IPC message*
Error code	`x11`

Description	An unexpected message has been received during component inter-process communication (IPC).

Resolving the error:

1. Uninstall Dr.Web for Linux by entering the following command:

   ```
   # service drweb-configd restart
   ```

If the error persists, contact technical support and be ready to name the error code.

Error message	*IPC protocol violation*
Error code	`x12`
Description	Protocol violation occurred during component inter-process communication (IPC).

Resolving the error:

1. Uninstall Dr.Web for Linux by entering the following command:

   ```
   # service drweb-configd restart
   ```

If the error persists, contact technical support and be ready to name the error code.

Error message	*Subsystem state is unknown*
Error code	`x13`
Description	The current state of a subsystem necessary to performing the requested operation is not known.

Resolving the error:

1. Repeat the operation.
2. If the error persists, restart Dr.Web for Linux by executing the command:

   ```
   # service drweb-configd restart
   ```

   and then repeat the operation.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Path must be absolute*
Error code	`x20`

<table>
<tr><td><b>Description</b></td><td>A relative path to a file or directory is specified whereas an absolute path is required</td></tr>
<tr><td colspan="2"><b>Resolving the error:</b>
1. Change the path to the file or the directory so as to make the path absolute.</td></tr>
<tr><td colspan="2">If the error persists, contact technical support and be ready to name the error code.</td></tr>
</table>

<table>
<tr><td><b>Error message</b></td><td><i>Not enough memory</i></td></tr>
<tr><td><b>Error code</b></td><td><code>x21</code></td></tr>
<tr><td><b>Description</b></td><td>Not enough memory to complete the required operation (for example, an attempt to open a large file).</td></tr>
<tr><td colspan="2"><b>Resolving the error:</b>
1. Increase size of available memory for Dr.Web for Linux processes (for example, by changing the limits with the <code>ulimit</code> command), restart the program and repeat the operation.</td></tr>
<tr><td colspan="2">If the error persists, contact technical support and be ready to name the error code.</td></tr>
</table>

<table>
<tr><td><b>Error message</b></td><td><i>IO error</i></td></tr>
<tr><td><b>Error code</b></td><td><code>x22</code></td></tr>
<tr><td><b>Description</b></td><td>An input/output (I/O) error has occurred (for example, the drive has not been initialized yet or the partition of the file system is not available anymore).</td></tr>
<tr><td colspan="2"><b>Resolving the error:</b>
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.</td></tr>
<tr><td colspan="2">If the error persists, contact technical support and be ready to name the error code.</td></tr>
</table>

<table>
<tr><td><b>Error message</b></td><td><i>No such file or directory</i></td></tr>
<tr><td><b>Error code</b></td><td><code>x23</code></td></tr>
<tr><td><b>Description</b></td><td>The specified object of the file system (file or directory) is missing. It may have been removed.</td></tr>
<tr><td colspan="2"><b>Resolving the error:</b>
1. Check the path. If necessary, change it and repeat the operation.</td></tr>
<tr><td colspan="2">If the error persists, contact technical support and be ready to name the error code.</td></tr>
</table>

Error message	*Permission denied*
Error code	`x24`
Description	Insufficient 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 the required permissions. If it is necessary to access the object, change access permissions or elevate component permissions. Repeat the operation.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Not a directory*
Error code	`x25`
Description	The specified object of the file system is not a directory. Enter the path to a 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	*Data file corrupted*
Error code	`x26`
Description	The requested data is corrupted.

Resolving the error:

1. Repeat the operation.
2. If the error persists, restart Dr.Web for Linux by executing the command

   ```
   # service drweb-configd restart
   ```

   and then repeat the operation.

If the error persists, contact technical support and be ready to name the error code.

