



User manual



© 2021 Doctor Web. All rights reserved

This document is for information and reference purposes in relation to the specified software of the Dr.Web family. This document is not a ground for exhaustive conclusions about the presence or absence of any functional and/or technical features in the software of the Dr.Web family and cannot be used to determine whether the software of the Dr.Web family matches any requirements, technical task and/or parameters, and other third-party documents.

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

Trademarks

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

Disclaimer

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

Dr.Web Security Space
Version 11.5
User manual
6/11/2021

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 which provide efficient protection from malicious software and spam.

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

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

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

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



Table of Contents

1. Introduction	7
1.1. About This Manual	8
1.2. Document Conventions	8
1.3. Detection Methods	9
2. System Requirements	13
3. Installing, Removing, or Changing Dr.Web	15
3.1. Installing the product	15
3.2. Configuring components	19
3.3. Removing the product	20
4. Licensing	23
4.1. How to activate your license	25
4.2. Renewing License	31
4.3. Key file	32
5. Getting Started	34
5.1. Testing the Anti-virus	35
6. Tools	37
6.1. License Manager	37
6.2. Data Loss Prevention	38
6.3. Anti-virus Network	40
6.4. Quarantine Manager	41
6.5. Support	42
6.5.1. Report Wizard	43
7. Updating of virus databases and program components	47
8. Dr.Web Scanner	49
8.1. Scanning Your System	49
8.2. Actions Upon Detection	51
8.3. Command-Line Scanning Mode	53
8.4. Console Scanner	53
8.5. Automatic Launch of Scanning	54
9. Settings	55
10. Main Settings	56
10.1. Notifications	56



10.2. Update	60
10.3. Network	63
10.4. Self-protection	65
10.5. Dr.Web Cloud	67
10.6. Anti-virus Network	68
10.7. Devices	69
10.8. Advanced	72
11. Parental Control	75
11.1. Configuring Parental Control	76
11.1.1. Internet	77
11.1.2. Time	80
11.1.3. Files and Folders	82
12. Exclusions	84
12.1. Websites	84
12.2. Files and Folders	86
12.3. Applications	88
12.4. Anti-spam	91
13. Protection Components	93
13.1. SplDer Guard	93
13.1.1. Configuring SplDer Guard	94
13.2. SplDer Gate	98
13.2.1. Configuring SplDer Gate	98
13.3. SplDer Mail	100
13.3.1. Configuring SplDer Mail	102
13.3.2. Anti-spam	104
13.4. Scanner	106
13.5. Firewall	109
13.5.1. Training Firewall	109
13.5.2. Configuring Firewall	111
13.6. Dr.Web for Microsoft Outlook	122
13.6.1. Virus Check	122
13.6.2. Spam Check	124
13.6.3. Event Logging	127
13.6.4. Statistics	129
13.7. Preventive Protection	129
14. Statistics	135



15. Technical support	137
16. Appendix A. Additional Command-Line Parameters	138
16.1. Scanner and Console Scanner Parameters	138
16.2. Dr.Web Updater Command-Line Parameters	144
16.3. Return Codes	147
17. Appendix B. Computer Threats and Neutralization Methods	149
17.1. Classification of Computer Threats	149
17.2. Actions Applied to Threats	154
18. Appendix C. Naming of Viruses	155



1. Introduction

Dr.Web Agent for Windows protects RAM, hard drives, and removable media of computers running Microsoft® Windows® operating system against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

Dr.Web Agent for Windows architecture consists of several modules responsible for different functionalities. Scan engine and virus databases are common for all components and different platforms.

Product components are constantly updated. New threat signatures are regularly added to the virus databases, databases of website categories and rules for email spam filtration. Constant update provides an up-to-date level of protection for users' devices, applications and data. Heuristic analysis methods implemented in the scan engine ensure an additional protection against unknown malicious software.

Dr.Web Agent for Windows can detect and remove unwanted programs: adware, dialers, jokes, riskware, and hacktools from your computer. To detect such programs and perform actions with the files contained in the programs, anti-virus components of Dr.Web are used.

Each of Dr.Web anti-virus solutions for Microsoft® Windows® operating systems includes a set of the following components:

[Dr.Web Scanner](#)—an anti-virus scanner with a graphical interface that launches on demand or as scheduled and scans your computer for viruses and other malicious software.

[Dr.Web Console Scanner](#)—a command-line version of Dr.Web Scanner.

[SpIDer Guard](#)—an on-access anti-virus scanner that constantly resides in memory while scanning processes and files on start or creation and instantly detecting any malicious activity.

[SpIDer Mail](#)—an anti-virus mail scanner for Windows workstations that monitors data exchange between mail clients on your computer and mail servers made via POP3/SMTP/IMAP4/NNTP protocols (IMAP4 stands for IMAPv4rev1), detects and neutralizes threats before they are transmitted to or from your computer thus preventing spread of infection via email. SpIDer Mail can also scan mail for spam messages using Dr.Web Anti-spam.

[Dr.Web for Microsoft Outlook](#)—a plug-in that checks Microsoft Outlook mailboxes for threats and spam.

[SpIDer Gate](#)—an HTTP monitor which, by default, automatically checks incoming HTTP-traffic and blocks all malicious objects. URL filtering of malicious and unreliable websites is also enabled by default.

[Parental Control](#)—a component that restricts access to websites, files and folders, and allows to set custom time limits on using your computer and the Internet for different Windows accounts.



Dr.Web Firewall—a personal firewall that protects your computer from unauthorized access and prevents leak of vital data through networks.

Dr.Web Updater—allows registered users to receive and automatically install updates to virus databases and Dr.Web modules.

Dr.Web Agent—helps you configure and manage your anti-virus product.

Preventive Protection—a component that controls access to critical system objects and provides exploit prevention and integrity of running applications and files.

1.1. About This Manual

This User Manual describes installation and effective utilization of Dr.Web.

You can find detailed descriptions of all graphical user interface (GUI) elements in the Help system which can be accessed from any component.

This User Manual describes how to install the program and contains some words of advice on how to use it and solve typical problems caused by virus threats. Mostly, it describes the standard operating modes of the Dr.Web components (with default settings).

The Appendices contain detailed information for experienced users on how to set up Dr.Web.



Due to constant development, program interface of your installation can mismatch the images given in this document. You can always find the actual documentation at <https://download.drweb.com/doc>.

1.2. Document Conventions

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

Convention	Comment
	Warning about possible errors or important notes to which you should pay special attention.
<i>Anti-virus network</i>	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.



Convention	Comment
CTRL	Keyboard keys names.
C:\Windows\	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

1.3. Detection Methods

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

Signature analysis

The scans begin with signature analysis that is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing

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

Execution emulation

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



polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

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

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

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

Behavior analysis

Behavior analysis methods analyze the sequence of actions of all the processes in the system. When the malicious behavior is detected, actions of this program are blocked.

Dr.Web Process Heuristic

The Dr.Web Process Heuristic behavioral analysis technology protects systems against new dangerous malicious programs that can avoid detection by traditional signature-based and heuristic analyses.

Dr.Web Process Heuristic analyzes the behavior of each running program in real time. Using the constantly updated Dr.Web cloud service, along with the information on malware behavior, it determines whether the program is dangerous and then takes necessary measures to neutralize the threat.

This data protection technology helps to minimize losses resulting from the actions of unknown malware while consuming very few of the protected system's resources.

Dr.Web Process Heuristic monitors any attempts to modify the system:



- Detects malicious processes that modify users' files (such as encryption attempts of ransomware), including those located in folders accessible through network.
- Prevents malware from injecting its code into the processes of other applications.
- Protects critical system areas from being modified by malware.
- Detects and shuts down the execution of malicious, suspicious or unreliable scripts and processes.
- Prevents malware from modifying boot sectors so that malicious code cannot be executed on the computer.
- Blocks changes in the Windows Registry to make sure that the safe mode won't be disabled.
- Prevents malware from changing launch permissions.
- Prevents new or unknown drivers from being downloaded without the user's consent.
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries into the Windows Registry, so that they could be launched automatically.
- Locks registry sections containing information about virtual device drivers, ensuring that no new virtual devices are created.
- Prevents malware from disrupting system routines such as scheduled backups.

Dr.Web Process Dumper

Dr.Web Process Dumper, a comprehensive analysis of packed threats significantly improves the detection of supposedly "new" malicious programs that were added to the Dr.Web virus database before they were concealed by new packers. In addition, this type of analysis eliminates the need to keep adding new entries into the virus database. With Dr.Web virus databases kept small, system requirements do not need to be constantly increased. Updates remain small, while the quality of detection and curing remains at the same high level.

Dr.Web ShellGuard

Dr.Web ShellGuard protects your device against exploits. *Exploits* are malicious objects that take advantage of software vulnerabilities. These vulnerabilities are used to gain control over a targeted application or the operating system.

Dr.Web ShellGuard protects the most common applications installed on almost all computers running Windows:

- popular web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Vivaldi Browser, and others);
- MS Office applications including MS Office 2016;
- system Applications;
- applications that use java, flash and pdf;
- media players (software).

To detect malicious actions, Dr.Web ShellGuard uses not only the information stored locally, but also the following data from the Dr.Web cloud service:



- information on algorithms of malicious programs;
- information about known clean files;
- information on the compromised digital signatures of well-known software developers;
- information about digital signatures used by adware and riskware;
- protection algorithms used by specific applications.

Machine learning

Machine learning is used for detecting and neutralizing malicious objects missing from the virus databases. The advantage of the method is detection of a malicious code without executing it, judging only by its features.

Threat detection is based on the malicious object classification according to specific features. Support vector machines (SVM) underlie machine learning technologies that are used for classification and adding code fragments written in scripting languages to the databases. Detected objects are then analyzed on the basis of whether they have features of a malicious code. Machine learning technology makes the process of updating these features and virus databases automatic. Large amounts of data are processed faster thanks to the connection to the cloud service, and continuous training of the system provides preventive protection from the latest threats. At that, the technology can function even without a constant connection to the cloud.

The machine learning method significantly saves the resources of the operating system, since it does not require code execution to detect threats, and dynamic machine learning of the classifier can be carried out without a constant update of the virus databases that is used for signature analysis.

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 servers, the files are scanned locally, and the cloud scan resumes when the connection is restored.

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



2. System Requirements




Before installing Dr.Web:

- Remove any anti-virus software from your computer to prevent possible incompatibility of resident Dr.Web components.
- In case of installation of Dr.Web Firewall, uninstall all other firewalls from your computer;
- Install all critical updates recommended by the operating system developer. If the operating system is no longer supported, then upgrade to a newer operating system.

Dr.Web is not compatible with proactive security products developed by other manufacturers.

Dr.Web can be installed and run on a computer that meets the following minimum requirements:

Component	Requirement
CPU	An i686-compatible processor.
Operating system	<p>For 32-bit platforms:</p> <ul style="list-style-type: none">• Windows XP with Service Pack 2 or later• Windows Vista with Service Pack 2 or later• Windows 7 with Service Pack 1 or later• Windows 8• Windows 8.1• Windows 10 21H1 or earlier <p>For 64-bit platforms:</p> <ul style="list-style-type: none">• Windows Vista with Service Pack 2 or later• Windows 7 with Service Pack 1 or later• Windows 8• Windows 8.1• Windows 10 21H1 or earlier <div> As Microsoft has stopped supporting SHA-1 hashing algorithm, please ensure that your operating system supports SHA-256 hashing algorithm before installing Dr.Web Agent for Windows on Windows Vista or Windows 7. For this, install all the recommended updates listed in</div>



Component	Requirement
	Windows Update section. For the detailed information, please visit Doctor Web official website
Free RAM	Minimum 512 MB.
Resolution	Minimum recommended screen resolution is 800x600.
Cloud and virtualization environment support	Operation of the program is guaranteed on the following environments: <ul style="list-style-type: none">• VMware• Hyper-V• Xen• KVM
Other	For the Dr.Web for Microsoft Outlook extension, one of the following Microsoft Outlook clients from the Microsoft Office package is required: <ul style="list-style-type: none">• Outlook 2000• Outlook 2002• Outlook 2003• Outlook 2007• Outlook 2010 with Service Pack 2• Outlook 2013• Outlook 2016

To ensure a correct operation of Dr.Web the following ports must be opened:

Purpose	Direction	Port numbers
To activate and renew the license	outgoing	443
To update (if the option to update using https is enabled)	outgoing	443
To update	outgoing	80
To send email notifications		25 or 465 (or depending on the settings of email notifications)
To connect to Dr.Web Cloud	outgoing	2075 (including UDP)

Other system requirements are similar to those for the corresponding operating system.



3. Installing, Removing, or Changing Dr.Web

Before installing Dr.Web Agent for Windows get familiar with [system requirements](#). In addition, it is recommended to do the following:

- Install all critical updates released by Microsoft for the OS version used on your computer (they are available on the company update site at <https://windowsupdate.microsoft.com>).
- Check the file system with system utilities and remove the detected defects.
- Close all active applications.



Remove any anti-virus software and firewalls from your computer to prevent possible incompatibility of resident components.

To install Dr.Web, the user must have administrative privileges.

There are two installation modes of Dr.Web anti-virus software:

- command line mode;
- wizard mode.

3.1. Installing the product



To install Dr.Web, the user must have administrative privileges.

Installation via the command line

To install Dr.Web in the background mode, enter in the command line the executable file name with necessary parameters (they affect installation in the background mode, installation language, reboot after installation, and Dr.Web Firewall installation).

Parameter	Value
installFirewall	Install Dr.Web Firewall.
lang	Language used for the installation. The value of this parameter is language in ISO 639-1 format.
reboot	Restart the computer automatically after installation is complete.
silent	Installation in the background mode.



For example, to start background installation of Dr.Web with reboot after the process completes, execute the following command:

```
drweb-11.5-ss-win.exe /silent yes /reboot yes
```

Installation in wizard mode

To start usual installation, do one of the following:

- If you have the executable file, run it.
- If you have the original disk containing installation package, insert the disk into the CD/DVD drive. If autorun is enabled, the installation will start automatically. If autorun is disabled, run the autorun.exe file of the installation kit manually. The window opens and displays the autorun menu. Click **Install**.

At any installation step, before the wizard starts copying files to your computer, you can do the following:

- Return to the previous step by clicking **Back**.
- Go to the next step by clicking **Next**.
- Abort installation by clicking **Cancel**.

Installing Dr.Web

1. If other anti-virus software is installed on your computer, the Installation Wizard informs you on incompatibility between Dr.Web and another anti-virus product and offers to remove it.



Before the installation starts, the Wizard checks if the installation file is the latest one. If a newer installation file exists, you will be offered to download it before the installation.

2. At this step, you are prompted to connect to [Dr.Web cloud services](#), which allow to perform checks using the newest information on threats. The information is updated in real-time mode. The option is enabled by default. You can also specify whether Dr.Web Firewall should be installed or not.

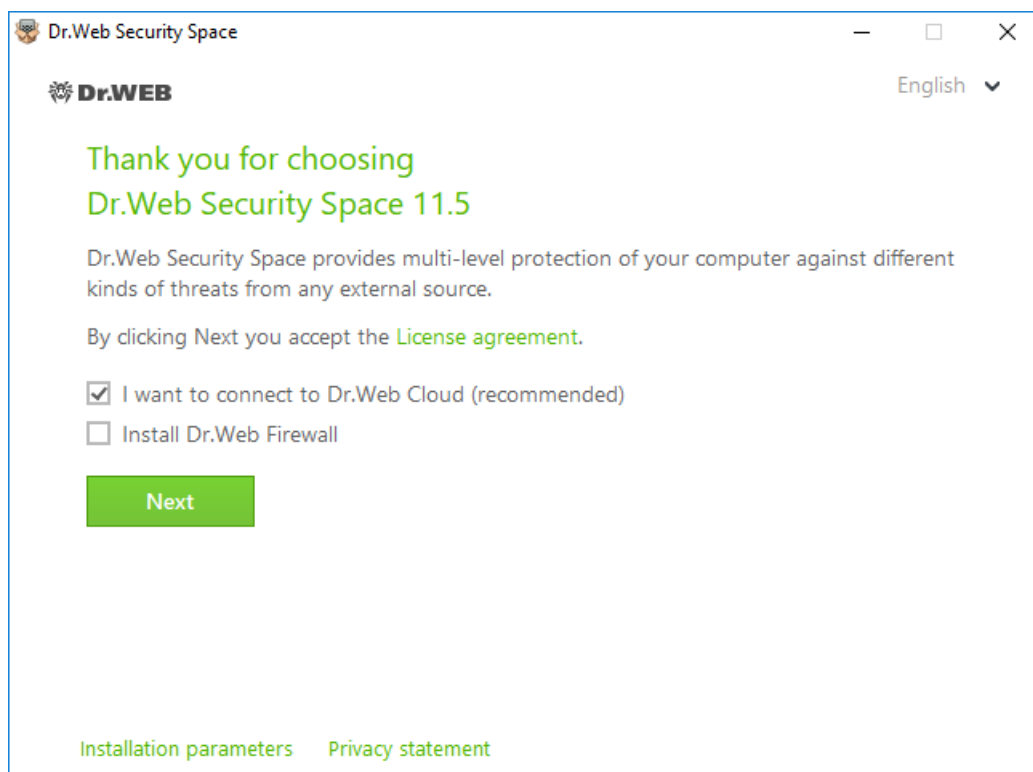


Figure 1. Installation Wizard

3. To select components you want to install, specify the installation path and configure other settings, click **Installation parameters**. The option is meant for experienced users. If you want to use default installation settings, go to step 4.
 - On the first tab, you can specify the components you want to install.
 - On the second tab, you can change the installation path.
 - The last tab of the window allows you to enable the **Update during installation** option to download updates to virus databases and other program components. The tab also prompts you to create shortcuts to Dr.Web.
 - If necessary, specify proxy server parameters.To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**.
4. Click **Next**. Please note that by clicking the Next button you accept the terms of the License agreement.
5. In **Registration Wizard** window select one of the following options:
 - If a [key file](#) is present on the hard drive or removable media, select **Specify path to an available valid key file**. To select the key file click **Browse** and select it in dialog box. More information can be found in [Activation using the key file](#) section.
 - If you do not have the key file, but you are ready to obtain it during the installation, select **Receive license during installation**. More information can be found in [Activation using serial number](#) section.
 - To continue installation [without a license](#), select **Receive license later**. Updates are not available until you specify or obtain a key file.

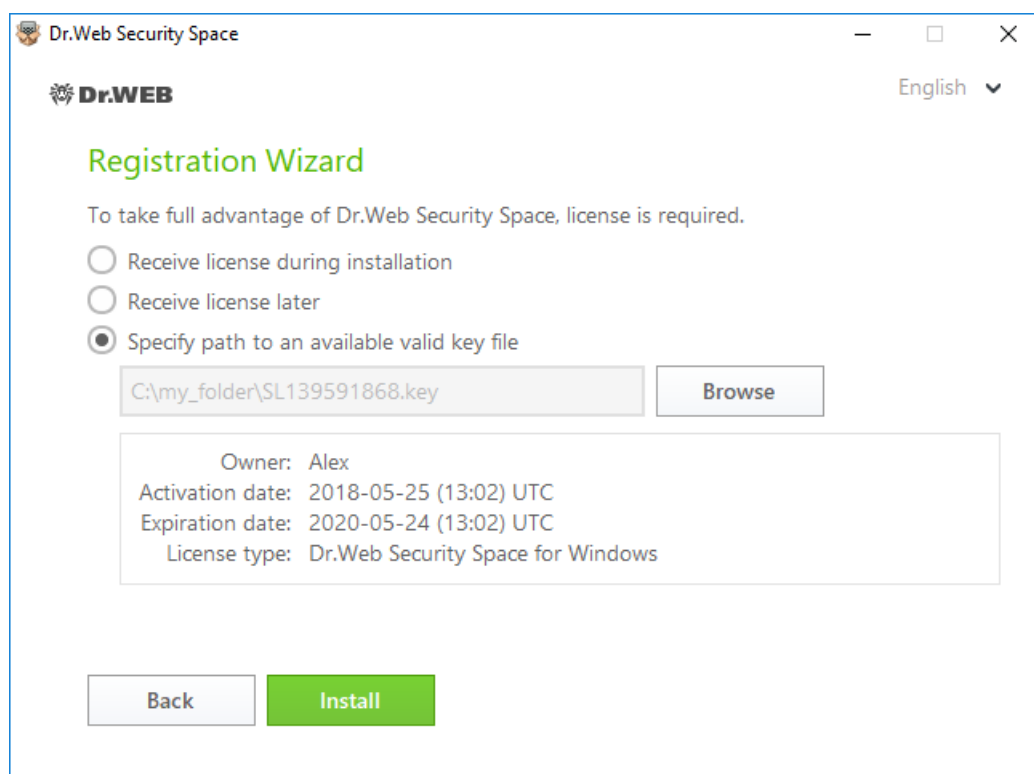


Figure 2. Registration wizard

Click **Install**.

6. If you specified a key file or received it during the installation and did not clear the **Update during installation** check box, the wizard updates virus databases and other Dr.Web components. Updating starts automatically and does not require any additional actions.
7. Restart your computer after the installation is complete.

BFE service error while installing Dr.Web

Several Dr.Web components require the BFE (Base Filtering Engine Service) running. In case this service is absent or damaged, the installation of Dr.Web will not be possible. The damage or the absence of BFE service may indicate the presence of security threats on your computer.

If the attempt of Dr.Web installation has ended with error, do the following:

1. Scan the system using free CureIt! utility by Doctor Web. You can download CureIt! from Doctor Web website: <https://free.drweb.com/download+cureit+free/>.
2. Restore BFE service. To do this, you can use the Windows firewall recovery utility (for Windows 7 and later). You can download the utility from Microsoft website: <https://support.microsoft.com/en-us/help/17613/automatically-diagnose-and-fix-problems-with-windows-firewall>.
3. Run Dr.Web installation wizard and perform the installation according the instruction described above.



If the problem continues to appear, address to Doctor Web technical support.

3.2. Configuring components

1. To delete or configure Dr.Web components, select (depends on operating system installed on your computer):

Operating system	Actions			
Windows XP	Start menu:	Start → Control Panel → Add or Remove programs		
	Classic Start menu:	Start → Settings → Control Panel → Add or Remove programs		
Windows Vista	Start menu:	Start → Control Panel	Classic view:	Programs and Features.
			Home page	Programs → Programs and Features.
	Classic Start menu:	Start → Settings → Control Panel → Add or Remove programs.		
Windows 7	Start → Control Panel	Small/large icons: Programs and Features.		
		Category: Programs → Uninstall a program		
Windows 8 Windows 8.1 Windows 10	Control Panel	Small/large icons: Programs and Features.		
		Category: Programs → Uninstall a program		

2. In the installed programs list select the line with the program name.



3. Click **Edit**, Uninstall/Change wizard launches.

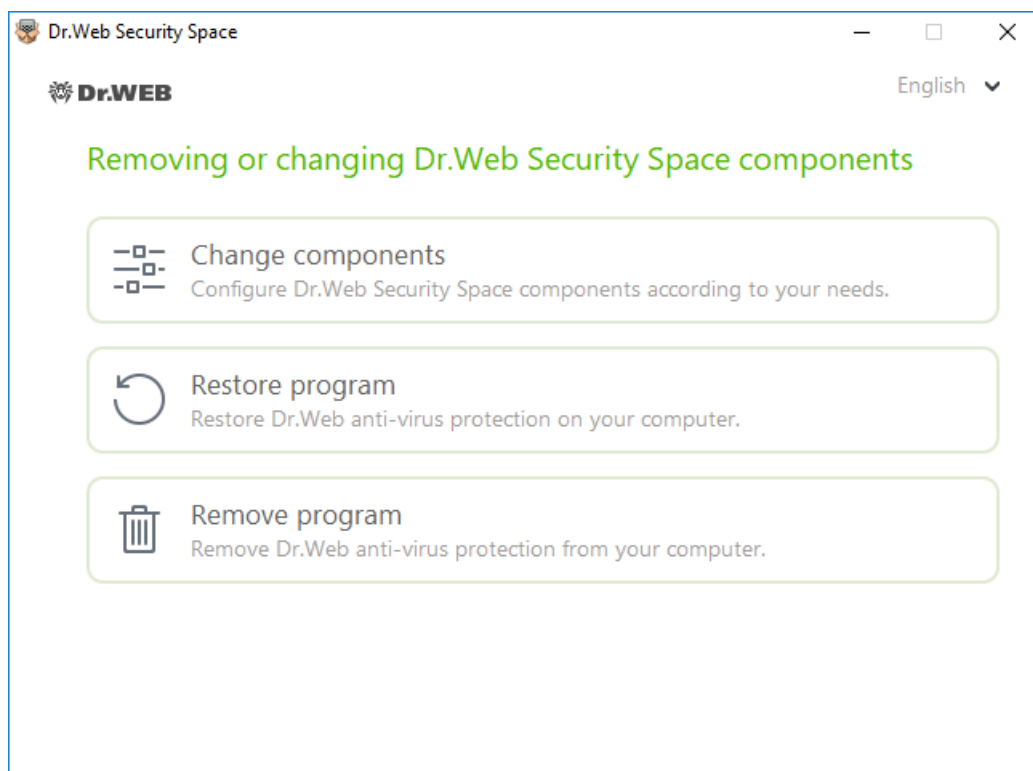


Figure 3. Uninstall/Change wizard

4. Select the option:

- **Change components.** In the open window, select check boxes of the components you want to add and clear check boxes of the components you want to remove. When you finish adjusting the component set, click **Apply**.
- **Restore program,** if you need to restore the anti-virus protection on your computer. This function is applied in case when some of Dr.Web components have been corrupted.
- **Remove program,** to delete all installed components.

3.3. Removing the product



After you uninstall Dr.Web, your computer will not be protected from viruses and other malware.

1. To remove the Dr.Web Agent for Windows program, select (depending on operating system):



Operating system	Actions			
Windows XP	Start menu:	Start → Control Panel → Add or Remove programs		
	Classic Start menu:	Start → Settings → Control Panel → Add or Remove programs		
Windows Vista	Start menu:	Start → Control Panel	Classic view:	Programs and Features.
			Home page	Programs → Programs and Features.
	Classic Start menu:	Start → Settings → Control Panel → Add or Remove programs.		
Windows 7	Start → Control Panel	Small/large icons: Programs and Features.		
		Category: Programs → Uninstall a program		
Windows 8 Windows 8.1 Windows 10	Control Panel	Small/large icons: Programs and Features.		
		Category: Programs → Uninstall a program		

In the list select the line with the program name.

2. Click **Delete**.



When removing components of Dr.Web, the **Disable Self-protection** window opens. Enter the displayed confirmation code and click **Disable Self-protection**.

3. In the **Parameters to save** window, select check boxes of those components that you do not want to remove from your system. Saved objects and settings can be used by the program if it



is installed again. By default, all options—**Quarantine**, **Dr.Web Settings Security Space** and **Protected copies of files**—are selected. Click **Install**.

4. In the next window, confirm deletion of Dr.Web by entering the displayed code and then click **Remove program**.
5. Once you reboot your computer, the changes are applied. You can snooze the reboot by clicking **Later**. Click **Restart now** to immediately complete the procedure of Dr.Web components deletion or modification.



4. Licensing

User rights are regulated by the license purchased on the Doctor Web website or through authorized partners. The license allows to take advantage of all product features during the whole period. User rights are set in accordance with the [License agreement](#), which conditions users accept during the program installation.

A unique *serial number* corresponds to each license, and a special file that regulates Dr.Web operation in accordance with license parameters is stored on the local computer. This file is called a *key file*. For details on the key file see the [Key file](#) section.

If you want to evaluate the product before purchasing it, you can activate a *demo period*. All product features and components are available during the demo period. A special key file is generated during the activation of the demo period too. It is possible to activate a demo period on the same computer once a year only.



A demo period cannot be activated and used on Windows XP.

License activation methods

You can activate your license in one of the following ways:

- during the installation via the Installation wizard;
- in any moment after the installation via the Installation wizard included in the License manager;
- on the official Doctor Web website at <https://products.drweb.com/register/>.

License activation via the Installation wizard is available using the serial number or the key file. Windows XP users can activate the license using the key file only.

For the detailed information on license activation, refer to the [How to activate your license](#) section.

Demo period

A trial license for 1 month is available for Dr.Web users. You can get the trial license right in the License manager window without entering your personal data.



A demo period cannot be activated and used on Windows XP.

If you have question on licensing, read the [FAQ](#) section on Doctor Web website.



Possible questions

How to transfer a license to another computer?

You are entitled to transfer your license for commercial use using the key file or serial number. If you want to transfer a license to a computer run by Windows XP, you can only do it using the key file.

To transfer a license to another computer

- using the serial number:
 1. Remove Dr.Web from the computer of license origin or activate another license on this computer.
 2. Activate the current license on target computer. To do this, use Registration wizard during the product installation or after the installation (see [Activation using serial number](#)).
- using the key file:
 1. Copy the key file from the computer of origin. By default, the [key file](#) is stored in Dr.Web installation folder and has .key extension.
 2. Remove Dr.Web from the computer of license origin or activate another license on this computer.
 3. Activate the current license on target computer. To do this, use the registration wizard during the product installation or after the product is installed ([Activation using the key file](#)).



It is impossible to transfer a demo period to another computer.

I forgot the registration email. How can I restore it?

If you forgot the email address, specified during registration, you should address to Dr.Web technical support site at <https://support.drweb.com>.

If you make a request from email address that differs from which your license is registered, a technical support specialist may ask you to provide: a photo or scan copy of the license certificate, payment receipt, an online store letter and other documents proving your license ownership.

How can I change the registration email?

If you need to change the email address specified during registration, use the special email address changing service at https://products.drweb.com/register/change_email.



4.1. How to activate your license

To get access to all product functions and components, activate the license. License activation via the Installation wizard is available using a key file or a serial number. Windows XP users can [activate the license](#) using the key file only.



If you have already been a user of Dr.Web, you are eligible for extension of your new license for another 150 days. To enable the bonus, enter your serial number or specify the path to the key file used for the previous registration in the open window.

Activation using a serial number

If you have a serial number, you can

- activate the license during the product installation via the Registration wizard:
1. Run product installation. At step 5 of the installation, select **Receive license during installation**. Click **Install**.

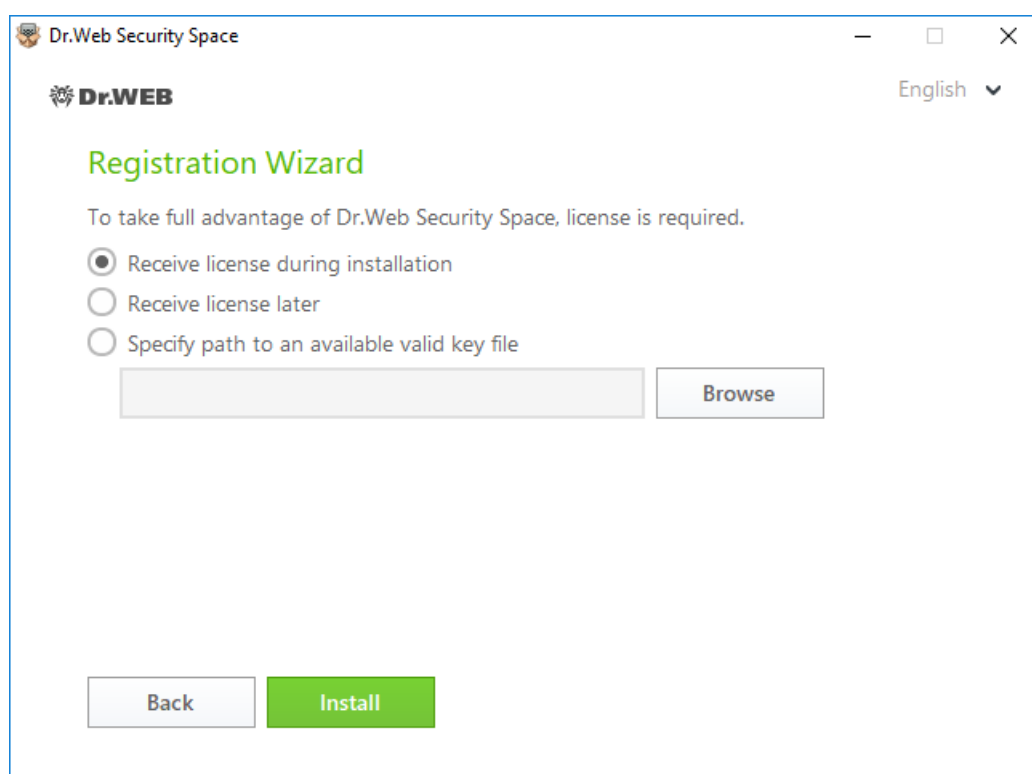


Figure 4. Installation. Registration wizard

2. Product installation starts. At the end of Obtaining license, the Installation wizard opens. Enter your serial number and click **Activate**. In case you have not registered your serial number yet, a window opens where you can enter your registration data.

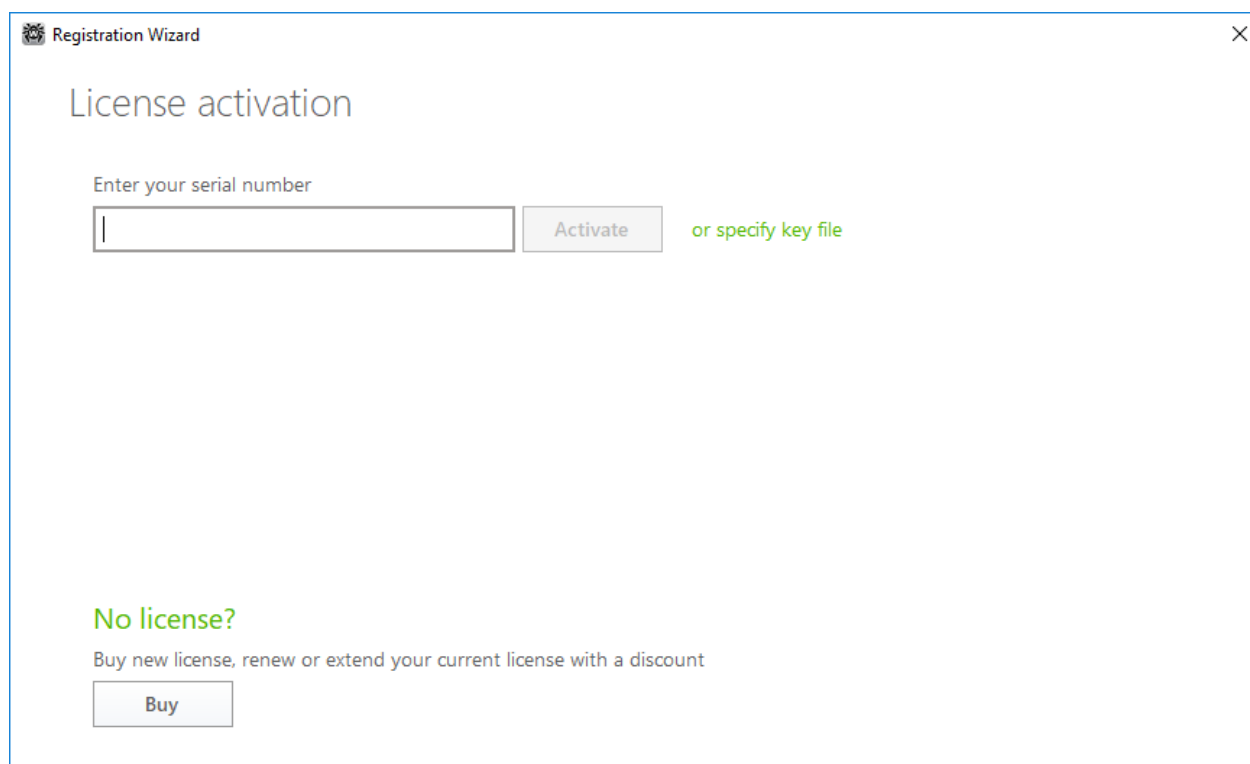



Figure 5. Registration wizard. License activation

3. Continue product installation following the instructions of Installation wizard.

If license activation failed, an error message displays. Check Internet connection parameters or click **Retry** to correct invalid data.

- activate the license in any moment after the installation via the Registration wizard included in the License manager:
 1. In the [Dr.Web menu](#) , select **License** item. License Manager opens. Click **Buy or activate new license**.

