



# Dr.WEB

Agent for Windows

## User manual



© Doctor Web, 2022. 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, SplDer Mail, SplDer 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 Agent for Windows**  
**Version 13.0**  
**User manual**  
**9/1/2022**

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

<b>1. Introduction</b>	<b>7</b>
1.1. Document Conventions and Abbreviations	7
<b>2. About the Product</b>	<b>9</b>
2.1. Protection Components and Management Modules	9
2.2. Detection Methods	10
2.3. System Requirements	14
2.4. Testing the Anti-virus	16
<b>3. Installing, Removing, or Changing Dr.Web</b>	<b>18</b>
3.1. Installing via Full Installer	18
3.2. Installing via Personal Installation Package	23
3.3. Configuring Components	30
3.4. Removing and Reinstalling the Product	32
<b>4. Program Menu</b>	<b>34</b>
<b>5. Security Center</b>	<b>37</b>
<b>6. Notification Feed</b>	<b>39</b>
<b>7. Program Settings</b>	<b>41</b>
<b>7.1. General Settings</b>	<b>41</b>
7.1.1. Program Settings Password Protection	42
7.1.2. Selecting Interface Color Theme	43
7.1.3. Selecting Program Language	45
7.1.4. Dr.Web Operation Logging	45
7.1.5. Quarantine Settings	48
7.1.6. Automatic Deletion of Statistics Records	49
<b>7.2. Notification Settings</b>	<b>50</b>
<b>7.3. Self-Protection</b>	<b>53</b>
<b>7.4. File Scan Options</b>	<b>55</b>
<b>7.5. Server</b>	<b>58</b>
<b>7.6. Server Notifications</b>	<b>64</b>
<b>8. Files and Network</b>	<b>65</b>
<b>8.1. Real-Time File System Protection</b>	<b>66</b>
<b>8.2. Checking Web Traffic</b>	<b>72</b>
<b>8.3. Email Scan</b>	<b>76</b>
8.3.1. Configuring Message Scan	78



8.3.2. Anti-Spam Parameters	82
<b>8.4. Firewall</b>	<b>86</b>
8.4.1. Configuring Firewall	87
<b>8.5. Computer Scan</b>	<b>105</b>
8.5.1. Scan Start and Scan Modes	105
8.5.2. Neutralizing Detected Threats	107
8.5.3. Additional Options	109
<b>8.6. Dr.Web for Microsoft Outlook</b>	<b>110</b>
8.6.1. Virus Check	111
8.6.2. Spam Check	113
8.6.3. Event Logging	116
8.6.4. Statistics	117
<b>9. Preventive Protection</b>	<b>118</b>
9.1. Ransomware Protection	119
9.2. Behavior Analysis	124
9.3. Exploit Prevention	132
<b>10. Devices</b>	<b>134</b>
10.1. Bus and Device Class Blocking	137
10.2. Allowed Devices	142
<b>11. Office Control</b>	<b>145</b>
11.1. Access to Internet Resources	148
11.2. Time Limits on Computer and Internet Use	153
11.3. Access to Files and Folders	155
<b>12. Quarantine Manager</b>	<b>156</b>
<b>13. Exclusions</b>	<b>158</b>
13.1. Websites	159
13.2. Files and Folders	161
13.3. Applications	163
13.4. Anti-Spam	167
<b>14. Statistics on Component Operation</b>	<b>170</b>
<b>15. Server Notifications</b>	<b>178</b>
<b>16. Technical Support</b>	<b>181</b>
16.1. Assistance in Resolving Problems	181
16.2. About	184
<b>17. Appendix A. Additional Command-Line Parameters</b>	<b>185</b>



17.1. Scanner and Console Scanner Parameters	185
17.2. Installation Packages Parameters	190
17.3. Return Codes	193
<b>18. Appendix B. Computer Threats and Neutralization Methods</b>	<b>194</b>
18.1. Types of Computer Threats	194
18.2. Actions Applied to Threats	198
<b>19. Appendix C. Naming of Viruses</b>	<b>199</b>
<b>20. Appendix D. Main Terms and Concepts</b>	<b>203</b>



## 1. Introduction


This manual describes how to install the Dr.Web Agent for Windows product and contains recommendations on how to use it and solve typical problems caused by virus threats. Mostly, the manual describes the standard operation modes of the Dr.Web components (with default settings).

The Appendices contain some general information and additional parameters for experienced users for Dr.Web setting-up.

### 1.1. Document Conventions and Abbreviations

#### 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.
<b>Save</b>	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
C:\Windows\	Names of files and folders, code examples.
<a href="#">Appendix A</a>	Cross-references on the document chapters or internal hyperlinks to web pages.

#### Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

- Dr.Web—Dr.Web Agent for Windows
- FTP—File Transfer Protocol
- HTTP—Hypertext Transfer Protocol
- IMAP—Internet Message Access Protocol
- IMAPS—Internet Message Access Protocol Secure
- MTU—Maximum Transmission Unit



- NNTP—Network News Transfer Protocol
- OS—Operating system
- POP3—Post Office Protocol Version 3
- POP3S—Post Office Protocol Version 3 Secure
- SIP—Session Initiation Protocol
- SMTPS—Simple Mail Transfer Protocol Secure
- SSL—Secure Sockets Layer
- TCP—Transmission Control Protocol
- TLS—Transport Layer Security
- UAC—User Account Control
- URL—Uniform Resource Locator





## 2. About the Product

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

Dr.Web Agent for Windows consists of several modules responsible for different functions. 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. Dr.Web uses default component features to detect unwanted programs and perform actions with the files containing them.

On the **Support** page, in the [About](#) section, you can find information about the product version, the last update date, and Dr.Web Agent identification number.

### 2.1. Protection Components and Management Modules

Dr.Web Agent for Windows contains the following protection components and management modules:

Component/module	Description
<a href="#">SpIDer Guard</a>	A component that constantly resides in memory. SpIDer Guard scans processes and files on their launch and creation and detects any malicious activity.
<a href="#">SpIDer Gate</a>	A component that scans an HTTP traffic. By default, the SpIDer Gate internet monitor automatically scans incoming HTTP traffic and blocks transferring objects, containing viruses and other malicious programs. URL filtering of malicious and unreliable websites is also enabled by default. SpIDer Gate scans traffic over the HTTP, XMPP (Jabber), and TLS (SSL) protocols.
<a href="#">SpIDer Mail</a>	A component that monitors data exchange between any 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 transferred to or from your computer thus preventing spread of infection via email. SpIDer Mail can also scan email for spam messages using <a href="#">Dr.Web Anti-Spam</a> .
<a href="#">Dr.Web Firewall</a>	A personal firewall that protects your computer from unauthorized access and prevents leak of vital data through networks.



Component/module	Description
<a href="#">Office Control</a>	A component that restricts access to websites, files and folders, and allows a user to set custom time limits on using the computer and the internet for different Windows accounts.
<a href="#">Behavior Analysis</a>	A component that controls application access to critical system objects and provides exploit prevention and integrity of running applications.
<a href="#">Exploit Prevention</a>	A component that blocks malicious objects that use application vulnerabilities.
<a href="#">Ransomware Protection</a>	A component that provides protection against ransomware.
<a href="#">Scanner</a>	A scanner with a graphical interface that launches on demand and scans your computer for viruses and other malicious software.
<a href="#">Console Dr.Web Scanner</a>	A command-line version of Dr.Web Scanner.
<a href="#">Dr.Web for Microsoft Outlook</a>	A plug-in that scans Microsoft Outlook mailboxes for threats and spam.
<a href="#">SplDer Agent</a>	A module that helps you configure and manage your anti-virus product.

## 2.2. 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 analyses the behavior of each running program in real time. Using the information on malware behavior, it determines whether the program is dangerous and then takes necessary measures to neutralize the threat. Objects detected using Dr.Web Process Heuristic are indicated with the `DPH` prefix added to their names.

This data protection technology helps to minimize losses resulting from the actions of unknown malware while consuming very few of the protected system 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 shared files and 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 traditionally small, while the quality of detection and curing remains at the same high level. Objects detected using Dr.Web Process Dumper are indicated with the `DPD` prefix added to their names.



## 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. Objects detected using Dr.Web ShellGuard are indicated with the `DPH:Trojan.Exploit` prefix added to their names.

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 others);
- MS Office applications;
- system Applications;
- applications that use java, flash and pdf;
- media players (software).

## Injection Protection

*Injection* is a method for introducing (or injecting) malicious code into the processes running on a device. Dr.Web monitors continuously the behavior of all the processes in the system and prevents any attempt to inject the code if considers it to be malicious. Objects detected using Injection Protection are indicated with the `DPH:Trojan.Inject` prefix added to their names.

Dr.Web scans the application that has executed the process according to the following criteria:

- If the application is a new one.
- How did it get into the system.
- Where is the application situated.
- What is its name.
- If the application is in the list of trusted applications.
- If it has a valid digital signature of a trusted certification center.

Dr.Web monitors the state of the executed process: checks whether remote threads are created in the process space, whether extraneous code is embedded in the active process.

The anti-virus program controls the changes that applications make, prohibits changing system and privileged processes. Separately, Dr.Web ensures that malicious code cannot modify the memory of popular browsers, for example, when you make purchases on the internet or make transfers in online banks.

## Ransomware Protection

*Ransomware Protection* is one of the methods of Behavior Analysis that protects users' files from cryptoware actions. When entering a user's computer, such malicious programs block the access to user's data and then demand money for decryption. Objects detected using



Ransomware Protection are indicated with the `DPH:Trojan.Encoder` prefix added to their names.

The component analyzes the behavior of a suspicious process paying particular attention to the processes of file search, reading the files and attempts to modify them.

The following information on the application is also checked:

- If the application is a new one.
- How did it get into the system.
- Where is the application situated.
- What is its name.
- If the application is a trusted one.
- If it has a valid digital signature of a trusted certification center.

The method for modification of files is also checked. When the malicious behavior is detected, actions of this program are blocked, and the attempts to modify files are prevented.

## 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.

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.

## 2.3. System Requirements

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

Parameter	Requirement
CPU	An i686-compatible processor



Parameter	Requirement
Operating system	<p>For 32-bit platforms:</p> <ul style="list-style-type: none"><li>• Windows XP with Service Pack 2 or later</li><li>• Windows Vista with Service Pack 2 or later</li><li>• Windows 7 with Service Pack 1 or later</li><li>• Windows 8</li><li>• Windows 8.1</li><li>• Windows 10 21H2 or earlier</li><li>• Windows Server 2003 with Service Pack 1</li><li>• Windows Server 2008 with Service Pack 2 or later</li></ul> <p>For 64-bit platforms:</p> <ul style="list-style-type: none"><li>• Windows Vista with Service Pack 2 or later</li><li>• Windows 7 with Service Pack 1 or later</li><li>• Windows 8</li><li>• Windows 8.1</li><li>• Windows 10 21H2 or earlier</li><li>• Windows 11 22H2 or earlier</li><li>• Windows Server 2008 with Service Pack 2 or later</li><li>• Windows Server 2008 R2 with Service Pack 1 or later</li><li>• Windows Server 2012</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li><li>• Windows Server 2022</li></ul>
Free RAM	Minimum 512 MB
Screen resolution	Recommended 1024×768 or higher
Cloud and virtualization environment support	<p>Operation of the program is guaranteed in the following environments:</p> <ul style="list-style-type: none"><li>• VMware</li><li>• Hyper-V</li><li>• Xen</li><li>• KVM</li></ul>
Other	<p>To update Dr.Web virus databases and Dr.Web components, connection to the central protection server or to the internet in the Mobile mode is required.</p> <p>For the Dr.Web for Microsoft Outlook plug-in, one of the following Microsoft Outlook clients from the Microsoft Office package is required:</p> <ul style="list-style-type: none"><li>• Outlook 2000</li></ul>



Parameter	Requirement
	<ul style="list-style-type: none"><li>• Outlook 2002</li><li>• Outlook 2003</li><li>• Outlook 2007</li><li>• Outlook 2010 with Service Pack 2</li><li>• Outlook 2013</li><li>• Outlook 2016</li><li>• Outlook 2019</li><li>• Outlook 2021</li></ul>



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, Windows 7, Windows Server 2008 or Windows Server 2008 R2. For this, install all the recommended updates listed in Windows Update section. For the detailed information, please visit [Doctor Web official website](#)



Dr.Web Agent for Windows of 13.0 version is compatible with Dr.Web plug-ins of 12.0 version only.

## 2.4. 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 `test.com` file 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.



## 3. Installing, Removing, or Changing Dr.Web

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

- Install all critical updates released by Microsoft for the OS version used on your computer (detailed information about [Windows](#) and [Windows Server](#)). If the operating system is no longer supported, then upgrade to a newer operating system.
- Check the file system with system utilities and remove the detected problems.
- Remove any anti-virus software from your computer to prevent possible incompatibility of Dr.Web components.
- In case of installation of Dr.Web Firewall, uninstall all other firewalls from your computer.
- In Windows Server 2016 and later, disable Windows Defender manually, using group policies.
- Close all active applications.



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

You can install, change, or uninstall Dr.Web in one of the following ways:

1. Remotely—from the central protection server via the network. This process performed by the administrator of the anti-virus network. No user action is required.
2. Locally—directly on the user's computer. For Dr.Web installation, you can use the [full installer](#) or [personal installation package](#).

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

- Command line mode
- Wizard mode

### 3.1. Installing via Full Installer

Full Installer `drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe` performs the installation of Dr.Web Agent and the antivirus package at a time. The server connection parameters and parameters for station authorization at the server are not provided with the installer.

#### Installation in wizard mode

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 **Exit**.

## To install Dr.Web

1. Run the installation package received from the administrator. Dr.Web Installation Wizard window opens.



If any anti-virus software is installed on the computer, the Installation Wizard attempts to remove it before starting the installation. If the attempt fails, you need to remove the current anti-virus software manually.

Dr.Web Agent

English ▼

### Dr.Web Agent installation

To continue installation, fill in the required fields: server address and the path to the public key or the certificate.

Central protection server

Find

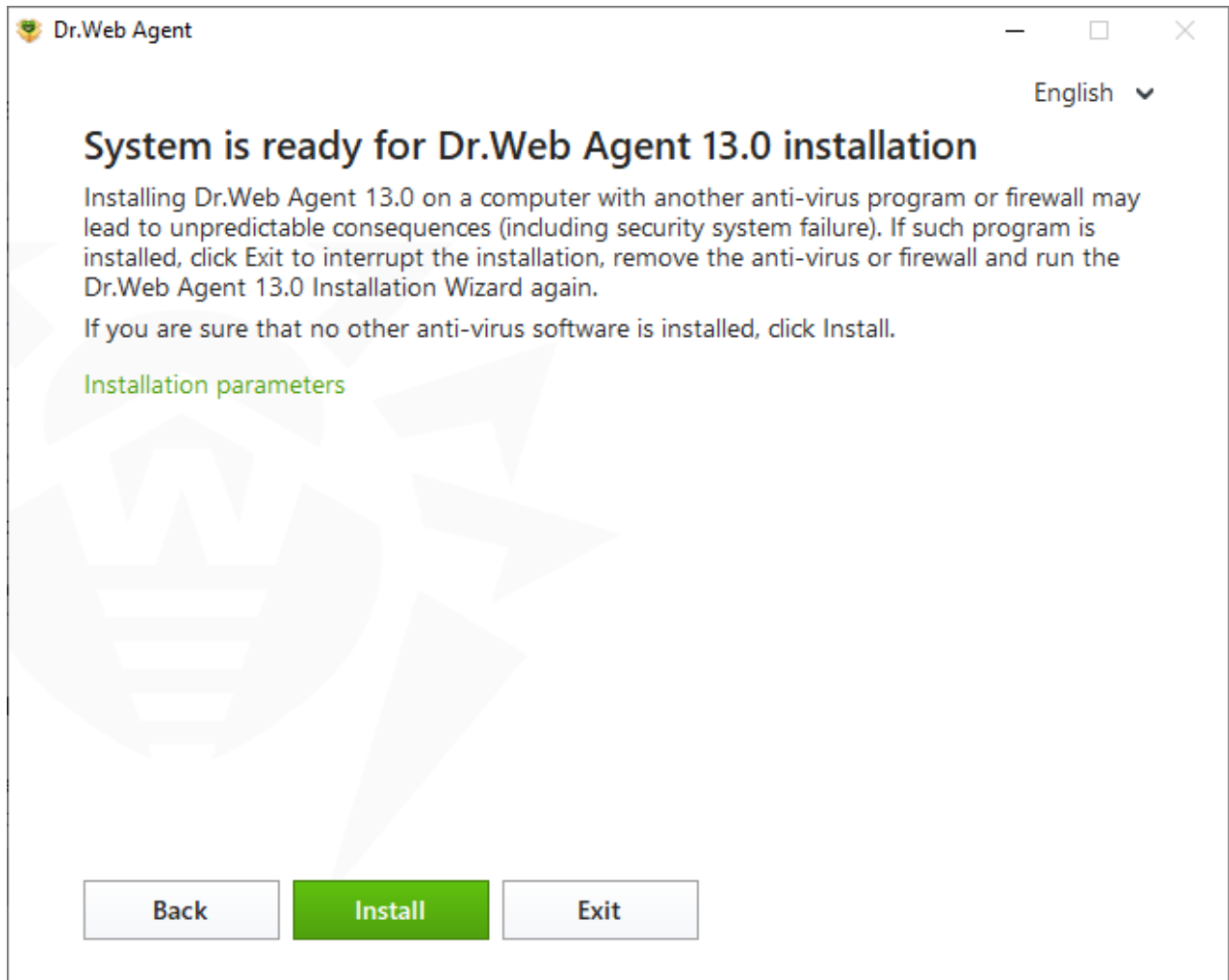
Public key or certificate

Browse...