Error message	*File already exists*
Error code	`x27`

Description	On attempt to create a file, another file with the same name has been 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	*Read-only file system*
Error code	`x28`
Description	The file system you are trying to request is read-only.
Resolving the error: 1. Check the path. Change it so that the path indicate 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	*Network error*
Error code	`x29`
Description	A network error has occurred (possibly, a remote host stops responding unexpectedly or the required connection fails).
Resolving the error: 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	*Not a drive*
Error code	`x30`
Description	The input/output (I/O) device you are trying to access is not a drive.
Resolving the error: 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	*Unexpected EOF*

Error code	`x31`
Description	While reading data, the end of the file has been 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	*File was changed*
Error code	`x32`
Description	Changes have been detected in a file while scanning it.
Resolving the error: 1. Repeat scanning.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	*Not a regular file*
Error code	`x33`
Description	The object you are trying to access is not a regular file. It may be a directory, a socket or an other object in 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	*Name already in use*
Error code	`x34`
Description	On attempt to create an object of the file system (directory, file or socket), another object with the same name has been 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	*Host is offline*
Error code	`x35`
Description	A remote host is not available via the network.
Resolving the error: 1. Check whether the required host is available. If necessary, change the host address and repeat the operation.	
If the error persists, contact technical support and be ready to name the error code.	

Error message	*Resource limit reached*
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	*Different mount points*
Error code	`x37`
Description	The attempt to restore the file implies moving between two 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	*Unpacking error*
Error code	`x38`
Description	The attempt to unpack the archive failed (the file may be 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	*Virus database corrupted*
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	*Non-supported virus database version*
Error code	`x41`
Description	The current virus databases are designed for an earlier version of the program.

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	*Empty virus database*
Error code	`x42`
Description	The 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	*Object cannot be cured*
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	*Non-supported virus database combination*
Error code	`x44`
Description	The current combination of virus databases 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:

   - 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	*Scan limit reached*

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 so on).

Resolving the error:

1. Change limits for scanning (in the component settings) by any of the following methods:
   - On the page with the component settings in the application settings window.
   - Use the `drweb-ctl cfshow` and `drweb-ctl cfset` commands.
2. After changing the settings, repeat the previously attempted operation.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Authentication failed*
Error code	`x47`
Description	Invalid user credentials have been used for authentication.

Resolving the error:

1. Try to complete authentication again by entering valid credentials of the user with the necessary privileges.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Authorization failed*
Error code	`x48`
Description	The current user does not have enough privileges to perform the requested operation.

Resolving the error:

1. Try to perform the authentication again by entering valid credentials of the user with the necessary privileges.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Access token is invalid*
Error code	`x49`
Description	One of the Dr.Web for Linux components provides invalid authorization token on attempt to access the operation, requiring elevated privileges.

Resolving the error:

1. Try to complete authentication again by entering valid credentials of the user with the necessary privileges.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Invalid argument*
Error code	`x60`
Description	An invalid argument has been used when trying to execute a command.

Resolving the error:

1. Repeat the required action again using a valid argument.

If the error persists, contact technical support and be ready to name the error code.

Error message	*Invalid operation*
Error code	`x61`
Description	An attempt to run an invalid command has been 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	*Root privileges required*
Error code	`x62`
Description	Only a user with root privileges can perform this action.

Resolving the error:

1. Elevate you 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	*Not allowed in centralized protection mode*
Error code	`x63`
Description	The required action can be performed only if Dr.Web for Linux operates in the standalone mode.

Resolving the error:

1. Change Dr.Web for Linux operation mode to standalone mode and repeat the operation.
2. For that,
   - Clear the **Enable the centralized protection mode** check box on the `Mode` settings page.
   - Or execute the command:

```
# drweb-ctl esdisconnect
```

If the error persists, contact technical support and be ready to name the error code.

Error message	*Non-supported OS*
Error code	`x64`
Description	Dr.Web for Linux does not support the operating system installed on the host.

Resolving the error:

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	*Feature not implemented*
Error code	`x65`
Description	The required features of one of the components are not implemented in the current version of the program.

Resolving the error:

1. Restore Dr.Web for Linux defaults by clearing the contents of the configuration file `/etc/opt/drweb.com/drweb.ini`. It is recommended to back up the file before the procedure. For example:

```
# cp /etc/opt/drweb.com/drweb.ini /etc/opt/drweb.com/drweb.ini.save
# echo "" > /etc/opt/drweb.com/drweb.ini
```

2. Restart Dr.Web for Linux 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	*Unknown option*
Error code	`x66`

Description	The configuration file contains parameters unknown or non-supported in the current version of Dr.Web for Linux.