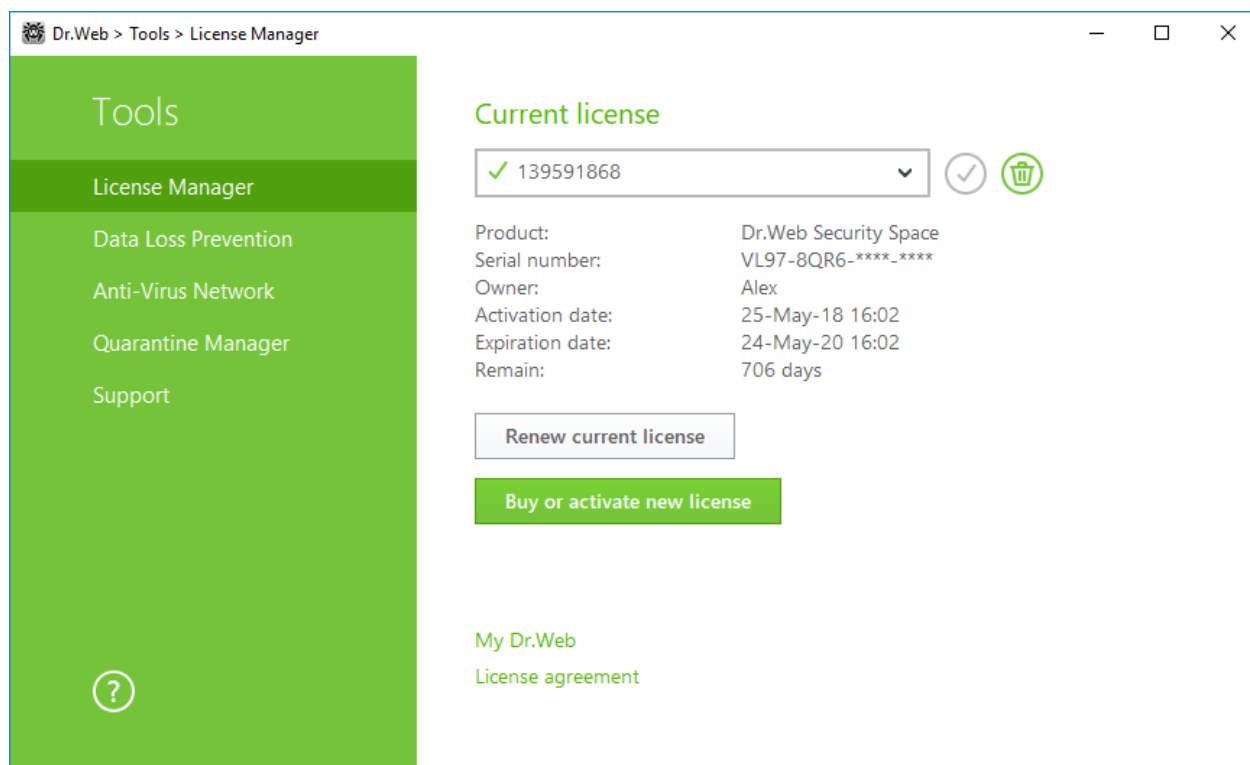


Figure 6. License Manager

2. The Installation wizard window opens. Enter your serial number and click **Activate**. In case you have not registered your serial number yet, a window opens where you can enter your registration data.

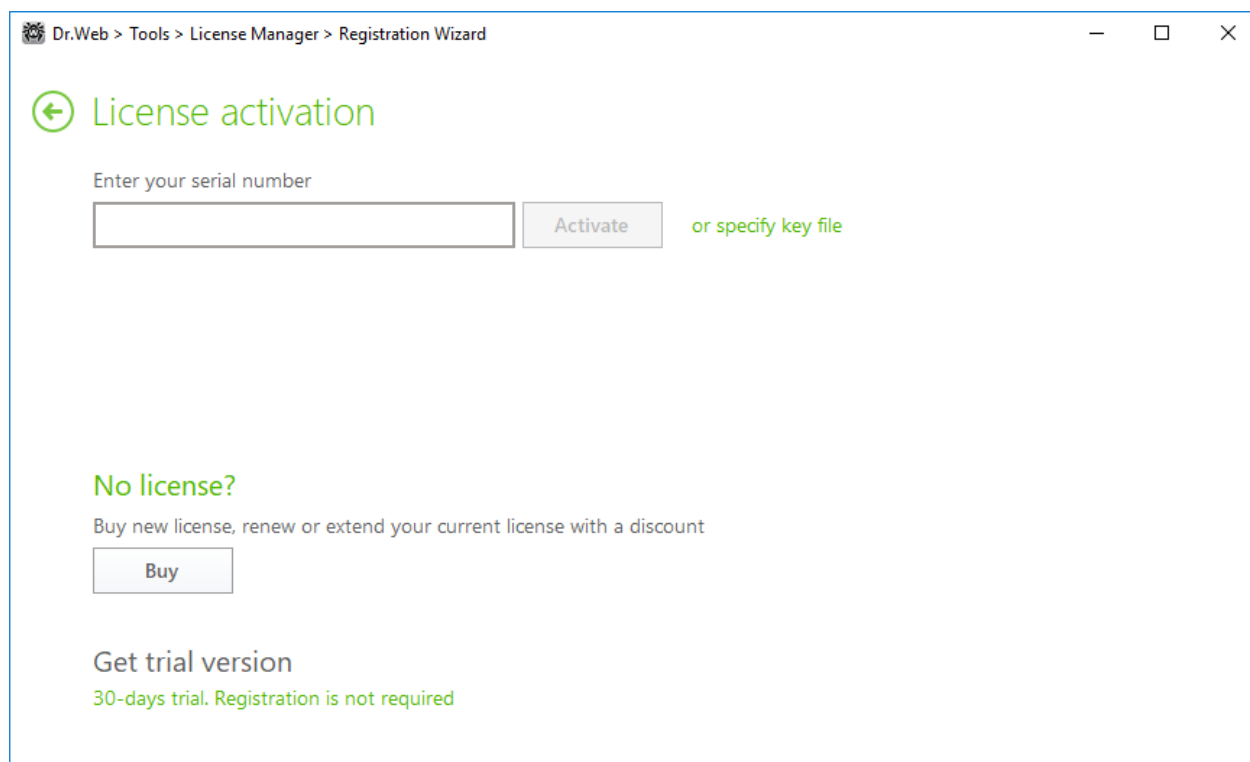


Figure 7. License activation



If license activation failed, an error message displays. Check Internet connection parameters or click **Retry** to correct invalid data.

- register your serial number on the Doctor Web [website](#) and get a key file for license activation.

Activation using the key file

If you have a key file, you can activate your license:

- during the installation via the Installation wizard:
 1. Start the product installation. At step 5 of the installation, select **Specify path to an available valid key file**. Click **Install**.

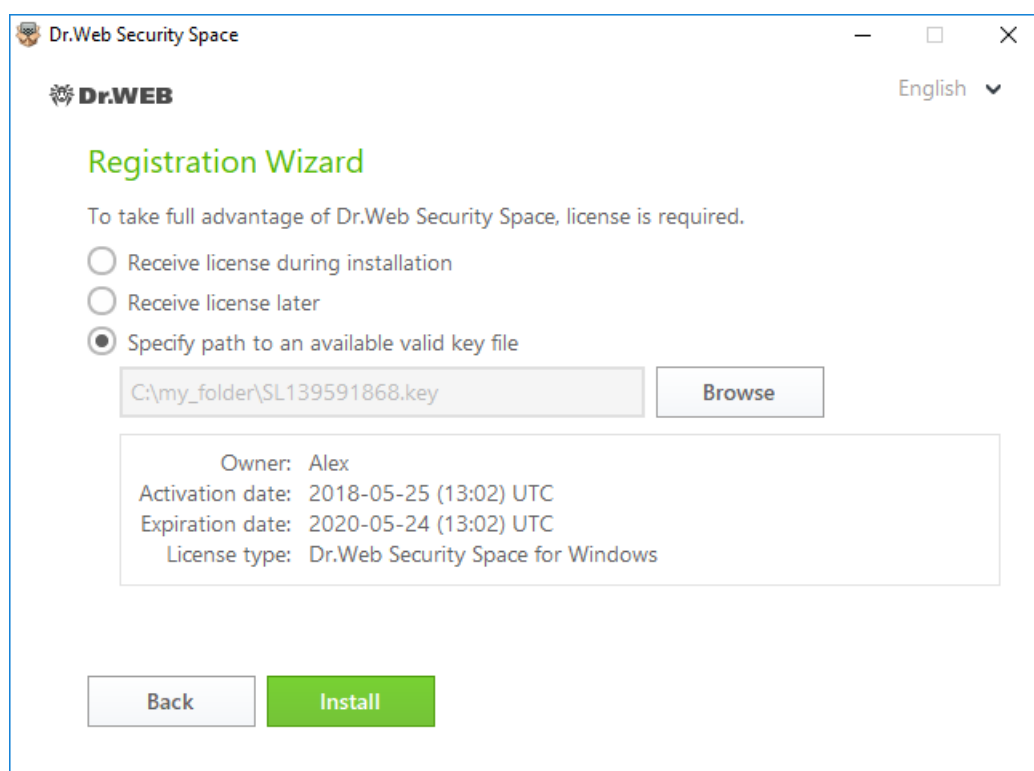



Figure 8. Installation. Registration wizard

2. Continue product installation following the instructions of Installation wizard.
- in any moment after the installation via the Registration wizard included in the License manager:
 1. In the [Dr.Web menu](#) , select **License** item. License Manager opens. Click **Buy or activate new license**.

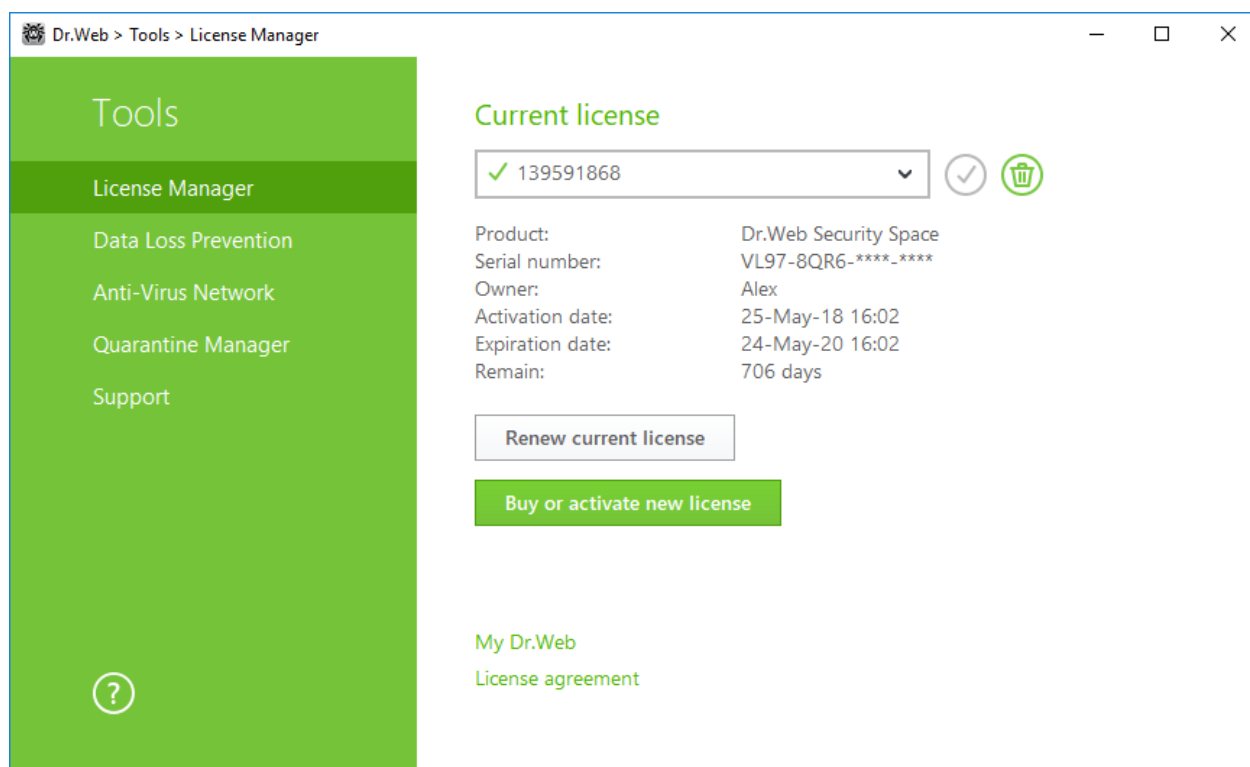


Figure 9. License Manager

2. The License manager window opens. Click the **or specify key file** link. In the open window, specify the path to the key file.

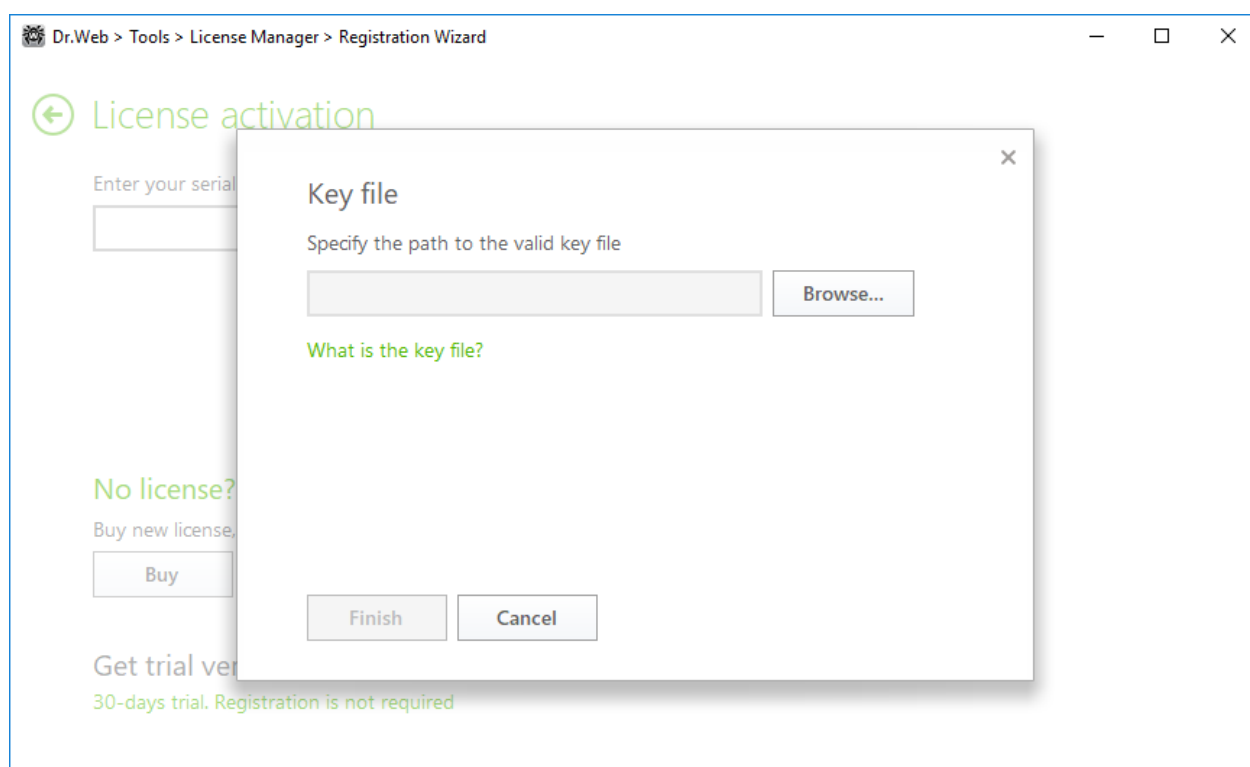


Figure 10. License activation



License activation on Windows XP

Users of Windows XP can activate license using the key file only. If there is only serial number without the key file, it is necessary to activate it on the Doctor Web [website](#). After the registration is over, the link for downloading the key file is available. Use this key file for [license activation](#).



A demo period cannot be activated and used on Windows XP.

Reactivating license

You may need to reactivate a license or a demo period if the key file is lost.



When reactivating a license or a demo period, you receive the same key file as during the previous registration providing that the validity period is not expired.

When you reinstall the product or install it on several computers, if the license allows for that, you will be able to use the previously registered key file. Reactivation of the key file is not required.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact [technical support](#) describing your problem in detail, stating your personal data input during the registration and the serial number. The key file will be sent by the technical support to your email address or delivered in a different way.

Possible questions

How to transfer a license to another computer?

You are entitled to transfer your license for commercial use using the key file or serial number. If you want to transfer a license to a computer run by Windows XP, you can only do it using the key file.

To transfer a license to another computer

- using the serial number:
 1. Remove Dr.Web from the computer of license origin or activate another license on this computer.
 2. Activate the current license on target computer. To do this, use Registration wizard during the product installation or after the installation (see [Activation using serial number](#)).




- using the key file:
 1. Copy the key file from the computer of origin. By default, the [key file](#) is stored in Dr.Web installation folder and has .key extension.
 2. Remove Dr.Web from the computer of license origin or activate another license on this computer.
 3. Activate the current license on target computer. To do this, use the registration wizard during the product installation or after the product is installed ([Activation using the key file](#)).



It is impossible to transfer a demo period to another computer.


4.2. Renewing License

You can renew the current license using License Manager.

1. Open Dr.Web [menu](#) , then select **License**.
2. In License Manager window click **Renew current license**. A page on Doctor Web website, where you can purchase the license, will open.

Dr.Web supports the update on the fly, thus you do not need to reinstall Dr.Web or interrupt it. To update the license, you need to activate a new license.

License activation

1. Open License Manager window, by selecting **License** in Dr.Web [menu](#) . Click **Buy or activate new license**.
2. In the open window enter the product serial number or go to the link **or specify key file** and specify the path to the key file. Windows XP user can [activate the license](#) only using the key file.

The detailed information on license activation is available in [How to activate the license](#) section.

If the period of the license you want to rebew, is over, Dr.Web will use the new license.

If the license you want to renew is still valid, then the number of days remaining will be automatically added to the new license. At the same time, the old license will be blocked, and you will receive a notification to the email address you provided during registration. It is also recommended to remove the old license using [License Manager](#).

If you have question on license renewal, read [FAQ](#) section on Doctor Web website.





Possible questions

After the license renewal I received an email that my key file will be blocked in 30 days period

If the validity period of the license that you have extended has not expired yet, then number of the remaining days is added to the new license automatically. At the same time the license, on which behalf the extension was made, will be blocked. If you use a blocked license, Dr.Web components do not function and the software is not updated.

It is recommended to remove the previous license. To remove the license, do the following:

1. In [Adiministrator mode](#), in Dr.Web [menu](#) , select **License** item. License Manager opens.
2. In the drop-down menu select the license, on which behalf the prolongation has been made, then click .

4.3. Key file

The use rights for Dr.Web are specified in the *key file*. Key files received during installation or within the product distribution kit are installed automatically.

The key file has the .key extension and contains the following information:

- List of licensed anti-virus components
- Licensed period for the product
- Availability of technical support for the user
- Other restrictions (for example, the number of remote computers allowed for simultaneous anti-virus check)



By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.

If no valid key file is found, Dr.Web components are blocked.


A valid key file for Dr.Web satisfies the following criteria:

- License is not expired.
- Integrity of the key file is not violated.

If any of the conditions is violated, the key file becomes invalid and Dr.Web stops detecting and neutralizing malicious programs in files, memory, and email messages.

If during Dr.Web installation, you did not receive a key file and did not specify a path to it, a temporary key file is used. Such a key file provides full functionality of Dr.Web. However, in the



Dr.Web  [menu](#), **Update** item is not available until you either activate a license or a trial version or specify a path to the valid key file via the **License Manager**.

It is recommended that you keep the key file until the license or the trial version expires.



A key file for a demo period activation can be used only on the computer where the registration procedure was run.






5. Getting Started

After Dr.Web application is set up, the icon  is added to Windows notification area.



If the application is not running, in **Start** menu expand the application group **Dr.Web** and then select **SpIDer Agent**.

Dr.Web icon displays the current application state:


- —all necessary components are running and protect your computer.
- —Dr.Web self-protection or an important component is disabled, which compromises security of the anti-virus and your computer. Enable self-protection or the disabled component.
- —components are expected to start after the operating system startup process is complete, thus wait until the components start; or an error occurred while starting one of the main Dr.Web components, and your computer is at risk of virus infection. Check that you have a valid key file and, if required, [install](#) it.

Also, according to [settings](#), above the  icon various hints or notifications can appear.

To open the menu, click the  icon in the Windows notification area.



To access the protection components and settings and to disable components, you need to have administrative privileges.

In the Dr.Web menu  main managing tools and program settings are located.

My Dr.Web. Opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

License. Opens [License Manager](#).

Tools. Opens a submenu providing access to:


- [Data Loss Prevention](#);
- [Anti-virus Network](#);
- [Quarantine Manager](#);
- [Support](#).


Protection components. Quick access to the protection components list where you can enable or disable each of the components.


Update. Information about actuality of the components or virus databases. Launches the update.

Scanner. Quick access to launching different kinds of scanning.



Operation mode . Allows to switch between user mode and administrator mode. By default, Dr.Web starts in restricted user mode, which does not provide access to [Settings](#) and settings of [Protection components](#). To switch to another mode, click the lock. If UAC is enabled, operating system will prompt a request for administrative privileges. Besides, you also need to enter the password to change the mode if you set the **Protect Dr.Web settings with a password** option in the [Settings](#) window. Note that you will be returned to user mode in 15 minutes after switching to administrator mode. If you are still configuring the settings when this time expires, you will be returned to user mode after closing the settings window.

Statistics . Opens statistics on the components operations in the current session including the number of scanned, infected and suspicious objects, actions performed, and so on.

Settings . Opens a window with access to the main settings, protection components settings, Parental Control, and exclusions.



To access the component settings and open your personal webpage **My Dr.Web**, you also need to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

If you forgot your password for the product settings, contact [technical support](#).

Help . Opens the help file.

5.1. Testing the Anti-virus

Testing the Anti-virus with EICAR file

The EICAR (European Institute for Computer Anti-Virus Research) test file helps to test performance of anti-virus programs that detect viruses using signature analysis.

For this purpose, most of the anti-virus software vendors generally use a standard test.com program. This program was designed specially so that users could test reaction of newly-installed anti-virus tools to virus detection without compromising security of their computers. Although the test.com program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this file, Dr.Web reports the following: EICAR Test File (Not a Virus!). Other anti-virus tools alert users in a similar way.

The test.com program is a 68-byte COM-file that prints the following line on the console when executed: EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

The file test.com contains the following character string only:

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



To make your own test file with the “virus”, create a new file with this line and save it as test.com.



When running in the [Optimal mode](#), SpIDer Guard does not terminate execution of an EICAR test file and the file is not processed as malicious since it does not pose any actual threat to your system. However, if you copy or create such a file in your system, it will be detected by SpIDer Guard and moved to Quarantine by default.

Testing the Anti-Virus with CloudCar file


To check the [Dr.Web Cloud](#) service, use the CloudCar test file by AMTSO (Anti-Malware Testing Standards Organization). This file is specially created to check cloud service operation. It is not a virus.

To check Dr.Web Cloud operation

1. Make sure the usage of the [Dr.Web Cloud](#) service is enabled.
2. Download the test file. For that, go to <https://www.amtso.org/feature-settings-check-cloud-lookups/> and click **Download the CloudCar Testfile** in the webpage.
3. If the SpIDer Guard is installed and enabled, Dr.Web automatically moves the file to quarantine after the file is saved to the computer. If the SpIDer Guard is not installed or disabled, scan the downloaded file. For that, select the **Check with Dr.Web** option in the context menu of the file shortcut.
4. Check that the test file is processed by Dr.Web as `CLOUD:AMTSO.Test.Virus`. The CLOUD prefix in the threat name indicates correct Dr.Web Cloud operation.



6. Tools

Open Dr.Web menu  and run **Tools**. To have an access to all options, switch to [administrator mode](#).

To get your license information or to get a new license, go to [License Manager](#).

To configure important data protection by creating protected copies, go to [Data Loss Prevention](#).

To access Dr.Web components installed on other computers of your local network, go to [Anti-virus Network](#).

To view the isolated files list and restoring files from the quarantine, select [Quarantine Manager](#).

If you encounter any questions or problems while using Dr.Web, go to [Support](#).

6.1. License Manager

In this window, you can view all Dr.Web [licenses](#) for your computer. You can also modify the current license, renew it or purchase a new license and activate it.

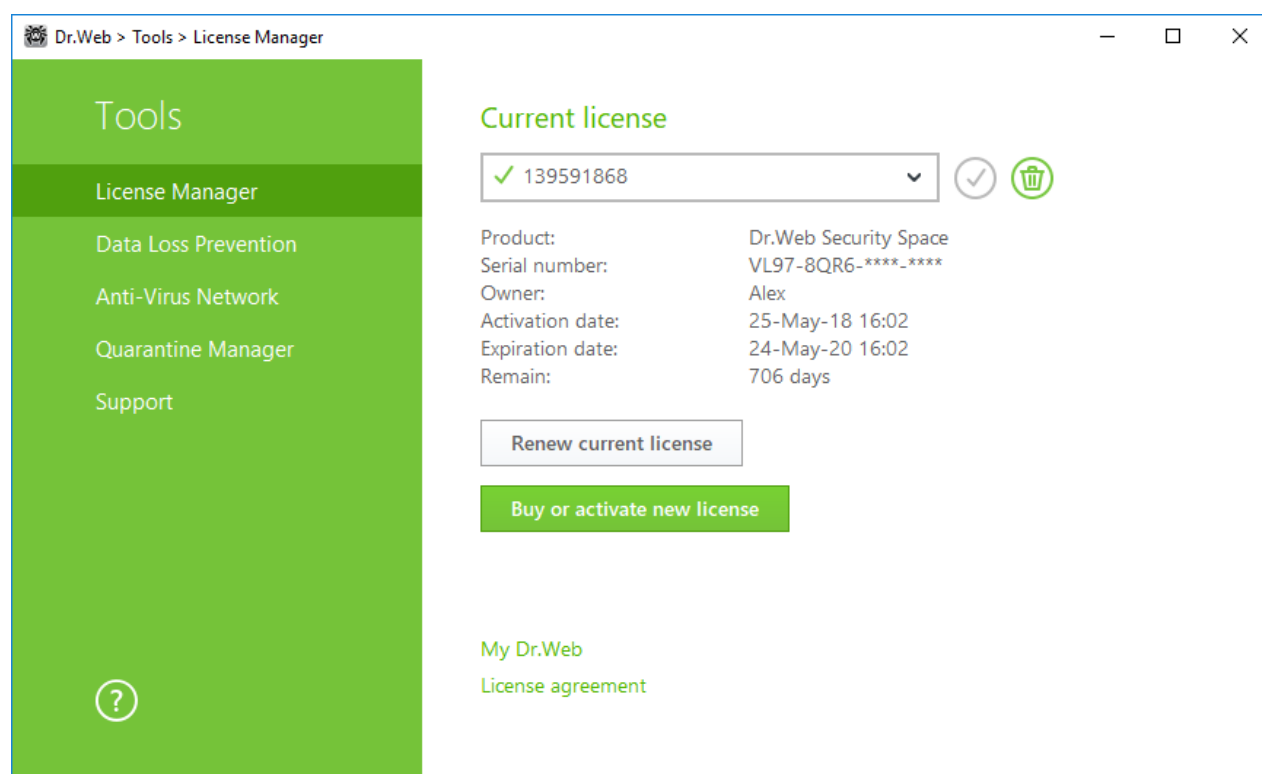




Figure 11. Current license information

To view information on a license that is not currently in use, select it from the drop-down list. In the administrator mode, click  to delete the selected license or click  to set it as current. Please note that the current license cannot be deleted.



Once you click **Buy or activate new license**, the Registration Wizard opens an additional window, where you can purchase or [activate the new license](#).

Once you click **Renew current license**, the program will open the page on the Doctor Web website where all parameters of the current license will be transmitted.

Advanced

The [My Dr.Web](#) link opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

The [License agreement](#) link opens the license agreement on the Doctor Web official website.

6.2. Data Loss Prevention

To protect important files from being changed by malicious software, enable the **Data Loss Prevention**. With this function, you can make copies of files that reside in the specified folders.



You cannot change data loss prevention parameters or restore files from copies in user mode. For this actions, switch to [administrator mode](#).

If a file is blocked, it will not be copied.

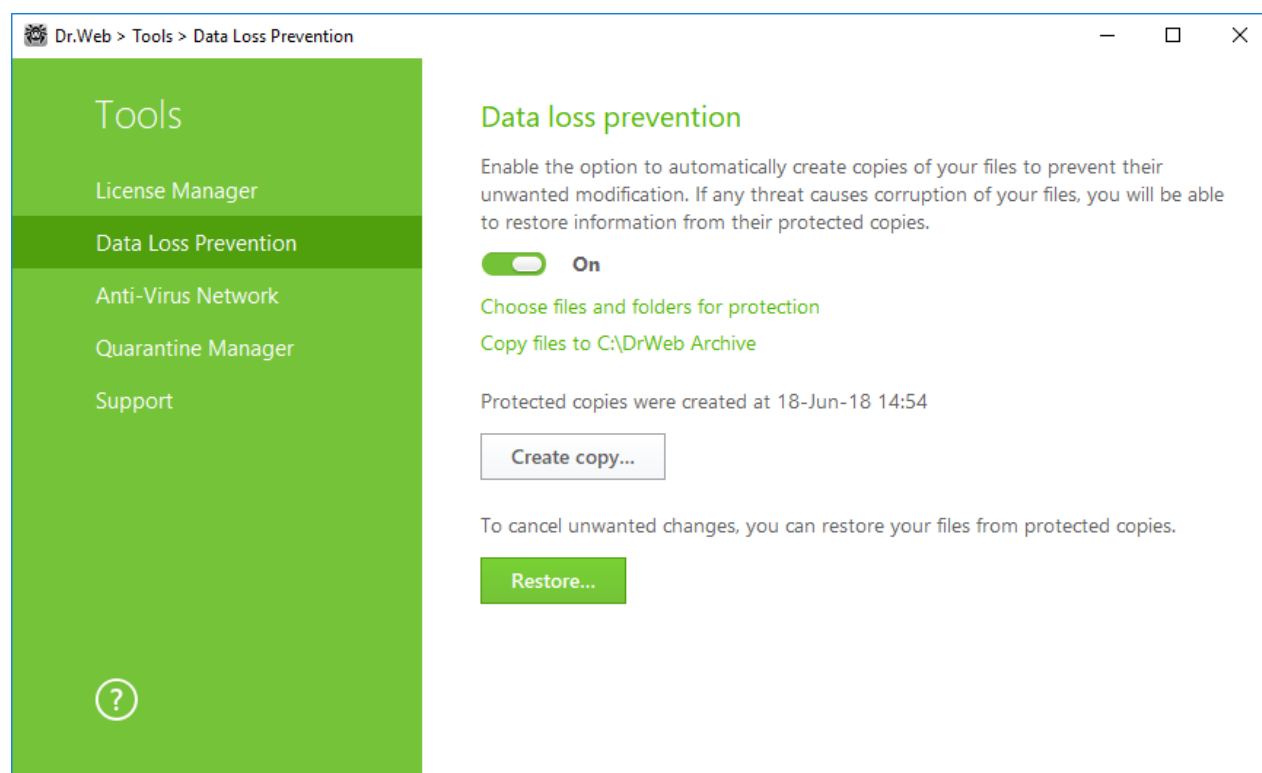




Figure 12. Data loss prevention



To configure list of files and folders for protection

Click the **Choose files and folders for protection** link to specify the objects for which protected copies will be created:

- to add a file or a folder, click  and select the required object;
- to remove an object from the list, select the corresponding item from the list and click .

You may change the objects list at any time.

Parameters for creating a copy

Click the link **Copy files to C:\DrWeb Archive**. Specify the required parameters in the appeared window.

1. Set common parameters for copies:
 - Specify a disk for storage of copies.
 - Specify frequency of copy creation. After the chosen interval, Dr.Web will inspect the specified objects for changes and create a copy if any changes have been made.
 - If necessary, block the copy creation option when running on battery power.
2. Specify a limit of available disk space:
 - Set maximum disk space used for storage of copies.
 - If necessary, specify a limit on number of copies.
 - Select one of the actions: if any of the specified limits is exceeded, copies are not created, or they overwrite the existing ones (starting from the oldest copy).

Removal of created copies

You may also delete copies to free up some disk space (deleting the copies will not affect the original files). To do that click **Copy files to C:\DrWeb Archive**, then click **Delete copies**.

Restoring files

If your files were corrupted, you can restore their copies created by a certain date. To do that, click the **Restore** button in the main window and then click **Next**. In the window displayed, select the required date and all copies that were available for the date will be restored to the specified folder.

Start creating copies manually

To start creation of protected copies manually, click the **Create copy** button in the main window. In the window displayed, specify the description for the new copy.



To ensure correct operation the **Data Loss Prevention** system, you need to have at least 20 GB free on the disk that is selected for storing protected copies.

6.3. Anti-virus Network

This section allows to manage Dr.Web Anti-virus for Windows, Dr.Web Anti-virus for Windows Servers, or Dr.Web Security Space within one product version on other computers of your network.

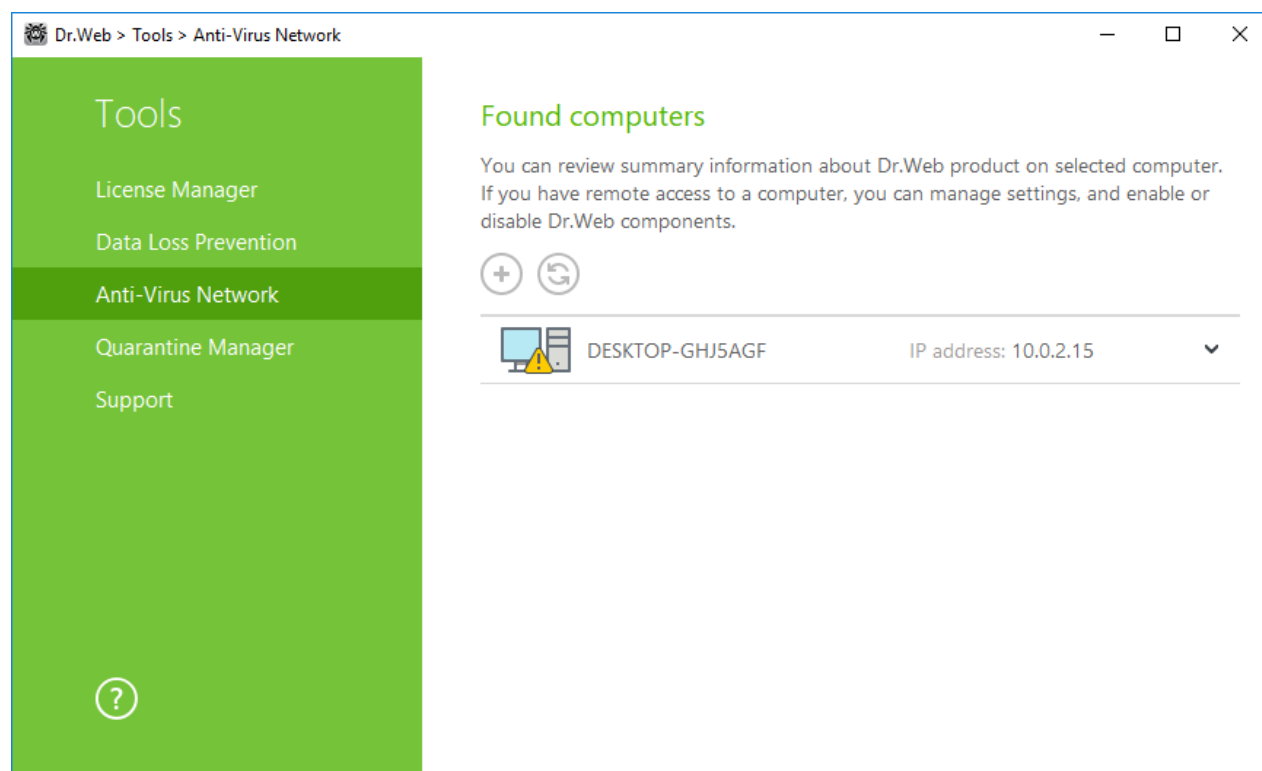




Figure 13. Anti-virus Network nodes

To access a remote anti-virus, select the computer from the list and click **Connect**. Enter the password specified in the settings of the remote anti-virus. An icon for the remote SpIDer Agent appears in the notification area , and the notification about successful connection will be displayed.

You can view settings, enable or disable components, and configure their settings. Anti-virus Network, Quarantine and Scanner are not available. Dr.Web Firewall settings and statistics are not available as well, but you can enable or disable this component (if you accessed Dr.Web Anti-virus for Windows or Dr.Web Security Space). Also you can select the **Disconnect** item to terminate the remote connection.

If the required computer is not on the list, you can try to add it manually. For this, click  and enter an IP-address.



You can establish only one connection with a remote Dr.Web product. If one connection is already established, the **Connect** button is disabled.

Computers are listed if Dr.Web products installed on these computers allow remote connection. You can allow connection to your Dr.Web on the **Anti-virus Network** page in [Main settings](#).

6.4. Quarantine Manager

This window contains information on the Quarantine component of Dr.Web which serves for isolation of files that are suspected to be malicious. Quarantine also stores backup copies of files processed by Dr.Web.