Next Exit

**Figure 1. Installation Wizard**

2. In the **Central protection server** field, specify the network address of the server, from which Dr.Web is to be installed, and in the **Public key or certificate** field specify the full path to the key file (`drwcsd.pub`) or to the certificate (`.pem`) residing on your computer.  
To search for active servers and to specify searching parameters, click the **Find** button.  
Click **Next**.
3. The Installation Wizard will notify you that it is ready to install.

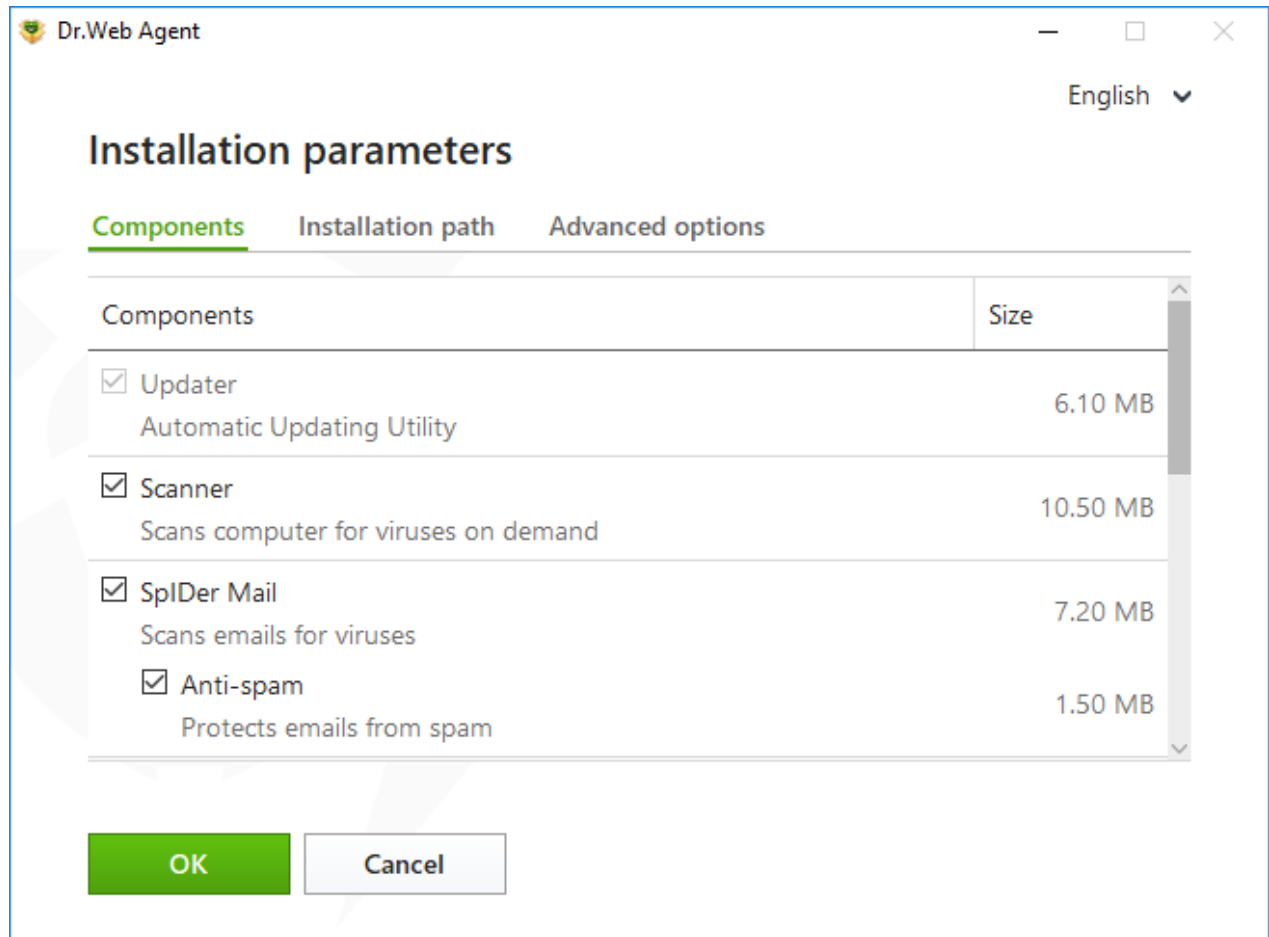


**Figure 2. Ready for installation**

You can run the installation with the default parameters by clicking **Install**.

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.

4. If you have selected **Install** at the previous step, go to the description of [step 8](#). Otherwise, the **Installation parameters** window opens.

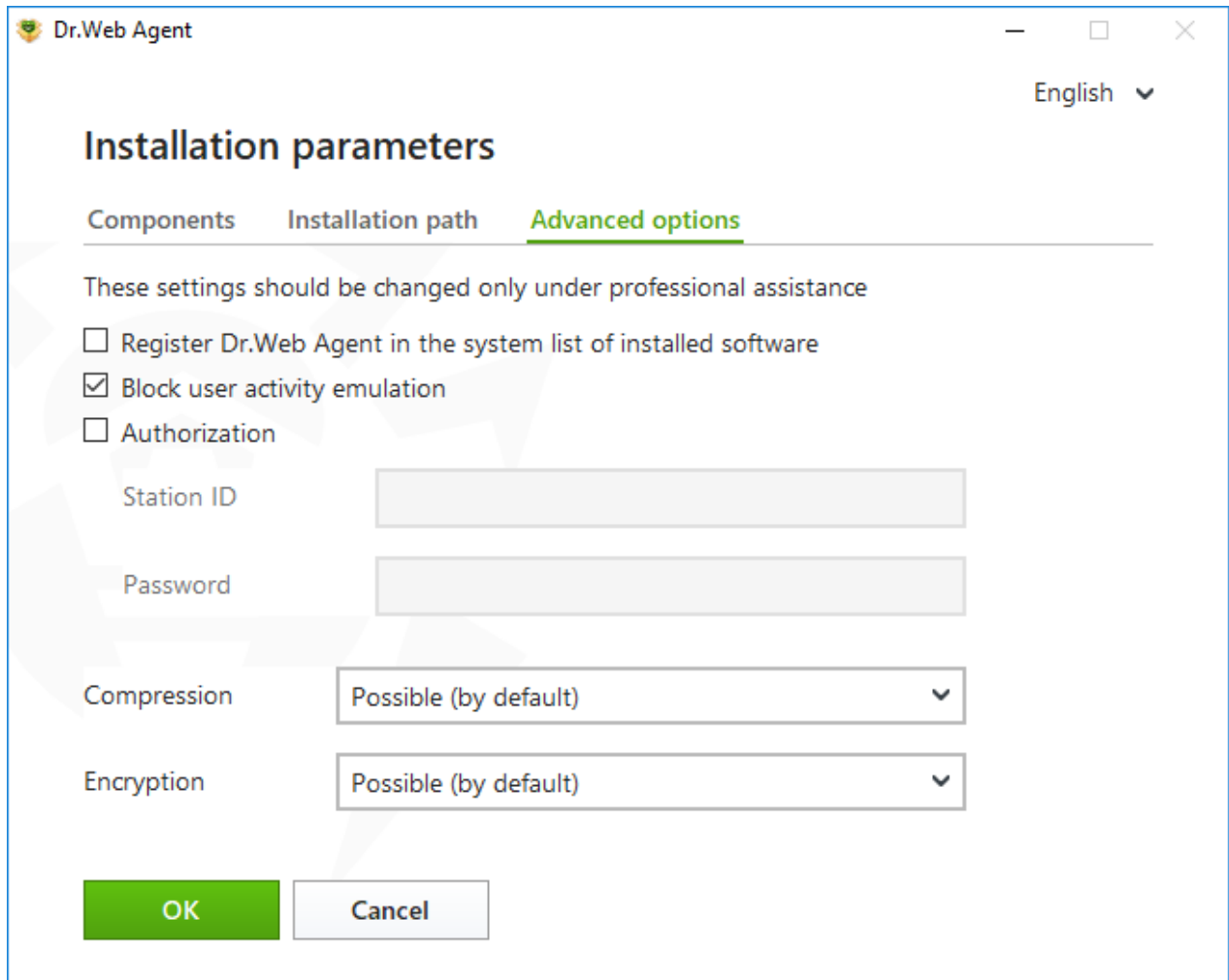


**Figure 3. Installation parameters**

On the **Components** tab, Dr.Web components are listed.

Select the check boxes next to those components that you want to install. By default, all components, except for Dr.Web Firewall, are selected.

5. On **Installation path** tab you can specify the installation folder for **Dr.Web Agent for Windows**. By default, it is installed into the Dr.Web folder in the Program Files folder on the system disk. To change the installation path, click **Browse** and specify the required folder.
6. On **Advanced options** tab you can configure the additional settings.



**Figure 4. Installation parameters advanced options**

The following options are available:

- **Register Dr.Web Agent in the system list of installed software.** This option also allows the user to [remove Dr.Web](#) and [configure its components](#) by the means of standard Windows tools.
- **Block user activity emulation.** Allows you 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 and other actions aimed at changing Dr.Web operation).
- To enable manual authorization on the central protection server, enable the **Authorization** check box. Then specify the parameters of authorization of the workstation:
  - **Station ID**—the identifier of the workstation on server;
  - **Password**—the password to access the server.

In this case, the workstation does not require manual approval of the administrator to get access to the server.

From the **Compression** and **Encryption** drop-down lists, select the required modes of transferring traffic between the server and Dr.Web.

To save the changes, click **OK**, then click **Install**.



7. Installation of Dr.Web starts. No user action is required.
8. Once the installation is completed, you are prompted to restart the computer. Click **Restart now**.

### Installation via the command line

To start the installation of Dr.Web using the command line, go to the folder where the installation file is located, then enter the executable file name (`drweb-13.0.0-xxxxxxx-esuite-agent-full-windows.exe`) using the needed command line options.

The full list of command-line parameters can be found in [Appendix A](#).

## 3.2. Installing via Personal Installation Package

When installing the product via personal installation package, the installation is performed though the network.

A personal installation package contains Dr.Web Agent installer and a set of parameters for Dr.Web server connection and station authorization on the server.

### Installation in wizard mode

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

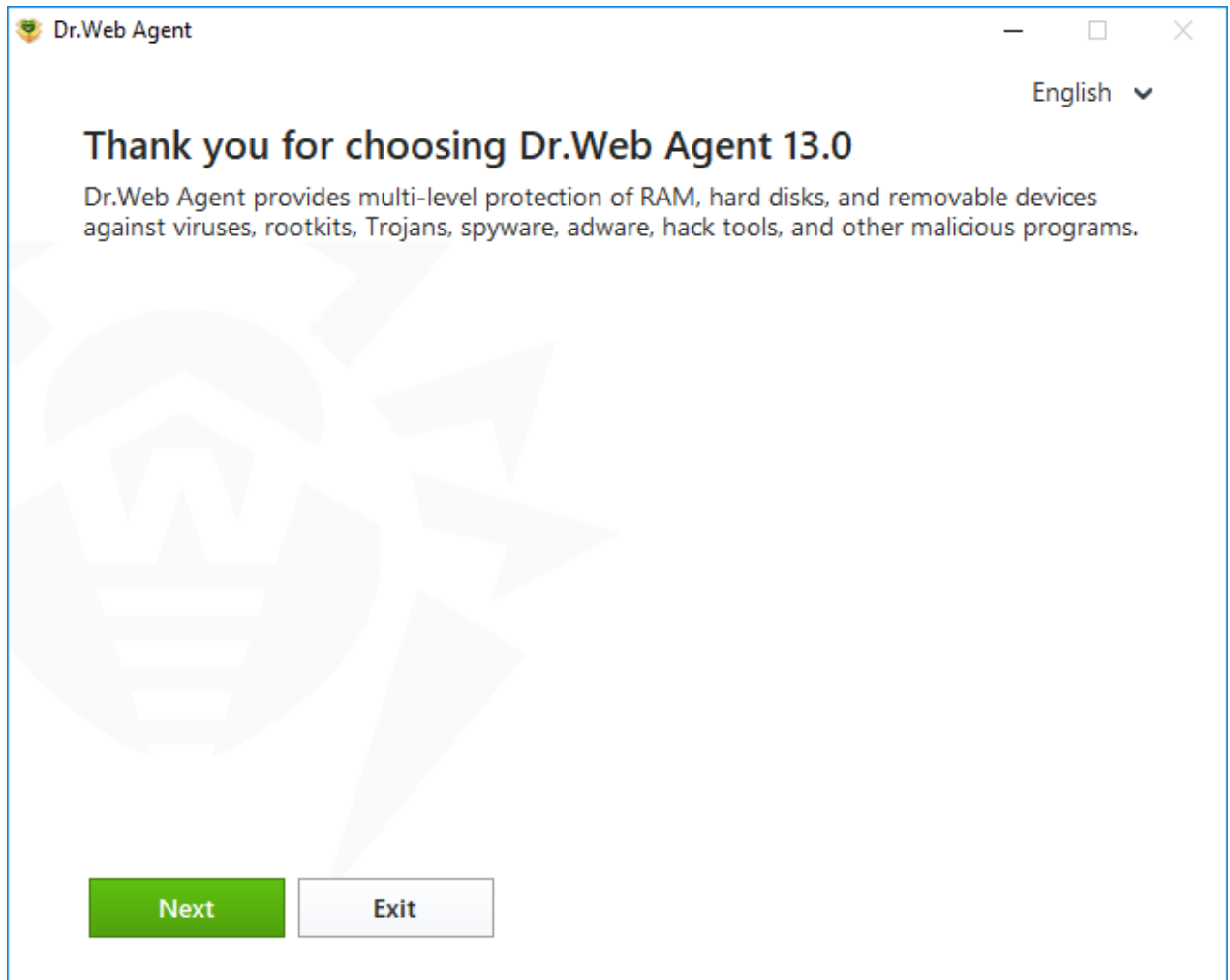
- Return to the previous step by clicking **Back**.
- Go to the next step by clicking **Next**.
- Abort installation by clicking **Exit**.

#### To install Dr.Web

1. Run the installation package `drweb_ess_windows_<Station_name>.exe` received from the administrator. Dr.Web Installation Wizard window opens.