Resolving the error:

1. Open the `/etc/opt/drweb.com/drweb.ini` file in any text editor, remove the line, containing invalid parameter. Save the file and restart Dr.Web for Linux by executing the command:

   ```
   # service drweb-configd restart
   ```

2. If it does not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Unknown section*
Error code	`x67`
Description	The configuration file contains sections unknown or non-supported in the current version of Dr.Web for Linux.

Resolving the error:

1. Open the `/etc/opt/drweb.com/drweb.ini` file in any text editor, remove the unknown section. Save the file and restart Dr.Web for Linux by executing the command:

   ```
   # service drweb-configd restart
   ```

2. If it does not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Invalid option value*
Error code	`x68`
Description	The value of one or more parameters in the configuration file is invalid.

Resolving the error:

1. Set the valid parameter value by any of the following methods:
   - 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 can also restore parameter value to the default.
2. You can also directly edit the configuration file `/etc/opt/drweb.com/drweb.ini`. 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 Dr.Web for Linux by executing the command:

   ```
   # service drweb-configd restart
   ```
3. If the previous steps did not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Invalid state*
Error code	`x69`
Description	Dr.Web for Linux or one of the components is in invalid state to complete the required operation.

Resolving the error:

1. Repeat the required action after some time.
2. If the error persists, restart Dr.Web for Linux 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	*Only one value allowed*
Error code	`x70`
Description	In the configuration file a list of values is attributed to the single-valued parameter.

Resolving the error:

1. Set the valid parameter value by any of the following methods:
   - 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 can also restore parameter value to the default.
2. You can also directly edit the configuration file `/etc/opt/drweb.com/drweb.ini`. 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 Dr.Web for Linux by executing the command:

```
# service drweb-configd restart
```

3. If the previous steps did not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Record not found*
Error code	`x80`
Description	The threat record is missing (it may have been processed by some other Dr.Web for Linux component).

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	*Record is in process now*
Error code	`x81`
Description	The threat record is being processed by an other Dr.Web for Linux component.

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	*File has already been quarantined*

Error code	`x82`
Description	The file is already in the quarantine (another Dr.Web for Linux component must have already 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	*Cannot backup before update*
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:

1. Check the path to the directory where the backup copies of the files that are updated, are stored. Change the path, if necessary (the `BackupDir` parameter in the `[Update]` section of the configuration file).

   To view and correct the path, you can use the commands of the command line management tool.

   - To view current parameter value, execute the following command:

   ```
   $ drweb-ctl cfshow Update.BackupDir
   ```

   - To set a new parameter value, execute the command

   ```
   # drweb-ctl cfset Update.BackupDir <new path>
   ```

   - To restore the parameter value to the default, execute the command

   ```
   # drweb-ctl cfset Update.BackupDir -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, 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 properties.

4. If the error persists, reinstall the `drweb-update` package.

   For details on how to install and uninstall Dr.Web for Linux or its 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	*Invalid DRL file*
Error code	`x90`
Description	The integrity of one or several files with the list of update servers has been violated

Resolving the error:

1. Check the path to the file with the list of servers. Change the path, if necessary (parameters with `*DrlDir` in the `[Update]` section of the configuration file. To do this, use commands of the command-line management tool.
   - To view the current parameter value, use the command (<**DrlDirPath*> needs to be substituted with a specified parameter name. If the parameter name is unclear, refer to all parameter values in the section, skipping the command part in square brackets):

   ```
   $ drweb-ctl cfshow Update[.<*DrlDir>]
   ```

   - To set new parameter value, execute the command (<**DrlDir*> needs to be substituted with a specified parameter name):

   ```
   # drweb-ctl cfset Update.<*DrlDir> <new path>
   ```

   - To restore parameter value to the default, execute the command (<**DrlDir*> needs to be substituted with a specified parameter name):

   ```
   # drweb-ctl cfset Update.<*DrlDir> -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 `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 Dr.Web for Linux or its 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	*Invalid LST file*
Error code	`x91`

Description	The integrity of the file with the list of updated virus databases has been violated.