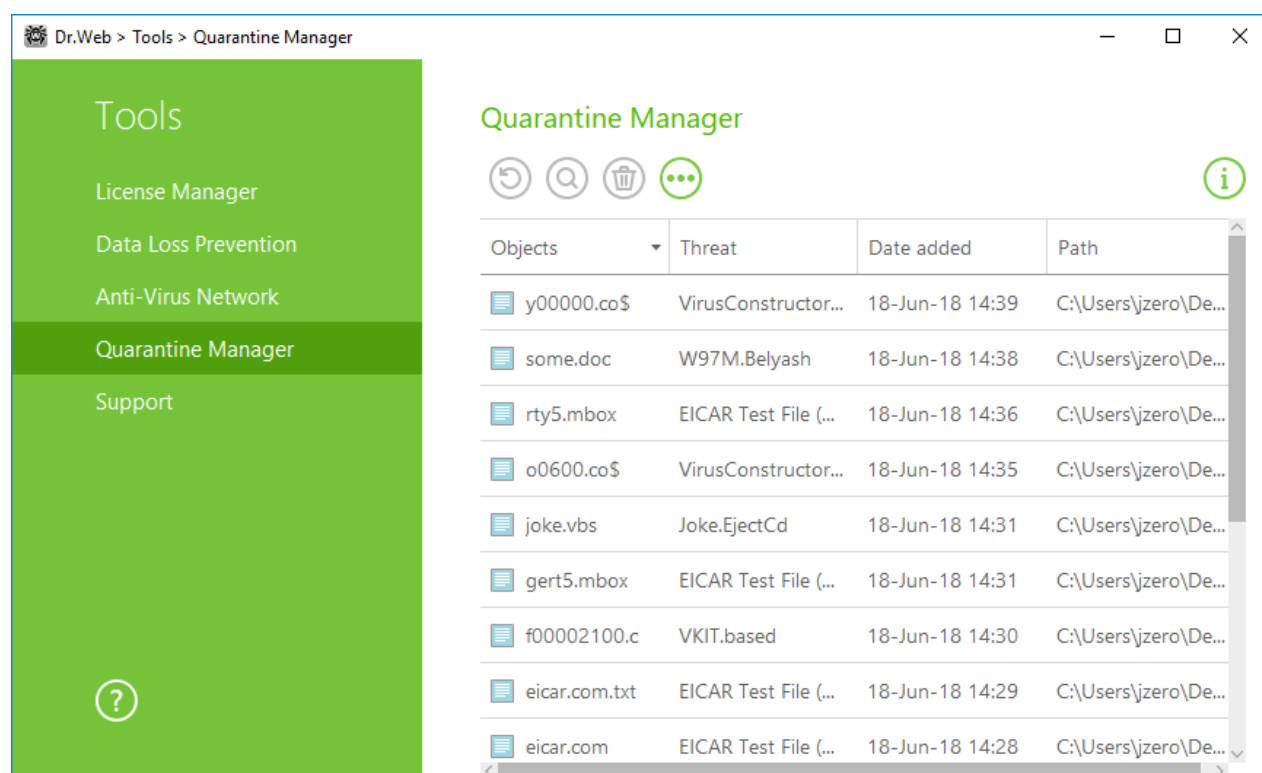


Figure 14. Objects in Quarantine

Use [Quarantine Manager settings](#) to select the isolation mode for infected objects detected on portable data carriers. When this option is enabled, detected threats are moved to the folder on this data carrier without being encrypted. The Quarantine folder is created only when the data carrier is accessible for writing. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss.

The central table lists the following information on quarantined objects:


- **Objects**—name of the quarantined object.
- **Threat**—malware class of the object, which is assigned by Dr.Web when the object is quarantined.



- **Date added**—date and time when the object was moved to the Quarantine.
- **Path**—full path to the object before it was quarantined.



Quarantine Manager displays objects that can be accessed by your user account. To view hidden objects, you need to have administrator privileges.

By default, backup copies stored in quarantine are not displayed. To view them, click  and select **Show backup copies** from the drop-down list.

Managing quarantined objects

In [administrator mode](#), the following buttons are available:

- **Restore**—move one or several objects to the selected folder.



Use this option only when you are sure that the selected object is not harmful.

- **Rescan**—scan the file in quarantine again.
- **Delete**—delete one or several objects from quarantine and from the system.

You can also access these settings by right-clicking the selected object or several selected objects.

To delete all objects from quarantine at once, click  and select **Delete all** from the drop-down list.

6.5. Support

This section provides information on the product version, components, the last update date, and the useful links that may help you to resolve issues or solve problems encountered while using Dr.Web.

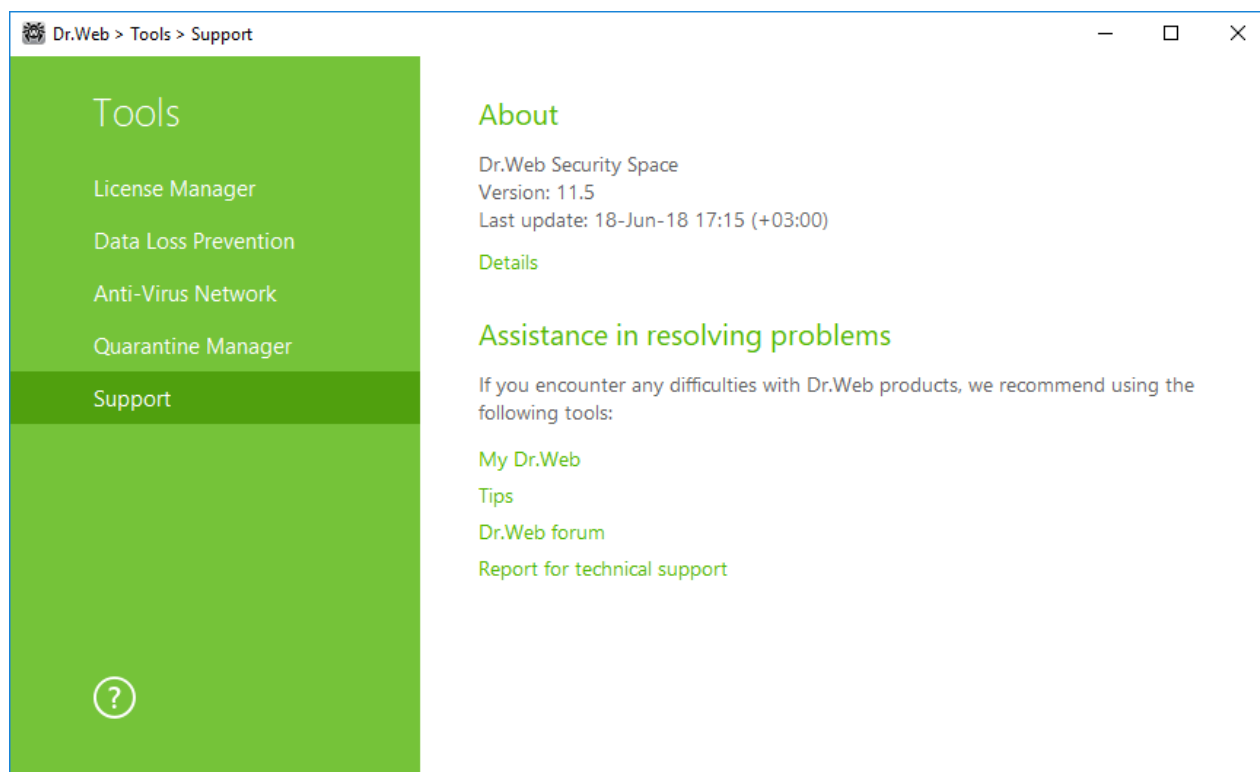


Figure 15. Product version information and support

In case of questions, we recommend using one of the following tools:

My Dr.Web. Opens your personal webpage on the Doctor Web official website. This page provides you with information on your license including usage period and serial number, allows to renew the license, contact technical support, and so on.

Tips. Opens tips on working with Dr.Web.

Dr.Web forum. Opens Dr.Web at <https://forum.drweb.com>.

Report for technical support. Launches the wizard that will help you to [create a report](#) containing important information on your system configuration and computer working.

If you have not found a solution for the problem after contacting the Dr.Web forum, you can fill in the web form in the corresponding section of the support site at <https://support.drweb.com/>. When filling the form, you can attach the report for technical support, screenshots and other required information.


For regional office information, visit the Doctor Web official website at <https://company.drweb.com/contacts/moscow>.

6.5.1. Report Wizard

When contacting Doctor Web technical support, you can generate a report on your operating system and Dr.Web operation.



To generate a report

1. Open the menu .
2. Go to **Tools**.
3. Select **Support**.

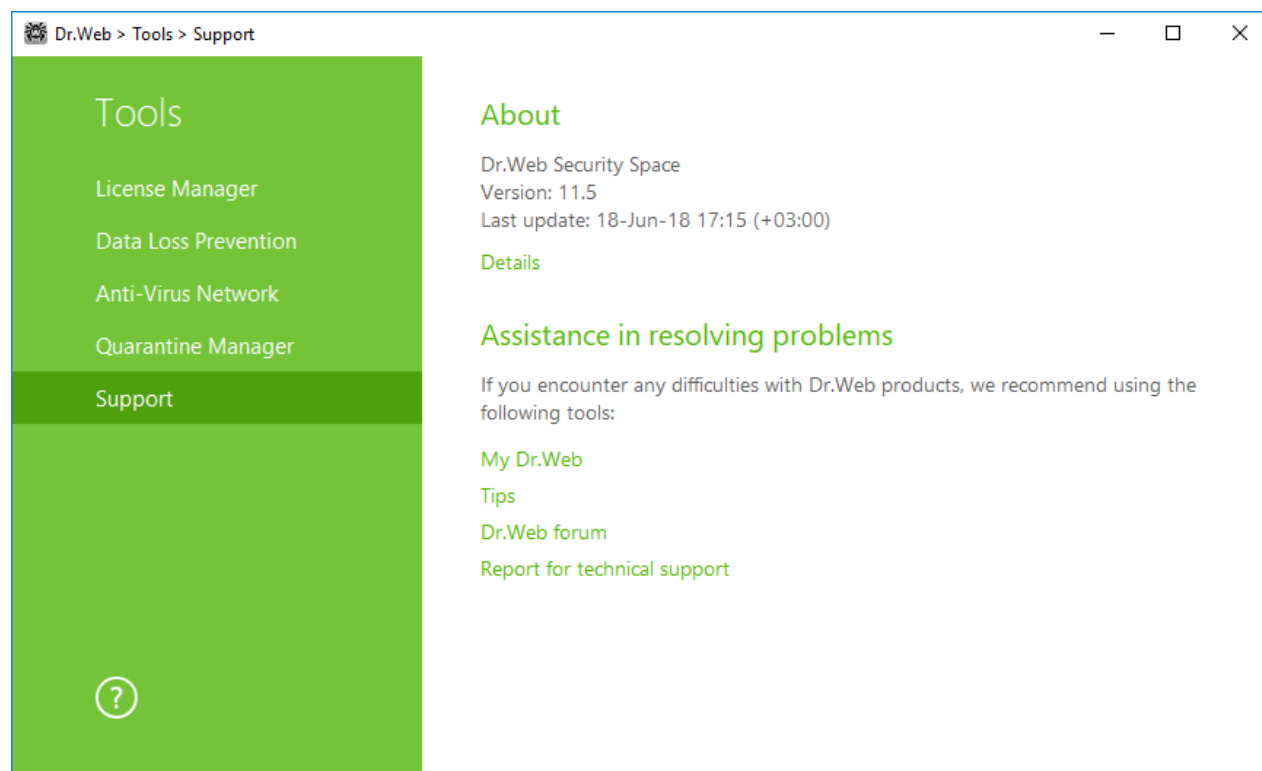


Figure 16. Support

4. Click the **Report for technical support** link.
5. In the open window, click **Generate report**.

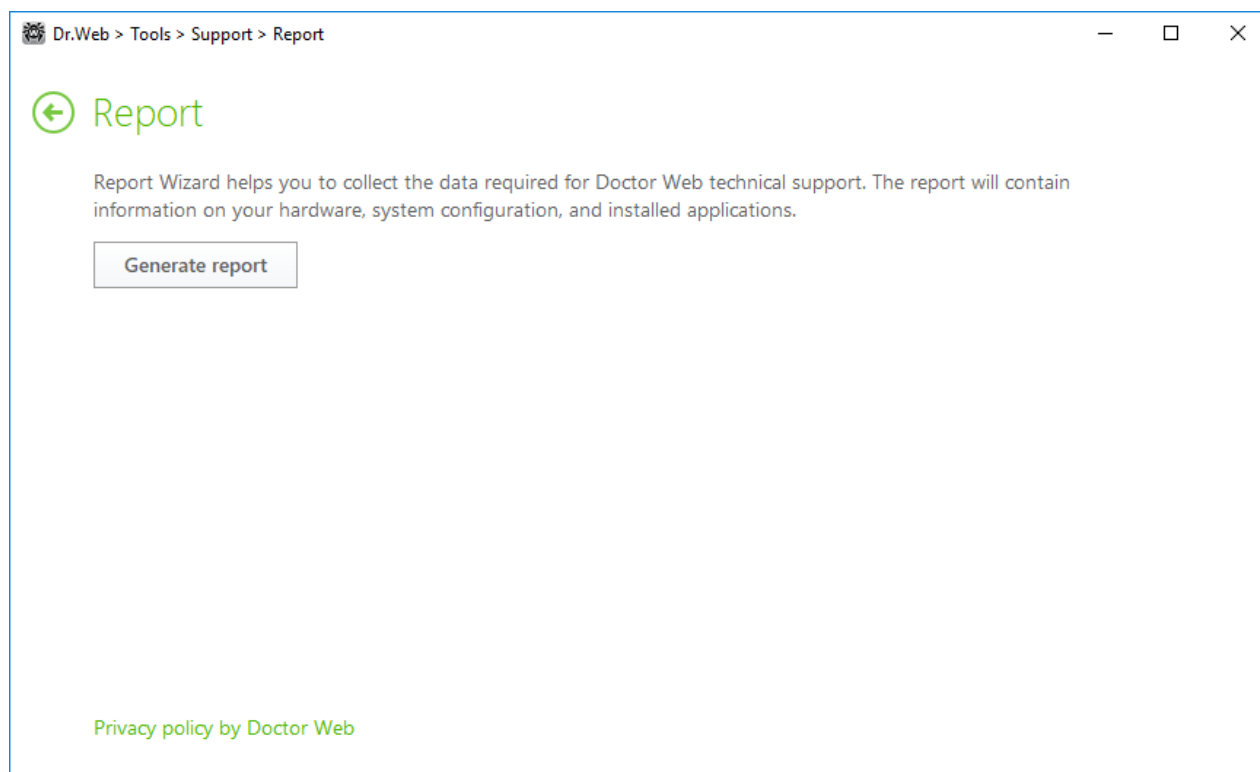


Figure 17. Generating a report

The report will be generated automatically and saved as an archive in the Doctor Web subfolder of the %USERPROFILE% folder.

To build the report, click the corresponding button. The report will include the following information:

1. Technical information about the operating system:

- General information about your computer
- Running processes
- Scheduled tasks
- Services, drivers
- Default browser
- Installed applications
- Policies
- HOSTS file
- DNS servers
- System event log
- System directories
- Registry branches
- Winsock providers
- Network connections



- Dr.Watson logs
 - Performance index
2. Information about Dr.Web anti-virus solutions.
 3. Information about the Dr.Web plug-ins:
 - Dr.Web for IBM Lotus Domino
 - Dr.Web for Kerio MailServer
 - Dr.Web for Kerio WinRoute

Information about Dr.Web anti-virus solutions is located in Event Viewer, in **Application and Services Logs** → **Doctor Web**.

Report generation from command line

To generate a report, use the following command:

```
/auto
```

For example: dwsysinfo.exe /auto

The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% folder.

You can also use the command:

```
/auto/report : [<full path to the archive>]
```

where

- *<full path to the archive>*—path to the report file.

For example: dwsysinfo.exe /auto /report:C:\report.zip




7. Updating of virus databases and program components

To detect malicious objects, Dr.Web products use virus databases that contain information about all known malicious programs. Regular updates of databases allows to detect previously unknown viruses, block their distribution, and in some cases to cure previously incurable infected files. Besides virus databases, Dr.Web software components and help documentation are updated as well.

For Dr.Web to update, you need a connection to the Internet or to the update mirror (local or network folder), or to the Anti-virus network with at least one computer that has an update mirror set. Customizing of update source settings can be done on settings page **Main** → **Update**. The details of customization of Dr.Web updating parameters is located in [Update](#) section.

Updates relevance check

To check the relevance of virus databases and program components, open Dr.Web [menu](#) . In case if updates are relevant, in menu **Update is not required** is displayed.

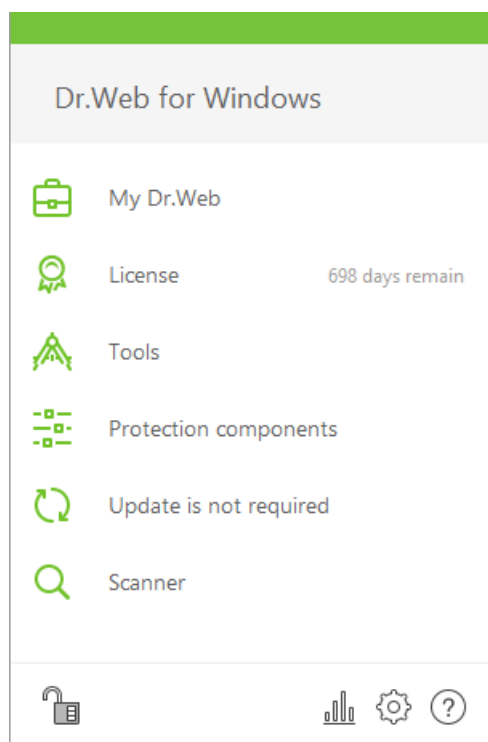


Figure 18. Dr.Web menu


Update launch

During the update, Dr.Web downloads all updated files that correspond to your version of Dr.Web and upgrades Dr.Web if a newer version is available.



After an update of executable files, drivers, or libraries, a program restart may be required. In such cases, an appropriate warning displays.



Update launch from Dr.Web menu

1. Open Dr.Web [menu](#) , then select **Update**. Depending on virus databases and program components relevance, the name of this menu item can vary.
2. This opens information on relevance of Dr.Web virus databases and other components as well as the date of their last update. Start updating by clicking **Update**.

Update launch from the command line

Open the Dr.Web installation folder (%PROGRAMFILES%\Common Files\Doctor Web\Updater) and run the `drwupsrv.exe` file. The list of command-line parameters can be found in [Appendix A](#).

Update logs

You can access the update logs in **Statistics** section. To access logs open Dr.Web [menu](#) , then open **Statistics**  page.

Dr.Web updates logs are stored in `dwupdater.log` file located in the `%allusersprofile%\Doctor Web\Logs\` folder.



8. Dr.Web Scanner

Dr.Web Scanner for Windows allows you to run anti-virus scans of disk boot sectors, random access memory (RAM), and both separate files and objects enclosed within complex structures (archives, containers, or email attachments). By default, Dr.Web Scanner uses all [detection methods](#) to detect viruses and other malicious software.

On detection of a malicious object, Dr.Web Scanner only informs you about it. Information on all infected or suspicious objects displays in the table where you can manually select a necessary action. You can apply default actions to all detected threats or select the required reaction to a certain object.


The default settings are optimal for most cases. However, if necessary, you can modify the suggested actions in the Dr.Web Scanner [settings window](#). Please note that you can specify a custom action for each detected threat after the scan is complete, but common reaction for a particular threat type should be configured beforehand.

8.1. Scanning Your System



When using Windows Vista or later operating systems, it is recommended to run Dr.Web Scanner with administrative privileges. Otherwise, all folders and files (including system folders) that are not accessible to an unprivileged user will not be scanned.

To select a scan mode

1. Click the Dr.Web [menu](#)  and select **Scanner**. The menu of quick access to different scan modes opens.

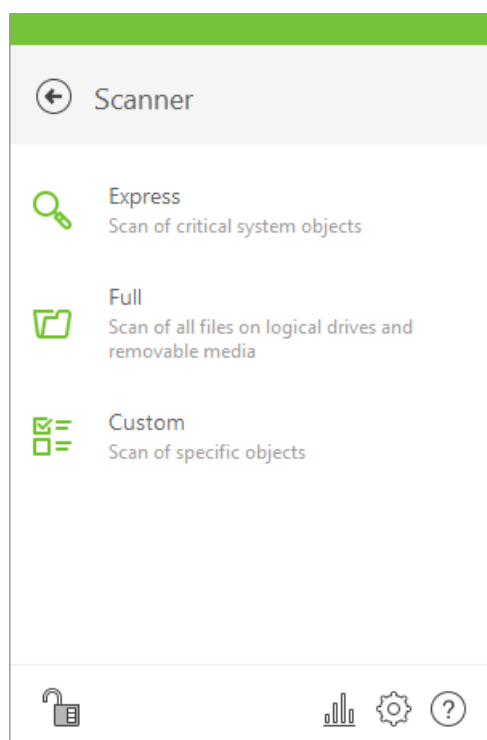


Figure 19. Selecting the scanning mode

2. Select a scan mode you need:

- **Custom** item to scan only selected objects. The Dr.Web Scanner window opens;
- **Express** item to scan only critical Windows objects;
- **Full** to scan all files.

To launch Scanner with default settings to scan a certain file or folder, select **Check with Dr.Web** in the shortcut menu.

Configuring Dr.Web Scanner

To configure Dr.Web Scanner and its reactions to detected threats, go to **Settings** → **Protection Components** → **Scanner**.

Scan modes

Express scan

In this mode, Scanner checks the following:

- Boot sectors of all disks
- Random access memory
- Boot disk root folder
- Windows system folder
- User documents folder ("My Documents")



- Temporary files
- System restore points
- Presence of rootkits (if the process is run with administrative privileges)




Scanner does not check archives and email files in this mode.

Full scan

In this mode, random access memory and all hard drives (including boot sectors of all disks) are scanned. Moreover, Scanner runs a check for rootkits.

Custom scan

In this mode, you can select objects to be scanned, for example, any files and folders and such objects as random access memory, boot sectors, and so on. To start scanning selected objects, click **Start scanning**. To select objects, click .

Scan process

When scanning starts, the **Pause** and **Stop** buttons become available. During scanning, you can do the following:

- To pause scanning, click **Pause**. To resume scanning after pause, click **Resume**.
- To stop scanning, click **Stop**.

From this window, you can return to the scan mode selection window.



The **Pause** button is not available while processes and RAM are scanned.

8.2. Actions Upon Detection

If any viruses or computer threats of other types are detected during scanning, Dr.Web Scanner informs you about them and recommends the most effective actions to neutralize them. You can neutralize all detected threats at once. To do this, select all threats and click **Neutralize**. In this case, Dr.Web Scanner applies the most effective actions according to its configuration and threat type.



By clicking **Neutralize**, you apply actions to the objects selected in the table. You should select objects or groups of objects manually to set an action applied by clicking **Neutralize**. To select a group of objects, you can use CTRL and SHIFT keys. To select



actions for neutralizing threats, right-click one or several selected objects and choose an option from the context menu.

To select an action

1. Where necessary, select a custom action from the drop-down list in the **Action** field. By default, Dr.Web Scanner selects a recommended action.
2. Click **Neutralize**. Dr.Web Scanner applies actions to the selected threats.

There are the following limitations:

- For suspicious objects, curing is impossible.
- For objects which are not files (boot sectors) moving and deletion is impossible.
- For files inside archives, installation packages, or attachments, no actions are possible.

The detailed report on program operation is stored in the dwscanner.log file that is located in %USERPROFILE%\Doctor Web folder.

Column name	Description
Object	This table column contains the name of an infected or suspicious object (either a file name if a file is infected, or Boot sector if a boot sector is infected, or Master Boot Record if an MBR of the hard drive is infected).
Threat	The names of viruses or virus modifications as per the internal classification of Doctor Web (modification of a known virus is a code resulting from such alteration of a known virus which can still be detected but cannot be cured with the algorithms applied to the initial virus). For suspicious objects, the following is displayed: indication that the object "is possibly infected" and the type of a possible virus according to the classification used by the heuristic analyzer.
Action	<p>The action recommended for the threat found. Click the arrow on the button to apply the action for the selected threat.</p> <p>You can apply the displayed action separately to each threat by clicking this button.</p>
Path	The full paths to the corresponding files.



If you enabled the **Neutralize detected threats** option on the [settings](#) page of Dr.Web Scanner to configure **After scanning**, threats will be neutralized automatically.



8.3. Command-Line Scanning Mode

You can run Dr.Web Scanner in the command-line mode that allows to specify settings of the current scanning session and the list of objects for scanning as additional parameters. Automatic activation of the Scanner [according to schedule](#) is performed in this mode.

The launching command syntax is as follows:

```
[<path_to_program>] dwscanner [<switches>] [<objects>]
```

The list of objects for scanning can be empty or contain several elements separated by spaces. If the path to objects is not specified, they are searched in the Dr.Web installation folder.

The most commonly used examples of specifying the objects for scanning are given below:

- /FAST— perform an [express scan](#) of the system.
- /FULL — perform a [full scan](#) of all hard and removable media (including boot sectors).
- /LITE—perform a basic scan of random access memory and boot sectors of all disks as well as run a check for rootkits.

Switches are command-line parameters that specify program settings. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them). Switches begin with the forward slash (/) character and are separated by blanks as other command-line parameters.

8.4. Console Scanner

Dr.Web also includes Console Scanner which allows you to run scanning from the command line and provides advanced settings.



Console Scanner moves suspicious files to Quarantine.

The command syntax to launch Console Scanner is as follows:

```
[<path_to_program>] dwscancl [<switches>] [<objects>]
```

Parameter begins with the forward slash (/) character; several parameters are separated by spaces. The list of objects for scanning can be empty or contain several elements separated by spaces.

All Console Scanner switches are listed in [Appendix A](#).

Return codes:

- 0—scanning completed successfully; infected objects were not found;
- 1—scanning completed successfully; infected objects were detected;



- 10—invalid keys are specified;
- 11—key file is not found or does not support Console Scanner;
- 12—Scanning Engine did not start;
- 255—scanning was aborted by user request.

8.5. Automatic Launch of Scanning

During installation of Dr.Web, an anti-virus scan task is automatically created in the Task Scheduler (the task is disabled by default).

To view task settings, open **Control Panel** (extended view) → **Administrative Tools** → **Task Scheduler**.

From the task list, select the scan task. You can enable the task, adjust trigger time, and set required parameters.

On the **General** page, you can review general information and security options on a certain task. On the **Triggers** and **Conditions** pages, various conditions for task launching are specified. To review event log, open the **Log** page.



You can also create your own anti-virus scan tasks. For details on the system scheduler operation, please refer to the Help system and Windows documentation.



If installed components include Firewall, after Dr.Web installation and the first system restart Task Scheduler will be blocked by Firewall. **Scheduled tasks** will operate only after a second restart when a new rule is already created.



9. Settings

To access the main settings, open the Dr.Web menu  in [administrator mode](#) and click **Settings** .

Password protection

To restrict access to Dr.Web settings on your computer, enable the **Protect Dr.Web settings with a password** option. In the open window, specify the password that will be required for configuring Dr.Web, confirm it, and click **OK**.



If you forgot your password for the product settings, contact [technical support](#).

Manage settings

To restore default settings, select **Reset settings** from the drop-down list.



If you want to use settings of the anti-virus that you already configured on another computer, select **Import** from the drop-down list.

If you want to use your settings on other computers, select **Export** from the drop-down list. Then apply them on the same page of another anti-virus.



10. Main Settings

Centralized settings adjustment allows you to configure main settings of the anti-virus package.

To access the main Dr.Web settings, open the  menu in [administrator mode](#), run **Settings**  and go to **Main**.



To access the main Dr.Web settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

To configure displaying pop-ups and receiving notifications by email, go to the [Notifications](#) page.

To configure advanced security parameters, go to the [Self-protection](#) page.

To configure access to Doctor Web cloud services, go to the [Dr.Web Cloud](#) page.

To allow access to Dr.Web installed on your computer from other computers, go to the [Anti-virus Network](#) page.


To restrict access to specific device or bus classes, go to the [Devices](#) page.

To change the interface language or logging and quarantine parameters, go to the [Advanced](#) page.

10.1. Notifications

In this section you can configure parameters of Dr.Web Agent for Windows performance notifications.

Pop-up notifications

Enable the appropriate option to get pop-up notifications above Dr.Web icon  in the Windows notification area.

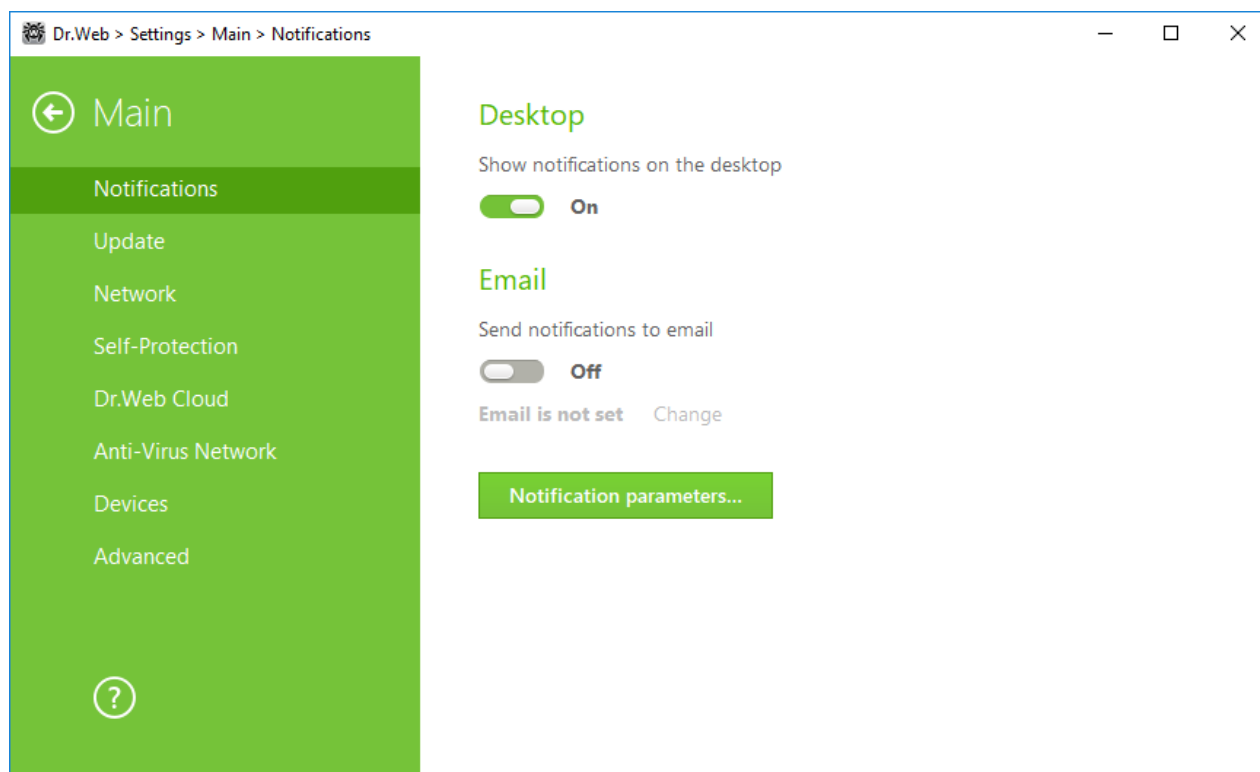


Figure 20. Notifications settings

Email notifications

To receive email notifications about events, do the following:

1. Enable the **Send notifications to email** option.
2. Specify the email address that you want to use for receiving notifications in the appeared window. You will need to confirm this email address at step 7.
3. Click **Next**.
4. Specify the data of the account that will be used to send notifications.
 - Select the mail server from the list and enter your account login and password.
 - If the required mail server is not on the list, select **Set manually**. In the open window, fill in the fields.

Option	Description
SMTP server	Specify the outgoing (SMTP) server for Dr.Web to use when sending email notifications.
Port	Enter the port for Dr.Web to use when connecting to the mail server.
Login	Enter the login for Dr.Web to use when connecting to the mail server.
Password	Enter the password for the login to be used when connecting to the mail server.



Option	Description
Use SSL/TLS	Select this check box to use SSL/TLS encryption when sending messages.
NTLM authentication	Select this check box to use NTLM authentication when connecting to the mail server.

- Click **Send a test message** if you want to make sure that all the details are specified correctly. The message is forwarded to the email address that will be used to send notifications (specified at step 4).
- Click **Next**.
- Enter the conformation code that was sent to the email address specified at step 2. If you do not receive the message within 10 minutes, click **Send the code again**. If you do not enter the code, notifications to this email address will not be sent.
- To change the email address and other parameters, click **Edit** and repeat all the actions starting from step 2.
- Click **Notifications parameters** and set the required notification types. By default, all types of email notifications are disabled.

Notifications parameters

- Click **Notifications parameters**.
- Select notifications that you want to receive. To display pop-up notifications, enable check boxes in the **Desktop** column. To receive mail notifications, enable check boxes in the **Mail** column. If you do not want to receive any notifications, disable all check boxes.

Notification type	Description
Threat is detected	Notifications on threats detected by SplDer Guard and SplDer Gate. By default, these notifications are enabled.
Critical notifications	Notifications on the following critical issues: <ul style="list-style-type: none">Failures to make a protected copy.Connections waiting for Firewall to reply are detected. By default, these notifications are enabled.
Major notifications	Important notifications on the following issues: <ul style="list-style-type: none">Expiration of the time limit set for working on the computer.Device is blocked.Attempt to change system date and time is blocked.Attempt to access a protected object is blocked by Preventive Protection.New version is available.



Notification type	Description
	<ul style="list-style-type: none">• Virus databases are out of date. By default, these notifications are enabled.
Minor notifications	Minor notifications on the following issues: <ul style="list-style-type: none">• Successful update.• Update failures.• Expiration of the time limit set for Internet use.• URL is blocked by Parental Control.• URL is blocked by SplDer Gate.• An attempt to access a protected object is blocked by Parental Control. By default, these notifications are disabled.
License	Notifications on the following issues: <ul style="list-style-type: none">• License expires.• Valid license is not found.• The current license is blocked.

3. If necessary, configure additional parameters:

Option	Description
Notify on new tips	Notifications about new tips on working with Dr.Web.
Do not show notifications in full-screen mode	Hide notifications when an application is running in full-screen mode on your computer (e.g., a game or a movie). Clear this check box to display notifications regardless of the mode.
Display Firewall notifications on separate desktop in full-screen mode	Notifications from Firewall on a separate desktop when an application is running in full-screen mode on your computer (a game or a movie). Clear this check box to display notifications on the same desktop where an application is running in full-screen mode.

4. If you selected one or more email notifications, configure [sending emails](#) from your computer.



Notifications on the following issues are not included in any of the specified groups and are always displayed to the user:

- Priority updates installed and restart is required.



- To finish neutralizing threats, restart the computer.
- To enable or disable the hypervisor, restart the computer.
- Request for allowing a process to modify an object.
- Successful connection to a remote computer in the Anti-virus Network.
- You activated a trial version. It is recommended to obtain a license.

10.2. Update

On this page, you can configure the following Dr.Web update parameters:

- [update frequency](#)
- [update source](#)
- [updating components](#)
- [update mirror](#)

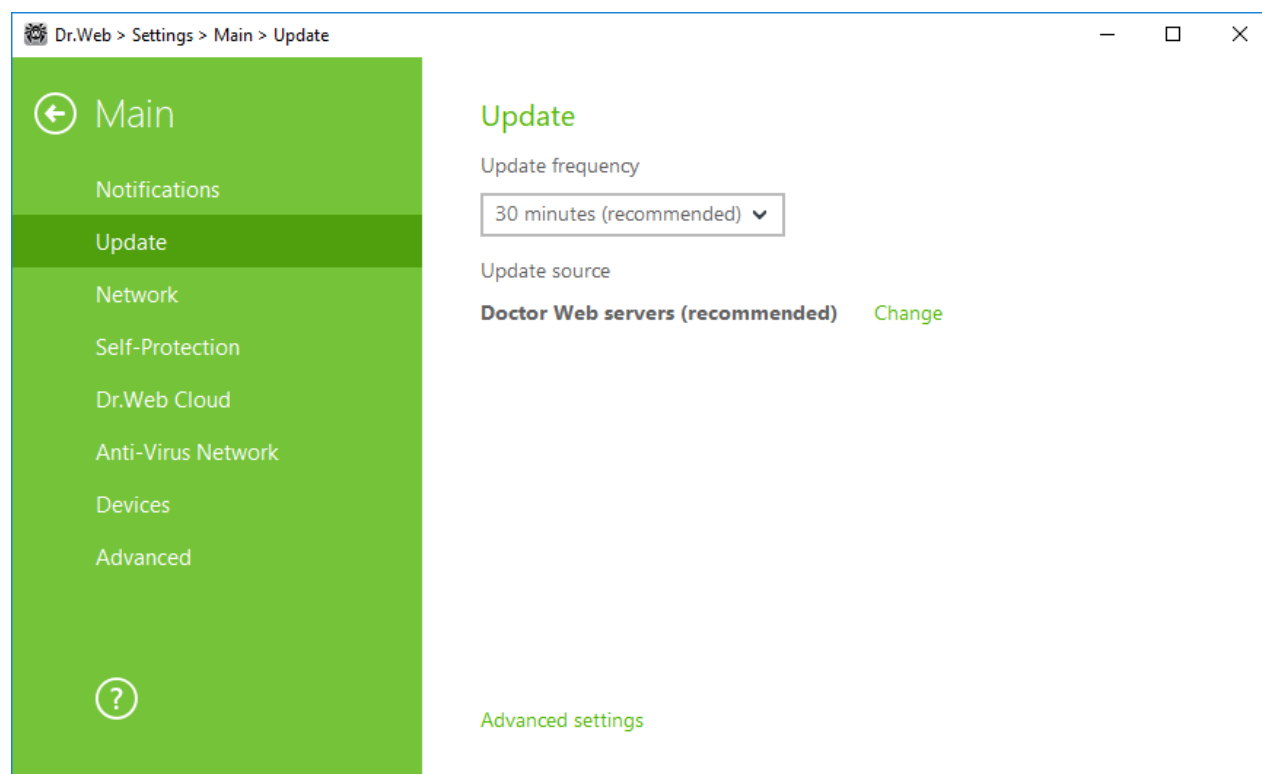



Figure 21. Update settings

Update frequency

The default value (30 minutes) is optimal to keep information on threats up-to-date. To specify the frequency of updates, select the necessary value from the drop-down list.