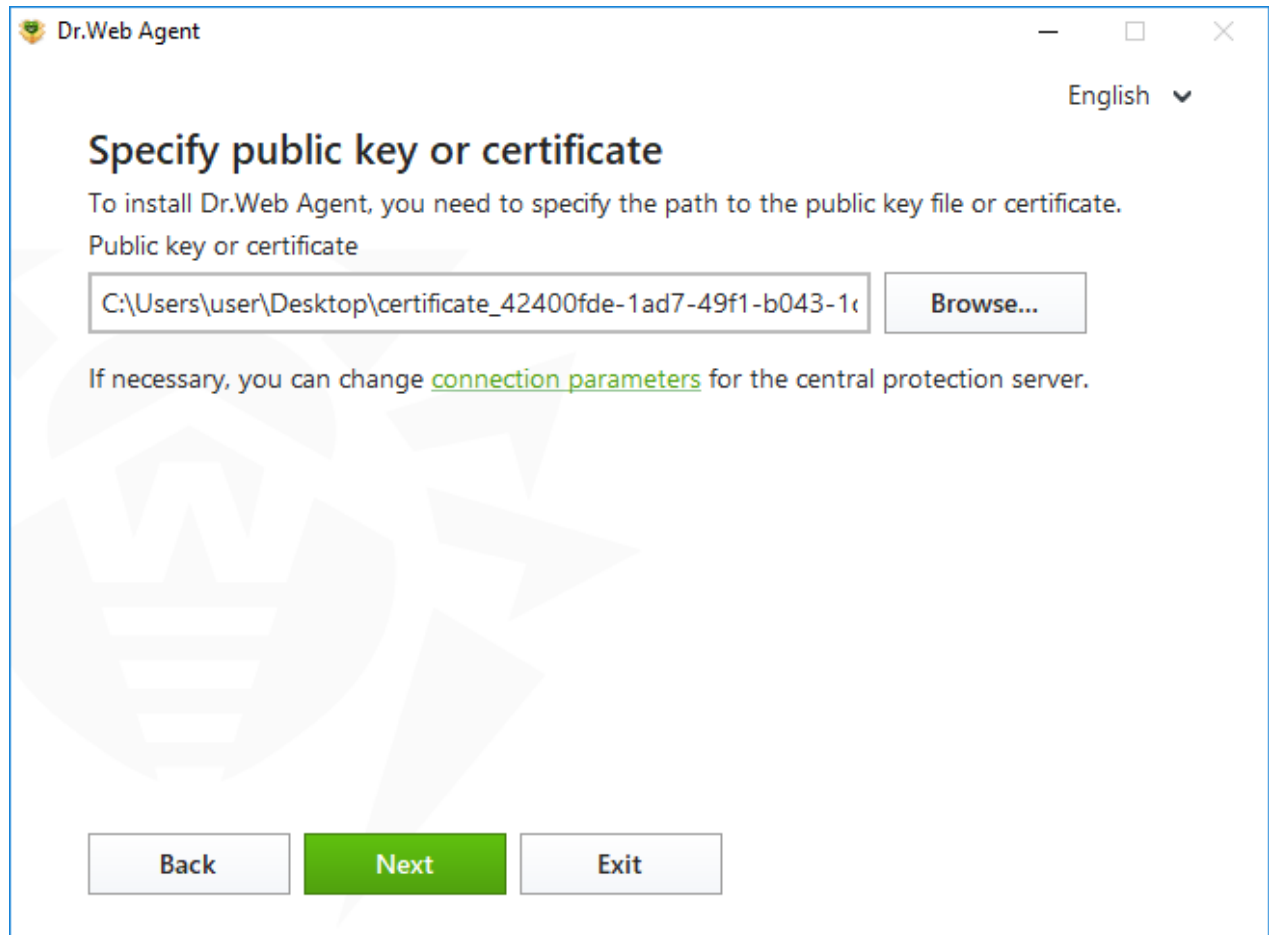
If any anti-virus software is installed on the computer, the Installation Wizard attempts to remove it before starting the installation. If the attempt fails, you need to remove the current anti-virus software manually.



**Figure 5. Installation Wizard**

2. Click **Next**.
3. On the next step, specify the full path to the public key (`drwcsd.pub`) or to the certificate `.pem`, residing on your computer.





**Figure 6. Public key or certificate specification**

4. If needed, you can adjust parameters of connection to the central protection server. To do that, click the corresponding link. The **Connection parameters** window opens. When installing via personal installation package, all required connection parameters are already specified.



It is strongly recommended that you do not change the parameters without approval of your anti-virus network administrator.



Dr.Web Agent

English ▼

### Connection parameters

For information about parameters for connection to central protection server, contact your system administrator.

Central protection server

**Find**

☒ Manual authorization on server

Station ID

Password

Compression

Encryption

**OK** Cancel

**Figure 7. Central protection server connection parameters**



For details on parameters for connection to the central protection server, contact the administrator.

In the **Central protection server** field, you can specify the network address of the server, from which Dr.Web is to be installed. By default, this field is filled in with parameters of the server on which the installation file has been created. To search for active servers and to specify searching parameters, click the **Find** button.

To enable manual authorization on the server, enable the corresponding check box. After that, specify the following authorization parameters:

- **Station ID**—the identifier of the workstation on server;
- **Password**—the password to access the server.

In this case, the workstation does not require manual approval of the administrator to get access to the server.



When installing Dr.Web using the installation file created in Dr.Web Control Center, the **Station ID** and **Password** entry fields are filled in automatically if you have selected the manual authorization option.

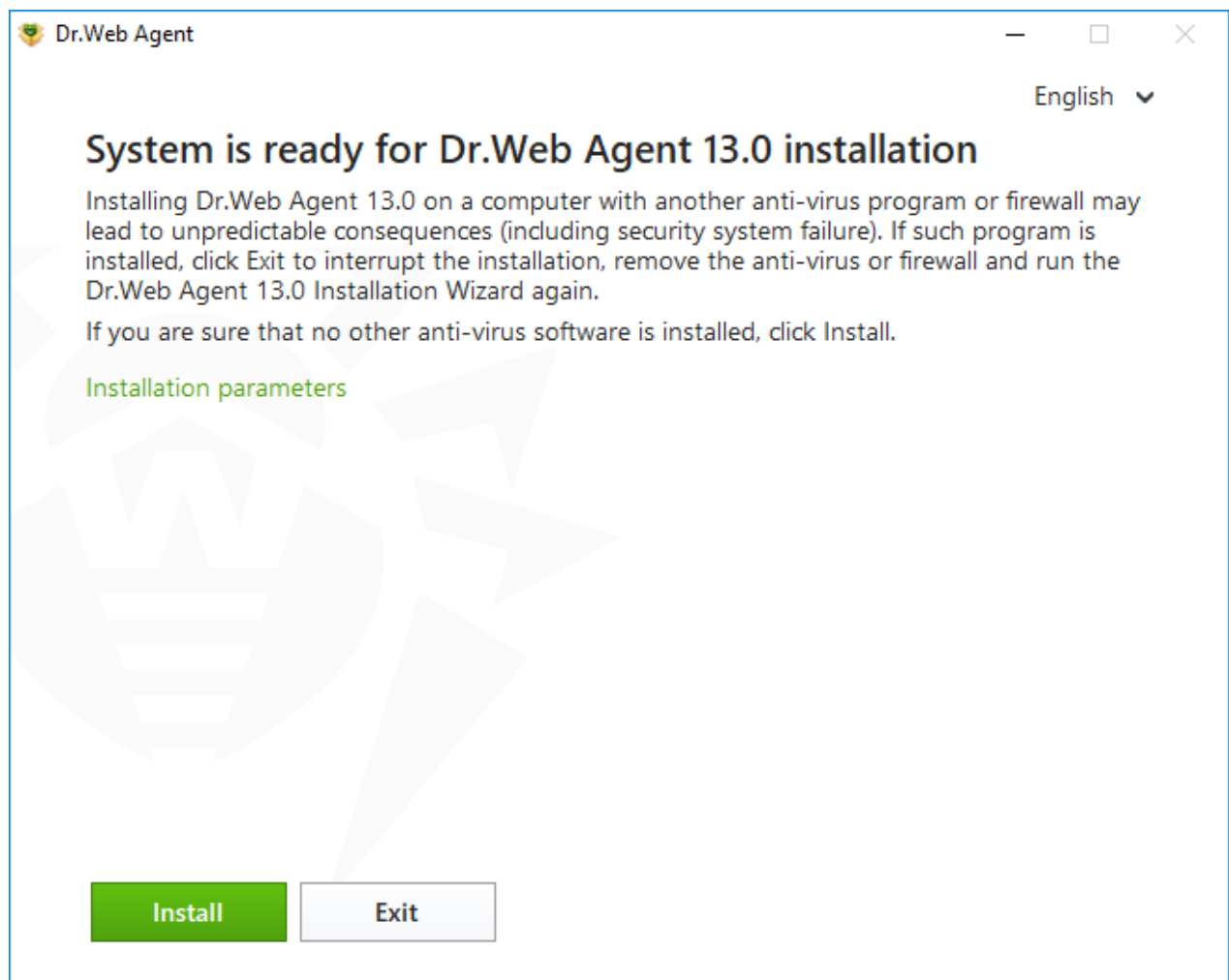
From the **Compression** and **Encryption** drop-down lists, select the required modes of transferring traffic between the server and Dr.Web.

To save the changes, click **OK**, then click **Next**.



If the attempt to establish connection fails, follow the link to check network parameters and/or try to connect to the server again by clicking the corresponding button.

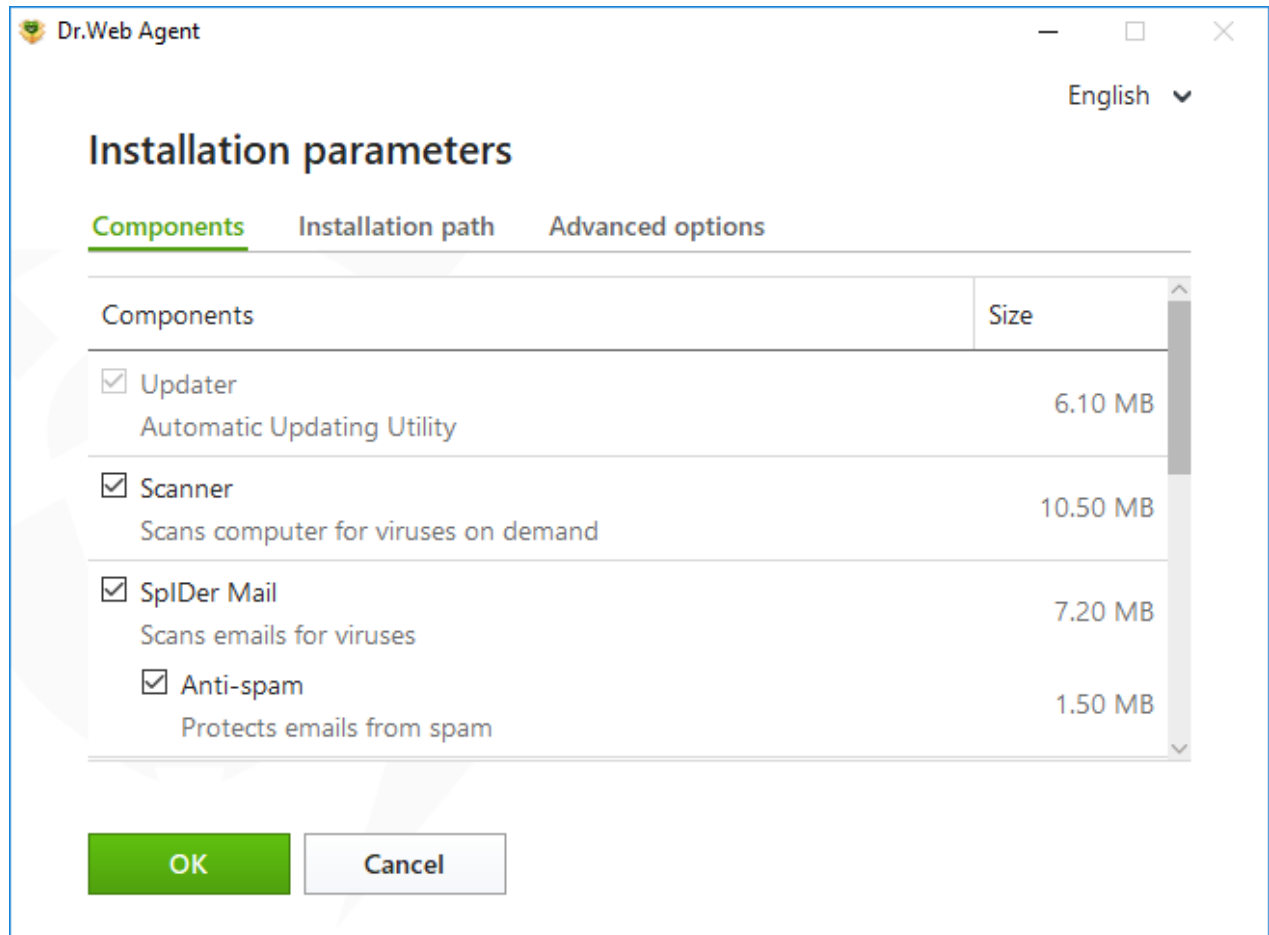
5. After the connection is established, the window opens notifying you that the product is ready to be installed. To start installation with the default parameters, click **Install**.



**Figure 8. Ready for installation**

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.

6. If you have selected **Install** at the previous step, go to the description of [step 9](#). Otherwise, the **Installation parameters** window opens.

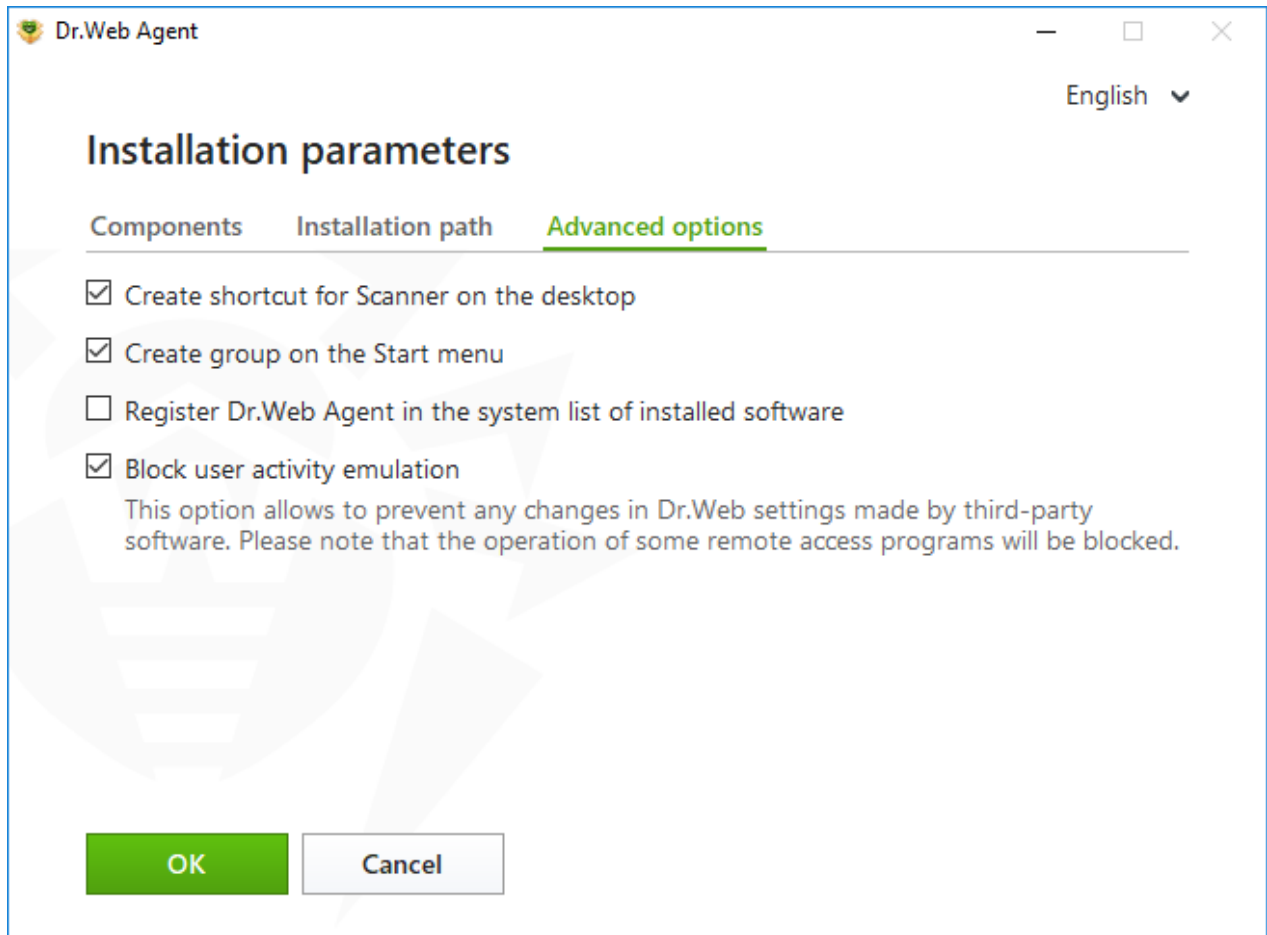


**Figure 9. Installation parameters**

On the **Components** tab, Dr.Web components are listed.

Select the check boxes next to those components that you want to install. By default, all components, except for Dr.Web Firewall, are selected.

- On **Installation path** tab you can specify the installation folder for **Dr.Web Agent for Windows**. By default, it is installed into the Dr.Web folder in the Program Files folder on the system disk. To change the installation path, click **Browse** and specify the required folder.
- On **Advanced options** tab you can configure additional installation settings.



**Figure 10. Installation parameters advanced options**

If required, enable the **Register Dr.Web Agent in the system list of installed software** option. This option also allows you to [remove Dr.Web](#) and [configure its components](#) by the means of standard Windows tools.

The **Block user activity emulation** option allows you 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 and other actions aimed at changing Dr.Web operation).

To save the changes, click **OK**, then click **Install**.

9. Installation of Dr.Web starts. No user action is required.

10. Once the installation is completed, you are prompted to restart the computer. Click **Restart now**.

## Installation via the command line

To start the installation of Dr.Web using the command line, go to the folder where the installation file is located, then enter the executable file name (`drweb_ess_windows_<Station_name>.exe`) using the needed command line options.