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 Dr.Web for Linux or its 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	*Invalid compressed file*
Error code	x92
Description	The integrity of the downloaded file with updates has been violated.

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
   ```

If the error persists, contact technical support and be ready to name the error code.

Error message	*Proxy authentication error*
Error code	x93
Description	The program fails to connect to update servers via the proxy server specified in the settings.

Resolving the error:

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 can also 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
```

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	*No update servers available*
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 can also 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 network connection parameters (including parameters of proxy server) are correct, but the error occurs, make sure you use the available list of update servers. The list of update servers used is displayed in parameters `*DrlDir` in `[Update]` section of configuration file. Note that, if parameters `*CustomDrlDir` indicate the existing correct file of servers list, the servers specified there will be used instead of the servers of the standard update zone (the value specified in the corresponding parameter`*DrlDir`, is ignored).

   In order to view and configure connection settings, you can use the commands of the command line management tool.

   To view the current parameter value, use the command (<**DrlDirPath*> needs to be substituted with a specified parameter name. If the parameter name is unclear, refer to all parameter values in the section, skipping the command part in square brackets):

   ```
   $ drweb-ctl cfshow Update[.<*DrlDir>]
   ```

   To set new parameter value, execute the command (<**DrlDir*> needs to be substituted with a specified parameter name):

   ```
   # drweb-ctl cfset Update.<*DrlDir> <new path>
   ```

   To restore parameter value to the default, execute the command (<**DrlDir*> needs to be substituted with a specified parameter name):

   ```
   # drweb-ctl cfset Update.<*DrlDir> -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	*Invalid key file format*
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 can also 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 your 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 can 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	*License is expired*
Error code	`x96`
Description	The 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 can 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	*Network operation timed out*
Error code	`x97`
Description	Network operation timed out (possibly, a remote host stops responding unexpectedly or the required connection fails).

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 your 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	*Invalid checksum*
Error code	`x98`
Description	The checksum of the downloaded file with updates is corrupted.

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	*Invalid demo key file*
Error code	`x99`
Description	The demo key file is invalid (for example, it was received from another computer).

Resolving the error:

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 can 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	*License key file is blocked*
Error code	`x100`
Description	The license is blocked (the license agreement conditions on using Dr.Web for Linux may be broken).

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 can 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	*Invalid license*
Error code	`x101`
Description	The current license is issued for an other Dr.Web product or does not allow operation of the installed Dr.Web for Linux components.

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 can 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	*Invalid configuration*
Error code	`x102`
Description	One of Dr.Web for Linux components cannot operate because of incorrect configuration settings.

Resolving the error:

1. If you do not know which component causes the error, try to determine it by reviewing the log file.
2. If the error is cause by the SpIDer Guard component, the mode selected for the component operation is probably 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).

   To view and correct the mode, you can 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, build and install the loadable kernel module for SpIDer Guard manually

   ⚠ Note that operation of SpIDer Guard and of the loadable kernel module is guaranteed only on the supported UNIX distributions (see System Requirements and Compatibility).

3. If this error is reported by SpIDer Gate, there is probably 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 Dr.Web for Linux 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 reported 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 did not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Invalid executable file*
Error code	`x104`
Description	One of the Dr.Web for Linux 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 by reviewing the log file.
2. Check the executable path to the component in the Dr.Web for Linux 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 Guard 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 Dr.Web for Linux or its 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	*Virus-Finding Engine is not available*
Error code	`x105`
Description	The file of the scan 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` scan engine file. Change the path, if necessary (the `CoreEnginePath` parameter in the `[Root]` section of the configuration file).

   To view and correct the path, you can 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 Dr.Web for Linux or its 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	*No virus databases*
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).

   To view and correct the path, you can 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 the scan 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 Dr.Web for Linux or its 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	*Process terminated by signal*
Error code	`x107`
Description	A component shuts down (possibly, because of the user command or being idle).

Resolving the error:

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:
   - Use the `drweb-ctl cfshow` and `drweb-ctl cfset` commands.
   - Edit the configuration file manually (by deleting all parameters from the component section).
3. If it did not help, restore Dr.Web for Linux 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 Dr.Web for Linux 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	*Unexpected process termination*
Error code	`x108`
Description	A component unexpectedly shuts down because of a failure.

Resolving the error:

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:
   - Use the `drweb-ctl cfshow` and `drweb-ctl cfset` commands.
   - Edit the configuration file manually (by deleting all parameters from the component section).
3. If it did not help, restore Dr.Web for Linux 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 Dr.Web for Linux after clearing the contents of the configuration file by executing the command:

```
# service drweb-configd restart
```

4. If the error persists after restoring Dr.Web for Linux 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 Dr.Web for Linux or its 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	*Incompatible software detected*
Error code	`x109`
Description	A Dr.Web for Linux 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 reported 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:

```
# rcSuSEfirewall2 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 reported 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	*Invalid library*
Error code	`x110`
Description	A file of the anti-spam library is missing, unavailable or corrupted (it is necessary for email scanning).

Resolving the error:

1. Check the path to the library file. Change the path, if necessary (the `AntispamCorePath` parameter in the `[Root]` section of the configuration file).

   To view and correct the path, you can use the commands of the command-line management tool.

   - To view current parameter value, execute the command

   ```
   $ drweb-ctl cfshow Root.AntispamCorePath
   ```

   - To set a new parameter value, execute the command

   ```
   # drweb-ctl cfset Root.AntispamCorePath <new path>
   ```

   - To restore the parameter value to the default, execute the command

   ```
   # drweb-ctl cfset Root.AntispamCorePath -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-maild` 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 Dr.Web for Linux or its 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	*Databases of web resource categories*
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).

   - To view and correct the path, you can 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 Dr.Web for Linux or its 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	*Linux kernel module for SpIDer Guard is unavailable*
Error code	`x113`
Description	SpIDer Guard 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).

   To view and correct the mode, you can 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 supported UNIX distributions (see System Requirements and Compatibility).

If the error persists, contact technical support and be ready to name the error code.

Error message	*SpIDer Gate is unavailable*
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 can 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 Dr.Web for Linux or its 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	*MailD is not available*
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 can 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 Dr.Web for Linux or its 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	*Scanning Engine is not available*
Error code	`x119`
Description	Cannot scan files as Dr.Web Scanning Engine 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 can 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 Dr.Web for Linux and receive a license. After receiving the license, check whether the key file is available and install it, if necessary.

   - 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 Dr.Web for Linux or its 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	`drweb-filecheck` is missing.

Resolving the error:

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 can use the commands of the command-line management tool.

   To view current parameter value, execute the following command:

   ```
   $ drweb-ctl cfshow FileCheck.ExePath
   ```

   To set a new parameter value, execute the command:

   ```
   # drweb-ctl cfset FileCheck.ExePath <new path>
   ```

To restore the parameter value to the default, execute the command:

```
# drweb-ctl cfset FileCheck.ExePath -r
```

2. If the error persists after entering the correct path,
   - 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 Dr.Web for Linux or its 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	*ES Agent is not available*
Error code	`x121`
Description	Dr.Web ES Agent component is missing (it is necessary to connect to the centralized protection server).

Resolving the error:

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 can use the commands of the command-line management tool.

   - To view current parameter value, execute the following command:

   ```
   $ drweb-ctl cfshow ESAgent.ExePath
   ```

   - To set a new parameter value, execute the command:

   ```
   # drweb-ctl cfset ESAgent.ExePath <new path>
   ```

   - To restore the parameter value to the default, execute the command:

   ```
   # drweb-ctl cfset ESAgent.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-esagent` 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 Dr.Web for Linux or its 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	*Firewall for Linux is not available*

Error code	`x122`
Description	`drweb-firewall` is missing or failed to start.

Resolving the error:

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 can use the commands of the command-line management tool.

   - To view current parameter value, execute the following command:

   ```
   $ drweb-ctl cfshow LinuxFirewall.ExePath
   ```

   - 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 component 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 Dr.Web for Linux or its 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	*Network Checker is not available*
Error code	`x123`
Description	Cannot control network connections as `drweb-netcheck` is missing or failed to start. The module is used to scan 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 can 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 Dr.Web for Linux or its 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	*CloudD is not available*
Error code	`x124`
Description	Dr.Web CloudD (required for requests to the Dr.Web Cloud service) is missing.