Automatic update is performed in the background mode. You can also select the option **Manually**. In this case, you will have to run the product update manually using the Dr.Web [menu](#) . The detailed information on running the update process is available in the [Update](#) section.

Update source settings

The default update source is **Doctor Web servers (recommended)**. To select an update source

1. In the **Main** → **Update** settings section, in **Update source**, click the **Edit** link. The update source settings window opens.

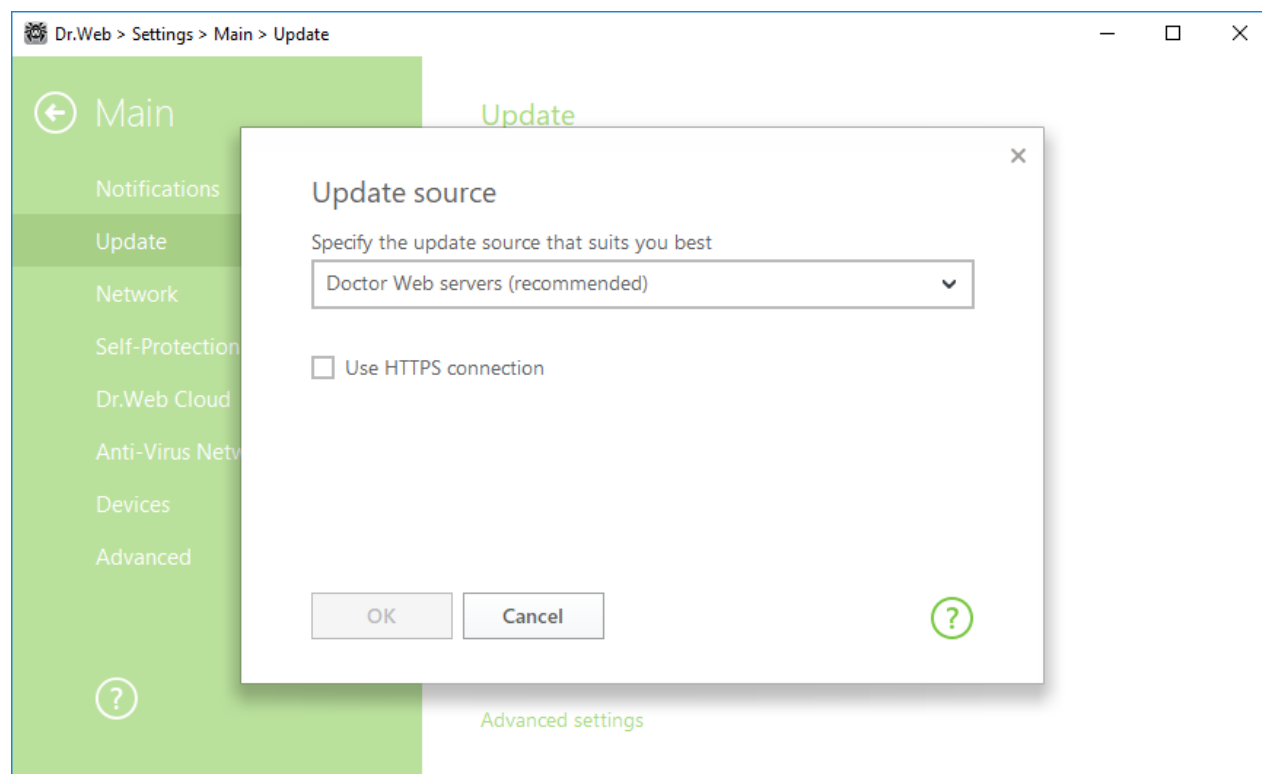


Figure 22. Update source

2. In the drop-down menu, specify the update source that suits you best.
 - **Doctor Web servers (recommended)**. Updating from Doctor Web servers via the Internet. If you want to download updates via a secure protocol, select the **Use HTTPS connection** check box.
 - **Local or network folder**. Updating from local or network folder where updates have been copied. Specify the path to the folder, enter the user name and password if necessary.
 - **Anti-virus Network**. Updating from a local network using a computer with Dr.Web product installed and an update mirror created. Select the computer that will be used as an update source.
3. To save the changes, click **OK**.



Advanced settings

Updating components settings

Updating components. You can choose one of the following ways of downloading the Dr.Web components update:

- **All (recommended)**, when updates are downloaded both for Dr.Web virus databases and anti-virus engine and for other program components of the Dr.Web.
- **Only virus databases**, when only the updates for Dr.Web virus databases and the anti-virus engine are downloaded; other components of Dr.Web are not updated.

Creating update mirror

Update mirror is a computer set as an update source for other computers of the local network. Update mirror can be used to update Dr.Web on computers without Internet connection.

To set your computer as an update mirror

1. In the **Main** → **Update** settings section, open **Advanced settings** and enable the update mirror using the switch . The update mirror settings window opens.

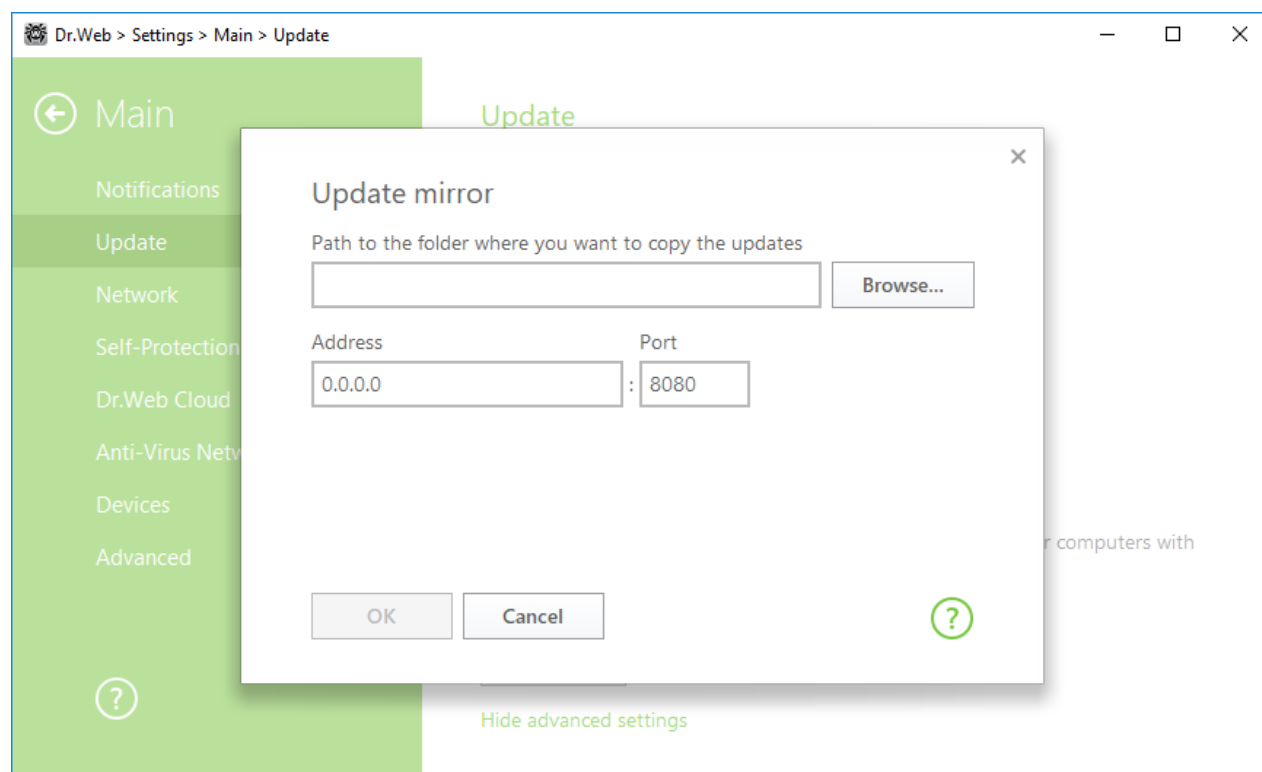


Figure 23. Update mirror

2. Specify the path to the folder where you want to copy the updates.



3. If your computer is connected to several subnets, you can specify the IP address available to computers of only one subnet. You can also specify the port for HTTP server to receive connection requests.
4. To save the changes, click **OK**.

The frequency of the mirror updates corresponds to the value selected in **Update frequency** of the **Main** → **Update** settings section.

10.3. Network

Proxy server

By default, all components use direct connection mode. If necessary, you can enable use of a proxy server and specify its connection settings. Click **Edit** to specify the following proxy server parameters:

Option	Description
Address	Specify the address of the proxy server.
Port	Specify the port of the proxy server.
Login	Specify the username to use when connecting to the proxy server.
Password	Specify the password to use when connecting to the proxy server under the provided username.
Authorization type	Select an authorization type required to connect to the proxy server.

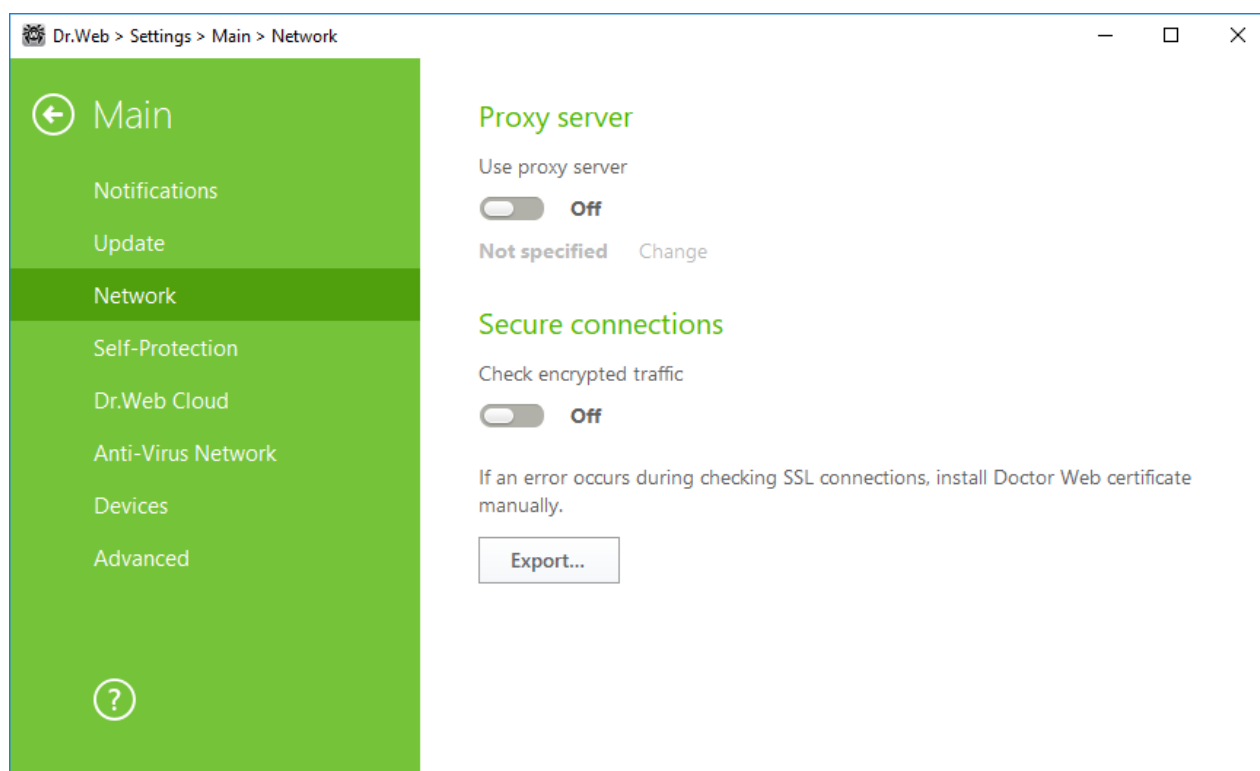


Figure 24. Connecting to proxy server and checking the encrypted traffic

Secure connections

If you want Dr.Web to check data transmitted over SSL, TLS or STARTTLS protocols, enable the **Check encrypted traffic** option. SpIDer Mail will check messages sent over POP3S, SMTPS, or IMAPS, and SpIDer Gate—messages sent over HTTPS.

If your client application that uses secure connections does not refer to the default Windows system certificate storage, then you need to export the Doctor Web security certificate and to import it to every application manually.



The security certificate is valid for one year. You should import the certificate again every year if necessary.

What is a security certificate

A security certificate is an electronic document which confirms that a certified program has been tested in one of the certification centers. Also, security certificates are name SSL-certificates, because SSL protocol (Secure Socket Layer) is used. It provides encrypted communication between hosts in Internet. for example, between a user and a web server.

Installing (importing) into a program which works with the Internet security certificate of a Web site ensures that communication will be carried out in a secure mode with authentication check. In this



case, criminals will face a number of difficulties with data interception.

The following applications may require the Doctor Web certificate import:

- Opera browser;
- Firefox browser;
- Mozilla Thunderbird mail client;
- The Bat! mail client and others.

How to export and import the Doctor Web certificate

1. Click **Export**.
2. Choose folder you want the certificate to be saved. Click **OK**.
3. Import the certificate to a target application using the application settings. Find more details about the importing of certificate in target application user documentation.



If **Check encrypted traffic** is activated, for correct working of cloud storages clients (such as Google Drive, Dropbox, Yandex.Disk etc.), [exclude these application form SplDer Gate checks](#).

10.4. Self-protection

On this page, you can configure protection of Dr.Web itself from unauthorized modification by malicious programs that target anti-viruses or from accidental damage.

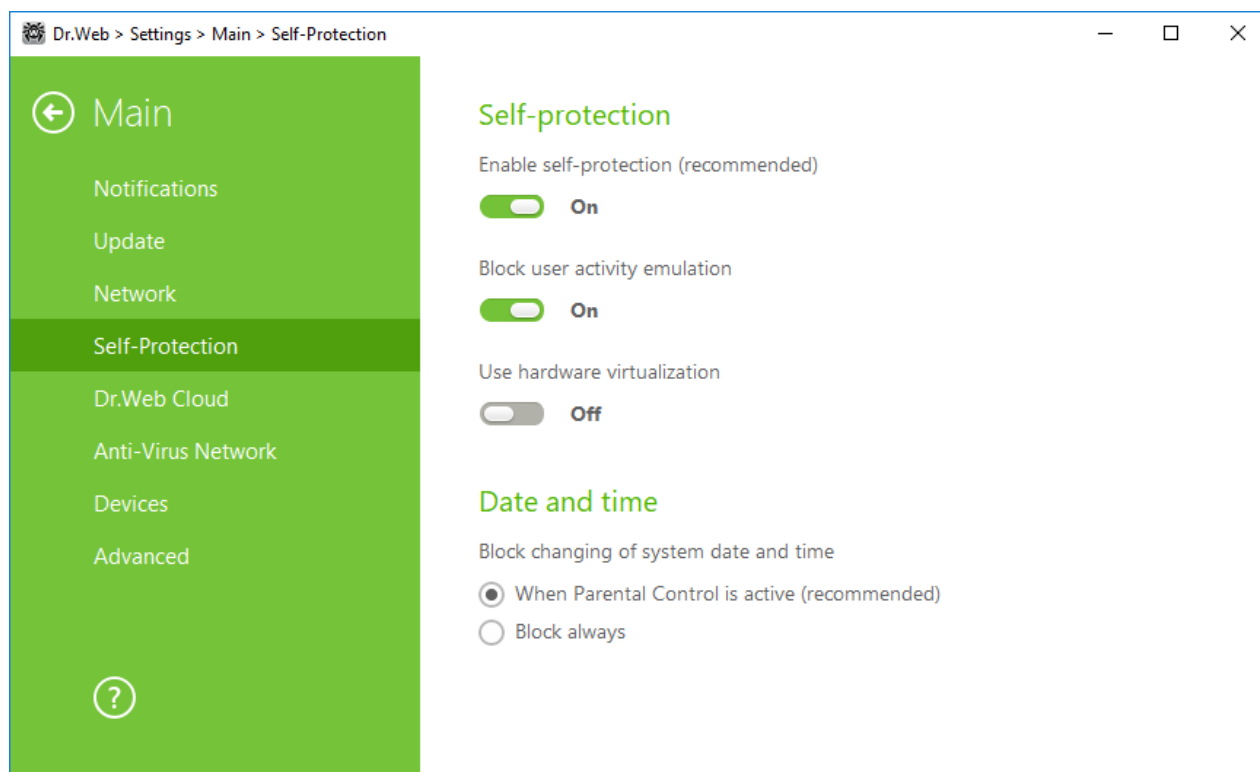


Figure 25. Dr.Web self-protection parameters

Self-protection

The **Enable self-protection (recommended)** option allows to protect Dr.Web files and processes from unauthorized access. It is not recommended to disable Self-protection.



If any problems occur during operation of defragmentation programs, disable self-protection temporary.

To rollback to a system restore point, disable self-protection.

The **Block user activity emulation** option allows to prevent any changes in Dr.Web settings made by third-party software, including execution of scripts that emulate the mouse and the keyboard functioning in Dr.Web windows (for example, scripts to make changes in Dr.Web settings, license removal and other actions aimed at changing Dr.Web operation).

The **Use hardware virtualization** option allows to take full advantage of computer resources, which makes detection and curing of threats easier and enhances self-protection of Dr.Web. To enable this option, restart the computer.



Hardware virtualization works only if your computer's hardware and operating system support hardware virtualization.



Enabling this option may cause a conflict with some third-party software.

If problems occur, disable this option.

32-bit platforms do not support hardware virtualization.

Date and time

Some malicious programs intentionally change system data and time. In this case virus databases are not updated as scheduled, license can be marked as expired, and protection components will be disabled.

The **Block changing of system date and time** option allows to prevent manual and automatic changes of the system date and time as well as of the time zone. This restriction is set for all system users. The option can improve performance of the [time limit function](#) implemented in Parental Control. If Internet or computer usage limits are set in Parental Control, this option is automatically enabled. You can configure [notification parameters](#) to be informed on an attempt to change the system time.

10.5. Dr.Web Cloud

On this page, you can connect to Doctor Web cloud service and take part in the Dr.Web quality improvement program.

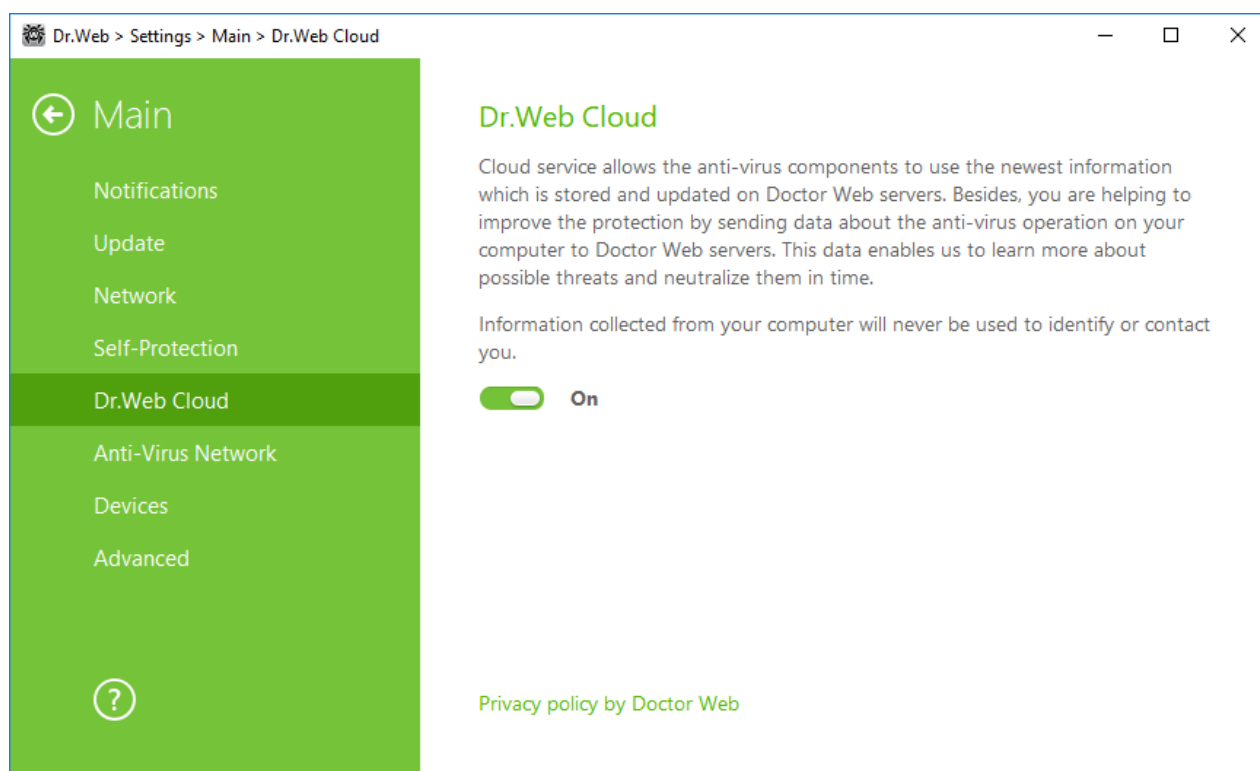


Figure 26. Connecting to Dr.Web Cloud

Cloud service

Dr.Web Cloud provides most recent information on threats which is updated on Doctor Web servers in real-time mode and is used for anti-virus protection.

Depending on [update settings](#), information on threats used by anti-virus components may become out of date. Cloud services can reliably prevent users from viewing unwanted websites and protect your system from infected files.

Software quality improvement program

If you participate in the software quality improvement program, impersonal data about Dr.Web operation on your computer will be periodically sent to Doctor Web servers, for example, information on created rule sets for Dr.Web Firewall. Received information is not used to identify or contact you.

Click the **Privacy policy by Doctor Web** link to look through a privacy policy on the Doctor Web official [website](#).

10.6. Anti-virus Network

On this page, you can enable remote control of your anti-virus from other local network computers by [Anti-virus Network](#). If your computer is connected to an anti-virus network, you can control anti-



virus protection state remotely (view statistics, enable or disable Dr.Web components and adjust their settings) and download updates from a local network computer. To allow local network computers with installed Dr.Web products to use a computer as an update source, configure an [Update mirror](#) on it.

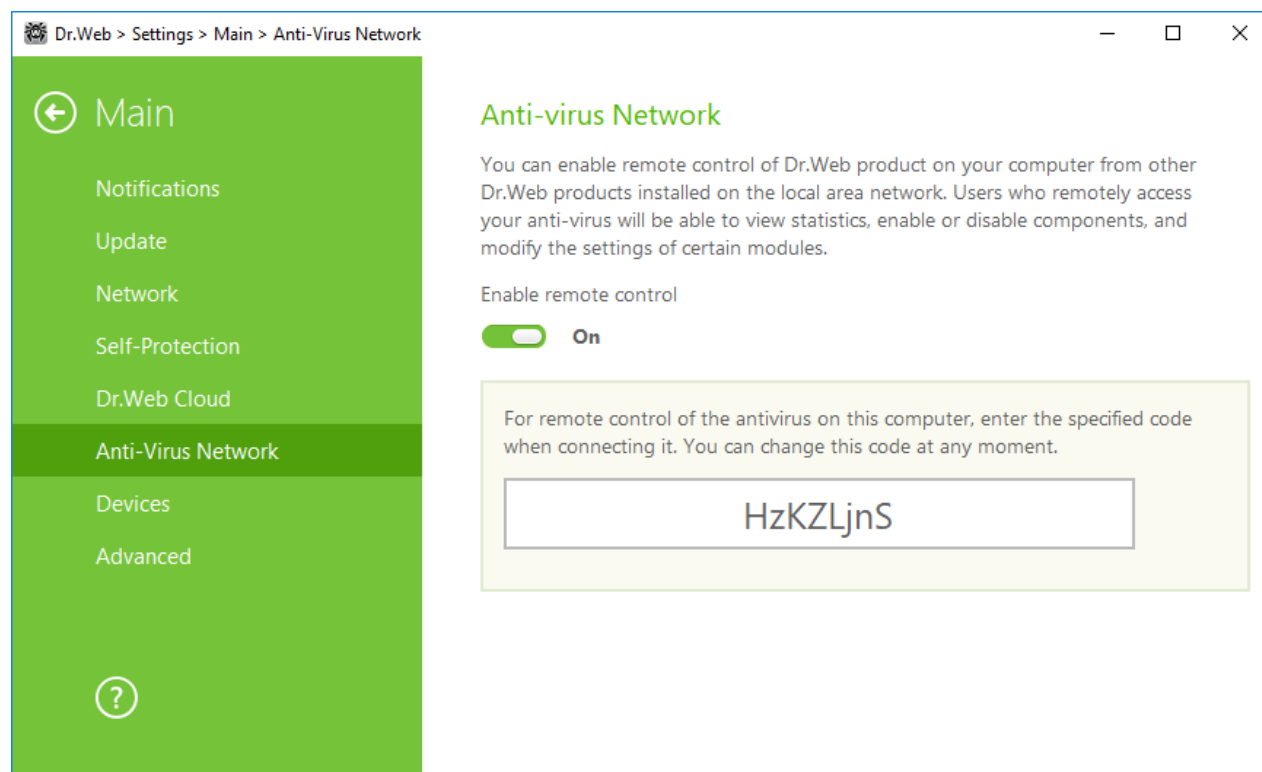


Figure 27. Switching on the Anti-virus remote access

For remote access to Dr.Web settings on your computer, the password is required. You may use the password that is automatically generated when the option is enabled or set a new one.

Remote control allows you to view statistics, enable or disable components and modify their settings. Quarantine Manager and Scanner are not available. Dr.Web Firewall settings and statistics are not available either, but it is allowed to enable or disable the component.

10.7. Devices

In this section, you can configure restrictions to access to certain devices or device buses and configure black and white lists.



Hardware access settings are applied for all Windows accounts.

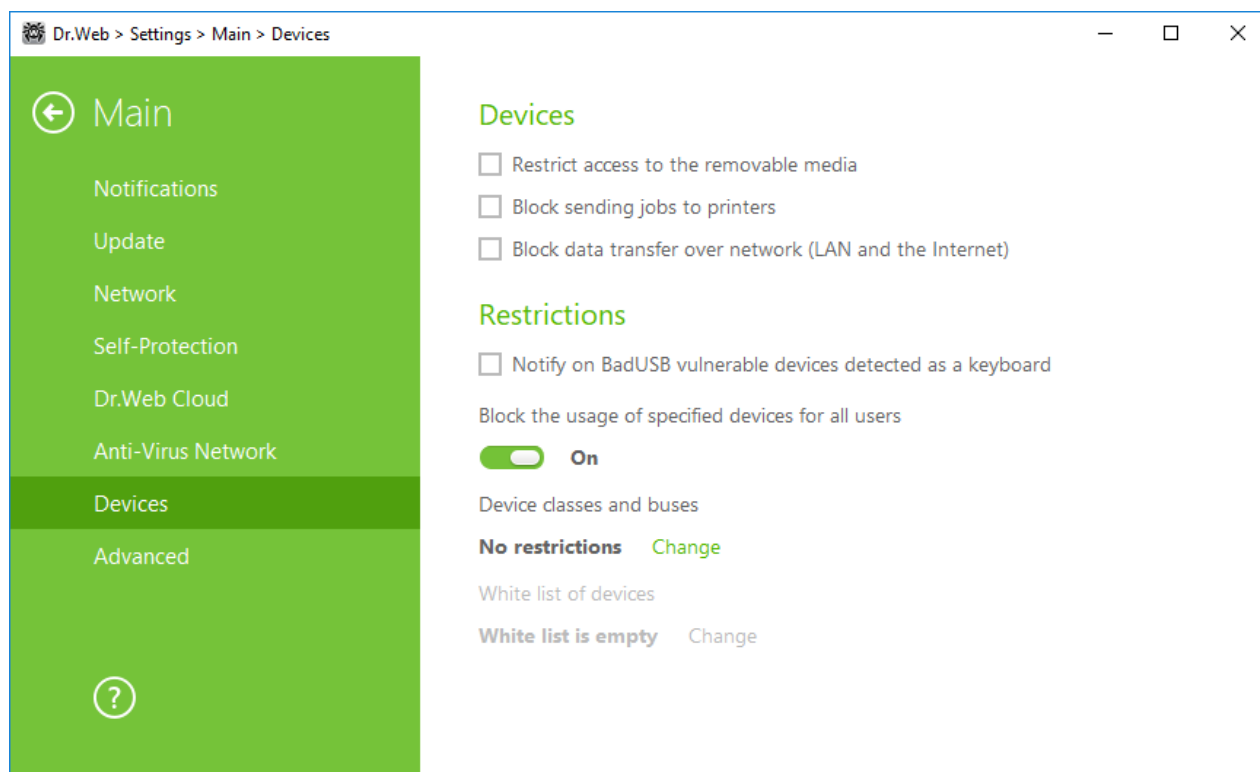


Figure 28. Devices lock settings

Devices

To block access to data on removable media (USB flash, floppy, CD/DVD, ZIP drives, etc.), enable the appropriate option. To block sending jobs to printers, enable the **Block sending jobs to printers** option. This option is disabled by default. You can also block data transfer over network (LAN and the Internet).

Infected USB devices can be identified by your computer as a keyboard. If you want Dr.Web to check whether the connected USB device is a keyboard, enable the **Notify on BadUSB vulnerable devices detected as a keyboard** option.



Device classes and buses

This function allows to block one or several device classes on all the buses and also to block all the devices connected to one or several buses. Device classes are all devices that perform the same functions (e.g., printing devices). Device buses are communication subsystems for transferring data between functional units of the computer (for example, the USB).




To block access to specified device classes or buses, enable the appropriate option. Click the **Edit** button to make a list of such objects. In the open window, you can select device classes or buses that you want to restrict access to.



Configuration of the list of blocked device classes

1. To block access to the device class completely, click  in the **Blocked classes** column.
2. In the open list, select the classes you want to block and click **OK**. The selected device classes will be blocked on all device buses. Only the classes that are not blocked are listed.
3. To unblock the device class, in the **Device classes and buses** window, select the necessary class and click .

To configure the list of blocked device buses

1. To block the entire bus or some devices on the device bus click  in the **Blocked device buses** column.
2. In the open window, select necessary device classes. To block the entire bus, select all classes in the list. Click **OK**.
3. To unblock the bus, in the **Device classes and buses** window select the bus and click .
4. To edit the list of blocked classes on a specific bus, click .







To block the device connected before the function activation, it is required to reconnect the device or to reboot the system. The access blocking function affects only devices connected after its activation.

White list of devices

After you restricted access to some device classes or buses, you can allow access to certain devices by adding them to the white list. You can also add a certain device to the white list if you do not want it to be checked for BadUSB vulnerability.

To add a device to the white list

1. Enable the option **White list of devices** (the option becomes available if restrictions are set).
2. To configure the list of devices, click **Edit**.
3. Make sure that the device is connected to the computer.
4. Click . In the open window, click **Browse** and select the device. You can use a filter to view only connected or only disconnected devices in the table. Click **OK**.
5. You can configure access rules for devices with file systems. For that, from the **Rule** column, select one of the following modes: **Allow all** or **Read-only**. To add a new rule for a specific user, click . To delete a rule, click .
6. To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**. The white list of devices opens.
7. To edit a rule set, select it from the list and click .



8. To remove a rule set, select it from the list and click .

10.8. Advanced

On this page, you can select a language, configure logging parameters and Quarantine settings.

To set another program language, select it from the corresponding drop-down list. New languages are automatically added to the list. Thus, it contains all localization languages that are currently available for the Dr.Web graphical interface.

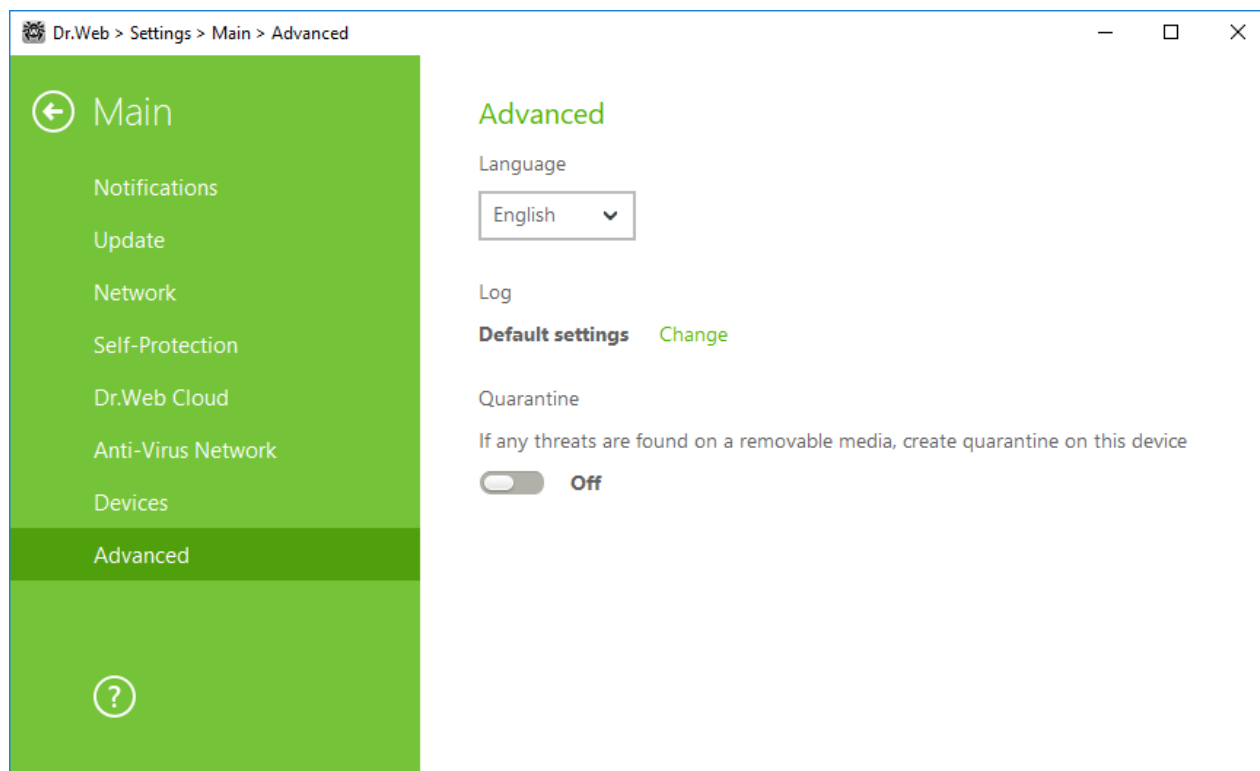


Figure 29. Advanced settings

Log settings

To configure log settings, click the corresponding **Edit** button.



Size of a log file is restricted to 10 MB by default (and 100 MB for SplDer Guard). If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.



By default, the standard logging mode is enabled for all the Dr.Web components and the following information is logged:

Component	Information
SplDer Guard	<p>Time of updates and SplDer Guard starts and stops, virus events, names of scanned files, names of packers, and contents of scanned complex objects (archives, email attachments, file containers).</p> <p>It is recommended to use this mode to determine the most frequent objects scanned by SplDer Guard. If necessary, you can add these objects to the list of exclusions in order to increase computer performance.</p>
SplDer Mail	<p>Time of updates and SplDer Mail starts and stops, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives.</p> <p>It is recommended to use this mode when testing mail interception settings.</p>
SplDer Gate	<p>Time of updates, starts and stops of SplDer Gate, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives.</p> <p>It is recommended to use this mode for reception of more detailed information on the checked objects and work of the HTTP watchman.</p>
Scanner	<p>In this mode, main events are logged, such as time of updates, time of Dr.Web Scanner starts and stops, information on detected threats, names of packers, and content of scanned archives.</p>
Firewall	<p>Firewall does not log its operation in the standard mode. When you enable detailed logging, the component collects data on network packets (pcap logs).</p>
Update Dr.Web	<p>List of updated Dr.Web files and their download status, date and time of updates, and details on auxiliary script execution and Dr.Web component restart.</p>
Dr.Web Service	<p>Information on Dr.Web components, changes in their settings, component starts and stops, preventive protection events, connections to anti-virus network.</p>

Memory dump creation

The **Create memory dumps at scan errors** option allows to save useful information on operation of several Dr.Web components. This helps Doctor Web technical support specialists analyze an occurred problem in detail and find a solution. It is recommended to enable this option on request of Doctor Web technical support specialists or when errors of scanning or neutralizing occur. Memory dump is saved to .dmp file located in the %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\ folder.



Enabling detailed logging



Upon logging detailed data on Dr.Web operation, the maximum amount of information is recorded. This will result in disabling of log file size limitations and will have an impact on system and Dr.Web performance. It is recommended to use this mode only when errors occur in component operation or by request of Doctor Web technical support.

1. To enable detailed logging for a Dr.Web component, select the corresponding check box.
2. By default, detailed logging is enabled until the first restart of the operating system. If it is necessary to log component activity before and after the restart, select the **Continue detailed logging after restart (use only by request of Doctor Web technical support)** check box.
3. Save the changes.



Quarantine settings

You can select the isolation mode for infected objects detected on portable data carriers. When this option is enabled, detected threats are moved to the folder on this data carrier without being encrypted. The Quarantine folder is created on portable data carriers only when they are accessible for writing. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss. If the option is enabled, the detected threat is moved to Quarantine on the local disk.