The full list of command-line parameters can be found in [Appendix A](#).



## 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 workstation system using CureNet! utility by Doctor Web. You can ask for demo version of the utility (diagnostics without curing function) at <https://download.drweb.com/curenet/>. You can check the terms of use and the price of the full version of this utility here: <https://estore.drweb.com/utilities/>.
2. Restore BFE service. To do this, you can use the Windows firewall recovery [utility](#)  for Windows 7 and later. On Windows Server operating systems enable or restart BFE service manually. If you cannot restart BFE service or it is missing from the list of services, please contact [Microsoft technical support](#) .
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.

## 3.3. Configuring Components



The components can be configured if your anti-virus network administrator enables this option.

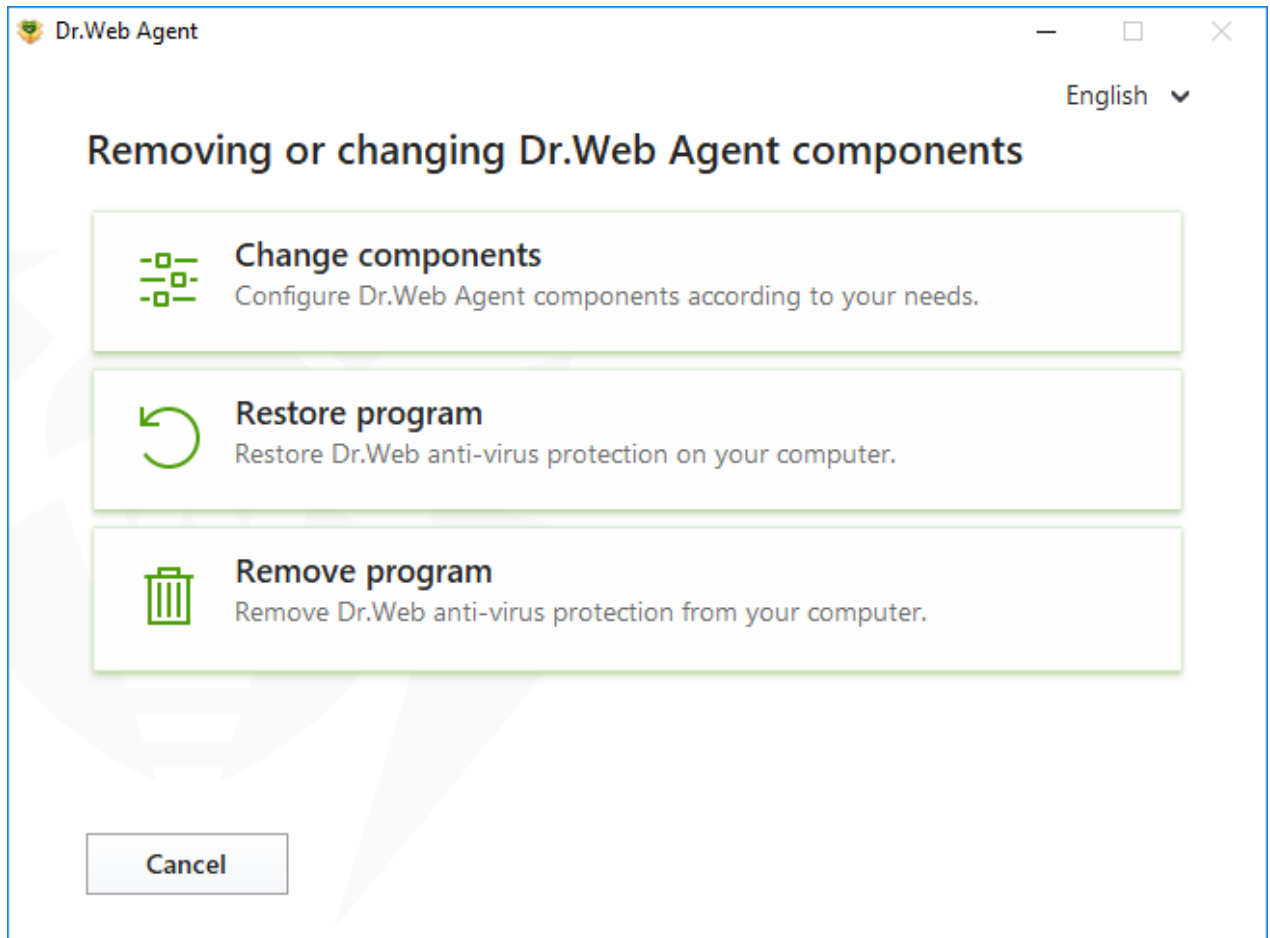
Configuring components can be done in Uninstall/Change wizard. You can open the Uninstall/Change wizard in one of two ways:

- If you have an installation file, run it.
- From Windows Control Panel:
  1. Go to Windows Control Panel, click Programs.
  2. In the list of installed programs select the line **Dr.Web Agent**.
  3. Click **Change**.



## To delete or add components

1. In the Uninstall/Change wizard window, click **Change components**:



**Figure 11. Uninstall/Change wizard**

2. 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.
3. Click **Apply**.

In the Uninstall/Change wizard window, the following options are also available:

- **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.



## 3.4. Removing and Reinstalling the Product



An option of the local uninstallation of Dr.Web must be allowed by the administrator on the central protection server.

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

### Removing Dr.Web from Windows Control Panel



This method is available only if you have enabled the **Register Dr.Web Agent in the system list of installed software** option during the product installation.

If you install Dr.Web in the background installation mode, uninstallation of Dr.Web with the standard Windows tools is available only if the `-regagent` switch has been specified.

If you have an installation file you can skip the steps 1–3. Run the installation file and go to the [step 4](#).

To remove Dr.Web Agent for Windows, run Windows removal component.

1. In the list select the line with the program name.
2. Click **Delete**.
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 Agent settings** and **Protected copies of files**—are selected. Click **Next**.
4. To confirm Dr.Web removing, in the next window click **Delete**.
5. Once you reboot your computer, the changes are applied. You can snooze the reboot by clicking **Restart later**. Click **Restart now** to immediately complete the procedure of Dr.Web components deletion or modification.

### Removing using the command line

To start uninstallation of Dr.Web from the command line, enter the executable file name (`win-es-agent-setup.exe`) and specify necessary parameters.



The `win-es-agent-setup.exe` file is located in the `C:\ProgramData\Doctor Web\Setup\` folder.

For example, to uninstall Dr.Web and restart the system after the process completes, use the following command:







```
win-es-agent-setup.exe /instMode remove /silent yes
```

## Reinstalling Dr.Web

1. Get the latest installation package from your anti-virus network administrator.
2. Uninstall the program, [as described above](#).
3. Restart your computer.
4. Using the installation package, [reinstall the program](#). While installing, specify the path to the key file.
5. Restart your computer.




## 4. Program Menu

After Dr.Web is installed,  icon is added to Windows notification area. The icon displays the current [application state](#). To open Dr.Web menu, click . If the application is not running, in **Start** menu expand the application group **Dr.Web** and then select **Security Center**.



The Dr.Web icon is not displayed in the notification area if the administrator of your anti-virus network enabled the corresponding option on the central protection server.

In the Dr.Web menu , you can view security status and get access to the main managing tools and program settings.



Adjustment of the settings or disabling of a component can be not available if the administrator of the central protection server, to which Dr.Web is connected, has blocked this option.

To access the component parameters, you also need to enter the password if you have enabled the **Protect Dr.Web settings with a password** option in the [settings](#) window.

If you have forgotten your password for the product settings, contact your system administrator.

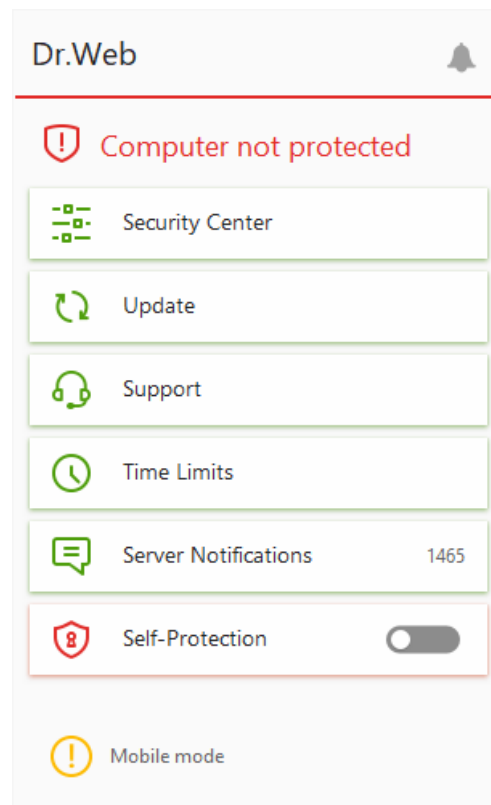


Figure 12. Program menu



## Menu items

**Computer security status.** If all the program components are enabled, the **Computer protected** status is displayed. If one or several components are disabled, the status is changed to **Computer not protected**.

**Security Center.** Opens a window with an access to the main settings, parameters of the protection components, including Office Control parameters, and exclusions.

**Update** (in Mobile mode only). Information about the actuality of virus databases and last update date. Launches the update of program components and virus databases.

**Support.** Opens support window.



**Time Limits** (if an option of internet or computer usage limits is enabled in the Office Control component). A brief information on internet or computer usage restrictions or on break duration if time intervals are specified.


**Server Notifications** (if you have new notifications and if a corresponding option is enabled on the server). Opens a window with [server notifications](#).

**Self-Protection** (if Self-Protection is disabled). You can enable Self-Protection using the switcher.

**Server connection status.** The status is shown only if the station cannot be connected to the server. If the station is connected successfully the status is not shown.

One of 5 possible status can be displayed:





Icon	Status
	<ul style="list-style-type: none"><li>• The station is waiting for approval on the server</li><li>• Mobile mode</li><li>• Connecting to the central protection server</li></ul>
	<ul style="list-style-type: none"><li>• No connection with the server</li><li>• Connection error</li></ul>

**Notification Feed** . Opens the [Notification Feed](#) window.



## Possible application states

Dr.Web icon displays the current application state:


Dr.Web icon	Description
	All necessary components are running and protecting your computer. Connection to the central protection server is established.
	Self-Protection or an important component is disabled, or virus databases are out-of-date, that compromises security of the anti-virus and your computer; or connection to the server is expected. Probably, the server refused the connection or denied access to its resources. Enable Self-Protection or the disabled component, wait until the connection to the server is established or contact your anti-virus network administrator if the connection is not established.
	Components are expected to start after the operating system startup process is completed, 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. If the icon does not change, contact your anti-virus network administrator.
	Scanner is currently running.



## 5. Security Center

The **Security Center** window provides you with an access to all the components, tools, statistics and program settings.

### To open Security Center window

1. Open Dr.Web [menu](#) .
2. Select **Security Center**.

### To open Security Center window from the Start Menu

1. In the **Start Menu** expand **Dr.Web** group.
2. Click **Security Center**.

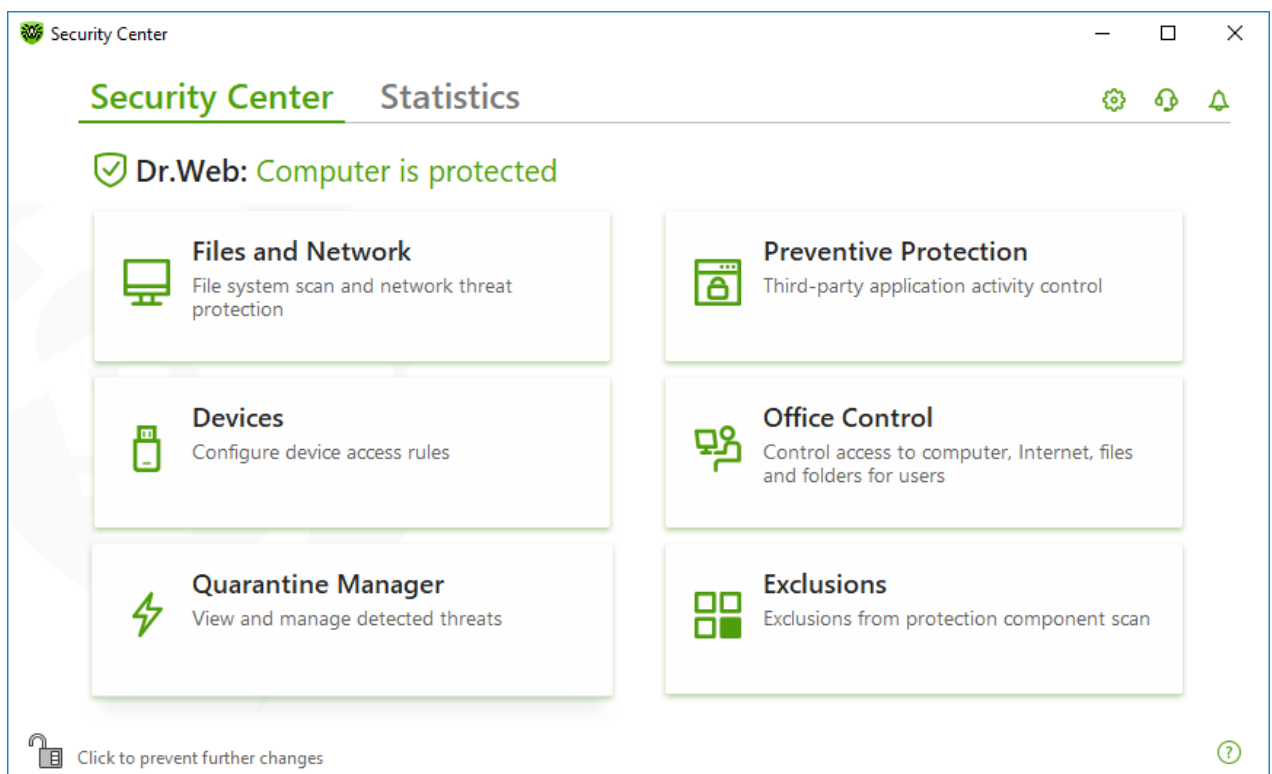





Figure 13. Security Center window

### Groups of settings



You have an access to the next groups of settings from the main window:

- **Security Center**, the main tab. Provides an access to all the security components and tools:
  - [Files and Network](#)
  - [Preventive Protection](#)
  - [Devices](#)



- [Office Control](#)
- [Quarantine Manager](#)
- [Exclusions](#)
- [Statistics](#) tab. Provides statistics on the main program operation events.
-  button at the top of the program window. Provides an access to the [program settings](#).
-  button at the top of the program window. Provides an access to **Support** window where you can generate [report for technical support](#) and review information on the product version and the date of the last update of the components and virus databases.
-  button at the top of the program window. Provides an access to **Notification Feed** window where you can review the important notifications on the program operation events.

## Administrative mode

To access all the groups of settings, switch Dr.Web to the [administrative mode](#) by clicking the lock  at the bottom of the program window. When Dr.Web is in the administrative mode, the lock is open .

You have full access to the **Quarantine Manager** in both modes. Besides, you can enable all the security components and start Scanner without switching to the administrative mode. To disable the security components, access the component parameters and program setting, you need to switch to the administrative mode.



Adjustment of the settings or disabling of a component can be not available if the administrator of the central protection server, to which Dr.Web is connected, has blocked this option.

## Protection status

At the top of the program window, the system protection status is displayed.




- **Computer is protected.** All the components are enabled and operating properly, Self-Protection is enabled, the license is valid. Displayed in green color.
- **Computer is not protected.** Displayed when at least one of the components is disabled. Displayed in red color. The disabled component tile is also highlighted in red.





## 6. Notification Feed

In this window, the important notifications on the program operation events are listed. The notifications in this window duplicate some of the desktop notifications.

### To access the Notification Feed from the program menu

1. Open Dr.Web [menu](#) .
2. Click  button. Above the  icon the number of saved notifications is displayed.
3. Window with the event notifications opens.

### To access the Notification Feed window from Security Center

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. At the top of the program window, click .
3. Window with the event notifications opens.