Resolving the error:

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 can use the commands of the command-line management tool.

   - To view current parameter value, execute the following command:

   ```
   $ drweb-ctl cfshow CloudD.ExePath
   ```

   - To set a new parameter value, execute the command:

   ```
   # drweb-ctl cfset CloudD.ExePath <new path>
   ```

   - To restore the parameter value to the default, execute the command:

   ```
   # drweb-ctl cfset CloudD.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-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 Dr.Web for Linux or its 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	*Unexpected error*
Error code	`x125`
Description	An unexpected error has occurred in operation of one of the components.

Resolving the error:

1. Restart Dr.Web for Linux by entering the following command:

```
# service drweb-configd restart
```

If the error persists, contact technical support and be ready to name the error code.

Errors Without Codes

Symptoms: After installation of the kernel module of SpIDer Guard, operating system abnormally shuts down with a kernel error "*Kernel panic*".

Description: SpIDer Guard kernel module cannot operate in the operating system kernel environment (for example, when the OS operates in the Xen hypervisor environment).

Resolving the error

1. Cancel the load of the SpIDer Guard kernel module (kernel module name is `drweb`) by adding to the grub loader the following string:

   ```
   drweb.blacklist=yes
   ```

   to the load settings string of the operating system kernel.
2. When the OS is loaded, uninstall the `drweb.ko` kernel module from the `/lib/`uname-r`/extra` directory of additional kernel modules.
3. Set operation mode for SpIDer Guard to *AUTO* by executing the following commands:

   ```
   # drweb-ctl cfset LinuxSpider.Mode AUTO
   # drweb-ctl reload
   ```

4. If operating system you are using does not support fanotify or this mode does not allow SpIDer Guard usage for full control of a file system and *LKM* mode usage is obligatory, do not use the Xen hypervisor.

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

1. Uninstall Dr.Web for Linux by entering the following command:

   ```
   # service drweb-configd restart
   ```

2. If this command returns error message, or has no any effect, install `drweb-configd` component (package) separately.

Also note that this may mean, that PAM authentication is not used in the system. If so, please install and configure it.

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 Dr.Web for Linux or its 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*).

   Also note that this may mean, that PAM authentication is not used in the system. If so, please install and configure it.

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 Dr.Web for Linux or its 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 Gate, 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 Gate 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 Gate cannot delete its rules of diverting connections.

Resolving the error

1. Enable the SpIDer Gate monitor again.
2. If you need SpIDer Gate 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 root 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 Gate into the Manual mode in the Dr.Web Firewall settings if you want to manually divert connections towards SpIDer Gate 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 directory runs the scanning in Dr.Web for Linux.

Description: The GUI has associated automatically files of a certaing type or directories with **Open With Dr.Web for Linux** action.

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, root 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` (`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

In this section:

- General Information.
- Building the Kernel Module.
- Possible Build Errors.

General Information

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.

> For E2K and ARM64 architectures work with the LKM is not supported.

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 your OS supports kernel module versions included in Dr.Web for Linux. 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 -xf drweb-spider-kmod-<version>-<date>.tar.bz2
```

unpacks the source codes to the created directory. This directory has the archive 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*>.

Appendix F. List of Abbreviations

The following abbreviations were used in this manual without further interpretation:

Convention	Complete form
FQDN	Fully Qualified Domain Name
GNU	GNU project (GNU is Not Unix)
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure (over SSL/TLS)
ID	Identifier
IMAP	Internet Message Access Protocol (email protocol)
IP	Internet Protocol
MBR	Master Boot Record
NSS	Novell Storage Services
PID	Process ID (system process identifier)
PAM	Pluggable Authentication Modules
POP	Post Office Protocol (email protocol)
RPM	Red Hat Package Manager
SMTP	Simple Mail Transfer Protocol (email protocol)
SP	Service Pack
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User ID (system user identifier)
URL	Uniform Resource Locator
VBR	Volume Boot Record

Convention	Complete form
OS	Operating System

Index

Index

Index

© Doctor Web, 2023