11. Parental Control

The Parental Control component allows you to manage the access to websites, files, and folders. You can also set time limits on using the Internet and computer for any of Windows accounts.

To configure Parental Control, open the menu  in [administrator mode](#), run **Settings**  and go to **Parental Control**.

By restricting access to the local file system, you can maintain integrity of important files, protect them from viruses, and secure confidentiality of stored data. You can limit access to separate files or folders on local drives and removable media.

By controlling access to web resources, you can restrict users from viewing undesirable websites (for example, pages on violence, gambling, adult content, etc.) or allow access only to certain websites that are specified in the Parental Control settings.



11.1. Configuring Parental Control



To access the Parental Control settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

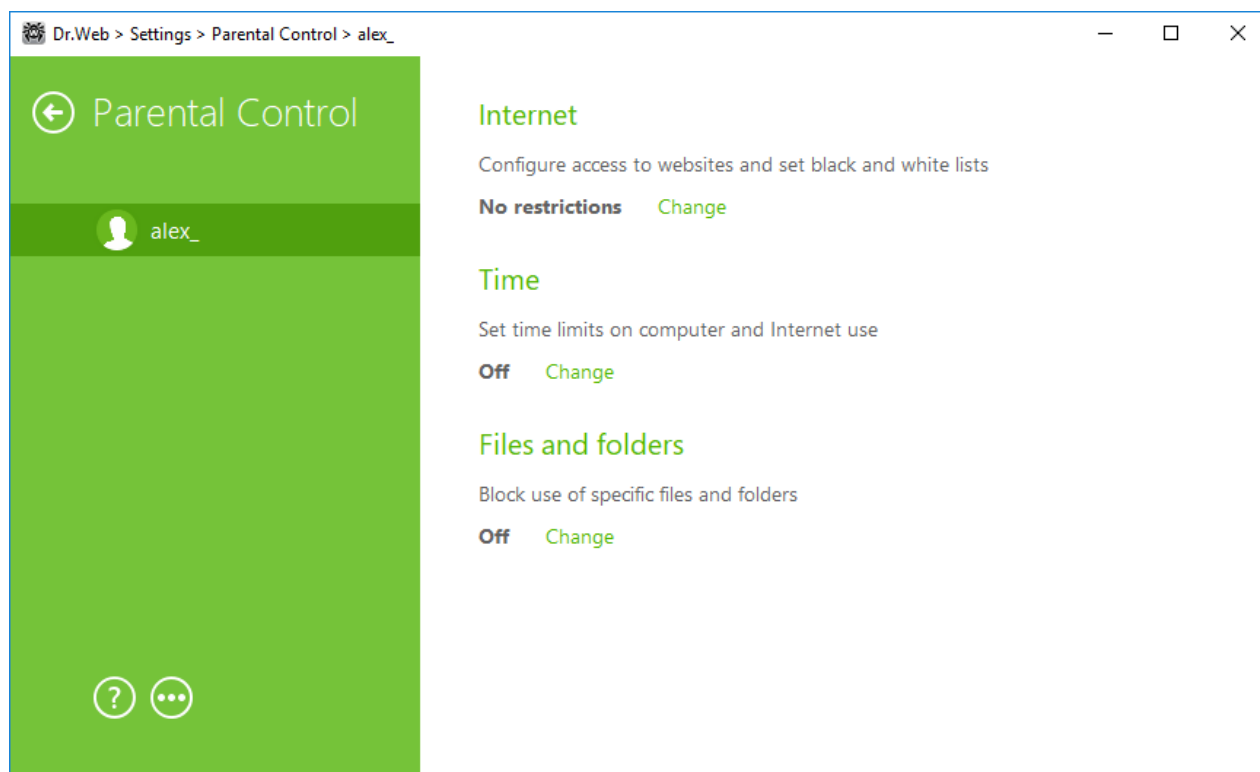


Figure 30. Parental Control settings

Configuring Parental Control parameters for different users

To configure access restriction for a user, select the user name in the left pane. In the main part of the window, you can view the settings specified for this user. By default, access to the Internet and to local resources is not restricted for all users of the computer; no time limits are set. To change these settings, click **Edit** next to the desired option.



New users are listed only after the first login into their account.

Quick setup

By clicking  you can access the menu that allows you to

- Copy restriction settings configured for one user and apply them to another user profile. For that, select **Copy settings** and **Use copied settings**.



- Disable Parental Control for the selected user. For that, select **Disable Parental Control**. Using this menu, you can enable Parental Control with the same settings again.



If necessary, you can [configure](#) desktop and email notifications on Parental Control actions.

11.1.1. Internet

By default, the **No restrictions** mode is set for all users. To change these settings, select another mode from the drop-down list.

Block by categories

The same website can be assigned to several different categories. In this case, Parental Control blocks access to the site if it belongs to at least one of the categories included in restrictions list.

In this mode, you can select categories of websites to block:

Category	Description
Adult content	Websites that contain pornographic or erotic materials, dating sites, etc.
Violence	Websites that encourage violence or contain materials about various fatal accidents, etc.
Weapons	Websites that describe weapons and explosives or provide information on their manufacturing.
Gambling	Websites that provide access to online games of chance, casinos, auctions, including sites for placing bets, etc.
Drugs	Websites that promote use, production or distribution of drugs, etc.
Online games	Websites that provide access to games using the permanent Internet connection.
Terrorism	Websites that contain aggressive and propaganda materials or terroristic attacks descriptions, etc.
Obscene language	Websites that contain the obscene language (in titles, articles, etc.).
Chats	Websites that offer a real-time transmission of text messages.
Email	Websites that offer the possibility of free registration of a web mailbox.



Category	Description
Social networks	Different social networking services: general, professional, corporate, interest-based; thematic dating sites.
Anonymizers	Websites that allow the user to hide personal information and providing the access to the blocked web resources.
Cryptocurrency mining pools	Websites that provide an access to common services for cryptocurrencies mining.

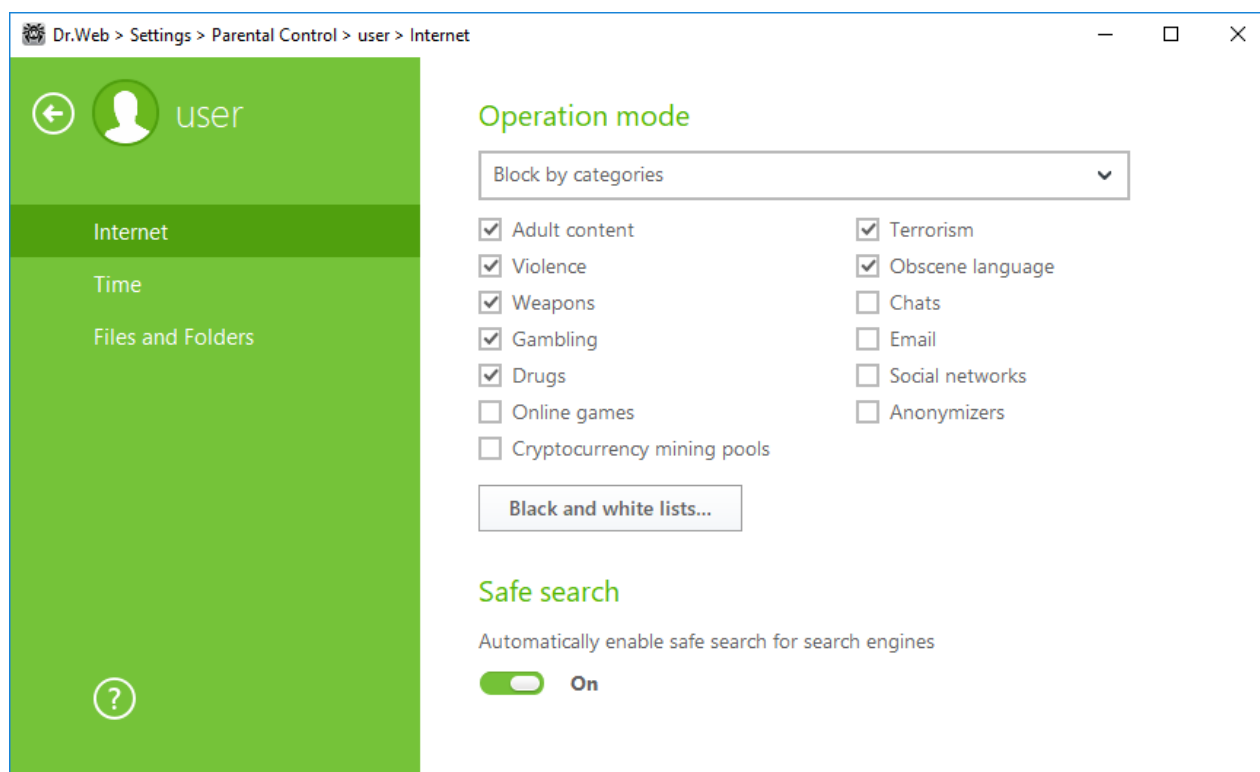


Figure 31. Managing the Internet access by websites categories

Select the corresponding check box to restrict the access to a certain website category.

In this mode you can also add websites to block or allow access to the resources regardless of other restrictions:

- To restrict an access to a website that is out of any specified categories, put it into user defined black list.
- To allow an access forcibly to a website, regardless if it is in one or more restricted categories, put it into user defined white list.

Block all except websites from the white list

In this mode, the access to all websites except the listed in white list is blocked.



Safe search

In any mode except the **No restrictions** mode, you can enable the **Safe search** option to manage results of search engines. This option allows to exclude unwanted webpages from search results by using the search engine tools.

To activate **Safe search** function, set the switch in **On** state.

Black and White Lists

In this window, you can configure lists of websites access to which is allowed or blocked regardless of other Parental Control settings.

To manage white and black lists, click **Black and White Lists**.

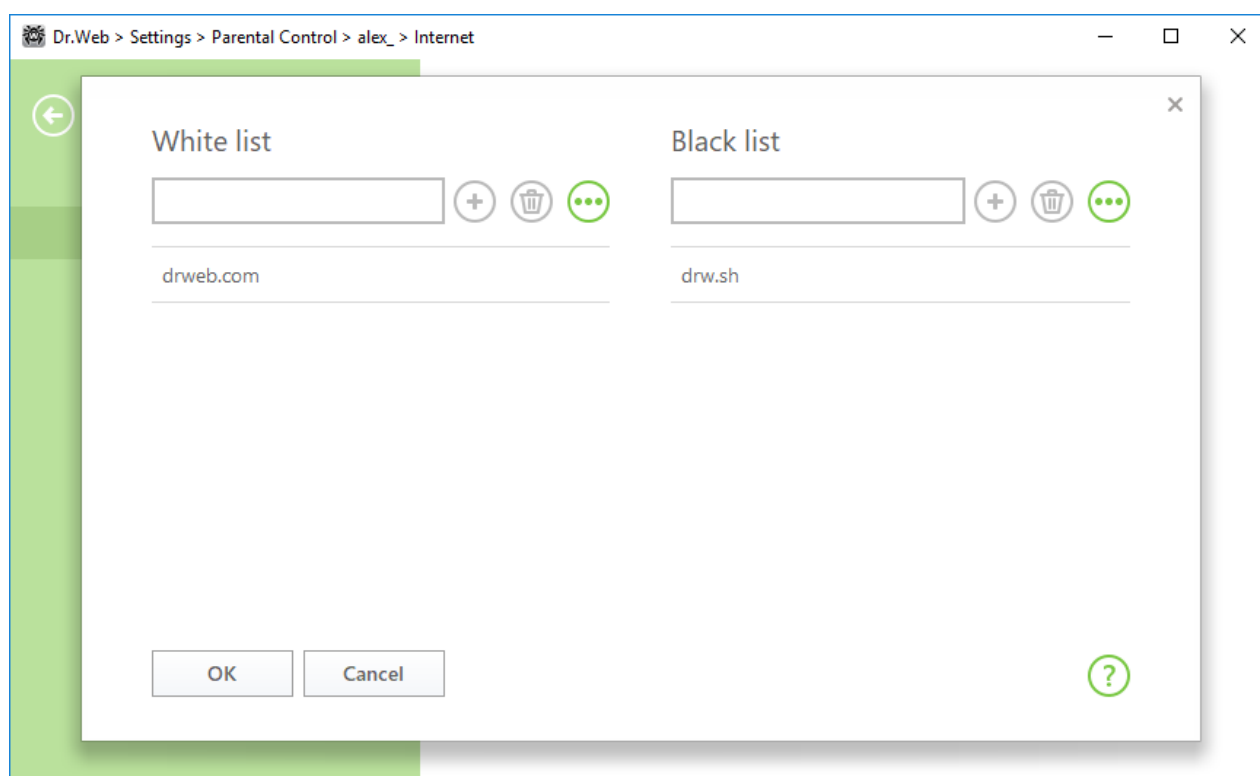


Figure 32. Creating white and black lists

By default, the lists are empty. If required, you can add website addresses to the black and white lists.

To configure black and white lists

1. Enter a domain name or a part of a domain name for the website in the **White list** or **Black list** field depending on whether you want to allow or block access to it:
 - To add a certain website, enter its URL (for example, `www.example.com`). This allows access to all webpages located on this website;



- To allow the access to websites whose URL contains a certain text, enter this text in the input field. Example: if you enter `example` text, then the access to the addresses `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` etc. will be granted;
- To allow access to websites within a particular domain, enter the domain name with a period (.) character. This allows access to all webpages located on this website. If the domain name includes a forward slash (/), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter `example.com/test`, Spider Gate will allow processing of such webpages as `example.com/test11`, `template.example.com/test22`, and so on;
- To add certain websites to the exclusions, enter the mask of their names. Masks will be added in the `mask://...` format.



A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any, including an empty, character (one).

Examples:

- `mask://*.com/` or `.com`—enable opening of all the domain .com websites;
- `mask://mail`—enable opening of all websites whose names contain the "mail" word;
- `mask://????.com/` or `.com`—enable opening of all the domain .com websites, whose names consist of three characters or less.

Your input may be unified. For example: the `http://www.example.com` address string will be transformed into `www.example.com`.

2. Click  to add the website to the list.
3. To remove an address from the list, select the corresponding item and click .
4. To add other websites, repeat steps 1 to 2.

11.1.2. Time

On this page, you can set restrictions on time spent on the Internet or working on the computer.

By default, no time limits on computer and Internet use are set.

You can set time limits using a table with timeslots or by specifying time intervals.

Setting time limits using the table

1. Select days of the week and time when the user is restricted from accessing the Internet, and then mark the corresponding timeslots blue:
 - To mark one timeslot, click it once.
 - To mark several adjacent timeslots, click the first slot once and select the rest of required squares while holding down the mouse button.




2. Select days of the week and time when the user is restricted from using the computer, and then mark the corresponding timeslots red:
 - To mark one timeslot, double-click it.
 - To mark several adjacent timeslots, double-click the first one and select the rest of required timeslots while holding down the mouse button.

You can also create different setting profiles for one user. This option allows you to easily switch between existing setting profiles (for example, you can set different time limits for the academic year and school holidays).

To create and edit a setting profile

You can change a user setting profile or create a new one.

1. To create a new profile, click  and specify the profile name. Click **OK**.
2. To edit user profile, select it in the list.
3. After that, edit the table as necessary.

If the **No restrictions** profile is selected and the table is changed, the profile is switched to the user profile automatically.

Interval time limit

If you want to specify the total number of hours when the user is allowed to work on the computer, select the **Interval time limit** option. Please note that this mode does not allow to set time limits on Internet use.

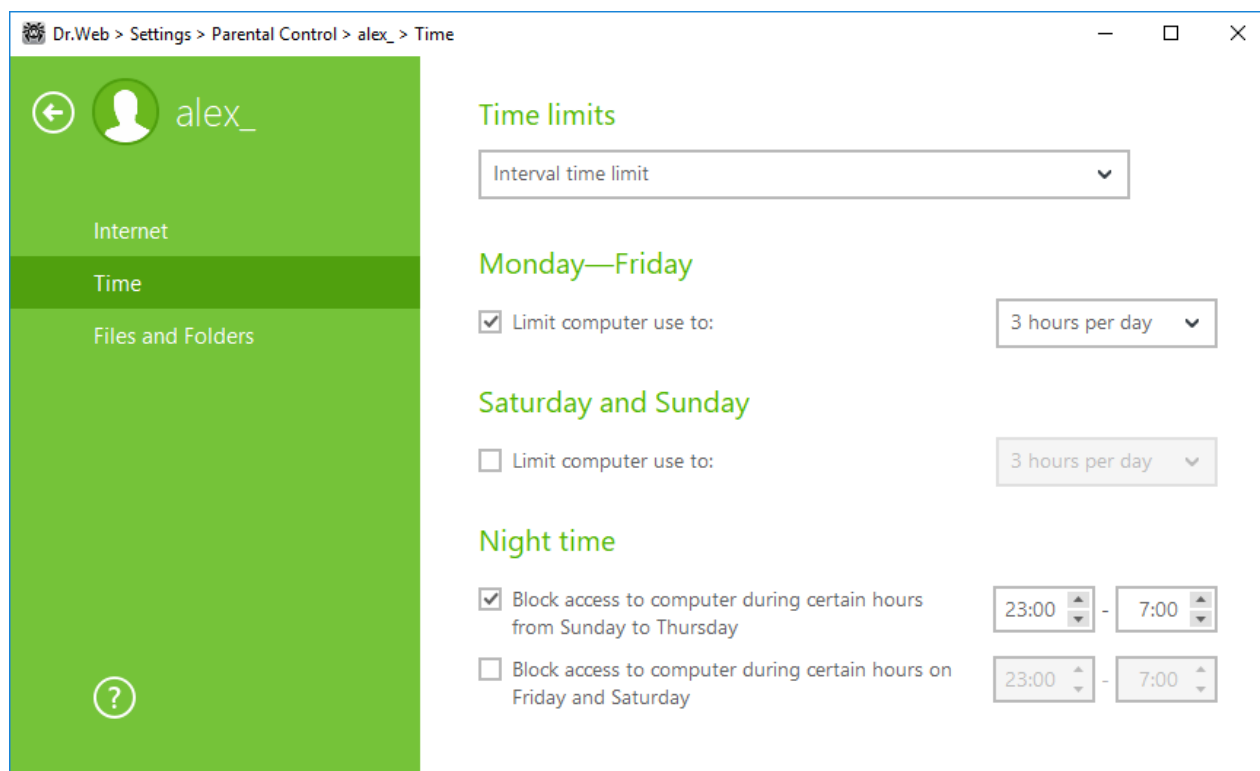


Figure 33. Managing the computer use restrictions

In this mode, you can set time limits on computer use during the following periods:

- From Monday to Friday
- Saturday and Sunday

You can also restrict a user from accessing the computer during the night-time period regardless of the total number of hours when access is allowed.

This option allows you to let your child manage the time spent working on the computer during the day by themselves.



Setting time limits for using the computer or the Internet automatically enables the **Block changing of system date and time** option on the [Self-protection](#) page of the main settings.

11.1.3. Files and Folders

By default, the No restrictions mode is set. To configure restriction parameters, enable the appropriate option and click **Objects**.

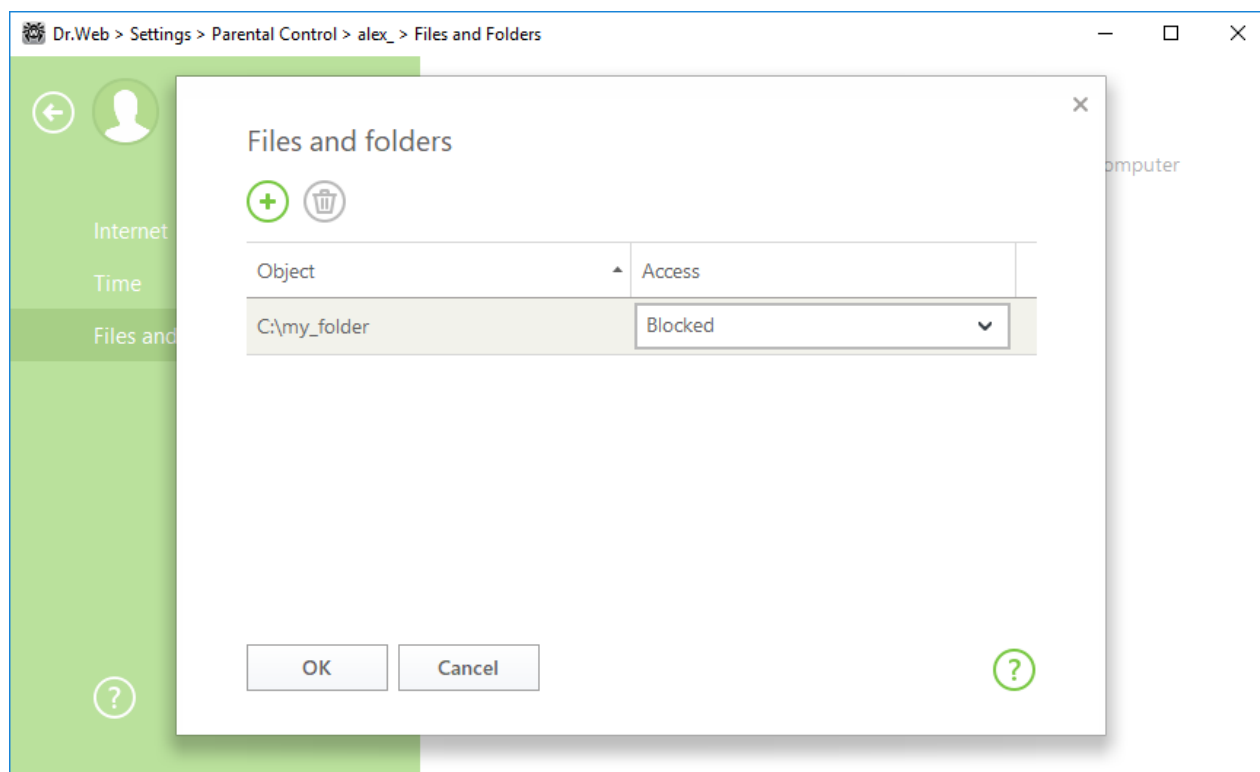




Figure 34. Managing the access to files and folders

To add an object to the list, click  and select a file or a folder. By default, an added object will become read only.

To block access to the selected object completely, click the restriction and select **Blocked** from the drop-down list.



To remove an object from the list, select it and click .

Please note that access blocking is not guaranteed when loading the computer from removable media or addressing the objects from other operating systems installed on your computer.



12. Exclusions

In this section you can configure the exclusions from SpIDer Guard, SpIDer Gate, SpIDer Mail and Scanner checks as well as add senders email addresses to white or black list, so mails from them would not be checked for spam.

To configure exclusions, open the Dr.Web menu  in [administrator mode](#), run **Settings**  and select **Exclusions**. To configure access to websites that are not recommended by Doctor Web, select [Websites](#).

To exclude specific files and folders from scanning, go to [Files and Folders](#).

To exclude specific processes from scanning by Dr.Web components, go to [Applications](#).

To configure scan of messages by SpIDer Mail for spam, go to [Anti-spam](#).

12.1. Websites

If you want to have access to the websites that are not recommended to visit by Doctor Web, add them to the exclusions. The access to the listed websites will be allowed, but the sites will be still checked for viruses. By default, the list is empty. If you add a website to the white list, users will be able to access it regardless of other SpIDer Gate settings. Please note that if the site is added both to the black list of Parental Control and to the exclusions, access will be blocked.

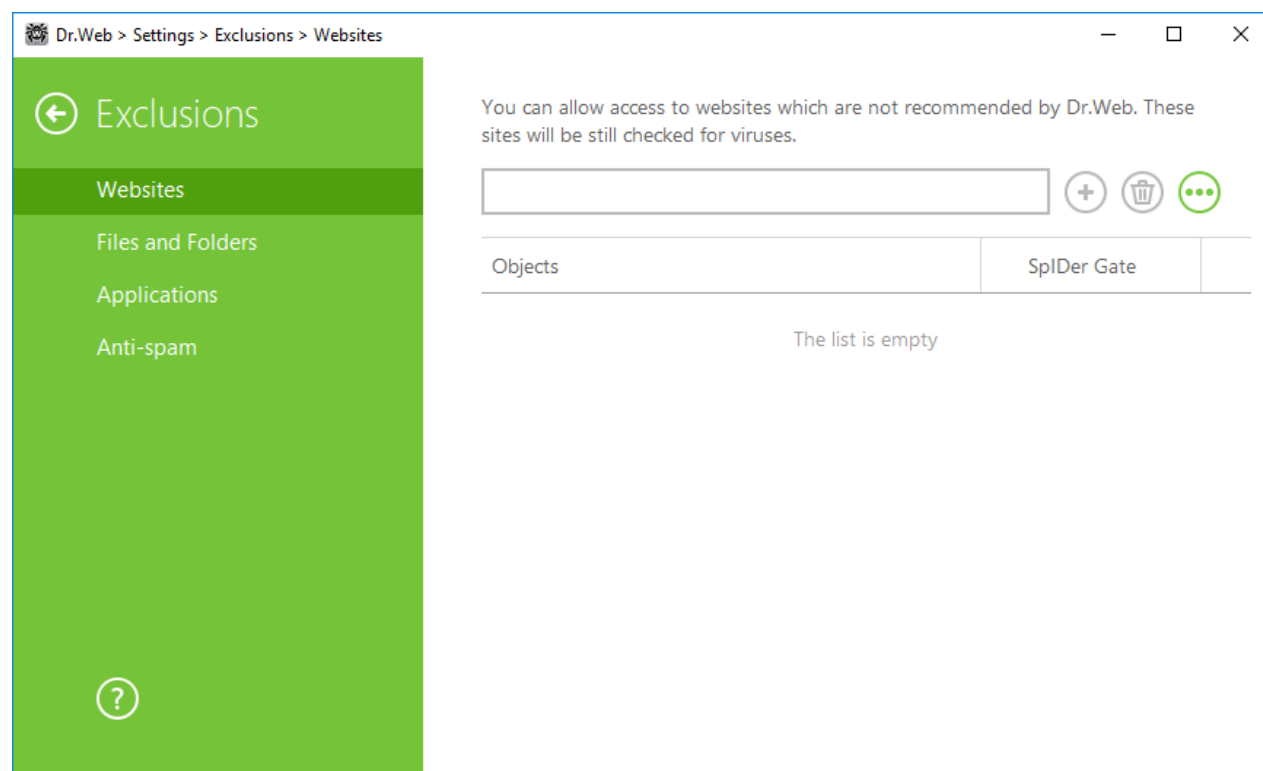


Figure 35. Adding websites to exclusions



To configure black and white lists

1. In the input field enter a domain name or a part of a domain name for the website that you want to access regardless of other restrictions:
 - To add a certain website, enter its name (for example, `www.example.com`). This allows access to all webpages located on this website.
 - to allow the access to websites whose URL contains a certain text, enter this text in the input field. Example: if you enter `example` text, then the access to the addresses `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru` etc. will be granted;
 - To allow access to websites within a particular domain, enter the domain name with a period (.) character. This allows access to all webpages located on this website. If the domain name includes a forward slash (/), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter `example.com/test`, SplDer Gate will allow access to such webpages as `example.com/test11`, `template.example.com/test22`, and so on.
 - To add certain websites to the exclusions, enter the mask of their names. Masks will be added in the `mask://...` format.



A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any, including an empty, character (one).


Examples:

- `mask://*.com`—enable opening of all the domain .com websites;
- `mask://mail`—enable opening of all websites whose names contain the “mail” word;
- `mask://??? .com`—enable opening of all the domain .com websites, whose names consist of three characters or less.

Your input may be unified. For example: the `http://www.example.com` address string will be transformed into `www.example.com`.

2. Click . The address will appear on the list.
3. To add other addresses, repeat steps 1 to 2. To remove an address from the white list, select the corresponding item and click .

Managing listed objects

Click  to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.



12.2. Files and Folders

In this section, you can manage the list of files and folders to be excluded from scanning by SpIDer Guard and Scanner. You can exclude the anti-virus quarantine folders, working folders of some programs, temporary files (paging file), and so on.

The default list is empty. Add particular files and folders to exclusions or use masks to disable scanning of a certain group of files. Any added object can be excluded from the scanning of both components or from scanning of each component separately.

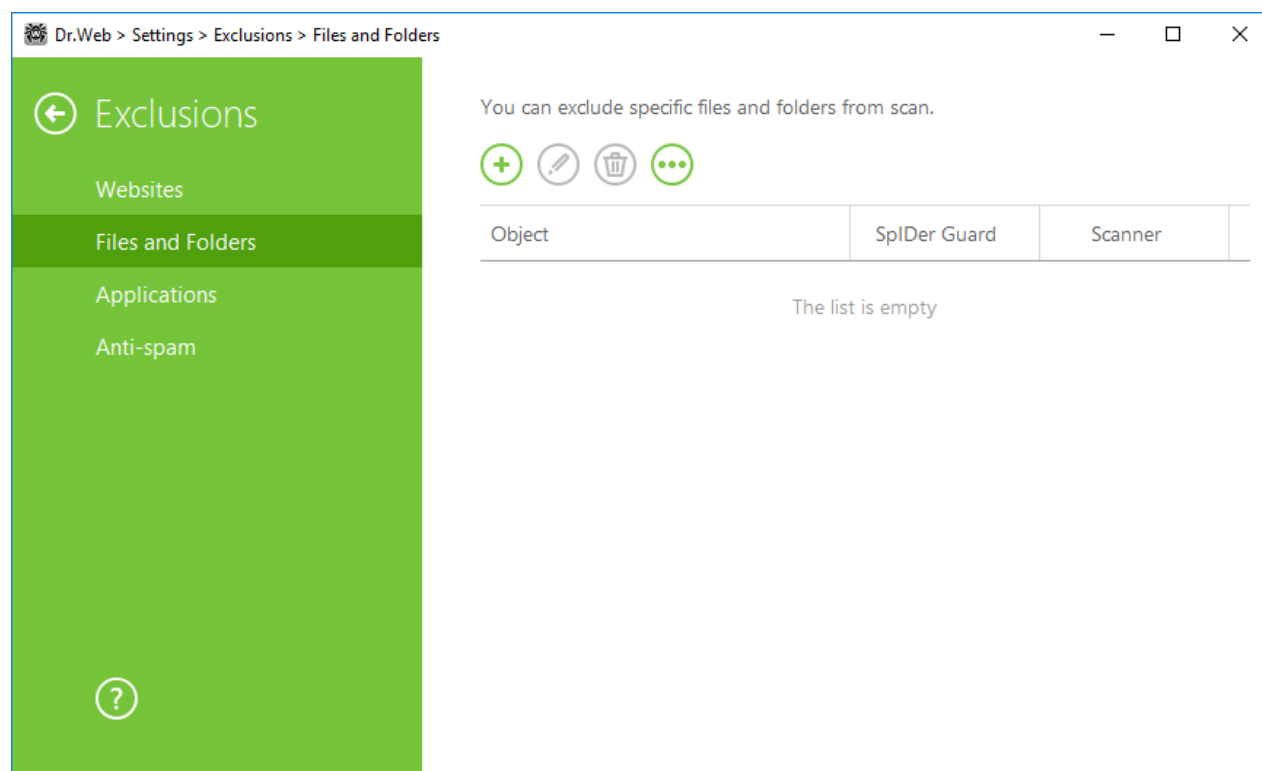


Figure 36. Excluding files and folders from scanning

To configure list of exclusions

1. To add a file or folder to the exclusion list, do one of the following:
 - To add an existing file or folder, click . In the open window, click **Browse** and select the item in the standard dialog window. You can enter the full path to the file or folder or edit the path in the field before adding it to the list.. For example:
 - `C:\folder\file.txt`—excludes file.txt file stored in C:\folder.
 - `C:\folder\`—excludes all files located in C:\folder and its subfolders.
 - To exclude a file with a particular name, enter the name and the extension without path.. For example:
 - `file.txt`—excludes all files with the name "file" and the .txt extension located in all folders.





- `file`—excludes all files with the name “file” located in all folders without regard for the extension.
- To exclude a group of files or folders, enter the mask of their names.

A mask denotes the common part of object names, at that:


- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any character (one).

Examples:

- `Report*.doc` defines all Microsoft Word documents whose names start with the word “Report” (ReportFebruary.doc, Report121209.doc, etc.)
- `*.exe` defines all executable files; i.e., that have the EXE extension (setup.exe, iTunes.exe, etc.)
- `photo????09.jpg` defines all JPG images which names start with the word “photo”, end with “09” and contain exact number of 4 other characters in the middle (photo121209.jpg, photoJoe09.jpg, or photo----09.jpg, etc.)
- `file*`—excludes all files located in all folders without regard for the extension with the names starting with “file” .
- `file.*`—excludes all files with the name “file” and with all extensions located in all folders.
- `C:\folder**`—excludes from scanning all subfolders and all files stored in C:\folder. The files stored within subfolders will be scanned.
- `C:\folder*`—excludes all files located in C:\folder and its subfolders on any nesting level.
- `C:\folder*.txt`—excludes all *.txt files stored in C:\folder. The *.txt files stored within subfolders will be scanned.
- `C:\folder**.txt`—excludes all *.txt files stored in the first nesting level subfolders of C:\folder.
- `C:\folder***.txt`—excludes all *.txt files stored in subfolders of any nesting level within C:\folder. The files stored in C:\folder itself, including *.txt files, will be still scanned.

2. In the configuration window, specify the components that must not scan this file.
3. Click **OK**. The file or folder will appear on the list.
4. To edit an existing exclusion, select the corresponding item from the list and click .
5. To list other files and folders, repeat steps 1 to 2. To remove a file or folder from the list, select the corresponding item and click .

Managing listed objects

Click  to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.



- **Clear all**—allows to remove all objects from the list of exclusions.

12.3. Applications

In this section you can specify a list of programs and processes to be excluded from scanning by SplDer Guard, SplDer Gate and SplDer Mail.

By default, the list is empty.

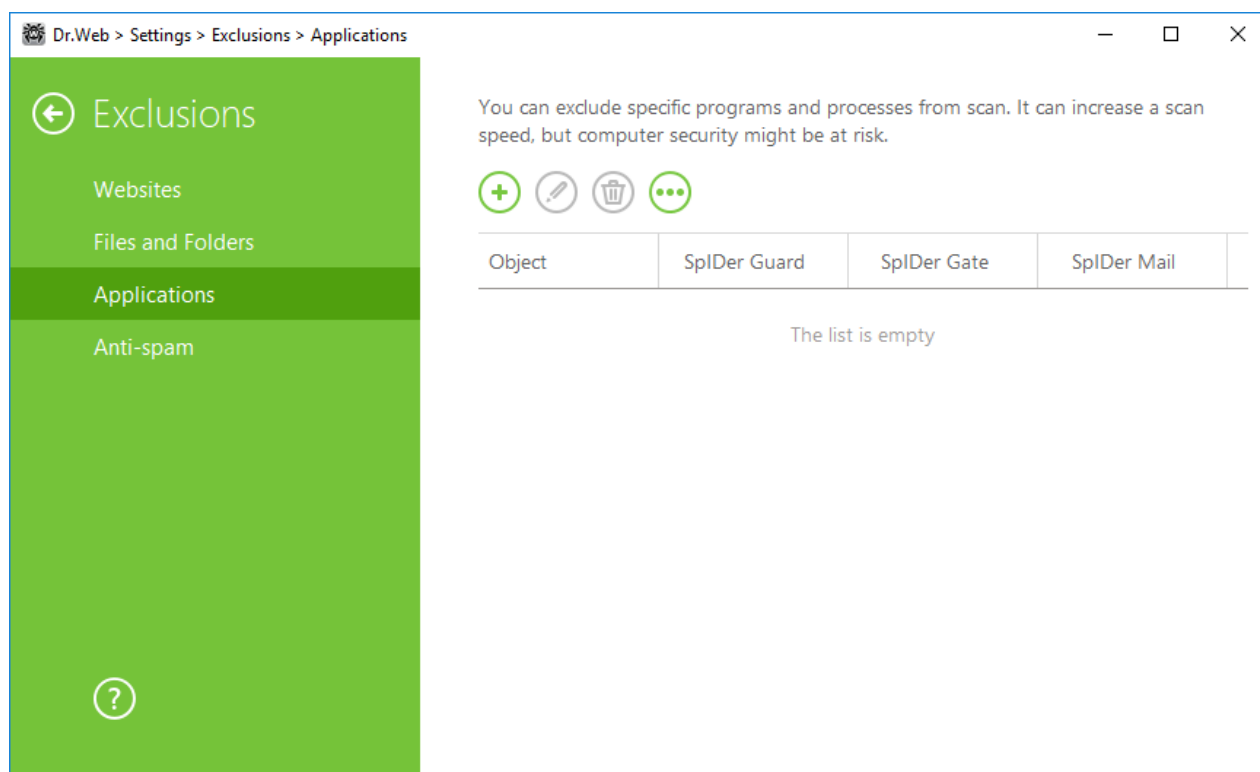



Figure 37. Excluded applications list

To configure list of exclusions

1. To add a program or a process to the exclusion list, click . Do one of the following:
 - In the open window, click **Browse** and select an application in the standard dialog window. You can enter the full path to the application in the field manually.. For example
`C:\Program Files\folder\example.exe`
 - To exclude an application from scanning, enter its name in the field. The full path to the application is not required. For example:
`example.exe`
 - To exclude applications, enter the mask of their names.

A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.



- The question mark (?) replaces any character (one).