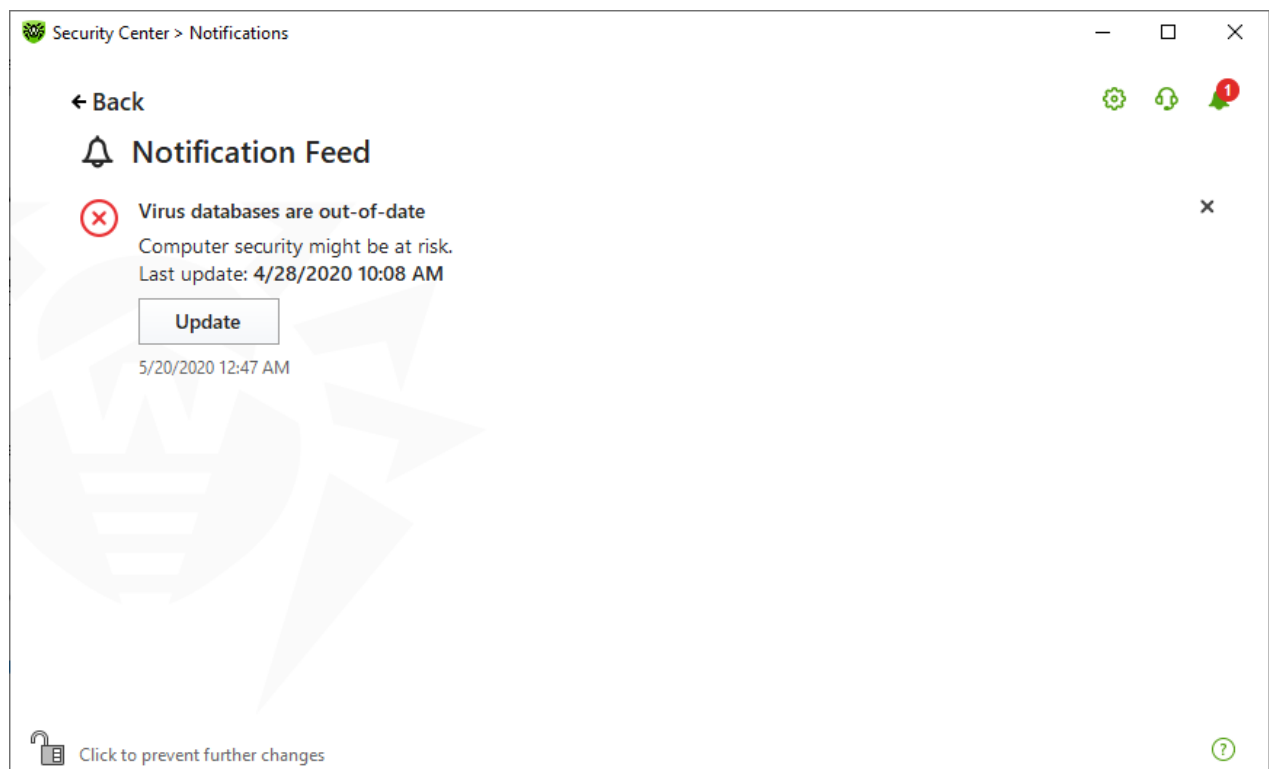





Figure 14. Notification Feed window



## Notification retention period

The notifications are kept for two weeks. After the problem is resolved, the notification is also removed.

## Notification types

 <b>Critical notifications</b>	
Threats	<ul style="list-style-type: none"><li>• Threat is detected.</li><li>• The reboot is required to neutralize the threats.</li><li>• Virus databases are out of date.</li></ul>
Connection with the server	<ul style="list-style-type: none"><li>• Connection with the server is prohibited.</li><li>• Server connection error.</li></ul>
Blocked access to the objects and devices	<ul style="list-style-type: none"><li>• Device is blocked according to settings.</li></ul>
 <b>Major notifications</b>	
Update	<ul style="list-style-type: none"><li>• The restart is required to complete the update.</li></ul>
 <b>Not important informative notifications</b>	
New version	<ul style="list-style-type: none"><li>• New version is available.</li></ul>
New message	<ul style="list-style-type: none"><li>• The administrator has sent a new message.</li></ul>

## Display settings





The display settings of the notifications in the feed duplicate those of desktop notifications. To change the display settings so that certain notifications are not displayed in the feed, disable the correspondent check box in the **Desktop** column in the **Notification parameters** window. See also [Notification settings](#) section.





## 7. Program Settings

### To open program settings

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. Window with the settings opens.



The settings can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.

If you enable the **Protect Dr.Web settings with a password** option in the [general settings](#), you are prompted to enter the password to access the main Dr.Web settings.

In this section:

- [General](#)—protect settings with password, select a language, select a color theme.
- [Notifications](#)—configure parameters to display pop-ups.
- [Self-Protection](#)—configure advanced security parameters.
- [File Scan Options](#)—configure Scanner parameters.
- [Server](#)—configure connection parameters to the central protection server.
- [Server Notifications](#)—configure parameters to display Server notifications.

### 7.1. General Settings




You can find the following features among general settings:

- [Program settings password protection](#)
- [Selecting interface color theme](#)
- [Selecting program language](#)
- [Operation logging settings](#)
- [Quarantine settings](#)
- [Settings of automatic deletion of statistics records](#)

### To access General Settings

1. Open Dr.Web [menu](#) , then select **Security Center**.



2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **General** at the left of the window.

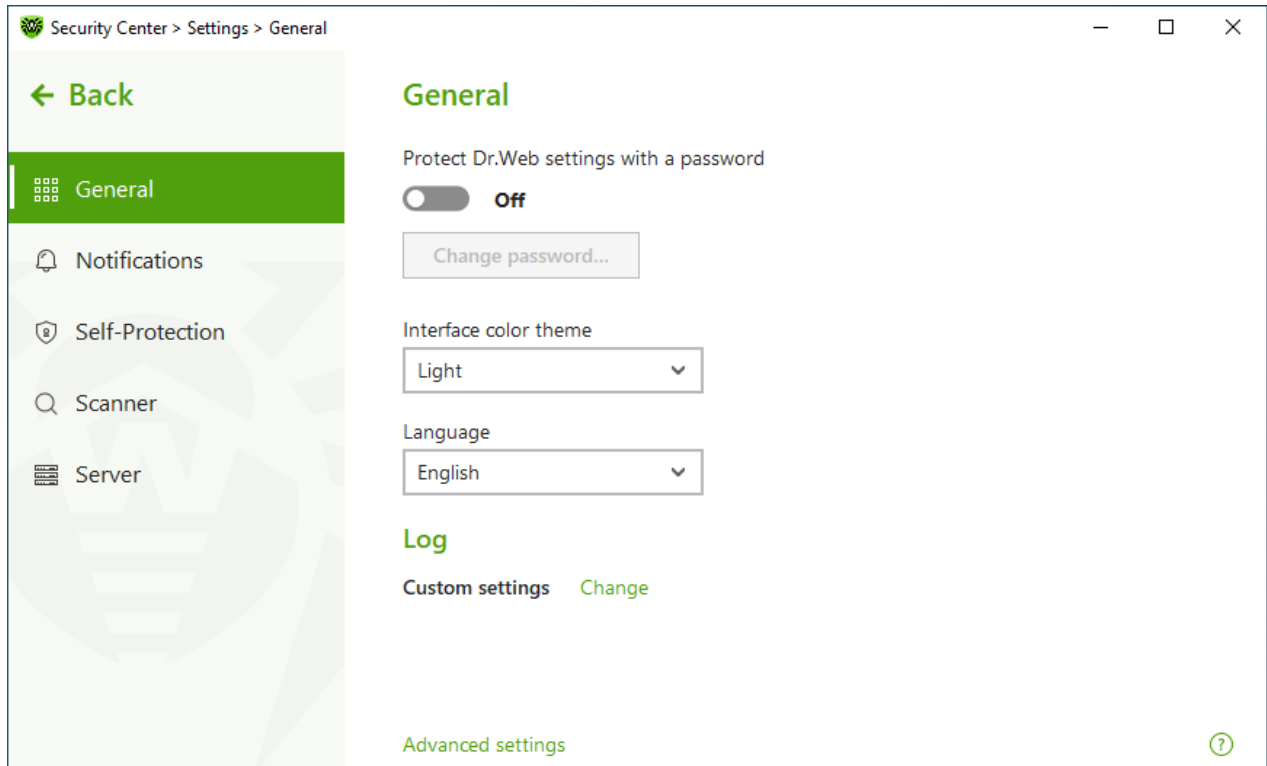



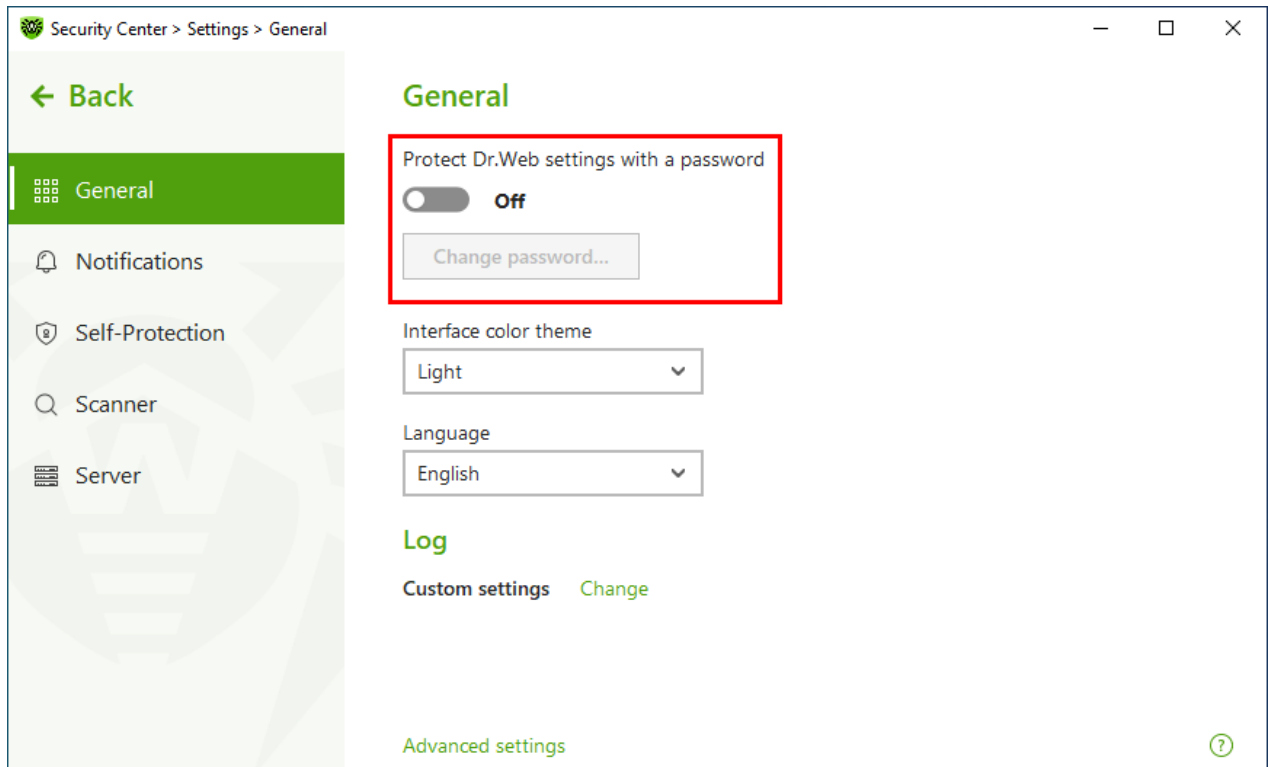
Figure 15. General Settings

### 7.1.1. Program Settings Password Protection

You can restrict access to Dr.Web settings on your computer by using a password. On every attempt to access Dr.Web settings, a password will be required.

#### To set a password

1. In the window with general settings, enable the **Protect Dr.Web settings with a password** option using the  switcher.



**Figure 16. Settings password protection**

2. In the open window, set a password and confirm it.
3. Click **OK**.

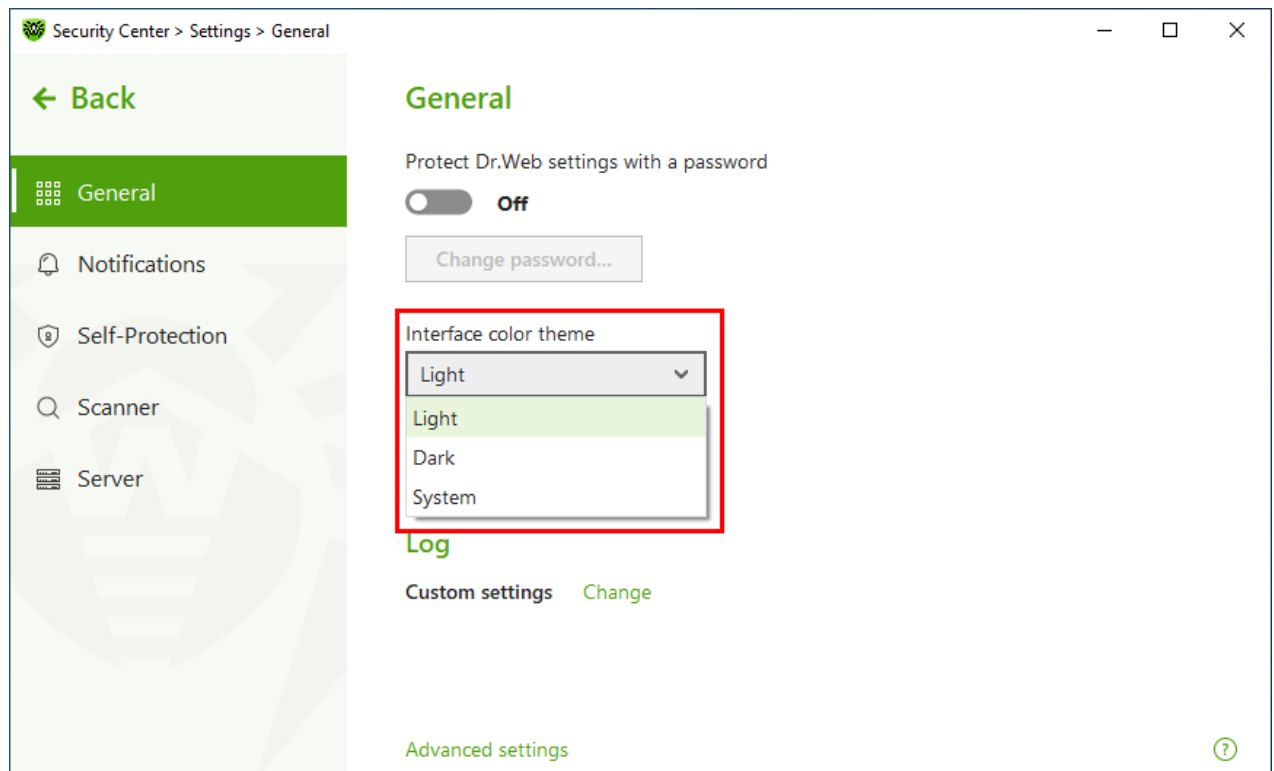


If you have forgotten your password for the product settings, contact your system administrator.

### 7.1.2. Selecting Interface Color Theme

If necessary, you can switch the program interface color theme. For this, select one of the following options from the **Interface color theme** drop-down list:

- **Light** to use the light appearance.
- **Dark** to use the dark appearance.
- **System** to use the system interface color. This option is selected by default.



**Figure 17. Selecting interface color theme**



The dark color theme is available for computers running Windows 10 (version 1909 and later), Windows 11 and Windows Server 2019 (starting with version 1809) and later. Interface color theme settings are hidden for earlier versions.

Update KB5011503 or later is required for the dark interface theme to function correctly.



### 7.1.3. Selecting Program Language

If necessary, you can switch the program interface language. The language list is updated automatically. Thus, it contains all localization languages that are currently available for the Dr.Web graphical interface. To switch the language, in the **Language** group, select a language from the drop-down menu.

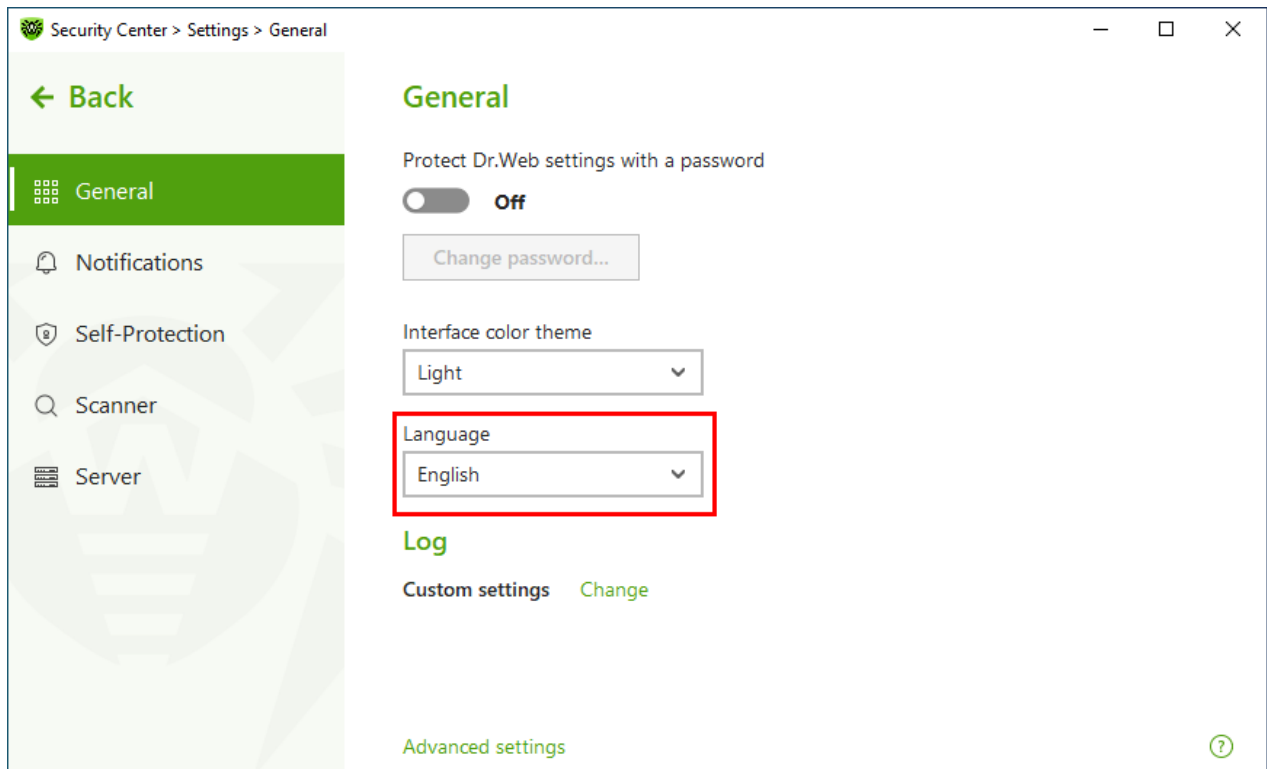


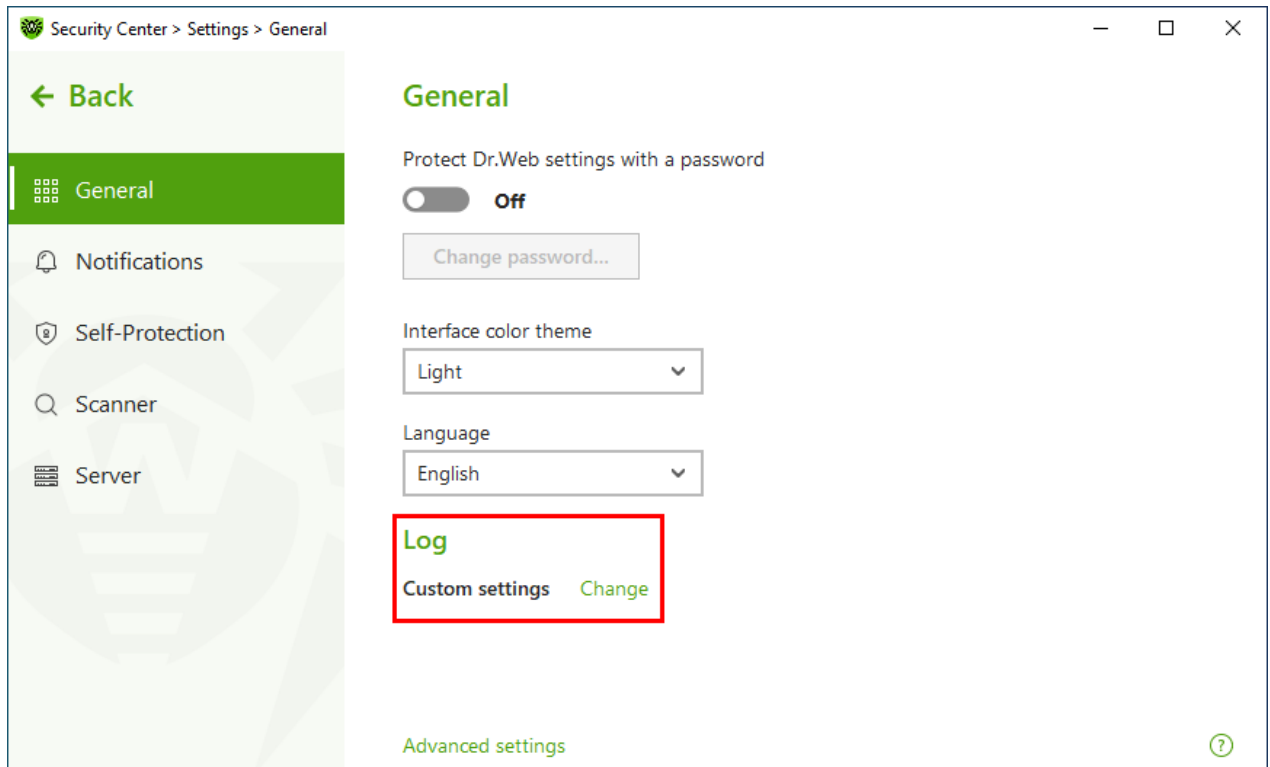
Figure 18. Selecting program language

### 7.1.4. Dr.Web Operation Logging

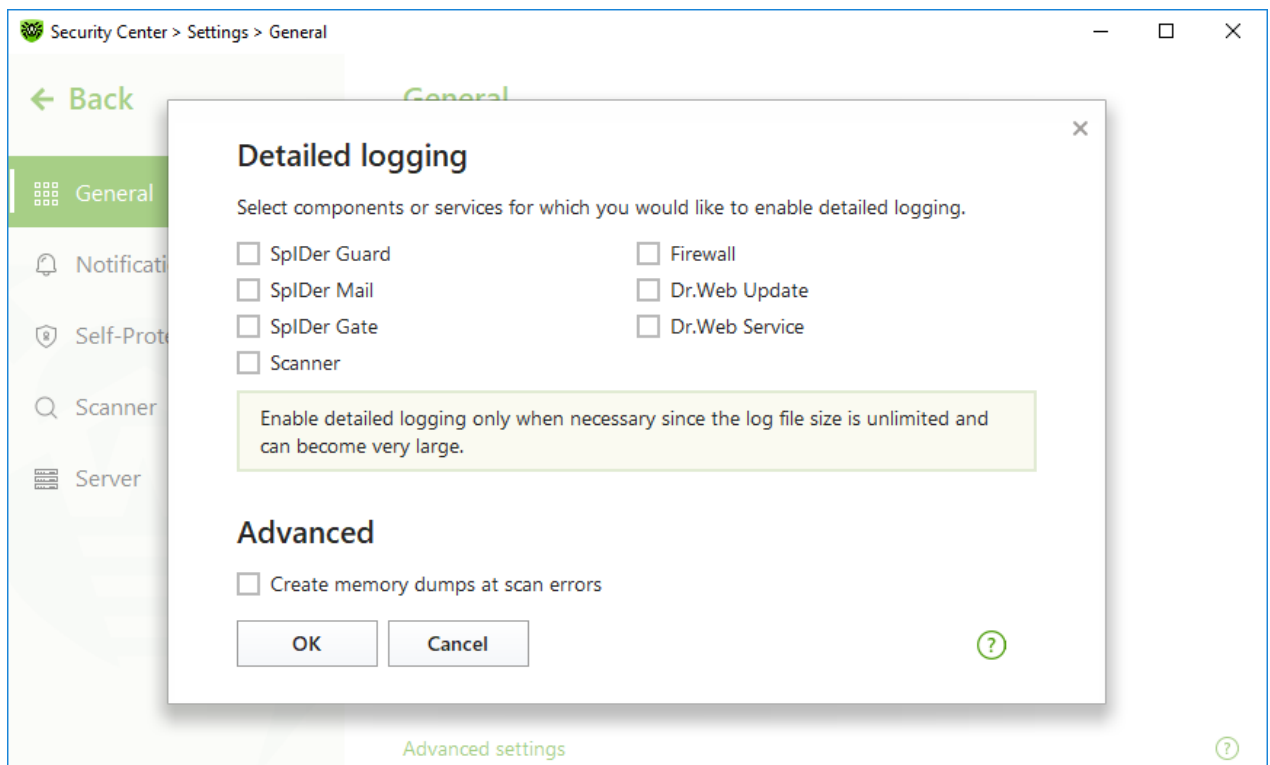
You can enable detailed logging for one or several Dr.Web components or services.

#### To change operation logging settings

1. In the **Log** section click **Edit**.

**Figure 19. General Settings. Log**

The window with detailed logging settings opens:

**Figure 20. Operation logging settings**

2. Select components, for which the detailed logging will be enabled. 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, data on scanned files, names of packers, and content of scanned complex objects (archives, email attachments, file containers).</p> <p>It is recommended that you use this mode to determine the most frequent objects scanned by SplDer Guard file monitor. If necessary, add these objects to the list of <a href="#">exclusions</a> in order to increase computer performance.</p>
SplDer Mail	<p>Time of updates and the mail anti-virus SplDer Mail starts and stops, virus events, connection interception settings, data on scanned files, names of packers, and content of scanned archives.</p> <p>It is recommended that you 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 that you use this mode for reception of more detailed information on the checked objects and work of the internet monitor.</p>
Scanner	<p>Updates of scanning modules and virus database information, time of Scanner starts and stops, information on detected threats, names of packers, and content of scanned archives.</p>
Firewall	<p>Information and decisions on requests coming to the service, information on unknown connections with reasons for the request, and information on errors.</p> <p>When you enable detailed logging, the component collects data on network packets (pcap logs).</p>
Dr.Web Update	<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 central protection server.</p>

## Memory dump creation

The **Create memory dumps at scan errors** option allows you 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. We recommend enabling 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



When logging detailed data on Dr.Web operation is enabled, 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. Make sure to use this mode only when errors occur in component operation or by request of your anti-virus network administrator.

1. To enable detailed logging for a Dr.Web component, select the corresponding check box.
2. Click **OK** to save the changes.



Log settings cannot be adjusted if the administrator of the central protection server to which Dr.Web is connected blocks this option.

---


Size of a log file is restricted to 10 MB by default (and 100 MB for SpIDer 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.

## 7.1.5. Quarantine Settings

To prevent the disk overuse, you can configure settings of storage of objects in quarantine, i.e. the period of storage, and to create the quarantine folder on a removable media.

### To change storage settings of the detected threats

1. In the window with general settings, click the **Advanced settings** link.
2. In the **Quarantine** section, enable or disable a necessary option using the  switcher.



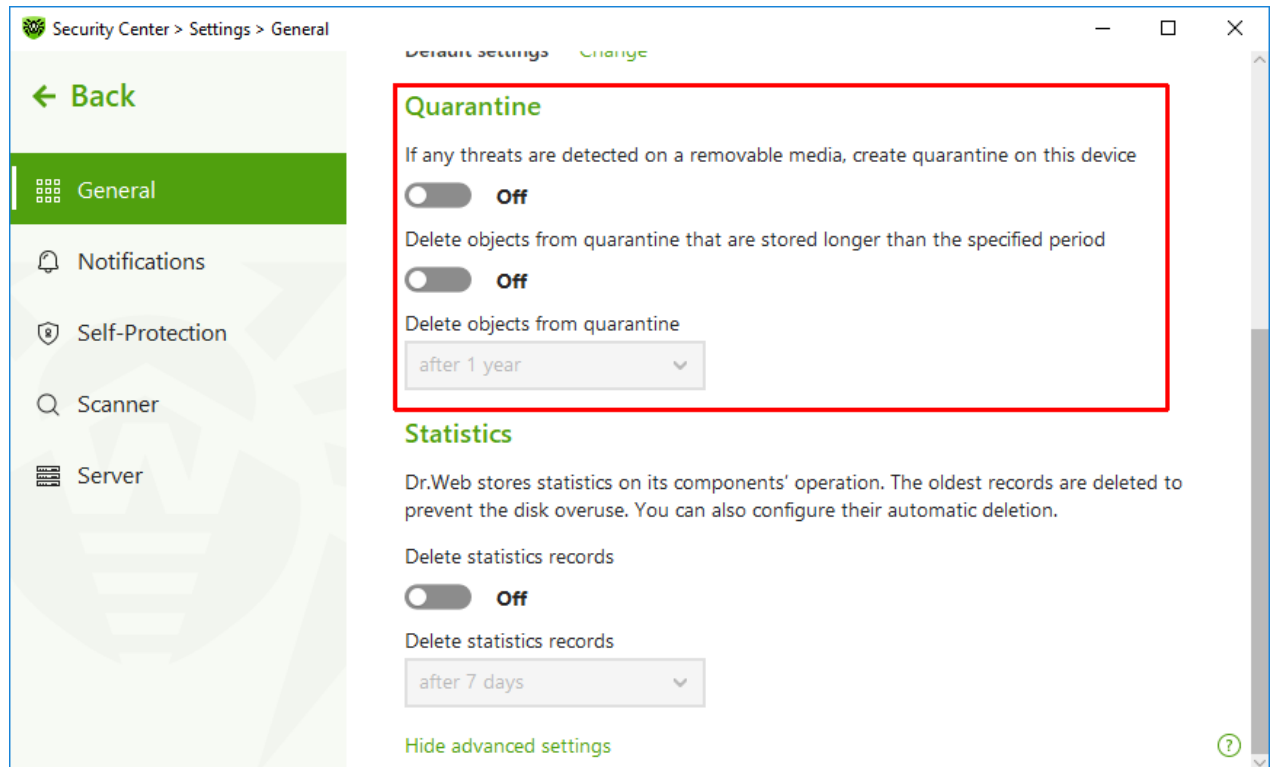


Figure 21. Quarantine settings

3. To enable the automatic deletion of objects from quarantine, select the time period in the drop-down menu. Objects stored more than the time specified will be deleted.

## Creating quarantine on removable media

The **If any threats are detected on a removable media, create quarantine on this device** option allows creating a quarantine folder on removable media for threats that are detected on the removable media. When this option is enabled, detected threats are moved to the quarantine folder without being encrypted. The quarantine folder can be created only when the removable media is accessible for writing. The use of separate folders and omission of encryption on removable media prevents possible data loss.

If the option is disabled, threats that are detected on removable media are moved to quarantine on the local disk.

## Automatic deletion of objects from quarantine


To prevent disk overuse, enable automatic deletion of objects from quarantine.

### 7.1.6. Automatic Deletion of Statistics Records

By default, Dr.Web stores optimal number of [statistics](#) records to prevent the disk overuse. In addition, you can enable automatic deletion of statistics records that are stored more than the specified period.



### To enable or disable automatic deletion of statistics records

1. In the window with general settings, click the **Advanced settings** link.
2. In the **Statistics** section, enable or disable automatic deletion of statistics records using the  switcher.

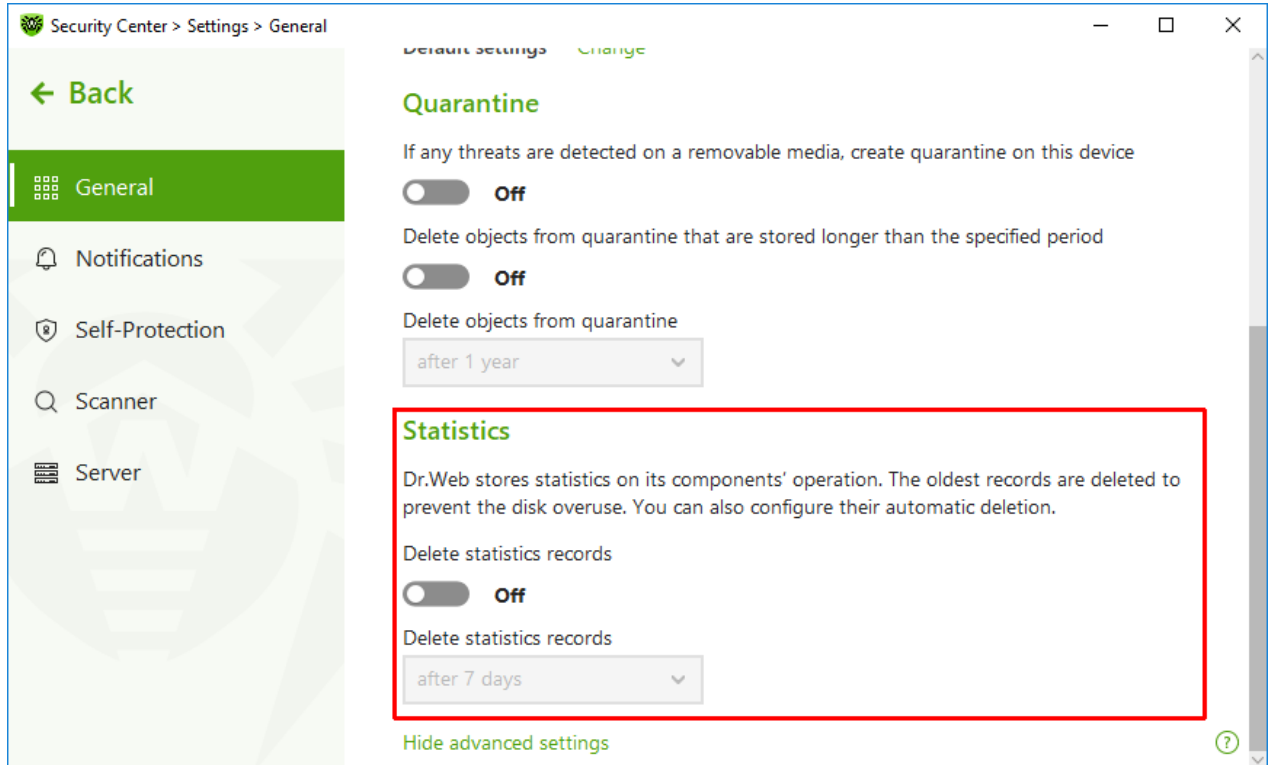


Figure 22. Statistics settings

3. Once this option is enabled, select the time period in the drop-down menu. Records stored more than the time specified will be deleted.