Examples:

- `C:\Program Files\folder*.exe` – excludes applications in the folder `C:\Program Files\folder` from scanning. Applications in subfolders will be scanned.
- `C:\Program Files**.exe` – excludes applications stored in the first nesting level subfolders of `C:\Program Files`.
- `C:\Program Files***.exe` – excludes applications in subfolders of any nesting level located in the folder `C:\Program Files` from scanning. Applications in the folder `C:\Program Files` will be scanned.
- `C:\Program Files\folder\exam*.exe` – excludes any application in the folder `C:\Program Files\folder` from scanning if their names begin with “exam”. In subfolders, these applications will be scanned.
- `example.txt`—excludes all applications with the name “example” and the .exe extension located in all folders.
- `example*` —excludes all types of applications with the name starting with “example” located in all folders.
- `example.*`—excludes all applications with the name “example” in all folders without regard for the extension.
- You can exclude an application from scanning by the name of a variable if the name and a value of this variable are specified in the system variable settings.. For example:
 - `%EXAMPLE_PATH%\example.exe` – excludes an application by the name of a system variable. A name of a system variable and its value can be specified in the operating system settings.

For Windows 7 and higher: **Control Panel** → **System** → **Advanced system settings** → **Advanced** → **Environment variables** → **System variables**.

A name of a variable in an example: `EXAMPLE_PATH`.

A value of a variable in an example: `C:\Program Files\folder`.

2. In setting window specify the components that should not check the selected application. For objects, excluded from checks by SpIDer Gate and SpIDer Mail components, specify additional conditions.

Parameter	Description
Regardless of whether the application has a digital signature	Select this parameter to exclude the application from scanning regardless of whether it has a valid digital signature or not.
If the application has a valid digital signature	Select this parameter to exclude the application from scanning only if it has a valid digital signature. Otherwise, the application will be scanned by the components.



Parameter	Description
Any traffic	Select this parameter to exclude encrypted and non-encrypted application traffic from scanning.
Encrypted traffic	Select this parameter to exclude only encrypted application traffic from scanning.
On all IP addresses and ports	Select this parameter to exclude traffic on all IP addresses and ports from scanning.
On specific IP addresses and ports	Select this parameter to exclude specific IP addresses and ports from scanning. Traffic from other IP addresses and ports will be scanned (unless specified otherwise).
To specify addresses and ports	<p>To configure exclusion settings follow the guidance below:</p> <ul style="list-style-type: none">• To exclude a specific domain corresponding to a particular port from scanning, enter <code>site.com:80</code>, for example.• To exclude scanning of traffic on a custom port (for example, 1111), enter <code>*:1111</code>.• To exclude scanning of traffic on any port, enter <code>site:*</code>.

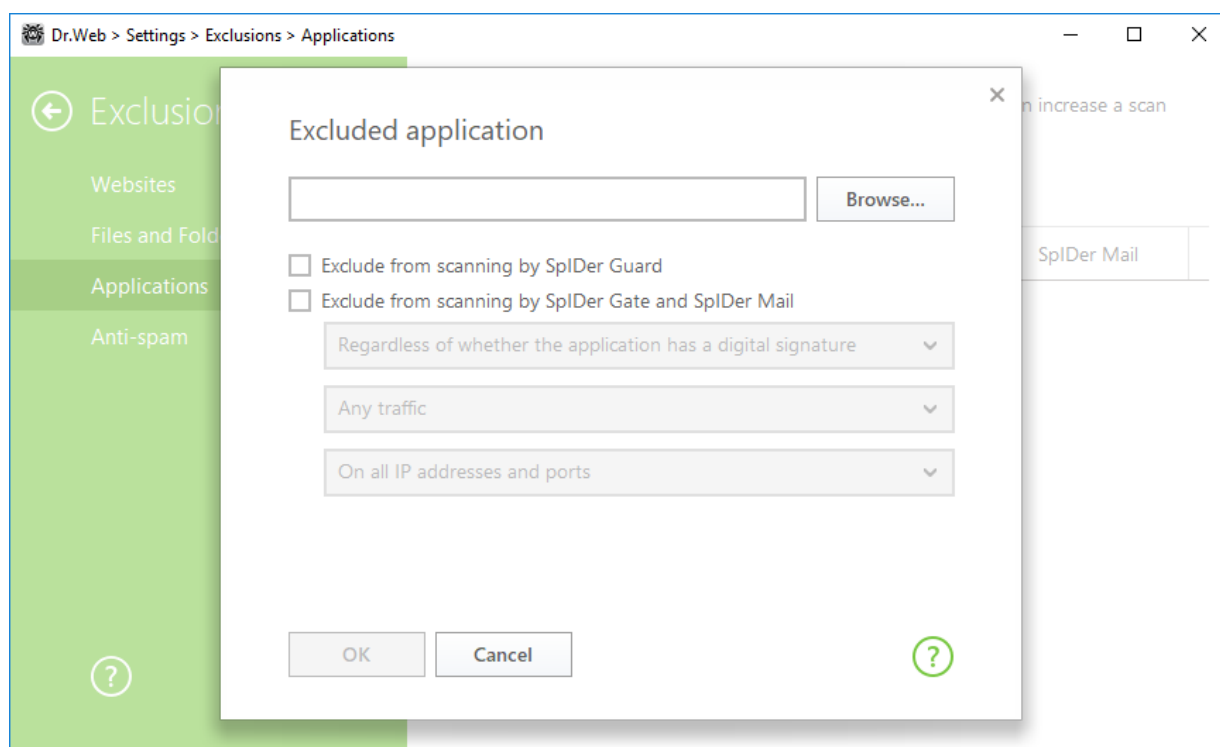





Figure 38. Adding applications to exclusions

3. Click **OK**. The selected application will appear on the list.
4. If necessary, repeat the procedure to add other programs.



Managing listed objects

To edit an existing exclusion, select the corresponding item from the list and press . To remove an application from the list, select the corresponding item and click .

Click  to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.

12.4. Anti-spam

In this window you can configure lists of senders whose messages will be excluded from spam checks. SpIDer Mail component bypasses them or considers as spam, without analyzing their contents).

If you add an address to the white list, messages from the sender will be always delivered to recipients. If you add an address to the black list, all messages from the sender will be regarded as spam automatically (that is, without scanning). By default, both lists are empty.

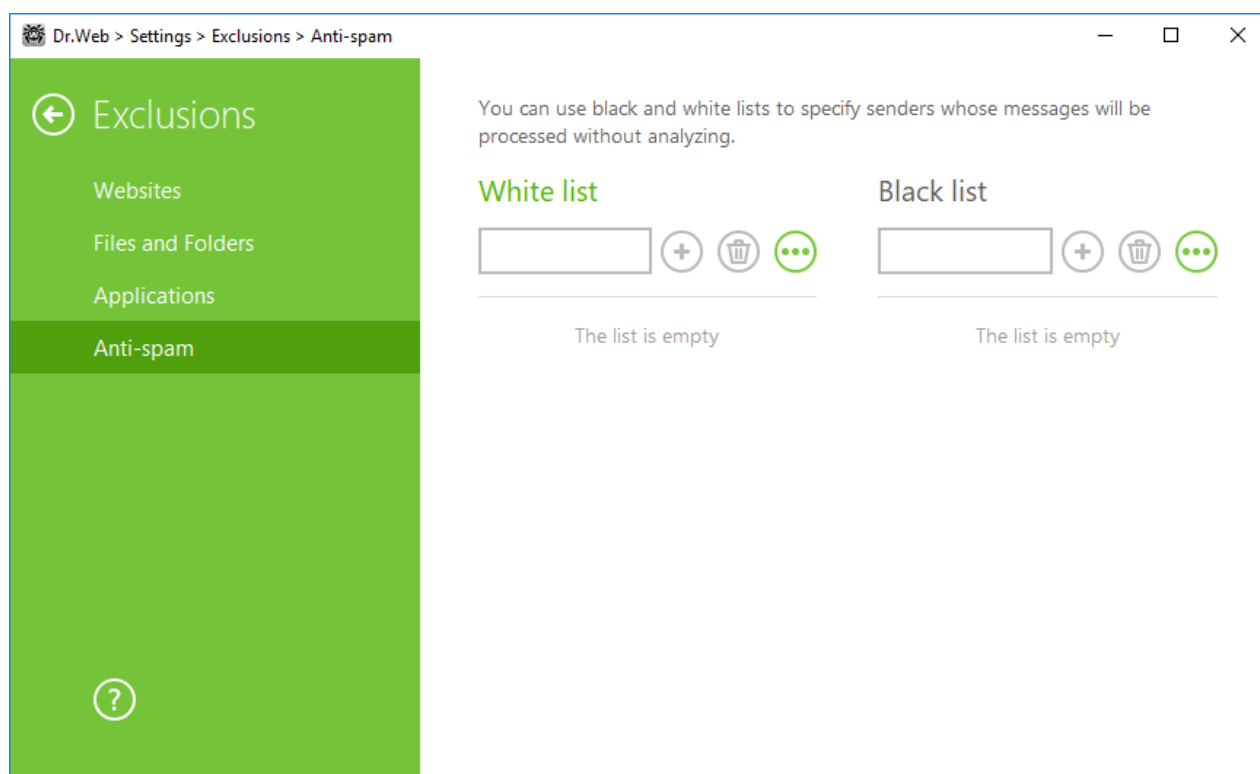





Figure 39. Adding addresses to exclusions list



To configure anti-spam lists

1. Enter an address or a mask for addresses of senders whose email messages you want to process automatically without analysis. Details:
 - To add a certain sender, enter the full email address (for example, `name@mail.com`). This ensures automatic processing of all messages from this sender without analysis.
 - To add senders with similar usernames, replace the differing part of their addresses with an asterisk (*) and a question mark (?). Use an asterisk (*) to substitute any character sequence or a question mark (?) to substitute any single character. For example, if you enter `name*@mail.com`, SpIDer Mail will process automatically messages from `name@mail.com`, `name1@mail.com`, `name_of_name@mail.com` and senders with other similar usernames.
 - To process automatically all messages sent from any email address within a domain, use an asterisk (*) instead of the username in the address. For example, to specify all messages sent from any email address within the `mail.com` domain, enter `*@mail.com`.
2. To add the entered address to the list, click .
3. To add other addresses, repeat steps 1 to 2. To remove an address from the list, select the corresponding item and click .

Managing listed objects



Click  to access the following options:

- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.



13. Protection Components

Security components provide system scanning, scanning of mails for threats and spam, monitoring of network connections and HTTP traffic.

To configure protection components, open the Dr.Web menu  in [administrator mode](#), run **Settings**  and go to **Protection components**.



To be able to configure protection components, you must have [administrator privileges](#).

To configure scanning of launched processes or files in use, go to [SpIDer Guard](#).

To configure HTTP traffic scanning, go to [SpIDer Gate](#).

To configure email scanning for threats, go to [SpIDer Mail](#).

To control the connections and data transfer via the Internet and to block suspicious connections both on network and application levels, go to [Firewall](#).

To change general parameters of scanning and reaction on detection of infected or suspicious files and archives or other malicious objects, go to [Scanner](#).

To control the third-party applications, go to [Preventive Protection](#).

13.1. SpIDer Guard

SpIDer Guard is an on-access anti-virus scanner that constantly resides in memory and scans files and RAM on the fly instantly detecting any malicious activity.

With the default settings, the component performs on-access scans of files that are being created or changed on the hard drives and all files that are opened on removable media. Moreover, SpIDer Guard constantly monitors running processes for virus-like activity and, if such is detected, blocks malicious processes and reports on the event. On detection of an infected object, SpIDer Guard processes it according to the specified settings.

Files within archives and mailboxes are not scanned. If a file within an archive or email attachment is infected, the malicious object will be detected and neutralized by SpIDer Guard immediately after you try to extract the archived files or download the attachment. To prevent spread of viruses and other malicious objects via email, [use](#) SpIDer Mail.

On detection of an infected object, SpIDer Guard applies actions to it according to the [specified settings](#). You can change settings to configure automatic reaction to different virus events. By default, SpIDer Guard loads automatically when Windows starts and cannot be unloaded during the current Windows session.



13.1.1. Configuring SplDer Guard



To access the SplDer Guard settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

The default settings are optimal for most cases. Do not change them unnecessarily.

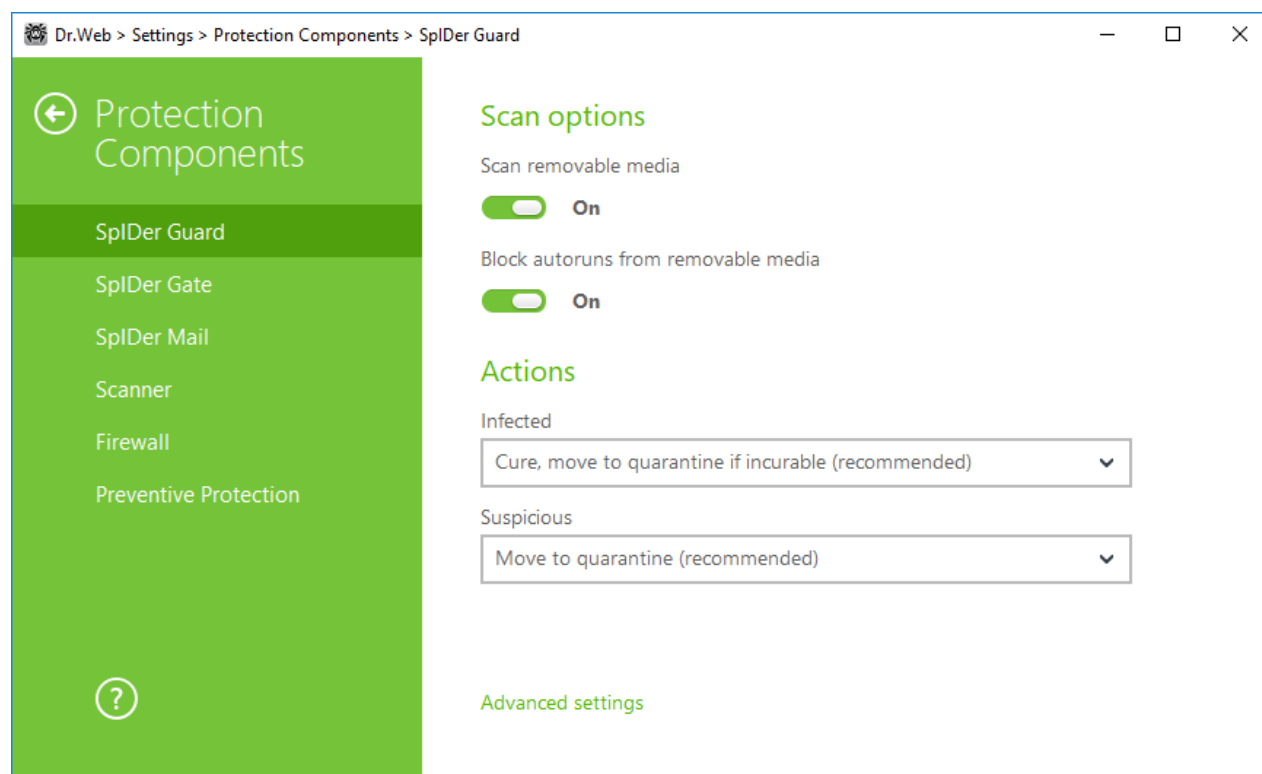


Figure 40. SplDer Guard settings

Scan options

By default, SplDer Guard checks files that are opened, changed or launched on removable media such as CD/DVD, flash drives, and so on. This option helps to protect your computer from viruses transmitted via removable media. When these options are disabled, the objects on removable media are not checked for viruses.



If any problem occurs during installation with the autorun option, it is recommended to temporary disable the **Block autoruns from removable media** option.

Actions

On this page, you can configure reactions of SplDer Guard to detection of infected or suspicious files and malware.



For different types of compromised objects, actions are assigned separately from the respective drop-down lists:

- **Infected**—objects infected with a known and (supposedly) curable virus.
- **Suspicious**—objects supposedly infected with a virus or containing a malicious object.
- Various potentially dangerous objects (riskware). To expand the entire list of objects, click the **Advanced settings** link.

Separate reaction of SpIDer Guard to detection of each object type. Set of actions available for the selection depends on the threat type.

By default, SpIDer Guard attempts to cure infected and supposedly curable files, moves other most dangerous objects to [Quarantine](#), and ignores minor threats such as jokes, hacktools, and riskware. The reactions of SpIDer Guard are similar to those of Dr.Web Scanner.

You can select one of the following actions for detected threats:

Action	Description
Cure, move to quarantine if not cured	<p>Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine.</p> <p>The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects such as archives, mailboxes, or file containers.</p>
Cure, delete if not cured	<p>Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted.</p> <p>The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects such as archives, mailboxes, or file containers.</p>
Delete	<p>Instructs to delete the object.</p> <p>This action is not available for boot sectors.</p>
Move to Quarantine	<p>Instructs to move the object to a specific folder of Quarantine.</p> <p>This action is not available for boot sectors.</p>
Ignore	<p>Instructs to skip the object without performing any action or displaying a notification.</p> <p>The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.</p>



SpIDer Guard does not check complex objects such as archives, mailboxes, or file containers. No action is performed on such objects or on files within them.

Copies of all processed objects are stored in [Quarantine](#).

Scan mode

In this group, you can set up what actions with objects require scanning “on-the-fly” with SpIDer Guard.

Option	Description
Optimal (recommended)	<p>This scan mode is used by default.</p> <p>In this mode, SpIDer Guard scans objects only when one of the following actions is traced:</p> <ul style="list-style-type: none">• For objects on hard drives, an attempt to execute a file, create a new file, or add a record to an existing file or boot sector.• For objects on removable media, an attempt to access file or boot sectors in any way (write, read, execute).
Paranoid	<p>In this mode, SpIDer Guard scans files and boot sectors on hard or network drives and removable media at any attempt to access them (create, write, read, execute).</p>



When running in the Optimal mode, SpIDer Guard does not terminate execution of an [EICAR test file](#) and the file is not processed as malicious since it does not pose any actual threat to your system. However, if you copy or create such a file in your system, it will be detected by SpIDer Guard and moved to Quarantine by default.

Details and recommendations

The **Optimal** mode is recommended to use after a thorough [scan](#) of all hard drives by Dr.Web Scanner. With this mode activated, SpIDer Guard prevents penetration of new viruses and other malicious objects via removable media into your computer while preserving performance by omitting knowingly “clean” objects from repeated scans.

The **Paranoid** mode ensures maximum protection but considerably reduces computer performance.

In any mode, objects on removable media and network drives are scanned only if the corresponding options in the **Scan options** group are enabled.



Operating system may register some removable media as hard drives (for example, portable USB hard drives). Scan such devices with Dr.Web Scanner when you connect them to the computer.

By default, files within archives and mailboxes are not scanned. This does not affect security of your computer when it is constantly protected by SplDer Guard, only delays the moment of detection. If a file within an archive or email attachment is infected, the malicious object will be detected and neutralized by SplDer Guard immediately when you try to extract the archived files or download the attachment.

Advanced settings

The settings of this group allow to specify parameters for scanning objects on-the-fly and are always applied regardless of the selected SplDer Guard operation mode. You can enable:

- Use of heuristic analysis;
- scan of programs and modules to download;
- scan of installation packages;
- scan of files on network drives (not recommended);
- scan of a computer for the presence of rootkits (recommended);
- scan of scripts executed with Windows Script Host and PowerShell (for Windows 10).

Heuristic analysis

By default, SplDer Guard performs scan using [heuristic analysis](#). If this option is disabled, SplDer Guard will use signature analysis only.

Background rootkit scanning

Anti-rootkit component included in Dr.Web provides options for background scanning of the operating system for complex threats and curing of detected active infections when necessary.

If this option is enabled, Dr.Web Anti-rootkit constantly resides in memory. In contrast to the on-the-fly scanning of files by SplDer Guard, scanning for rootkits i.e. malicious programs that are used for hiding changes in the operating system such as running of particular processes, registry changes, modifications of files and folders includes checking of autorun objects, running processes and modules, Random Access Memory (RAM), MBR/VBR disks, computer BIOS system, and other system objects.

One of the key features of Dr.Web Anti-rootkit is delicate attitude towards consumption of system resources (processor time, free RAM, and others) as well as consideration of hardware capacity.



When Dr.Web Anti-rootkit detects a threat, it notifies you on the detection and neutralizes the malicious activity.



During background rootkit scanning, files and folders specified on the [Excluded files](#) page are excluded from scanning.

Background rootkit scanning is enabled by default.



Disabling of SpIDer Guard does not affect background scanning. If the option is enabled, background scanning is performed regardless of whether SpIDer Guard is running or not.

13.2. SpIDer Gate

SpIDer Gate is an anti-virus HTTP monitor. By default, SpIDer Gate automatically checks incoming HTTP traffic and blocks all malicious objects. HTTP is used by Web browsers, download managers, and other applications which exchange data with web servers, that is, which work with the Internet.

You can [configure](#) SpIDer Gate settings to completely disable monitoring of incoming traffic or enable scanning of outgoing traffic, compose a list of applications whose HTTP traffic is to be always checked, or exclude certain applications from monitoring.

By default, SpIDer Gate blocks all incoming malicious objects. URL filtering of malicious and unreliable websites is also enabled by default.

SpIDer Gate checks data transmitted over cryptographic protocols.

SpIDer Gate automatically launches on Windows startup and resides in memory.

13.2.1. Configuring SpIDer Gate

If you want SpIDer Gate to check data transmitted over cryptographic protocol, enable the **Check encrypted traffic** option in the [Network](#) section.



To access the SpIDer Gate settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

The default settings are optimal for most cases. Do not change them unnecessarily.

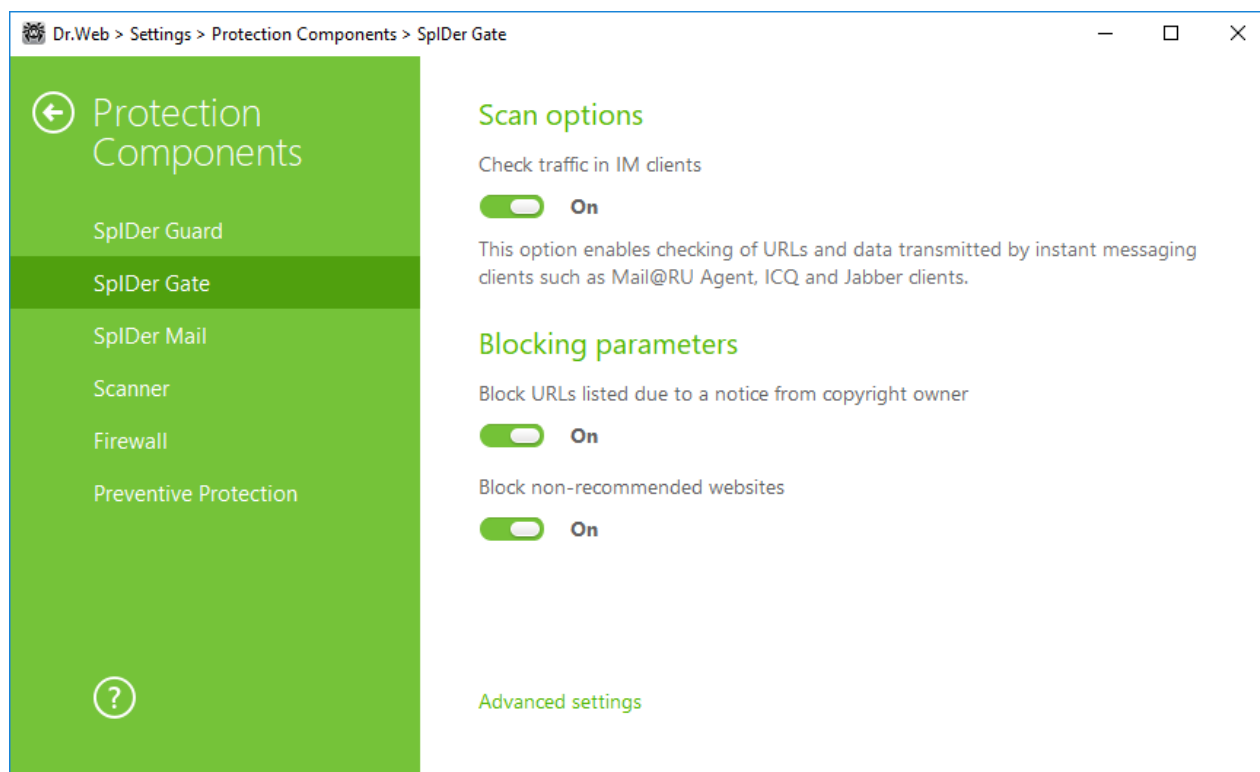


Figure 41. SpIDer Gate settings

Check traffic in IM clients

In the **Scan options** group, you can enable checking of URLs and data transmitted by instant messaging clients (Mail.ru Agent, ICQ, and Jabber clients). Only incoming traffic is checked. By default, this option is enabled.

The links transmitted in messages are checked according to SpIDer Gate settings: links to the websites known as infection sources are blocked automatically, the links to websites that are not recommended for visiting or to URLs specified on a notice from copyright owners are blocked only if the corresponding options are enabled in the **Blocking parameters** section. Herewith, the [white list](#) and [the list of applications excluded from checks](#), also have an effect.

Files transmitted by instant messaging clients are also checked. When a threat is detected, file transmission is blocked if the corresponding option is enabled on the **Block programs** page. Viruses are blocked automatically if the **Check traffic in IM clients** option is enabled.

Blocking parameters

In the **Blocking parameters** group you can enable automatic blocking of URLs listed due to a notice from copyright owners (enable the corresponding option) and blocking of unreliable websites (enable the **Block non-recommended websites** option). On the **Exclusions** page, you can [specify websites](#) access to which must be allowed regardless of other restrictions.



By default, SpIDer Gate blocks the access to websites known as infection sources. Herewith, [the list of exclusions](#) has an effect.

Programs to block

By default, SpIDer Gate detects and blocks the following malicious programs:

- Suspicious;
- Riskware;
- Dialers;
- Hacktools;
- Adware;
- Jokes.

By default, SpIDer Gate blocks suspicious programs, adware and dialers.

Objects to block

SpIDer Gate can block malformed or not checked objects. This option is disabled by default.

Advanced settings

You can configure scans of archive and installation packages. By default, all malicious programs are blocked and scanning of archives and installation packages is disabled.

You can also adjust **Scan priority** that determines distribution of resources depending on traffic scanning priority. Internet connection speed decreases when SpIDer Gate operates with lower priority, since the monitor have to wait longer for downloading and scans larger portions of data. When you increase the priority, SpIDer Gate starts scanning data more often, thus increasing speed of your Internet connection. However, frequent scans also increase processor load.

Also you can select the type of HTTP traffic to check. By default, only incoming traffic is scanned. Herewith the specified actions, [the white list](#) and [the list of excluded applications](#) also have an effect.

13.3. SpIDer Mail

SpIDer Mail is an anti-virus mail scanner that is installed by default. It resides in memory and automatically launches on system startup.

SpIDer Mail supports scanning of encrypted email traffic.



Mail processing

Any incoming messages are intercepted by SpIDer Mail before they are received by mail clients. Messages are scanned for viruses with the maximum possible level of detail. If no viruses or suspicious objects are found, messages are passed on to the mail program in a “transparent” mode as if they were received directly from the server. Similar procedure is applied to outgoing messages before they are sent to servers.

By default, SpIDer Mail [reacts](#) to detection of infected incoming messages and messages that have not been scanned (for example, due to a complicated structure) as follows:

- Malicious code is removed from infected messages, then messages are delivered as usual. This action is called *curing* the message.
- Messages with suspicious objects are moved to [Quarantine](#) as separate files; the mail client receives a notification about this. This action is called *moving* the message. All moved messages are deleted from the POP3 or IMAP4 mail servers.
- Messages that have not been scanned and safe messages are passed on to the mail client (*skipped*).

Infected or suspicious outgoing messages are not sent to the server. The user is notified that a message will not be sent (usually the mail program will save such a message).

The default SpIDer Mail settings are optimal for beginners, provide maximum protection and require minimum user interference. However, by default SpIDer Mail may block some options of mail programs (for example, sending a message to multiple addresses might be considered as mass distribution, incoming mail is not scanned for spam), useful information from safe text part of infected messages becomes unavailable in case of automatic deletion. Advanced users can [configure](#) mail scanning settings and reaction of SpIDer Mail to various virus events.

Mail check by other components

Dr.Web Scanner can also detect viruses in mailboxes of several formats, but SpIDer Mail has several advantages:

- Not all formats of popular mailboxes are supported by Dr.Web Scanner. When using SpIDer Mail, the infected messages are not even delivered to mailboxes.
- Dr.Web Scanner does not check mailboxes at the moment of the mail receipt, but either on user demand or according to schedule. Furthermore, this action is resource consuming and takes a lot of time.

Thus, when all Dr.Web components operate with their default settings, SpIDer Mail detects viruses and suspicious objects distributed via email first and prevents them from infiltrating your computer. SpIDer Mail operation is rather resource sparing. Scanning of email files can be performed without other components.



13.3.1. Configuring SplDer Mail

If you want SplDer Mail to check data transmitted over cryptographic protocol, enable the **Check encrypted traffic** option in the [Network](#) section.



To access the SplDer Mail settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

The default settings are optimal for most cases. Do not change them unnecessarily.

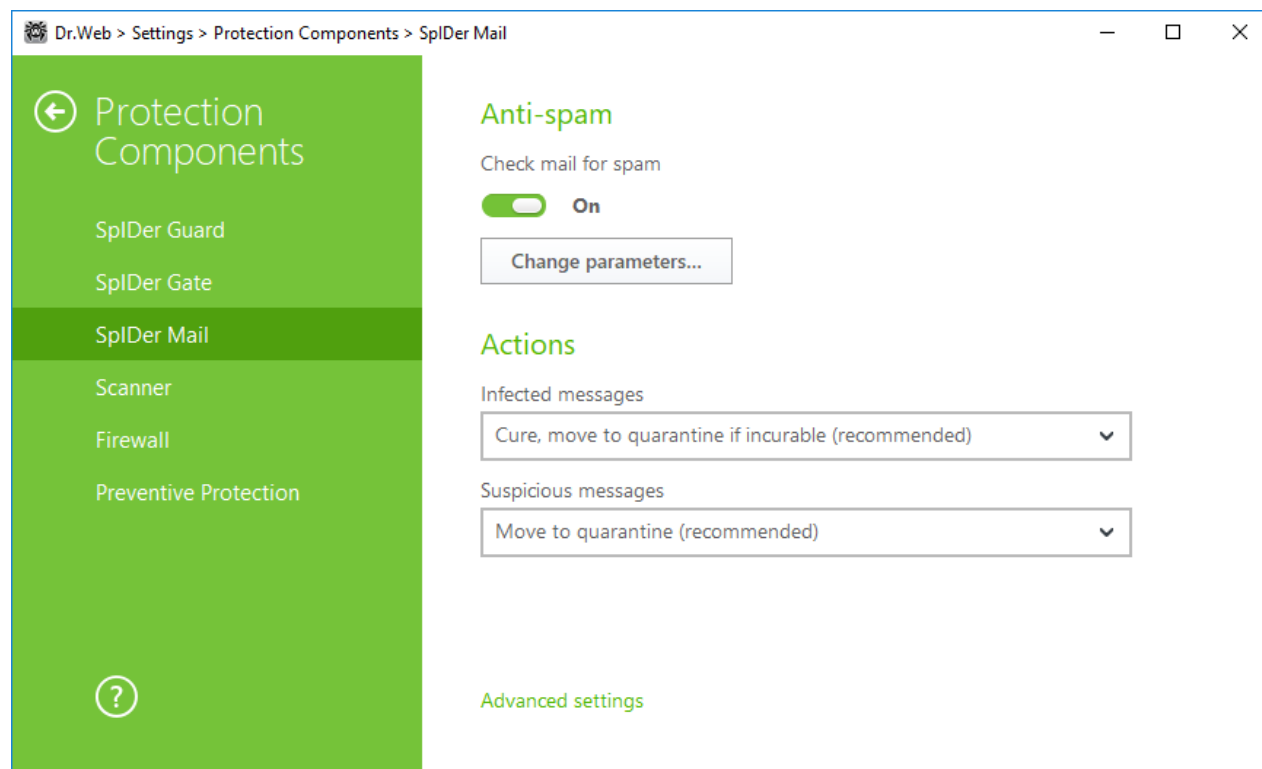


Figure 42. SplDer Mail settings

Anti-spam

By default, SplDer Mail checks emails for spam. You can disable this option using the corresponding switch or change scanning parameters by clicking **Change parameters**. Anti-spam technologies and adjustable parameters are described in the [Anti-spam](#) section.

Actions

By default, SplDer Mail attempts to cure messages infected with a known and (supposedly) curable virus and moves incurable and suspicious messages as well as adware and dialers to [Quarantine](#) at the same time ignoring all other minor threats. Other messages are transmitted unchanged by SplDer Mail (*skipped*).



The SpIDer Mail reactions are similar to those of Dr.Web Scanner.

You can select one of the following actions to be applied by SpIDer Mail to detected threats:

Action	Description
Cure, move to quarantine if not cured	<p>Instructs to restore the original state of the message before infection. If the message is incurable, or the attempt of curing fails, the object is moved to quarantine.</p> <p>Available only for objects infected with a known virus that can be cured except for Trojan programs, which are deleted on detection. This action is not applicable to files within archives.</p>
Cure, delete if not cured	Instructs to restore the original state of the message before infection. If the message is incurable, or the attempt of curing fails, the object is deleted.
Delete	Instructs to delete the message. The message is not sent to the recipient; the mail client receives a notification about this.
Move to Quarantine	Instructs to move the message to the special Quarantine folder. The message is not sent to the recipient; the mail client receives a notification about this.
Ignore	Instructs to pass the message to the mail client as usual, that is, without performing any action.

If an email contains a malicious object, any reaction except **Ignore** results in failure to send the message to a mail server or recipient.

To increase security above the default level, you may select the **Move to quarantine** action for **Not checked** and then scan the moved file with Dr.Web Scanner.



If you want to disable scans of email, ensure that SpIDer Guard monitors your computer constantly.

Actions on messages

In this group, you can configure additional actions to be applied when SpIDer Mail processes messages.

Option	Description
Insert 'X-AntiVirus' header into messages	<p>This option is enabled by default.</p> <p>Instructs SpIDer Mail to add scan results and information on Dr.Web version to message headers after processing. You cannot edit data format.</p>



Option	Description
Delete modified messages on server	Instructs to remove messages to which either Delete or Move to Quarantine action was applied by SpIDer Mail. The messages are removed from mail servers regardless of the mail client settings.

Scanning optimization options

You can set the condition under which SpIDer Mail should acknowledge complex messages, whose scanning is time consuming, as unchecked. To do that, enable the **Message scan timeout** option and set the maximum message scanning time. After the expiry of the specified period (by default, 250 sec.), SpIDer Mail stops checking of the message.

Scanning archives

Enable the **Scan archives** option if you want SpIDer Mail to scan archived files transferred via email. You can configure the following parameters:

- **Maximum file size to extract.** If an archive size exceeds the specified value (by default, 30,720 KB), SpIDer Mail does not unpack and check the archive.
- **Maximum compression ratio.** If an archive compression ratio exceeds the specified value (by default, 0), SpIDer Mail does not unpack and check the archive.
- **Maximum archive nesting level.** If a nesting level is greater than the specified value (by default, 64), SpIDer Mail proceeds unpacking and scanning the archive until this limit is exceeded.

You can enable one or more options.



There is no restrictions for a parameter if the value is set to 0.

Advanced settings

The following settings allow you to configure additional mail scanning parameters:

- Use heuristic analysis—in this mode, [special methods](#) are used to detect suspicious objects that are most likely infected with unknown viruses. To disable the analyzer, disable the **Use heuristic analysis (recommended)** option.
- Scan installation packages. This option is disabled by default.

13.3.2. Anti-spam

Dr.Web Anti-spam technologies consist of several thousand rules that can be divided into several groups:



- **Heuristic analysis**—a highly intelligent technology that empirically analyzes all parts of a message: header, message body, and attachments, if any.
- **Detection of evasion techniques**—this advanced anti-spam technology allows detecting evasion techniques adopted by spammers to bypass anti-spam filters.
- **HTML signature analysis**—messages containing HTML code are compared with a list of known patterns from the anti-spam library. Such comparison, in combination with the data on sizes of images typically used by spammers, helps to protect users against spam messages with HTML code linked to online content.
- **Semantic analysis**—the words and phrases of a message (both visible to the human eye and hidden) are compared with words and phrases typical of spam using a special dictionary.
- **Anti-scamming**—scam and phishing messages include so-called “Nigerian” scams, loan scams, lottery and casino scams and false messages from banks and credit organizations. A special module is used to filter scams.
- **Technical spam**—Bounces are delivery-failure messages sent by a mail server. Such messages are also sent by a mail worm. Therefore, bounces are as unwanted as spam.