## 7.2. Notification Settings

You can configure parameters of receiving notifications on critical and important events of Dr.Web operation.

In this section:

- [Configuring notification parameters](#)

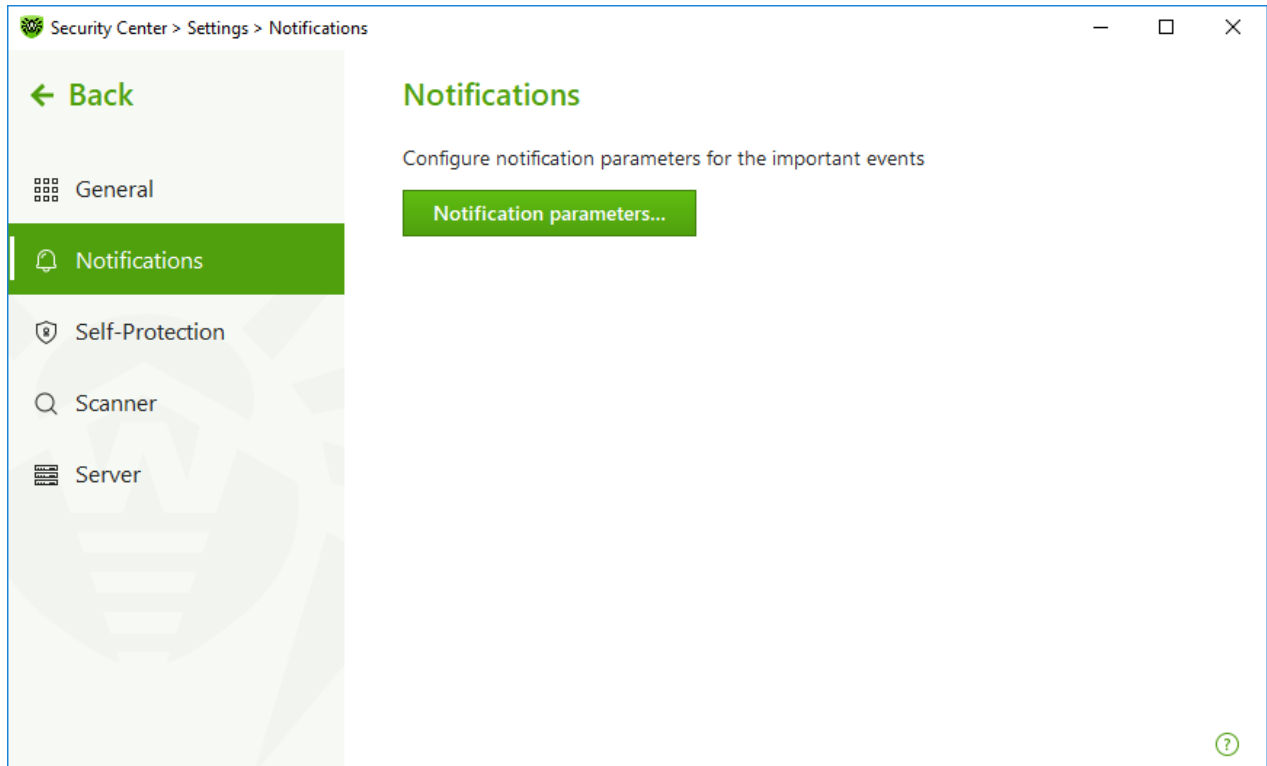
If necessary, configure parameters of receiving notifications on critical and important events of Dr.Web operation.

### To open the notification settings

1. Open Dr.Web [menu](#) , then select **Security Center**.



2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **Notifications** at the left of the window.



**Figure 23. Notification settings**

### To configure notification parameters

1. Click **Notification parameters**.
2. Select notifications that you want to receive. To display pop-up notifications, enable check boxes next to the necessary types of notifications.

Clear check boxes if you do not want to receive notifications on the event.

Notification type	Description
Threat is detected	Notifications on threats detected by SpIDer Guard and SpIDer Gate.  By default, these notifications are enabled.
Critical notifications	Notifications on the following critical issues: <ul style="list-style-type: none"><li>• Connections waiting for Firewall to reply are detected.</li><li>• Your login and password are already used for connection to the central protection server.</li></ul> By default, these notifications are enabled.



Notification type	Description
Major notifications	<p>Important notifications on the following issues:</p> <ul style="list-style-type: none"><li>• Working time on computer has expired.</li><li>• Virus databases are out of date (when operating in Mobile mode).</li><li>• Device is blocked.</li><li>• Attempt to change system date and time is blocked.</li><li>• Access to the protected object is blocked by Behavior Analysis.</li><li>• Access to the protected object is blocked by Exploit Prevention.</li><li>• Access to the protected object is blocked by Ransomware Protection.</li><li>• Process launch is blocked by the administrator.</li><li>• MSI package installation is blocked by the administrator.</li><li>• Script launch is blocked by the administrator.</li><li>• Object loading is blocked for the process.</li><li>• Creation of the executable file is blocked for the process.</li><li>• Modification of the executable file is blocked for the process.</li></ul> <p>By default, these notifications are disabled.</p>
Minor notifications	<p>Minor notifications on the following issues:</p> <ul style="list-style-type: none"><li>• URL is blocked by Office Control.</li><li>• URL is blocked by SplDer Gate.</li><li>• Working time in the internet has expired.</li><li>• Access to the protected object is blocked by Office Control.</li><li>• Scan of your computer is run by the administrator of your anti-virus network.</li><li>• Scan of your computer is run according to the schedule.</li><li>• Scan of your computer is finished.</li><li>• Successful update.</li><li>• Update error.</li></ul> <p>By default, these notifications are disabled.</p>

3. If necessary, configure additional parameters:

Option	Description
Do not show notifications in full-screen mode	<p>Hide notifications when an application is running in full-screen mode on your computer (e.g., a game or a movie).</p> <p>Clear this check box to display notifications regardless of the mode.</p>
Display Firewall notifications on separate desktop in full-screen	<p>Notifications from Firewall on a separate desktop when an application is running in full-screen mode on your computer (a</p>



Option	Description
mode	game or a movie).  Clear this check box to display notifications on the same desktop where an application is running in full-screen mode.



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.
- Automatic restart.
- Request for allowing a process to modify an object.
- Message sent by central protection server administrator.
- Successful connection to the server.
- New keyboard connected.





## 7.3. Self-Protection

You can configure protection of Dr.Web itself from unauthorized modification by malicious programs that target anti-viruses or from accidental damage.

In this section:

- [Enable and disable Self-Protection](#)
- [Block changing the system date and time](#)

### To open Self-Protection settings

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **Self-Protection** at the left of the window.

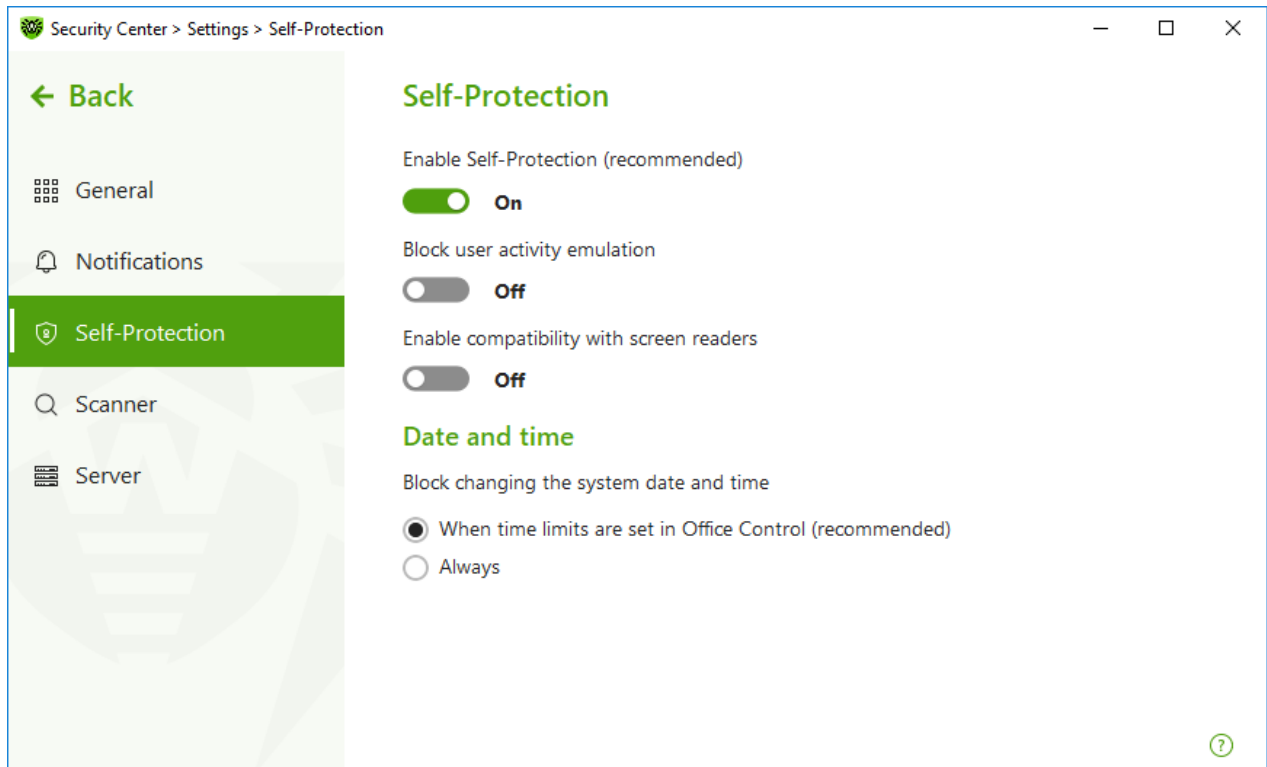


Figure 24. Dr.Web self-protection parameters

## Self-Protection settings

The **Enable Self-Protection (recommended)** option allows you to protect Dr.Web files and processes from unauthorized access. Self-Protection is enabled by default. It is not recommended disabling 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 you 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 and other actions aimed at changing Dr.Web operation).

The **Enable compatibility with screen readers** option allows you to use such screen readers as, for example, JAWS and NVDA for reading loud the information on Dr.Web interface elements. This option makes Dr.Web interface accessible for disabled people.



## 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 the system date and time** option allows you 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 Office Control. If internet or computer usage limits are set in Office Control, this option is automatically enabled. You can configure [notification parameters](#) to be informed on an attempt to change the system time.

## 7.4. File Scan Options

You can configure Scanner parameters, and change default actions for detected threats. The default settings are optimal for most cases. Do not change them unnecessarily.

### To open file scan options

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **Scanner** at the left of the window.



The component settings can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.

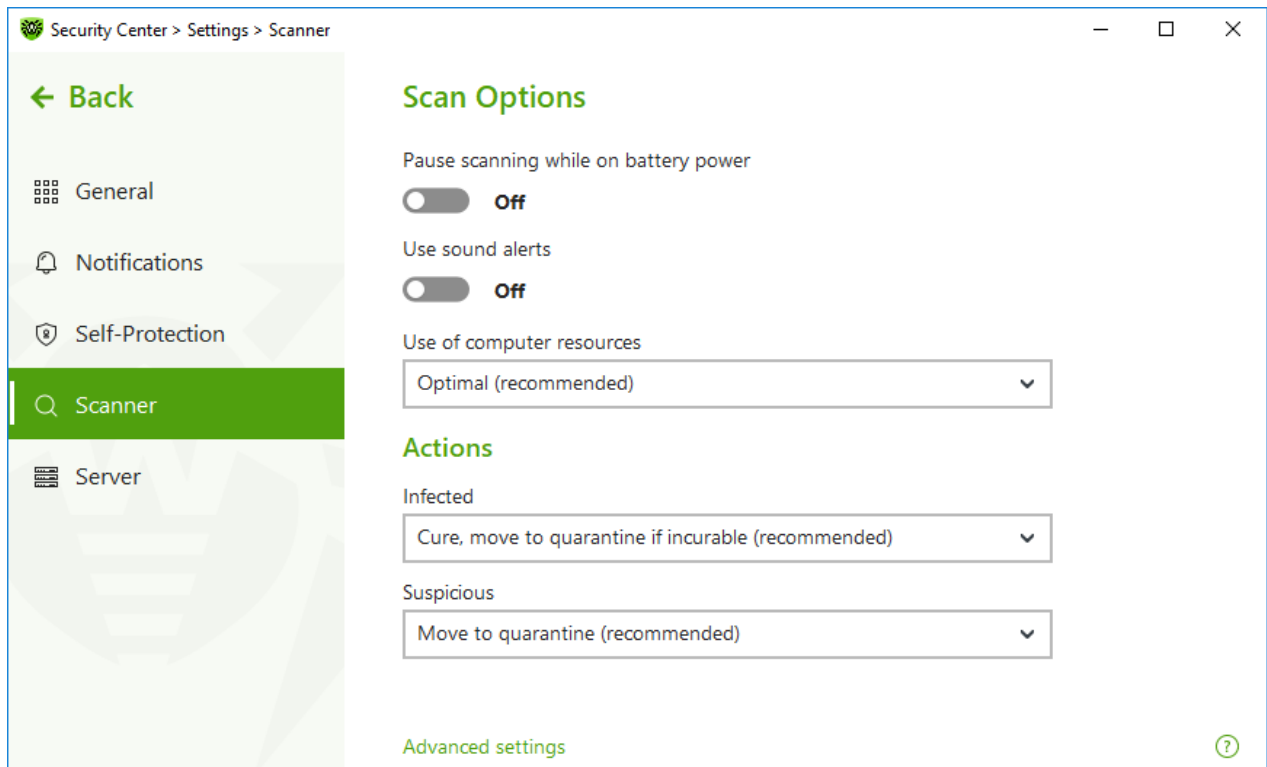


Figure 25. Scanner settings

## Scan Options

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

- **Pause scanning while on battery power.** Enable this option to pause 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 of detecting or neutralizing a threat. 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

In this setting group, you can specify Scanner reaction 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.
- Objects that pose potential threat (riskware).





By default, Scanner attempts to cure files infected by a known or potentially curable virus. Scanner moves the other most dangerous objects to [Quarantine](#). You can change reaction of Scanner to detection of each type of malware separately. Set of available reactions depends on the threat type. The default actions are optimal and marked as recommended.

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 incurable	<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 <a href="#">Quarantine</a>.</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.

## Additional options

To open advanced settings, click the **Advanced settings** link in the **Scan Options** window Figure [Scanner 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 completed:

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





## 7.5. Server

You can view and adjust parameters of interaction between Dr.Web and the Server as well as specify settings for the Mobile mode of Dr.Web. The administrator of the anti-virus network can restrict you from adjusting the server connection parameters. If so, the buttons and check boxes are unavailable.

In this section:

- [Connection parameters](#)
- [Settings of the connection to the central protection server](#)
- [Certificates](#)
- [Station connection parameters](#)
- [Advanced settings](#)
- [Mobile mode](#)

### To go to parameters of interaction between station and server

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **Server** at the left of the window.