You can configure the following Anti-spam options:

Option	Description
Allow Cyrillic text	<p>This option is enabled by default.</p> <p>Select this check box to prevent SpIDer Mail from marking Cyrillic emails as spam without prior analysis. Otherwise, such emails are most likely to be marked as spam.</p>
Allow Asian text	<p>This option is enabled by default.</p> <p>Select this check box to prevent SpIDer Mail from marking Asian emails as spam without prior analysis. Otherwise, such emails are most likely to be marked as spam.</p>
Add the prefix to subjects of spam messages	<p>By default, this option is enabled, and SpIDer Mail adds the [SPAM] prefix to the Subject field of all spam messages.</p> <p>Instructs SpIDer Mail to add a special prefix to subjects of spam messages.</p> <p>Using a prefix allows you to create filter rules for spam in those mail clients (for example, Microsoft Outlook Express) where it is not possible to enable filtering by headers.</p>

Processing mail by spam filter

SpIDer Mail adds the following header to the processed messages:



- X-DrWeb-SpamState: *<value>*, where *<value>* indicates whether the message is considered by SpIDer Mail as spam (Yes) or not (No).
- X-DrWeb-SpamVersion: *<version>*, where *<version>* indicates Dr.Web Anti-spam version.
- X-DrWeb-SpamReason: *<spam rate>*, where *<spam rate>* includes a list of evaluations on various spam criteria.

You can use these headers and the prefix in the Subject field, if selected, to configure email filtering for your mail client.



If you use IMAP/NNTP protocols, configure your mail client to download complete messages from mail server at once, i.e. without previewing their headers. This is required for correct operation of the spam filter.

To improve performance of the spam filter, you can report errors in spam detection.



Spam filter processes email messages composed in accordance with the MIME RFC 822 standard.

To report spam detection errors

1. Create a new email and attach the message that was processed incorrectly by the spam filter. Messages included within the email body are not analyzed.
2. Send the message with the attachment to one of the following addresses:
 - If the attached message is detected as spam incorrectly, send the email to vrnonspam@drweb.com.
 - If the attached messages is an undetected spam, send it to vrspam@drweb.com.

13.4. Scanner



To access the Scanner settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

The default settings are optimal for most cases. Do not change them unnecessarily.

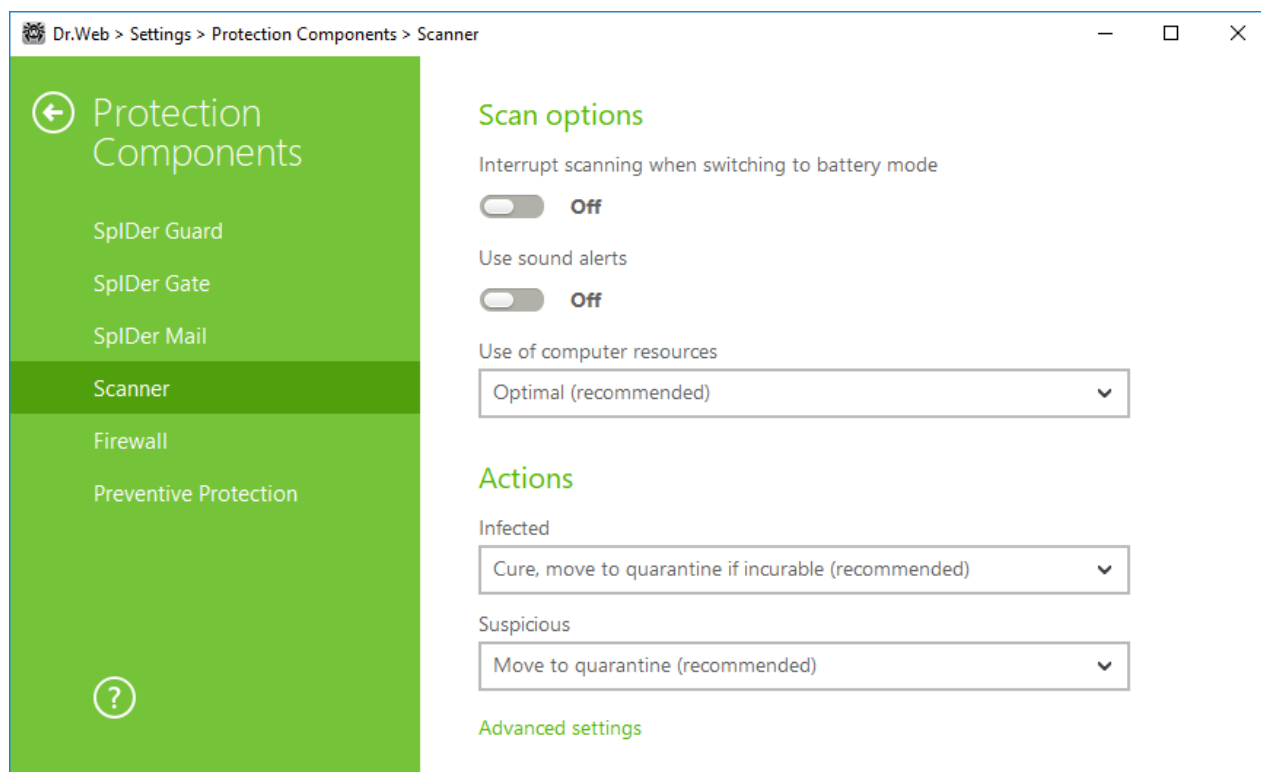


Figure 43. Scanner settings

Scan options

In this group, you can configure general parameters of Dr.Web Scanner operation.

- **Interrupt scanning when switching to battery mode.** Enable this option to interrupt scanning when switching to battery mode. Option is disabled by default.
- **Use sound alerts.** Enable this option for Dr.Web Scanner to use sound alerts for every event. Option is disabled by default.
- **Use of computer resources.** This option limits the use of computer resources by Dr.Web Scanner. The default value is optimal for most cases.

Actions

On this page, you can configure reaction of Scanner on detection of infected or suspicious files and archives or other malicious objects.

For different types of compromised objects, actions are assigned separately from the respective drop-down lists:

- **Infected**—objects infected with a known and (supposedly) curable virus.
- **Suspicious**—objects supposedly infected with a virus or containing a malicious object.
- Objects that pose potential threat (riskware).



Reaction of Scanner to detection of various malicious software is also set separately. Set of actions available for the selection depends on the threat type.

By default, Scanner attempts to cure the infected and supposedly curable files, moves other most dangerous objects to [Quarantine](#).

You can select one of the following actions for detected threats:

Action	Description
Cure, move to quarantine if not cured	<p>Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine.</p> <p>The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects such as archives, mailboxes, or file containers.</p>
Cure, delete if not cured	<p>Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted.</p> <p>The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects such as archives, mailboxes, or file containers.</p>
Delete	<p>Instructs to delete the object.</p> <p>This action is not available for boot sectors.</p>
Move to Quarantine	<p>Instructs to move the object to a specific folder of Quarantine.</p> <p>This action is not available for boot sectors.</p>
Ignore	<p>Instructs to skip the object without performing any action or displaying a notification.</p> <p>The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.</p>



Threats within complex objects (archives, email attachments, file containers) cannot be processed individually. For such threats, Dr.Web Scanner applies an action selected for this type of a complex object.

Advanced settings

You can disable check of installation packages, archives, and email files. This option is enabled by default.



You can also select one of the following actions for Scanner to perform once scanning is complete:

1. **Do not apply action.** Scanner will display the list of detected threats.
2. **Neutralize detected threats.** Scanner will neutralize threats automatically.
3. **Neutralize detected threats and shut down computer.** Scanner will shut down the computer once threats are automatically neutralized.

13.5. Firewall

Dr.Web Firewall protects your computer from unauthorized access and prevents leak of vital data through networks. It monitors connection attempts and data transfer and helps you block unwanted or suspicious connections both on network and application levels.

Firewall provides you with the following features:

- Control and filtration of all incoming and outgoing traffic
- Access control on the application level
- Filtration of packets on the network level
- Fast selection of rule sets
- Event logging

13.5.1. Training Firewall

Once installation is complete, Firewall starts learning by intercepting all connection attempts from your operating system or user applications. Firewall works in a learning mode if the following operation modes (see the [Configuring Firewall](#) section for detailed information about Firewall operation modes):

- **Allow connections for trusted applications** (set by default)
- **Interactive mode**

In the **Allow connections for trusted applications** mode, when operating system or applications attempt to connect to a network, Firewall checks whether these applications are trusted and whether filtering rules have been created for them. If no filtering rules have been set, Firewall prompts you to set a rule. In the same time, no rules are created for trusted applications. Such applications are allowed to connect to a network.

Among trusted applications are system applications, applications with Microsoft certificate, and applications from Dr.Web list of trusted applications.

In the **Interactive mode** mode, when operating system or applications attempt to connect to a network, Firewall checks whether filtering rules have been created for these programs. If no filtering rules have been set, Firewall prompts you to set a rule. Then, this rule will be applied each time this type of connection is detected.



When running under limited user account (Guest), Dr.Web Firewall does not display notifications on network access attempts. Notifications are shown for the session with administrator privileges if such session is simultaneously active.

Application Rules

1. To make a decision, consider the following information displayed in the notification:

Field	Description
Application	The name of the application. Ensure that the path to the application executable, specified in the Application path entry field, corresponds to the file location.
Application path	The full path to the application executable file and its name.
Digital signature	Digital signature of the application.
Address	The used protocol and network address to which the application is trying to connect.
Port	The network port used for the connection attempt.
Direction	The direction of the connection.

2. Once you make a decision, select an appropriate action:
 - To block this connection once, select **Block once**.
 - To allow this connection once, select **Allow once**.
 - To open a window where you can create a new application filter rule, select **Create rule**. In the open window, you can either choose one of the predefined rules or [create your rule](#) for the application.
3. Click **OK**. Firewall executes the selected action and closes the notification window.



In some cases Windows operating system does not allow to identify uniquely a service that acts as a system process. If a connection attempt is detected by the system process, take note on the port specified in the information about the connection. If you use an application which can access the specified port, allow this connection.

In cases when a connection is initiated by a trusted application (an application with existing rules), but this application is run by an unknown parent process, Firewall displays the corresponding notification.



To set parent process rules

1. Consider information about the parent process in the notification displayed on a connection attempt.
2. Once you make a decision about what action to perform, select one of the following:
 - To block this connection once, select **Block**.
 - To allow this connection, click **Allow**.
 - To create a rule for the parent process, click **Create rule** and in the open window specify [required settings](#).
3. Click **OK**. Firewall executes the selected action and closes the notification window.

When an unknown process is run by another unknown process, a notification displays the corresponding details. If you click **Create rule**, a new window appears allowing you to create new rules for this application and its parent process.

13.5.2. Configuring Firewall

You can configure the following Firewall options:

- Select the operation mode;
- [List](#) authorized applications;
- Configure parameters for known networks.



To access the Firewall settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

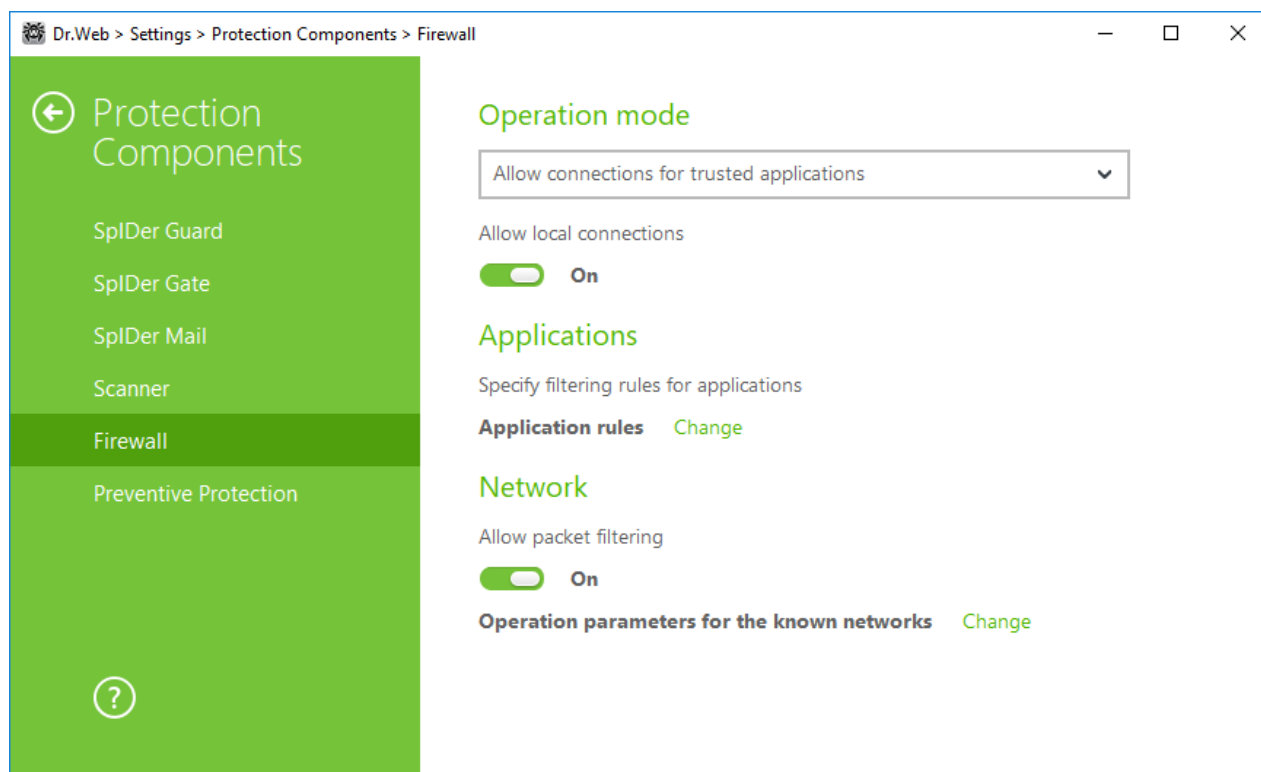


Figure 44. Firewall main settings

By default, Firewall does not automatically create rules for known applications. Regardless of the operation mode, events are logged.

The default settings are optimal for most cases. Do not change them unnecessarily.

The **Allow local connections** option allows all applications on your computer to interconnect (i.e., allow unlimited local connections (to or from 127.0.0.1 interface (localhost)) between applications installed on your computer). This option is applied after verifying that the connections match the set rules. Disable this option to apply filtering rules to connections carried out both through the network and within your computer.

To set operation mode

Select one of the following operation modes:

- **Allow connections for trusted applications**—an access mode, when all trusted applications are allowed to access network resources (used as default), for all other applications, a warning is displayed. You can set an application rule via such warning (see the [Training Firewall](#) section);
- **Allow unknown connections**—free access mode, when all unknown applications are permitted to access networks.
- **Interactive mode**—[learning mode](#), when the user is provided with full control over Firewall reaction.
- **Block unknown connections**—restricted access mode, when all unknown connections are blocked. For known connections, Firewall applies the appropriate rules.



Allow connections for trusted applications

This mode is used by default.

In this mode, all trusted applications are allowed to access network resources, including the Internet. Among trusted applications are system applications, applications with Microsoft certificate, and applications from Dr.Web list of trusted applications. Rules for such applications are not displayed in the rule list. For other applications, Firewall prompts you to allow or block the unknown connection manually, as well as create a new rule for it.

When a user application or operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If no filtering rules have been set, you are prompted to select a temporary solution or create a rule to be applied each time this type of connection is detected.

Allow unknown connections

In this mode, Firewall allows all unknown applications for which filtering rules have not been set to access network resources, including the Internet. No notification on access attempt is displayed by Firewall.

Interactive mode

In this mode, you have total control over Firewall reaction to the detection of unknown connections. Thus, the program is trained while you work on your computer.

When a user application or operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If no filtering rules have been set, you are prompted to select a temporary solution or create a rule to be applied each time this type of connection is detected.

Block unknown connections

In this mode, Firewall automatically blocks all unknown connections to network resources, including the Internet.

When a user application or the operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If there are no filtering rules, Firewall blocks network access for the application without displaying any notification to the user. If filtering rules for the application are set, Firewall processes the connection according to the specified actions.



Settings for Applications



Firewall allows you to create no more than one set of rules per each application.

Application level filtering helps you to control access of various applications and processes to network resources as well as enable or disable applications to run other processes. You can create rules for both system and user applications.

This page lists all applications and processes for which you can modify [application filter rule sets](#) by creating new rules, editing existing ones, or deleting those that are no longer needed. Each application is explicitly identified by the path to its executable file. Firewall uses the `SYSTEM` name to indicate the rule set applied to the operating system kernel (the system process for which there is no unique executable file).





If you created a blocking rule for a process or set Block unknown connections mode and then disabled the rule or changed the work mode, the process will be blocked till it will be restarted and attempts to establish connection again.

When an application is deleted from your computer, the related rules are not automatically deleted. You can delete them manually by clicking **Remove unused rules** in the shortcut menu of the list.

Application Rules

In the **New application rule set** (or **New application rule set**) window, you can configure access to network resources as well as enable or disable launch of other applications.

To open this window, in the [Firewall settings](#) window click **Edit** next to the **Applications rules** option and click  in the open window or select the application and click .

When Firewall is operating in [training mode](#), you can start creating a new rule directly from the window with notification on an unknown connection attempt.

Launching other applications

To enable or disable launch of other applications, from the **Launching network applications** drop-down list select one of the following:

- **Allow**—if you want to enable the application to run other processes.
- **Block**—if you want to disable the application to run other processes.
- **Not specified**—if you want to use the settings specified for the selected [operation mode](#) of Firewall.



Access to network resources

1. Specify one of the following modes to access network resources:
 - **Allow all**—all connections are allowed.
 - **Block all**—all connections are blocked.
 - **Not specified**—if you want to use the settings specified for the selected [operation mode](#) of Firewall.
 - **User-defined**—enables you to create a set of rules that allow or block different connections.
2. When you select the **User-defined** mode, a table with details on the application rule set displays below.

Parameter	Description
Enabled	Status of the rule.
Action	The action for Dr.Web Firewall to perform when an attempt to connect to the Internet is detected: <ul style="list-style-type: none">• Block packets—block the connection.• Allow packets—allow the connection.
Rule name	The rule name.
Connection type	The direction of the connection: <ul style="list-style-type: none">• Inbound—the rule is applied when someone from the network attempts to connect to an application on your computer.• Outbound—the rule is applied when an application on your computer attempts to connect to the network.• Any—the rule is applied regardless of packet transfer direction.
Description	User description of the rule.

3. If necessary, edit the predefined rule set or create a new one.
4. If you selected to create a new rule set or edit an existing one, [adjust the settings](#) in the open window.
5. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to cancel them. When shifting to another mode, all changes made in the rule set will be kept.



Enable the **Require confirmation on object change (recommended)** option if you want the access to network resources to be confirmed each time when the application is changed or updated.



Rule Settings

Application filtering rules control interaction of a particular application with certain network hosts.

Create and edit rule

To add a new rule in **Edit rule set** window, press . To edit an existing rule, select the appropriate rule and press . Herewith in **Access to network resources** section **User-defined** must be on.

Configure the following parameters:

Parameter	Description
General	
Rule name	The name of the created/edited rule.
Description	The rule description.
Action	The action for Dr.Web Firewall to perform when an attempt to connect to the Internet is detected: <ul style="list-style-type: none">• Block packets—block the connection.• Allow packets—allow the connection.
State	Rule status: <ul style="list-style-type: none">• Enabled—the rule is applied for all matching connections.• Disabled—the rule is temporary not applied.
Connection type	The direction of the connection: <ul style="list-style-type: none">• Inbound—the rule is applied when someone from the network attempts to connect to an application on your computer.• Outbound—the rule is applied when an application on your computer attempts to connect to the network.• Any—the rule is applied regardless of packet transfer direction.
Logging	Logging mode: <ul style="list-style-type: none">• Enabled—register events.• Disabled—do no log rule information.
Rule Settings	
Protocol	The network and transport level protocols used for the connection attempt.



Parameter	Description
	<p>The following protocols of the network level are supported:</p> <ul style="list-style-type: none">• IPv4• IPv6• IP all—any version of the IP protocol <p>The following protocols of the transport level are supported:</p> <ul style="list-style-type: none">• TCP• UDP• TCP & UDP—TCP or UDP protocol• RAW
Local address/Remote address	<p>The IP address of the remote host. You can specify either a certain address (Equal) or several IP addresses using a range (In range), specific subnet mask (Mask) or masks of all subnets in which your computer has a network address (MY_NETWORK).</p> <p>To apply the rule for all remote hosts, select Any.</p>
Local port/Remote port	<p>The port used for the connection. You can specify either a specific port number (Equal) or a port range (In range).</p> <p>To apply the rule for all ports, select Any.</p>

Settings for Networks

Packet filtering allows you to control access to network regardless of what program initiates the connection. These rules are applied to all network packets transmitted through a network interface of your computer.

Thus, packet filtering provides you with more general mechanisms to control access to network than the [application level filtering](#).

Packet Filter

In the **Network** window, you can create a set of rules for filtering packets transmitted through a certain interface.

To open this window from Firewall settings, click **Edit** near **Operation parameters for the known networks**. For the required interface, select the appropriate rule set. If the appropriate rule set does not exist, you can create a new set of packet filtering rules.


Firewall uses the following predefined rule sets:

- **Default Rule**—this rule set is used by default for new [network interfaces](#).



- **Allow All**—this rule set configures the component to pass through all packets.
- **Block All**—this rule set configures the component to block all packets.

For fast switching between filtering modes, you can [create custom sets of filtering rules](#).

To list all available interfaces or add a new interface, click . This opens a window where you can select interfaces that are to be permanently listed in the table. Active interfaces are listed in the table automatically.

You can delete inactive interfaces by pressing  button.

Packet filter settings





To configure the existing rule sets and to add new ones, go to **Packet filter settings** window by clicking **Rule sets** button.

On this page you can:

- [Configure](#) sets of filtering rules by adding new rules, modifying existing ones or deleting them.
- [Configure](#) additional filtering settings.

To configure rule sets

Do one of the following:

- To add a new set of rules for the network interface, click .
- To edit an existing set of rules, select the rule set in the list and click .
- To add a copy of an existing set of rules, select the rule set and click . The copy is added after the selected rule set.
- To delete the selected rule set, click .

Advanced settings

In the **Packet filter settings** window, you can select the following options:

Option	Description
Use TCP stateful packet filtering	<p>Select this check box to filter packets according to the state of existing TCP connections. Firewall will block packets that do not match the TCP protocol specification. This option helps to protect your computer from DoS attacks (denial of service), resource scanning, data injection, and other malicious operations.</p> <p>It is also recommended to enable stateful packet filtering when using complex data transfer protocols (FTP, SIP, etc.).</p>






Option	Description
	Clear this check box to filter packets without regard to the TCP session state.
Management of fragmented IP packets	Select this check box to ensure correct processing of large amounts of data. The maximum transmission unit (MTU) may vary for different networks, therefore large IP packets may be fragmented. When this option is enabled, the rule selected for the first fragment of a large IP packet is applied to all other fragments. Clear this check box to process fragmented packets independently.

Click **OK** to save changes or **Cancel** to exit the window without saving the changes.





The **Edit rule set** window lists packet filtering rules for the selected rule set. You can configure the list by adding new rules or modifying existing ones and the order of their execution. The rules are applied according to their order in the set.

For each rule in the set, the following information is displayed:

Parameter	Description
Enabled	Status of the rule.
Action	The action for Firewall to perform when a packet is intercepted: <ul style="list-style-type: none">• Block packets—block a packet;• Allow packets—allow a packet.
Rule name	The rule name.
Direction	The direction of the connection: <ul style="list-style-type: none">•  —the rule is applied when a packet is received from the network.•  —the rule is applied when a packet is sent into the network from your computer.•  —the rule is applied regardless of packet transfer direction.
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log: <ul style="list-style-type: none">• Headers only—log packet headers only.• Entire packet—log the whole packet.• Disabled—do no log packet information.
Description	The rule description.





To edit and create a rules set

1. If required, add or change the rules set name.
2. Use the following options to create filtering rules:
 - To add a new rule, click . The new rule is added to the beginning of the list.
 - To modify a rule, select it and click .
 - To add a copy of the selected rule, click . The copy is added before the selected rule.
 - To remove the selected rule, click .
3. If you selected to create or edit a rule, [configure the rule settings](#) in the open window.
4. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.
5. When you finish the list adjustments, click **OK** to save changes or **Cancel** to cancel them.



Packets with no rules in a rule set are blocked automatically except for packets allowed by [Application Filter](#) rules.

To add or edit a rule

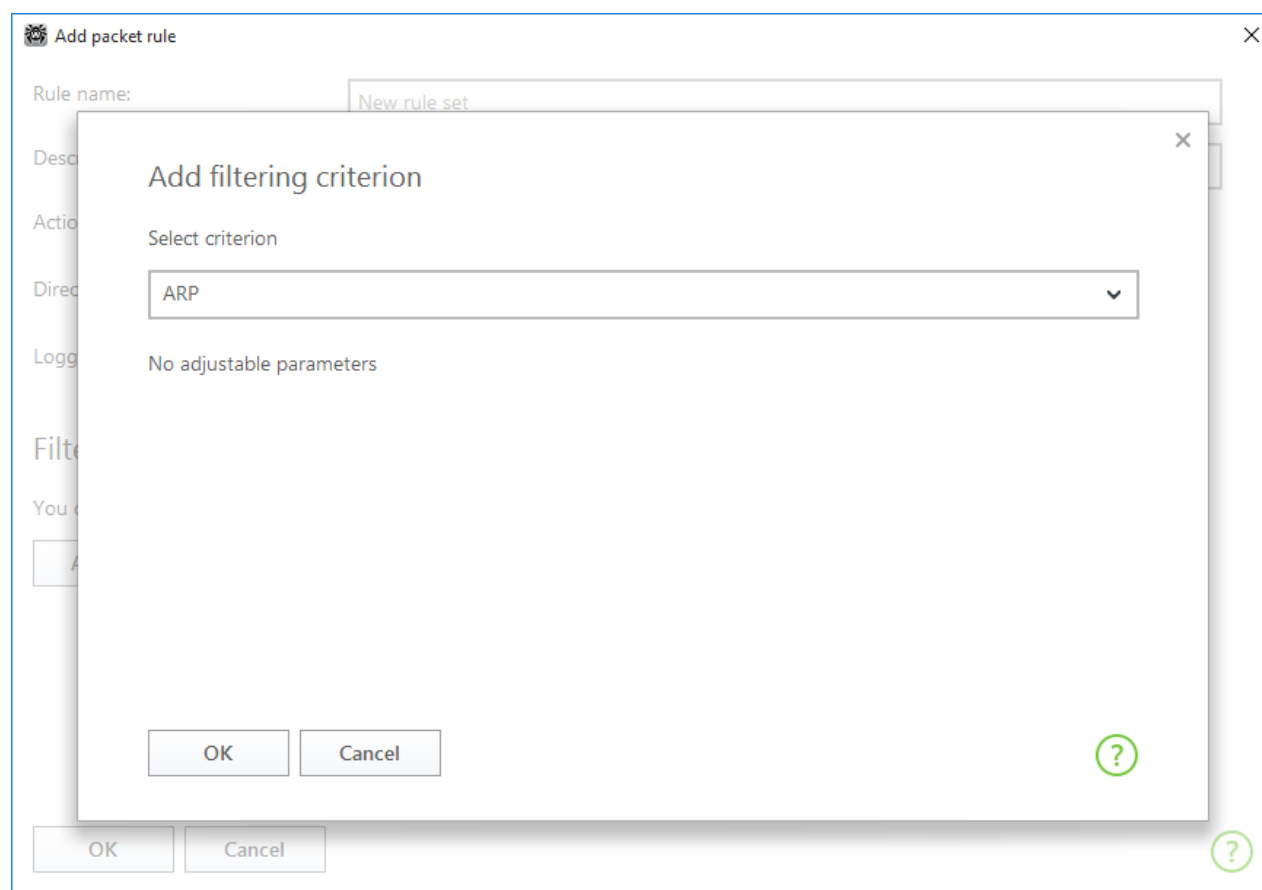
1. In the packet filter rule set creation or modification window, click  or . This opens a rule creation or rule modification window.
2. Configure the following parameters:

Parameter	Description
Rule name	The name of the created/edited rule.
Description	The rule description.
Action	The action for Firewall to perform when a packet is intercepted: <ul style="list-style-type: none">• Block packets—block a packet;• Allow packets—allow a packet.
Direction	The direction of the connection: <ul style="list-style-type: none">• Inbound—the rule is applied when a packet is received from the network.• Outbound—the rule is applied when a packet is sent into the network from your computer.• Any—the rule is applied regardless of packet transfer direction.
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log:



Parameter	Description
	<ul style="list-style-type: none">• Entire packet—log the whole packet.• Headers only—log packet headers only.• Disabled—do no log packet information.

3. You can add a filtering criterion if needed, for example, transport or network protocol, by clicking **Add criterion**. **Add filtering criterion** window will be opened:



Figures 45. Adding filtering criterion

Select the required filtering criterion from the drop-down list. In this window, you can also configure parameters for the selected criterion. You can add any number of filtering criteria. Herewith, the packet should meet all the criteria of the rule in order for the rule action to be applied to the packet.

For certain headers, there are additional criteria available. All added criteria are listed in the edit packet rule window and can be modified.

4. When you finish the adjustments, click **OK** to save changes or **Cancel** to exit the window without saving the changes.



If you do not add any criterion, the rule will allow or block all packets depending on the setting specified in the **Action** field.



If you select **Any** for the **Local IP address** and **Remote IP address** fields, the rule is applied for any packet which contains an IPv4 header and was sent from a physical address of the local computer.

13.6. Dr.Web for Microsoft Outlook

Main functions

The Dr.Web for Microsoft Outlook plug-in performs the following functions:

- Anti-virus check of incoming email attachments;
- Check of email attachments transferred over encrypted SSL connections;
- Spam check;
- malware detection and its neutralization;
- Heuristic analysis for additional protection against unknown viruses.

Configuring Dr.Web for Microsoft Outlook plug-in

You can set up parameters of plug-in operation and view statistics on Microsoft Outlook mail application, in the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select Dr.Web for Microsoft Outlook and click the **Add-in Options** button).



The **Dr.Web Anti-virus** page of Microsoft Outlook settings is active only if the user has permissions to change these settings.

On the **Dr.Web Anti-virus** page, the current protection status is displayed (enabled/disabled). This page also provides access to the following program functions:

- [Log](#)—allows to configure the program logging.
- [Check attachments](#) — allows to configure email check and to specify program actions on detection of malicious objects;
- [Spam filter](#)—allows to specify program actions on spam detection and to create black and white lists of email addresses.
- [Statistics](#)—allows to view the number of checked and processed objects.

13.6.1. Virus Check

Dr.Web for Microsoft Outlook uses different [detection methods](#). Infected objects are processed according to the actions defined by the user: the program can cure such objects, remove them, or move them to [Quarantine](#) to isolate the objects from the rest of the system.

Dr.Web for Microsoft Outlook detects the following malicious objects:



- Infected objects
- Bomb viruses in files or archives
- Adware
- Hacktools
- Dialers
- Jokes
- Riskware
- Spyware
- Trojans
- Computer worms and viruses

Actions

Dr.Web for Microsoft Outlook allows to specify program reaction to detection of infected or suspicious files and malicious objects in email attachments.

To configure virus check of email attachments and to specify program actions for detected malicious objects, in the Microsoft Outlook mail application, go to the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select Dr.Web for Microsoft Outlook, then click the **Add-in Options** button) and click **Check attachments**.



The **Check attachments** window is available only for users with administrative privileges.

For Windows Vista and later operating systems, after clicking **Check attachments**:

- If UAC is enabled: administrator is requested to confirm program actions; user without administrative privileges is requested to enter system administrator credentials.
- If UAC is disabled: administrator can change program settings; user does not have the permission to change program settings.

In the **Check attachments** window, specify actions for different types of checked objects and also for the check failure. You can also enable/disable check of archives.

To set actions to be applied on threat detection, use the following options:

- The **Infected** drop-down list sets the reaction to the detection of a file infected with a known and (presumably) curable virus.
- The **Not cured** drop-down list sets the reaction to the detection of a file infected with a known incurable virus (and in case an attempt to cure a file failed).
- The **Suspicious** drop-down list sets the reaction to the detection of a file presumably infected with a virus (upon reaction of the heuristic analyzer).



- In the **Malware** section, set a reaction to detection of unsolicited software of the following types:
 - Adware
 - Dialers
 - Jokes
 - Hacktools
 - Riskware
- The **If check failed** drop-down list allows to configure actions if the attachment cannot be checked, that is, if the attached file is corrupted or password protected.
- The **Check archives (recommended)** check box allows to enable or disable check of attached archived files. Select this check box to enable checking; clear this check box to disable.

For different types of objects, actions are specified separately.

The following actions for detected virus threats are available:

- **Cure** (only for infected objects)—instructs to try to restore the original state of an object before infection.
- **As incurable** (only for infected objects)—instructs to apply the action specified for incurable objects.
- **Delete**—delete the object.
- **Move to quarantine**—move the object to the special [Quarantine](#) folder.
- **Skip**—skip the object without performing any action or displaying a notification.

13.6.2. Spam Check

Dr.Web for Microsoft Outlook checks emails for spam by means of Dr.Web Anti-spam and filters messages according to the user-defined [settings](#).

To configure spam check, go to the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select Dr.Web for Microsoft Outlook and click the **Add-in Options** button) and click **Spam filter**. The [Spam filter](#) window opens.



The **Spam filter** window is available only for users with administrative privileges.

For Windows Vista and later operating systems, after clicking **Check attachments**:

- If UAC is enabled: administrator is requested to confirm program actions; user without administrative privileges is requested to enter system administrator credentials.
- If UAC is disabled: administrator can change program settings; user does not have the permission to change program settings.



Spam Filter Settings

To configure spam filter operation settings

- Select the **Check for spam** check box to enable the spam filter.
- You can add special text to the spam message header by enabling the **Add prefix to message header** option. Text of the added prefix is specified to the right of the option. The default prefix is *****SPAM*****.
- The checked messages can be marked as read in message options. For that purpose, enable the **Mark message as read** option. This option is enabled by default.
- You can also configure [white and black lists](#) for message filtration.



If spam filter processes certain messages incorrectly, you are advised to forward such messages to special email addresses for analysis and improvement of filtering methods.

- messages that are wrongly regarded as spam should be forwarded to vrnospam@drweb.com;
- unblocked spam messages should be forwarded to vrspam@drweb.com.

Forward messages as attachments, that is, do not include them in the message body.

Black and White Lists

Black and white lists are used for message filtration.

To review and to edit the white and black lists, in the [spam filter window](#) click **White list** or **Black list** respectively.

To add an address to the white or black list:

1. Click **Add**.
2. Enter the email address in the corresponding field.
3. Click **OK** in the **Edit list** window.

To change an address on the list:

1. Select the address you want to change and click **Edit**.
2. Make necessary changes to the information.
3. Click **OK** in the **Edit list** window.

To remove an address from the list:

1. Select the address from the list.



2. Click **Delete**.

In the **Black and White lists** window, click **OK** to save the changes.

White list

However, if the domain names in the receiver's and sender's addresses are similar, and this domain name is specified in the white list using the (*) character, this message is checked for spam. Details:

- To add a specific sender, enter the full email address (for example, `mail@example.net`). This ensures delivery of all messages from this sender.
- Each list item can contain only one address or address mask.
- To add a group of sender addresses, enter the mask that determines their names. The mask defines a template for an object definition. It may contain regular characters from email addresses and a special asterisk character (*), which replaces any (including an empty one) sequence of characters.

For example, the following variations are possible:

- `mailbox@domain.com`
- `*box@domain.com`
- `mailbox@dom*`
- `*box@dom*`



The asterisk (*) can be specified at the start or at the end of an address only.

The 'at' sign (@) is mandatory.

- To ensure delivery of messages sent from any email address within a certain domain, use an asterisk (*) instead of the username in the address. For example, if you enter `*@example.net`, messages from all senders within the example.net domain will be delivered without scanning.
- To ensure delivery of messages sent from email address with a certain user name from any domain, use an asterisk (*) instead of the domain name in the address. For example, if you want to receive messages from all senders with the "someone" mailbox, enter `name@*`.

Black list

If the sender's address is on the black list, the message will be automatically regarded as spam. Details:

- To add a specific sender, enter the full email address (for example, `spam@spam.com`). All messages, received from these addresses, will be automatically regarded as spam.
- Each list item can contain only one address or address mask.
- To add a group of sender addresses, enter the mask that determines their names. The mask defines a template for an object definition. It may contain regular characters from email addresses



and a special asterisk character (*), which replaces any (including an empty one) sequence of characters.

For example, the following variations are possible:

- mailbox@domain.com
- *box@domain.com
- mailbox@dom*
- *box@dom*



The asterisk (*) can be specified at the start or at the end of an address only.

The 'at' sign (@) is mandatory.

- To regard messages sent from any email address within a domain as spam, use an asterisk character (*) instead of the username in the address. For example, if you enter *@spam.com, all messages from addresses within the spam.com domain will be regarded as spam automatically.
- To regard messages sent from an email address with a certain user name from any domain as spam, enter an asterisk character (*) instead of the domain name in the address. For example, if you enter name@*, all messages from all senders with the "someone" mailbox name will be regarded as spam automatically.
- Addresses from the recipient domain are not processed. For example, if the recipient mailbox (your mailbox) is in the mail.com domain, then messages from mail.com domain will not be processed with the anti-spam filter.

13.6.3. Event Logging

Dr.Web for Microsoft Outlook registers errors and application events in the following logs:

- [Windows Event Log](#)
- [Debug Text Log](#)

Event Log

The following information is registered in the Windows Event Log:

- Program starts and stops;
- Key file parameters: license validation, license expiration date (information is logged on program startup, while the program is running, and when the key file is changed);
- Parameters of program modules: scanner, engine, virus databases (information is logged on program startup and module update);
- License errors: the key file is absent, permission for program module usage is absent in the key file, the license is blocked, the key file is corrupted (information is logged on program startup and while the program is running);



- Information on threat detection;
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2, and 1 days before expiration).

To view Windows Event Log

1. Open **Control Panel** of the operating system.
2. Select **Administrative Tools** → **Event Viewer**.
3. In the tree view, select **Application**. The list of events, registered in the log file by user applications, opens. The source of Dr.Web for Microsoft Outlook messages is the Dr.Web for Microsoft Outlook application.

Debug Text Log

The following information is registered in the debug log:

- License validity status;
- Information on threat detection;
- Read/write errors or errors occurred while scanning archives or password-protected files;
- Parameters of program modules: scanner, engine, virus databases;
- Core failures;
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2, and 1 days before expiration).

Configure logging

1. On the **Dr.Web Anti-virus** tab, click **Log**. The window with logging settings opens.
2. To set the maximum detailing for the logging, select the **Detailed logging** check box. By default, logging is set to regular mode.



The maximum detailing for the logging decreases server performance; therefore, it is recommended to enable detailed logging only in case an error in operation of Dr.Web for Microsoft Outlook occurs.

3. Click **OK** to save changes.



The **Log** window is available only for users with administrative privileges.

For Windows Vista and later operating systems, after clicking **Log**:

- If UAC is enabled: administrator is requested to confirm program actions; user without administrative privileges is requested to enter system administrator credentials.



- If UAC is disabled: administrator can change program settings; user does not have the permission to change program settings.

View program log

To open the text log, click **Show in folder**. The folder with the log opens.

13.6.4. Statistics

In the Microsoft Outlook mail application, on the **Tools** → **Options** → **Dr.Web Anti-virus** page (in Microsoft Outlook 2010, go to **Files** → **Options** → **Add-ins**, select **Dr.Web for Microsoft Outlook** and click the **Add-in Options** button), statistic information about total number of objects, which have been checked and processed by the program, is listed.

These scanned objects are classified as follows:

- **Checked**—total number of checked messages.
- **Infected**—number of messages with viruses.
- **Suspicious**—number of messages presumably infected with a virus (upon a reaction of the heuristic analyzer).
- **Cured**—number of objects successfully cured by the program.
- **Not checked**—number of objects which cannot be checked or check of which failed due to an error.
- **Clear**—number of messages which are not infected.

Then the number of processed objects is specified:

- **Moved**—number of objects moved to Quarantine.
- **Deleted**—number of objects removed from the system.
- **Skipped**—number of objects skipped without changes.
- **Spam messages**—number of objects detected as spam.

By default, statistics is saved to the drwebforoutlook.stat file located in the %USERPROFILE%\Doctor Web folder.



Statistics accumulates during a session. It is reset to zero if the computer or Dr.Web Agent for Windows is restarted.

13.7. Preventive Protection

On this page, you can configure Dr.Web reaction to such actions of other programs that can compromise security of your computer and select protection level against exploits.

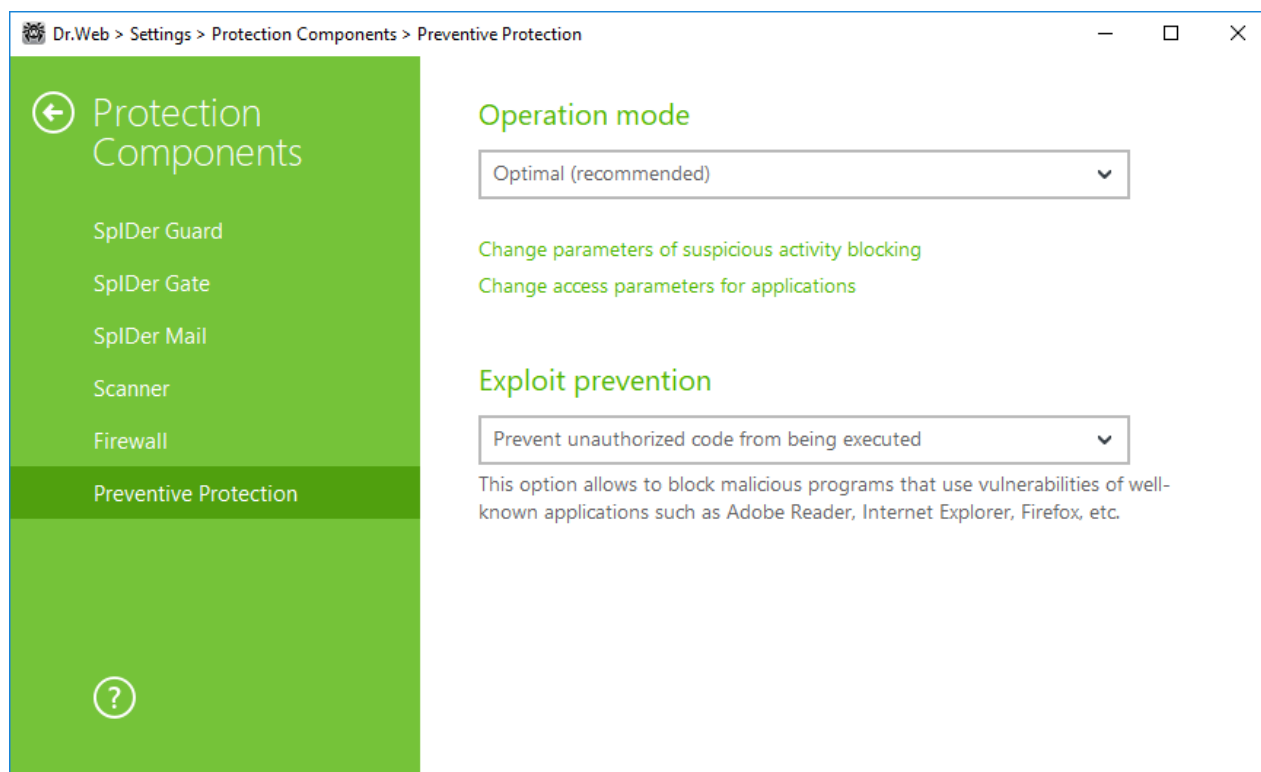



Figure 46. Preventive Protection settings

At that, you can configure a separate protection mode for particular applications or configure a general mode whose settings will be applied to all other processes.


To configure the general mode, select it from the **Operation mode** list or click **Change parameters of suspicious activity blocking**. As a result of the second action, a window opens providing you with details on each mode and editing options. All changes are saved in the User mode. In this window, you can also create a new profile for saving necessary settings.

To create a new profile

1. Click .
2. In the open window, enter a name for the new profile.
3. Look through default settings and, if necessary, edit them.

To configure preventive protection settings for particular applications, click **Change access parameters for applications**. In the open window, you can add a new rule or edit or delete an existing rule.

To add a rule

1. Click .
2. In the open window, click **Browse** and specify the path to the application executable file.
3. Look through default settings and, if necessary, edit them.



To edit an existing rule, select it from the list and click .

To delete an existing rule, select it from the list and click .

For more information about settings of each operation mode, refer to the Preventive Protection Level section.

Preventive protection level

In the mode **Optimal** mode, which is set by default Dr.Web disables automatic changes of system objects, whose modification explicitly signifies a malicious attempt to harm the operating system. It also blocks low-level access to disk and protects the HOSTS file from modification.



Only actions by the applications that are not trusted, are blocked.

If there is a high risk of your computer getting infected, you can increase protection by selecting the **Medium**. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.



Using this mode may lead to compatibility problems with legitimate software that uses the protected registry branches.

When required to have total control of access to critical Windows objects, you can select the **Paranoid**. In this mode, Dr.Web also provides you with interactive control over loading of drivers and automatic running of programs.

With the **User-defined** mode, you can set a custom protection level for various objects.

Protected object	Description
Integrity of running applications	This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored.
Integrity of user files	This option allows detection of processes that modify user files with the known algorithm, which indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored. To protect your data from modification, you can enable creation of protected copies that contain important data.
HOSTS file	The operating system uses the HOSTS file when connecting to the Internet. Changes to this file may indicate virus infection.



Protected object	Description
Low level disk access	Block applications from writing on disks by sectors while avoiding the file system.
Drivers loading	Block applications from loading new or unknown drivers.
Critical Windows objects	<p>Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).</p> <p>Image File Execution Options:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>User Drivers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Winlogon registry keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Winlogon notifiers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Windows registry startup keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib <p>Executable file associations:</p> <ul style="list-style-type: none">• Software\Classes\exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) <p>Software Restriction Policies (SRP):</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer <p>Browser Helper Objects for Internet Explorer (BHO):</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>Autorun of programs:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup



Protected object	Description
	<ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup• Software\Microsoft\Windows\CurrentVersion\RunServices• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce Autorun of policies: <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Safe mode configuration: <ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal• SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager parameters: <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows System services: <ul style="list-style-type: none">• System\CurrentControlXXX\Services



If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), temporarily disable Preventive Protection.

If necessary, you can [configure](#) desktop and email notifications on Preventive Protection actions.

Exploit prevention

This option allows to block malicious programs that use vulnerabilities of well-known applications. From the corresponding drop-down list, select the required level of protection.

Protection level	Description
Prevent unauthorized code from being executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be blocked automatically.
Interactive mode	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, Dr.Web will display an appropriate message. Read the information and select a suitable action.





Allow unauthorized code to be executed

If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be allowed automatically.



14. Statistics

This window contains the statistics on important events of protection components operation.

To view statistics on the components operation, open the menu  then go to **Statistics** . On the **Statistics** page, reports for the following groups are available:

- Threats
- Update
- Parental Control


A detailed report is available for the **Threats** and **Update** groups. You can also apply filters to these reports.

In the **Parental Control** group, you can view the statistics of blocked URLs for every user account.

The following information is logged in the report:

- Frequency of visits;
- Action;
- URL.

All the report entries have preset filters that are available in a drop-down list on the top of a page.

Click  to remove, copy, export selected events or a report file, or clear a report.

Network activity

You can view the report of network activity if Dr.Web Firewall is installed on your computer.

To view information on active applications, an application log, and a packet filter log, select necessary object from the drop-down list.

The report shows the following information for every active application:

- Direction
- Operation protocol
- Local address
- Remote address
- Size of sent data packet
- Size of received data packet

The application log stores the following data:

- Application start time
- Application name




- Application processing rule name
- Direction
- Action
- Endpoint


Packet Filter Log shows the following information:

- Start time of data packet processing
- Direction
- Processing rule name
- Interface
- Packet data

Click  to export or clear logs.

Detailed report


To view a detailed report about Dr.Web operation events, choose a necessary event and click . Click the button again to hide the detailed report.

Click  to remove, copy, export selected events or a report file, or clear a report.

You can use filters to select a certain event.

Filters

To view a list of only those events that correspond to specific parameters, use filters. All the reports have preset filters that are available in a drop-down list on the top of a page.

You can create custom event filters. To create a new filter, click , select **Create** in a drop-down list, and then specify necessary filtering criteria. In the **Component** field, you can specify several components at once.

Events can be filtered by codes. To do this, specify them in the **Code (Example: 100-103, -102, 403)** field according to the following rules:

- Codes can be separated by commas
- You can specify a range of necessary codes (for example, 100-103).
- A code can be excluded from the range by using the - symbol

Therefore, "100-103, -102, 403" means to show all events from 100 to 103, exclude the "-102" code from filtering and show the event "403".

All custom filters can be edited or removed.



15. Technical support

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

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

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

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

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



16. Appendix A. Additional Command-Line Parameters

Additional command-line parameters (switches) are used to set parameters for programs, which can be launched by opening an executable file. This relates to Dr.Web Scanner, Console Scanner and Dr.Web Updater. The switches can set parameters that are either not present in the configuration file or have a higher priority than those specified in the file.

Switches begin with the forward slash (/) character and are separated by spaces as other command-line parameters.

16.1. Scanner and Console Scanner Parameters

Switch	Description
/AA	Apply actions to detected threats automatically. (For Scanner only.)
/AC	Scan installation packages. Option is enabled by default.
/AFS	Use forward slash to separate paths in an archive. Option is disabled by default.
/AR	Scan archives. Option is enabled by default.
/ARC: <compression_ratio>	Maximum compression level. If the compression ratio of the archive exceeds the limit, Scanner neither unpacks nor scans the archive. By default: unlimited.
/ARL: <nesting_level>	Maximum archive nesting level. By default: unlimited.
/ARS: <size>	Maximum archive size (in KB). By default: unlimited.
/ART: <size>	Minimum size of a file inside an archive beginning from which compression ratio check is performed (in KB). By default: unlimited.
/ARX: <size>	Maximum size of a file inside an archive that is scanned (in KB). By default: unlimited.
/BI	Show information on virus databases. Option is enabled by default.
/CUSTOM	Perform a custom scan. If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), only the specified objects will be scanned. (For Scanner only.)



Switch	Description
/CL	Use cloud checking. Option is enabled by default. (For Console Scanner only.)
/DCT	Do not display estimated scan time. (For Console Scanner only.)
/DR	Scan folders recursively (scan subfolders). Option is enabled by default.
/E: <number_of_threads>	Perform scanning in specified number of threads.
/FAST	Perform an express scan of the system. If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), the specified objects will also be scanned. (For Scanner only.)
/FL: <file_name>	Scan paths listed in the specified file.
/FM: <mask>	Scan files matching the specified mask. By default, all files are scanned.
/FR: <regexpr>	Scan files matching the specified regular expression. By default, all files are scanned.
/FULL	Perform a full scan of all hard drives and removable media (including boot sectors). If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), an express scan will be performed, and the specified objects will be scanned. (For Scanner only.)
/FX: <mask>	Exclude from scan files that match the specified mask. (For Console Scanner only.)
/GO	Scanner operation mode that skips the questions that require answers from a user; decisions that require a selection are made automatically. This mode is useful for the automatic file scan; for example, for the daily or weekly hard disk scanning. An object for scanning must be indicated in the command line. Along with the /GO parameter, it is also possible to use the following parameters: /LITE, /FAST, /FULL. In this mode, the scanning stops when switching to the battery power.
/H or /?	Show brief help. (For Console Scanner only.)
/HA	Use heuristic analysis to detect unknown threats. Option is enabled by default.



Switch	Description
/KEY: <key_file>	Specify a path to the key file. It is necessary to use this parameter if your key file is stored outside of the installation folder where the scanner executables reside. By default, drweb32.key or another suitable file from the C:\Program Files\DrWeb\ folder is used.
/LITE	Perform a basic scan of random access memory and boot sectors of all disks as well as run a scan for rootkits. (For Scanner only.)
/LN	Resolve shell links. Option is disabled by default.
/LS	Scan using LocalSystem account rights. Option is disabled by default.
/MA	Scan mail files. Option is enabled by default.
/MC: <number_of_attempts>	Set the maximum number of cure attempts. By default: unlimited.
/NB	Do not backup cured or deleted files. Option is disabled by default.
/NI [:X]	Limits usage of system resources at scanning (%). Defines the amount of memory required for scanning and the system priority of scanning process. By default: unlimited.
/NOREBOOT	Cancel system reboot or shutdown after scanning. (For Scanner only.)
/NT	Scan NTFS streams. Option is enabled by default.
OK	Show the full list of scanned objects and mark clean files with Ok. Option is disabled by default.
/P: <priority>	Priority of the current scanning task. Can be as follows: 0—the lowest. L—low. N—normal (default priority). H—high. M—maximal.
/PAL: <nesting_level>	Maximum nesting level for executable packers. If a nesting level is greater than the specified value, scanning proceeds until this limit is reached. The nesting level is 1,000 by default.



Switch	Description
/QL	Show the list of files quarantined on all disks. (For Console Scanner only.)
/QL: <logical_drive_letter>	Show the list of files quarantined on the specified logical drive. (For Console Scanner only.)
/QNA	Double quote paths.
/QR[:[d]][:p]]	Delete quarantined files on drive <d> (logical_drive_letter) that are older than <p> (number) days. If <d> and <p> are not specified, all quarantined files on all drives are deleted. (For Console Scanner only.)
/QUIT	/QUIT—terminate Scanner once scanning is complete regardless of whether or not any actions have been applied to the detected threats. (For Scanner only.)
/RA: <file_name>	Append the report on program operation to the specified file. By default, logging is disabled.
/REP	Follow symbolic links while scanning. Option is disabled by default.
/RK	Scan for rootkits. Option is disabled by default.
/RP: <file_name>	Append the report on program operation to the specified file. By default, logging is disabled.
/RPC: <sec>	Scanning Engine connection timeout. Timeout is 30 seconds by default. (For Console Scanner only.)
/RPCD	Use dynamic RPC identification. (For Console Scanner only.)
/RPCE	Use dynamic RPC endpoint. (For Console Scanner only.)
/RPCE: <target_address>	Use specified RPC endpoint. (For Console Scanner only.)
/RPCH: <host_name>	Use specified host name for remote call. (For Console Scanner only.)
/RPCP: <protocol>	Use specified RPC protocol. Possible protocols are as follows: lpc, np, tcp. (For Console Scanner only.)
/SCC	Show content of complex objects. Option is disabled by default.
/SCN	Show installation package name. Option is disabled by default.



Switch	Description
/SLS	Show logs on the screen. Option is enabled by default. (For Console Scanner only.)
/SPN	Show packer name. Option is disabled by default.
/SPS	Display the scan progress on the screen. Option is enabled by default. (For Console Scanner only.)
/SST	Sisplay object scan time. Option is disabled by default.
/ST	Start of Scanner in the background mode. If the /GO parameter is not set, the graphical mode is displayed only in case of threat detection. In this mode, the scanning stops when switching to the battery power.
/TB	Scan boot sectors including master boot record (MBR) of the hard drive.
/TM	Scan processes in memory including Windows system control area.
/TR	Scan system restore points.
/W: <sec>	Maximum time to scan (sec.). By default: unlimited.
/WCL	drwebwcl compatible output. (For Console Scanner only.)
/X:S[:R]	Set one of the following states for the computer to enter once scanning is complete: Shutdown/Reboot/Suspend/Hibernate.

The following actions can be specified for different objects ('C'—cure, 'Q'—move to quarantine, 'D'—delete, 'I'—ignore, 'R'—inform; 'R' is available for Console Scanner only; 'R' is set by default for all objects in Console Scanner):

Action	Description
/AAD:<action>	action for adware (possible: DQIR)
/AAR:<action>	action for infected archives (possible: DQIR)
/ACN:<action>	action for infected installation packages (possible: DQIR)
/ADL:<action>	action for dialers (possible: DQIR)
/AHT:<action>	action for hacktools (possible: DQIR)



Action	Description
/AIC:<action>	action for incurable files (possible: DQR)
/AIN:<action>	action for infected files (possible: CDQR)
/AJK:<action>	action for jokes (possible: DQIR)
/AML:<action>	action for infected mail files (possible: QIR)
/ARW:<action>	action for riskware (possible: DQIR)
/ASU:<action>	action for suspicious files (possible: DQIR)

Several switches can have modifiers that explicitly enable or disable options specified by these switches. For example, as follows:

/AC-	option is clearly disabled
/AC, /AC+	option is clearly enabled

These modifiers can be useful if the option was enabled or disabled by default or was set in the configuration file earlier. The following switches can have modifiers:

/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.

For /FL parameter '-' modifier directs to scan the paths listed in the specified file and then delete this file.

For /ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W parameters "0" value means that there is no limit.

The following example shows how to use command-line switches with Console Scanner:

```
[<path_to_program>]dwscancl /AR- /AIN:C /AIC:Q C:\
```

scan all files on disk 'C:', excluding those in archives; cure the infected files and move to quarantine those that cannot be cured. To run Scanner the same way, enter the `dwscancl` command name instead of `dwscanner`.



16.2. Dr.Web Updater Command-Line Parameters

Common options

Parameter	Description
-h [--help]	Show a short help message on how to use the program.
-v [--verbosity] arg	Log level. Can be one of following: error (standard), info (extended), debug.
-d [--data-dir] arg	Folder where repository and settings are located.
--log-dir arg	Folder for storing the log file.
--log-file arg (=dwupdater.log)	Log file name.
-r [--repo-dir] arg	Repository folder (<data_dir>/repo by default).
-t [--trace]	Enable tracing.
-c [--command] arg (=update)	Command to execute: getversions, getcomponents, init, update, uninstall, exec, keyupdate, and download.
-z [--zone] arg	Zones that are to be used instead of those specified in the configuration file.

init command parameters

Parameter	Description
-s [--version] arg	Version number.
-p [--product] arg	Product name.
-a [--path] arg	Product directory path. This folder will be used as the default directory for all components included in the product. Dr.Web Updater will search for a key file in this directory.
-n [--component] arg	Component name and installation folder. <name>, <install path>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-g [--proxy] arg	Proxy server for updating. <Address>:<port>.



Parameter	Description
-e [--exclude] arg	Component name that will be excluded from the product during installation.

update command parameters

Parameter	Description
-p [--product] arg	Product name. If specified, only this product will be updated. If neither a product nor certain components are specified, all products will be updated. If certain components are specified, only they will be updated.
-n [--component] arg	Components that are to be updated to the specified version. <Name>, <target revision>.
-x [--selfrestart] arg (=yes)	Reboot after an update of Dr.Web Updater. Default value is <code>yes</code> . If the value is set to <code>no</code> , notification that reboot is required will appear.
--geo-update	Get the list of IP addresses from update.drweb.com before updating.
--type arg (=normal)	Can be one of the following: <ul style="list-style-type: none">• Reset-all—forced update of all components• Reset-failed—reset revision for damaged components• Normal-failed—try to update all components including damaged from the current revision to the newest or specified• Update-revision—try to update all components of the current revision to the newest if exists• Normal—update all components
-g [--proxy] arg	Proxy server for updating. <Address>:<port>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
--param arg	Pass additional parameters to the script. <Name>: <value>.
-l [--progress-to-console]	Print information about downloading and script execution to the console.



Getcomponents command parameters

Parameter	Description
-s [--version] arg	Version number.
-p [--product] arg	Specify the product to get the list of components that are included in this product. If the product is not specified, all components of this version will be listed.

getrevisions command parameters

Parameter	Description
-s [--version] arg	Version number.
-n [--component] arg	Component name.

uninstall command parameters

Parameter	Description
-n [--component] arg	Name of the component that is to be uninstalled.
-l [--progress-to-console]	Print information about command execution to the console.
--param arg	Pass additional parameters to the script. <Name>: <value>.
-e [--add-to-exclude]	Components to be deleted. Update of this components will not be performed.

keyupdate command parameters

Parameter	Description
-m [--md5] arg	MD5 hash of the previous key file.
-o [--output] arg	Output file name to store new key.
-b [--backup]	Backup of an old key file if exists.
-g [--proxy] arg	Proxy server for updating. <Address>:<port>.



Parameter	Description
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-l [--progress-to-console]	Print information about downloading of the key file to the console.

download command parameters

Parameter	Description
--zones arg	Zone description file.
--key-dir arg	Folder where the key file is located.
-l [--progress-to-console]	Print information about command execution to the console.
-g [--proxy] arg	Proxy server for updating. <Address>:<port>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-s [--version] arg	Version name.
-p [--product] arg	Name of the product to download.

16.3. Return Codes

The values of the return code and corresponding events are as follows:

Return code value	Event
0	OK, no virus found.
1	Known virus detected.
2	Modification of known virus detected.
4	Suspicious object found.
8	Known virus detected in file archive, mail archive, or container.
16	Modification of known virus detected in file archive, mail archive, or container.



Return code value	Event
32	Suspicious file found in file archive, mail archive, or container.
64	At least one infected object successfully cured.
128	At least one infected or suspicious file deleted/renamed/moved.

The actual value returned by the program is equal to the sum of codes for the events that occurred during scanning. Obviously, the sum can be easily decomposed into separate event codes.

For example, return code $9 = 1 + 8$ means that known viruses were detected, including viruses in archives, mail archives or containers; curing and others actions were not executed; no other "virus" events occurred during scanning.



17. Appendix B. Computer Threats and Neutralization Methods

With the development of computer technologies and network solutions malicious programs (malware) of different kinds, meant to strafe users, become more and more widespread. Their development began together with computer science and facilities of protection against them progressed alongside. Nevertheless, there is still no common classification for all possible threats due to their unpredictable development character and constant improvement of applicable technologies.

Malicious programs can be distributed through the Internet, local area networks, email and portable data mediums. Some of them rely on the user's carelessness and lack of experience and can be run in completely automatic mode. Others are tools controlled by a computer cracker and they can harm even the most secure systems.

This chapter describes all of the most common and widespread types of malware, against which products of Doctor Web are aimed.

17.1. Classification of Computer Threats

Herein, the term "threat" defines any kind of software that can potentially or directly inflict damage on a computer or network or compromise the user's information or rights (in other words, malicious and other unwanted programs). However, generally speaking, the term "threat" may be used to indicate any potential danger to computer or network security (that is, vulnerabilities that can be exploited to launch attacks).

All program types described below have the ability to endanger the user's data or confidentiality. Programs that do not hide their presence from the user (for example, spam-sending software or traffic analyzers) usually are not considered to be computer threats, although they can become threats under certain circumstances.

In the documentation and products by Doctor Web, threats are divided into two categories in accordance with the severity of danger they pose.

- **Major threats** are classic computer threats that can perform destructive or illegal actions in the system on their own (erase or steal important data, crash networks, and so on). To this type of computer threats belong programs that are traditionally referred to as "malicious" (viruses, worms, and Trojans).
- **Minor threats** are less dangerous than major threats, but may be used by a third party to carry out malicious activities. Moreover, mere presence of minor threats in the system indicates its low protection level. Information security specialists sometimes refer to this type of threats as "grayware" or potentially unwanted programs. This category consists of adware, dialers, jokes, riskware, and hacktools.



Major threats

Computer viruses

This type of computer threats is characterized by their ability to inject malicious code into running processes of other programs. This action is called *infection*. In most cases, the infected file becomes a virus carrier itself, and the injected code does not necessarily match the original one. The majority of viruses are created with a purpose to damage or destroy data in the system.

Doctor Web divides viruses by the type of objects they infect into the following categories:

- **File viruses** infect operating system files (usually, executable files and dynamic-link libraries) and are activated when an infected file is run.
- **Micro viruses** infect documents used by Microsoft® Office or other programs supporting macro commands (usually, written in Visual Basic). Macro commands are a type of built-in programs (macros) that are written in a fully functional programming language and can be launched under specific circumstances (for example, in Microsoft® Word, macros can be activated upon opening, closing, or saving a document).
- **Script viruses** are created using script languages, and, mostly, they infect other scripts (such as OS service files). By exploiting vulnerable scripts in web applications, they can also infect other file types that support script execution.
- **Boot viruses** infect boot sectors of disks and partitions or master boot records of hard disks. They require little memory and can perform their tasks until the operating system is rolled out, restarted, or shut down.

Most viruses have special mechanisms that protect them against detection. These mechanisms are constantly improved, and ways to overcome them are constantly developed. According to the type of protection they use, all viruses can be divided into two following groups:

- **Encrypted viruses** self-encrypt their malicious code upon every infection to make its detection in a file, boot sector, or memory more difficult. Each sample of such viruses contains only a short common code fragment (decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** use a special decryption procedure in addition to code encryption. This procedure is different in every new virus copy. This means that such viruses do not have byte signatures.

Viruses can also be classified according to the language they are written in (most viruses are written in Assembly, high-level programming languages, script languages, and so on) and operating systems that can be infected by these viruses.

Computer worms

Recently, worms have become much more widespread than viruses and other malicious programs. Like viruses, these malicious programs can replicate themselves. A worm infiltrates a computer from



a network (usually, as an email attachment) and spreads its functional copies among other computers. Distribution can be triggered by some user action or automatically.

Worms do not necessarily consist of only one file (the worm's body). Many of them have a so-called infectious part (shellcode) that is loaded into the main memory. After that, it 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 easily removed by restarting the system (at that, RAM is reset). However, if the worm's body infiltrates the computer, only an anti-virus program can fight it.

Even if worms do not bear any payload (do not cause direct damage to a system), they can still cripple entire networks because of how intensely they spread.

Doctor Web classifies worms in accordance with their distribution methods as follows:

- **Network worms** spread via various network and file-sharing protocols.
- **Mail worms** spread via mail protocols (POP3, SMTP, and others).

Trojan programs (Trojans)

These programs cannot replicate themselves. However, they can perform malicious actions on their own (damage or delete data, forward confidential information, and others) or provide cybercriminals with authorized access to a computer to harm a third party.

Like viruses, these programs can perform various malicious activities, hide their presence from the user, and even be a virus component. However, usually, Trojans are distributed as separate executable files (through file-exchange servers, data carriers, or email attachments) that are run by users themselves or by some specific system process.

Here are some Trojan types divided by Doctor Web into separate categories as follows:

- **Backdoors** are Trojans that allow an intruder to get privileged access to the system bypassing any existing protection mechanisms. Backdoors do not infect files—they register themselves in the registry modifying registry keys.
- **Droppers** are file carriers that contain malicious programs in their bodies. Once launched, a dropper copies malicious files to a hard disk without user consent and runs them.
- **Keyloggers** can log data that users enter by means of a keyboard. These malicious programs can steal various confidential information (including network passwords, logins, bank card data, and so on).
- **Clickers** redirect users to specified Internet resources (may be malicious) in order to increase traffic to those websites or to perform DoS attacks.
- **Proxy Trojans** provide cybercriminals with anonymous Internet access via the victim's computer.
- **Rootkits** are used to intercept operating system functions in order to hide their presence. Moreover, a rootkit can conceal processes of other programs, registry keys, folders, and files. It can be distributed either as an independent program or as a component of another malicious application. Based on the operation mode, rootkits can be divided into two following categories: User Mode Rootkits (UMR) that operate in user mode (intercept functions of user-mode libraries)



and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions at the system kernel level, which makes these malicious programs hard to detect).

Trojans can also perform other malicious actions besides those listed above. For example, they can change the browser home page or delete certain files. However, such actions can also be performed by threats of other types (viruses or worms).

Minor threats

Hacktools

Hacktools are designed to assist intruders with hacking. The most common among these programs are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Such tools can be used not only by hackers but also by administrators to check security of their networks. Sometimes various programs that use social engineering techniques are designated as hacktools too.

Adware

Usually, this term refers to a program code incorporated into freeware programs that forcefully display advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements, for example, in web browsers. Many adware programs operate based on data collected by spyware.

Jokes

Like adware, this type of minor threats cannot be used to inflict any direct damage on the system. Joke programs usually just generate messages about allegedly detected errors and threaten to perform actions that may lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that, after asking for user's permission, employ Internet connection to access specific websites. Usually, these programs have a signed certificate and inform the user about all their actions.

Riskware

These programs are not intended to be computer threats. However, they can still cripple system security due to certain features and, therefore, are classified as minor threats. This type of threats includes not only programs that can accidentally damage or delete data but also programs that can be used by hackers or some malicious applications to harm the system. Among such programs are various remote chat and administrative tools, FTP-servers, and so on.



Suspicious objects

These are potential computer threats detected by the heuristic analyzer. Such objects can be any type of threat (even unknown to information security specialists) or turn out safe in case of a false detection. It is strongly recommended to move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.



17.2. Actions Applied to Threats

There are many methods of neutralizing computer threats. Products of Doctor Web combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and a comprehensive approach to security assurance. The main actions for neutralizing malicious programs are:

1. **Cure**—an action applied to viruses, worms and Trojans. It implies deletion of malicious code from infected files or deletion of a malicious program's functional copies as well as the recovery of affected objects (that is, return of the object's structure and operability to the state which was before the infection) if it is possible. Not all malicious programs can be cured. However, products of Doctor Web are based on most effective curing and file recovery algorithms.
2. **Move to quarantine**—an action when the malicious object is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to Doctor Web anti-virus laboratory.
3. **Delete**—the most effective action for neutralizing computer threats. It can be applied to any type of malicious objects. Note that deletion will sometimes be applied to certain files for which curing was selected. This will happen if the file contains only malicious code and no useful information. For example, curing of a computer worm implies deletion of all its functional copies.
4. **Block, rename**—these actions can also be used for neutralizing malicious programs. In the former case, all access attempts to or from the file are blocked. In the latter case, the extension of the file is renamed, which makes it inoperative.



18. Appendix C. Naming of Viruses

When Dr.Web components detect a threat, the notification in the user interface and the report file contain a name of the threat sample given by the specialists of Doctor Web anti-virus laboratory. These names are formed according to certain principles and reflect a threat's design, classes of vulnerable objects, distribution environment (OS and applications), and some other features. Knowing these principles may be useful for understanding software and organizational vulnerabilities of the protected system. The full and constantly updated version of this classification is available at <https://vms.drweb.com/classification/>.

In certain cases this classification is conventional as some viruses can possess several features at the same time. Besides, it should not be considered exhaustive as new types of viruses constantly appear, and the classification is made more precise.

The full name of a virus consists of several elements, separated by full stops. Some elements at the beginning of the full name (prefixes) and at the end of it (suffixes) are standard for the accepted classification.

Prefixes

Affected operating systems

The prefixes listed below are used for naming viruses infecting executable files of certain operating systems:

- Win—16-bit Windows 3.1 programs
- Win95—32-bit Windows 95/98/Me programs
- WinNT—32-bit Windows NT/2000/XP/Vista programs
- Win32—32-bit Windows 95/98/Me and NT/2000/XP/Vista programs
- Win32.NET—programs in Microsoft .NET Framework operating system
- OS2—OS/2 programs
- Unix—programs in various Unix-based systems
- Linux—Linux programs
- FreeBSD—FreeBSD programs
- SunOS—SunOS (Solaris) programs
- Symbian—Symbian OS (mobile OS) programs

Note that some viruses can infect programs of one system even if they are designed to operate in another system.



Macrovirus prefixes

The list of prefixes for viruses which infect MS Office objects (the language of the macros infected by such type of virus is specified):

- WM—Word Basic (MS Word 6.0-7.0)
- XM—VBA3 (MS Excel 5.0-7.0)
- W97M—VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- X97M—VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- A97M—databases of MS Access'97/2000
- PP97M—MS PowerPoint presentations
- O97M—VBA5 (MS Office'97), VBA6 (MS Office 2000); this virus infects files of more than one component of MS Office

Development languages

The HLL group is used to name viruses written in high-level programming languages, such as C, C++, Pascal, Basic, and others. To specify functioning algorithms, the following modifiers can be used:

- HLLW—worms
- HLLM—mail worms
- HLL0—viruses overwriting the code of the victim program
- HLLP—parasitic viruses
- HLLC—companion viruses

The following prefix also refers to development language:

- Java—viruses designed for the Java virtual machine

Trojan programs (Trojans)

Trojan—a general name for different Trojan programs (Trojans). In many cases the prefixes of this group are used with the Trojan prefix.

- PWS—password stealing Trojan
- Backdoor—Trojan with RAT-function (Remote Administration Tool—a utility for remote administration)
- IRC—Trojan which uses Internet Relay Chat channels
- DownLoader—Trojan which secretly downloads different malicious programs from the Internet
- MulDrop—Trojan which secretly downloads different viruses contained in its body
- Proxy—Trojan which allows a third-party user to work anonymously in the Internet via the infected computer



- `StartPage` (synonym: `Seeker`)—Trojan which makes unauthorized replacement of the browser home page address (start page)
- `Click`—Trojan which redirects a user's browser to a certain website (or websites)
- `KeyLogger`—a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- `AVKill`—terminates or deletes anti-virus programs, firewalls, etc.
- `KillFiles`, `KillDisk`, `DiskEraser`—deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- `DelWin`—deletes files vital for the operation of Windows OS
- `FormatC`—formats drive C (synonym: `FormatAll`—formats all drives)
- `KillMBR`—corrupts or deletes master boot records (MBR)
- `KillCMOS`—corrupts or deletes CMOS memory

Tool for attacking vulnerabilities

- `Exploit`—a tool exploiting known vulnerabilities of an OS or application to implant malicious code or perform unauthorized actions

Tools for network attacks

- `Nuke`—tools for network attacks on known vulnerabilities of operating systems leading to abnormal shutdowns of the attacked system
- `DDoS`—agent program for performing a DDoS attack (Distributed Denial Of Service)
- `FDoS` (synonym: `Flooder`)—Flooder Denial Of Service—programs for performing malicious actions in the Internet which use the idea of DDoS attacks; in contrast to DDoS, when several agents on different computers are used simultaneously to attack one victim system, an FDoS program operates as an independent "self-sufficient" program (Flooder Denial of Service).

Script viruses

Prefixes of viruses written in different scrip languages:

- `VBS`—Visual Basic Script
- `JS`—Java Script
- `Wscript`—Visual Basic Script and/or Java Script
- `Perl`—Perl
- `PHP`—PHP
- `BAT`—MS-DOS command interpreter



Malicious programs

Prefixes of malicious programs that are not viruses:

- **Adware**—an advertising program
- **Dialer**—a dialer program (redirecting modem calls to predefined paid numbers or paid resources)
- **Joke**—a joke program
- **Program**—a potentially dangerous program (riskware)
- **Tool**—a program used for hacking (hacktool)

Miscellaneous

Generic—this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.

Silly—this prefix was used with different modifiers to name simple featureless viruses in the past.

Suffixes

Suffixes are used to name some specific virus objects:

- **generator**—an object which is not a virus but a virus generator.
- **based**—a virus which is developed with the help of the specified generator or a modified virus. In both cases the names of this type are generic and can define hundreds and sometimes even thousands of viruses.
- **dropper**—an object which is not a virus but an installer of the given virus.