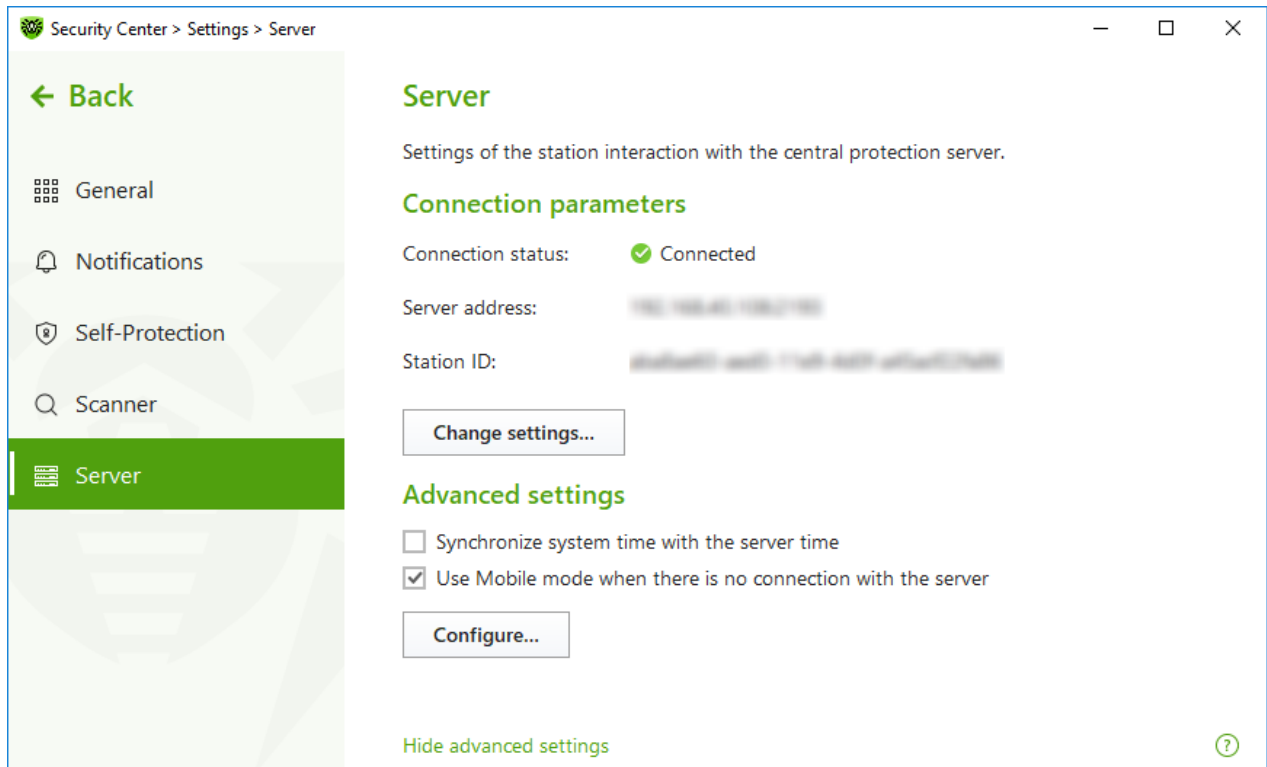


Figure 26. Station connection settings

## Connection parameters

In the **Connection parameters** group, you can see:

- **Connection status**—central protection server connection status of the station.
- **Server address**—central protection server address to which the station is connected.
- **Station ID**—workstation ID for server connection.

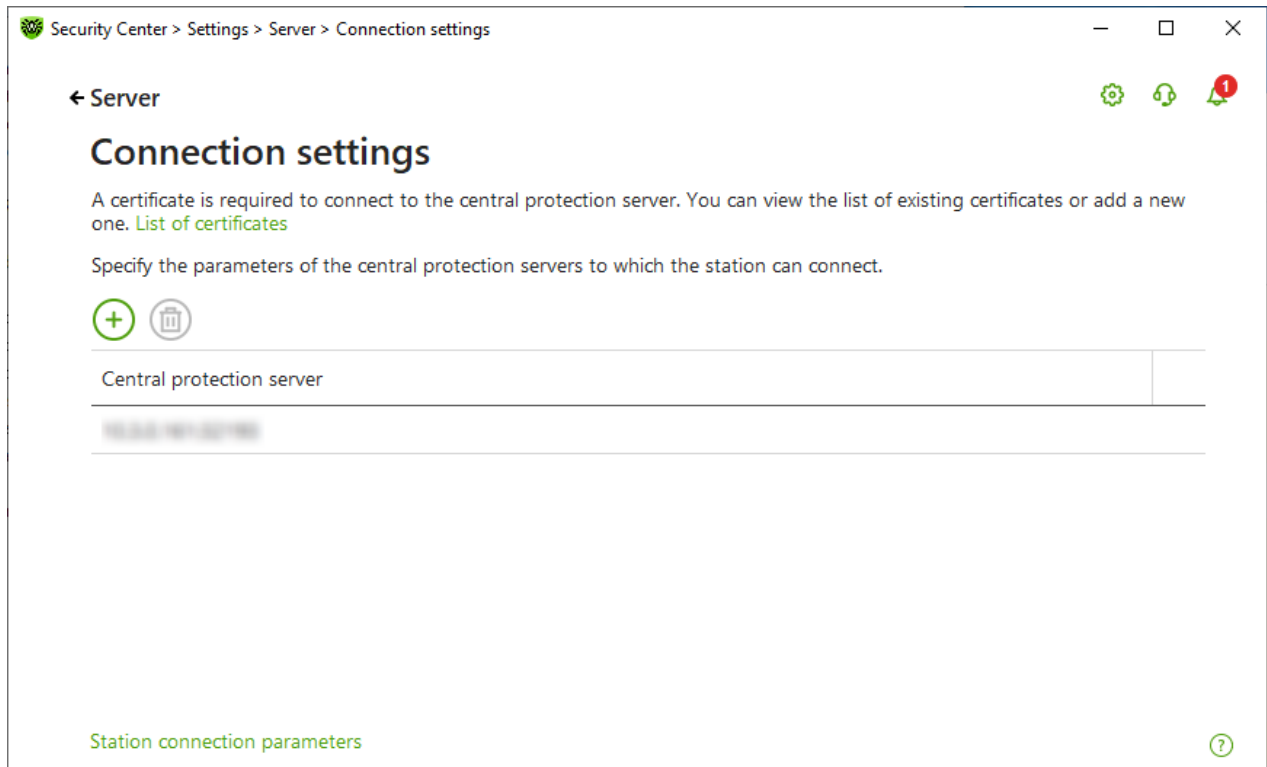
You can view and manage server connection settings, if the network administrator provides you with the corresponding privileges.



You can configure connection to the central protection server only in coordination with the anti-virus network administrator; otherwise, the computer will be disconnected from the anti-virus network.

## Connection settings


To configure connection to the current server or to a new one, click **Change settings**. The **Connection settings** window opens:



**Figure 27. Server connection settings**

In the table, you can see the list of all servers to which the station can connect. You can remove servers from the table and add new ones.


The following management elements are available to work with objects in the table:


- The  button—deleting the entry.

## Certificates

A valid certificate is required so that the station can connect to the central protection server. The certificate can be unique for each specific server or can match several servers. You can add several certificates used for connection to several servers. A valid certificate should be provided by the administrator of the anti-virus network.

By default, the certificate that was used during the installation process is specified, unless the administrator has not changed the encryption keys on the server. If the keys have been changed, the latest certificate from the list of generated certificates is shown. To view the list of available certificates or add another one, click the **List of certificates** link.

To add a new certificate, click . In the open window, select the necessary file.

To delete unused certificate, click .



## Station connection parameters

### To edit the station connection parameters

1. In the **Station connection parameters** window, specify the station ID and the password used for server connection. This information is provided by the server administrator.
2. Click **OK** to save changes.

### To reset connection parameters and connect to the central protection server as a newbie

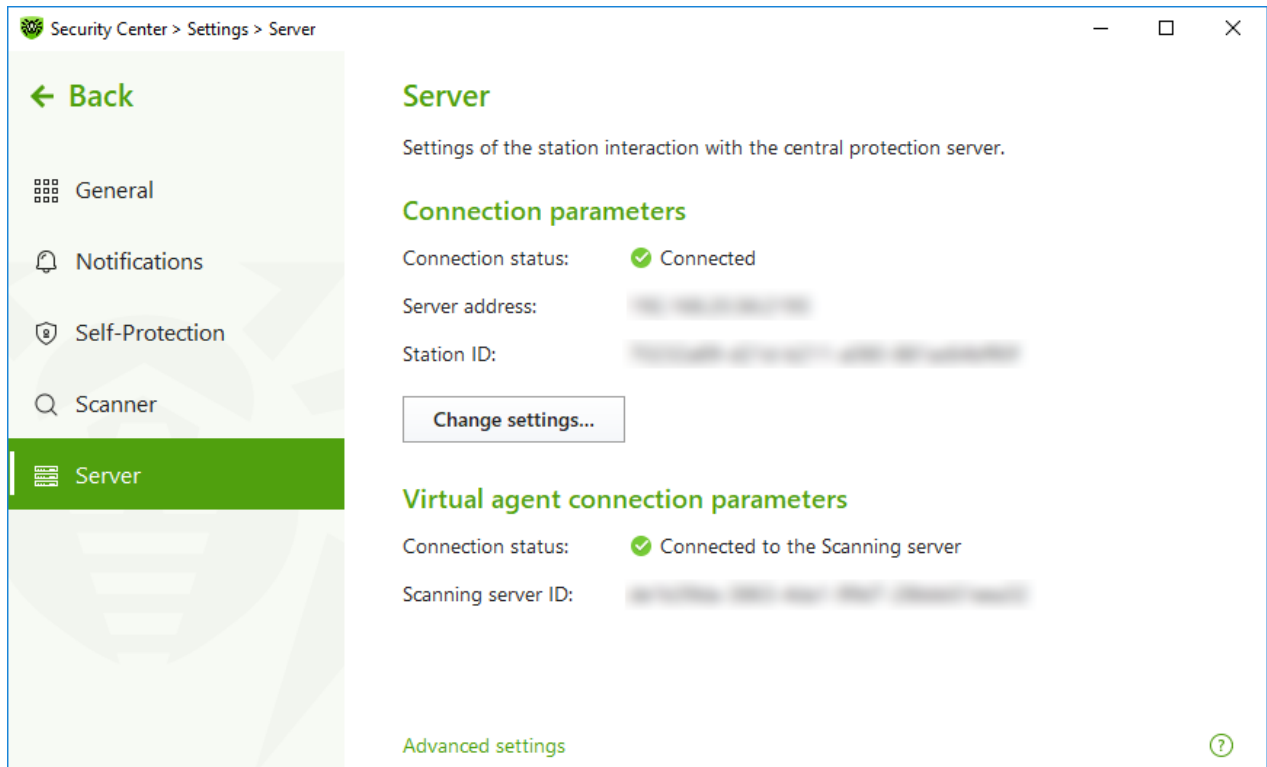
1. In the **Station connection parameters** window, click **Reset the parameters and connect as a newbie**.
2. In the open window, confirm that you want to reset the connection parameters and connect as a newbie. Please note that this action cannot be undone.
3. Dr.Web receives new station ID and password after the station registration is confirmed on the central protection server. The new station ID and password will be used for server connection.

## Virtual agent connection parameters

Depending on settings on the server side, the station can connect to the Scanning Server. In this case, the station is considered *virtual agent*; it sends requests to scan files and URLs to the server. Virus databases and filter bases are not stored on the station.

When using the Scanning Server, the **Virtual agent connection parameters** group of settings is displayed on the station with the following information:

- Scanning Server connection status of the station;
- Scanning Server ID.



**Figure 28. Connecting to the Scanning Server**



If there is no connection to the Scanning Server, the station is not protected. Please contact your anti-virus network administrator.

## Advanced settings

To open advanced settings, click the **Advanced settings** link in the **Server** window (see Figure [Station connection settings](#)). You can choose the following options in the **Advanced settings** group:

- **Synchronize system time with the server time**—synchronize system time on your computer with the time on the central protection server. In this mode, Dr.Web periodically sets the time on you computer in accordance with the server time.
- **Use Mobile mode when there is no connection with the server**—keep virus databases up-to-date.

## Mobile mode

If your computer is disconnected from the central protection server for a long time, we recommend enabling the Mobile mode of Dr.Web operation in order to receive updates from the Doctor Web update servers. For that purpose, select the **Use Mobile mode when there is no connection with the server** check box.



The **Use Mobile mode when there is no connection with the server** option can be enabled or disabled only if use of this mode is allowed for this workstation in the settings of the central protection server.

In the Mobile mode, Dr.Web attempts to connect to the central protection server. After three unsuccessful attempts, it performs an update of the virus databases from Doctor Web update servers. Attempts to establish server connection are performed with an interval of about one minute.

### To configure Mobile mode settings

1. Click **Configure** button. The **Mobile mode** window opens.
2. From the **Receive updates** drop-down list, select the frequency of checking updates on the Doctor Web update servers.



If you select **Manually** from the **Receive updates** list, automatic updates are not performed. You can enable the update in the Dr.Web menu.

3. To use proxy server, select the corresponding check box. The following fields will become active:

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.

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



In the Mobile mode, only virus databases are updated.

If you disable the **Use Mobile mode when there is no connection with the server** option when there is no connection with the server before the connection to the central protection server is reestablished, the virus databases will stop updating, but searching for the server will be continued.



All changes specified for the workstation on the server take effect only after the Mobile mode is disabled and connection between Dr.Web and the central protection server is reestablished.

## 7.6. Server Notifications

The network administrator can enable sending server notifications to a station. This feature can be convenient to work with the notifications on the central protection server. If this feature is enabled for the station, the **Server Notifications** section appears in the **General** window.

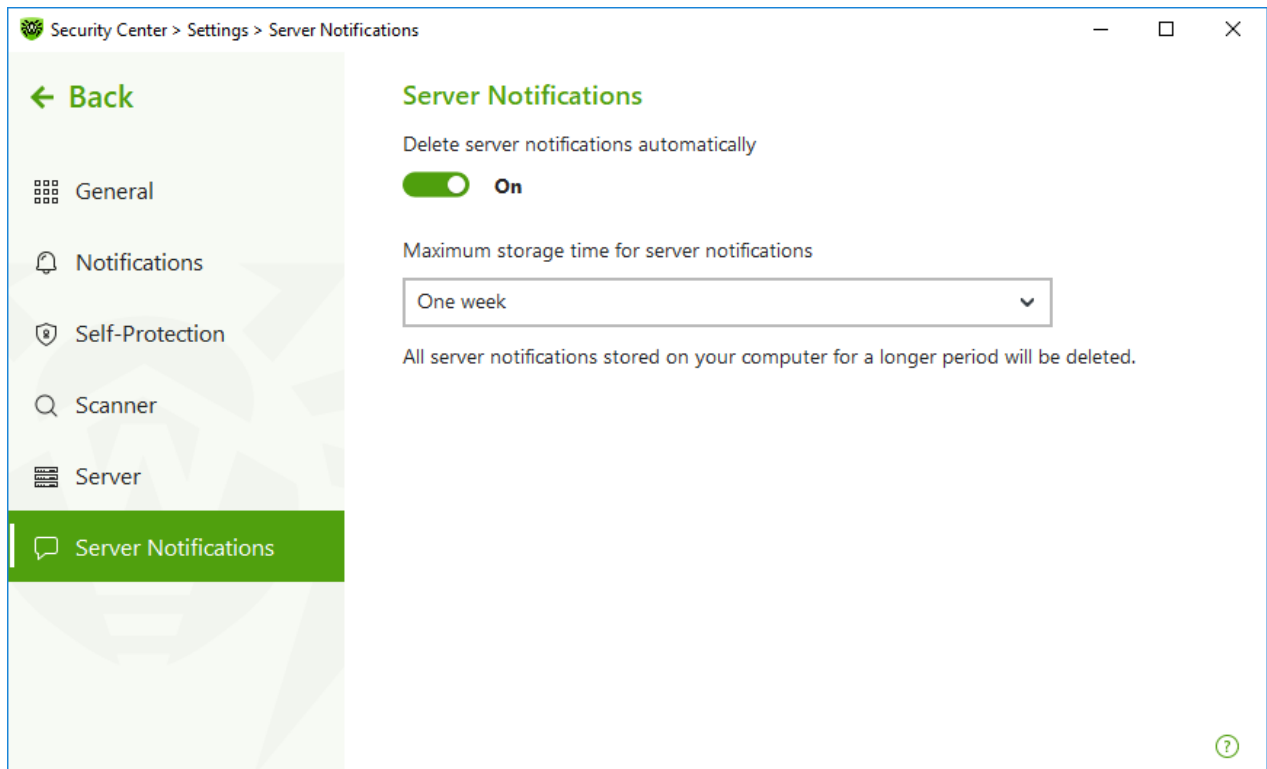







Figure 29. Automatic server notifications deletion settings

### To enable or disable automatic deletion of server notifications

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. At the top of the program window, click .
4. A product main settings window opens. Select **Server Notifications** at the left of the window.
5. Enable or disable **Delete server notifications automatically** option by using the switcher .
6. When this option is enabled, select the necessary period of time in the **Maximum storage time for server notifications** drop-down list. Notifications will be deleted after this period of time.






## 8. Files and Network

This group of settings provides you with an access to the parameters of the main protection components and Scanner.

### To open the Files and Network group of settings

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.

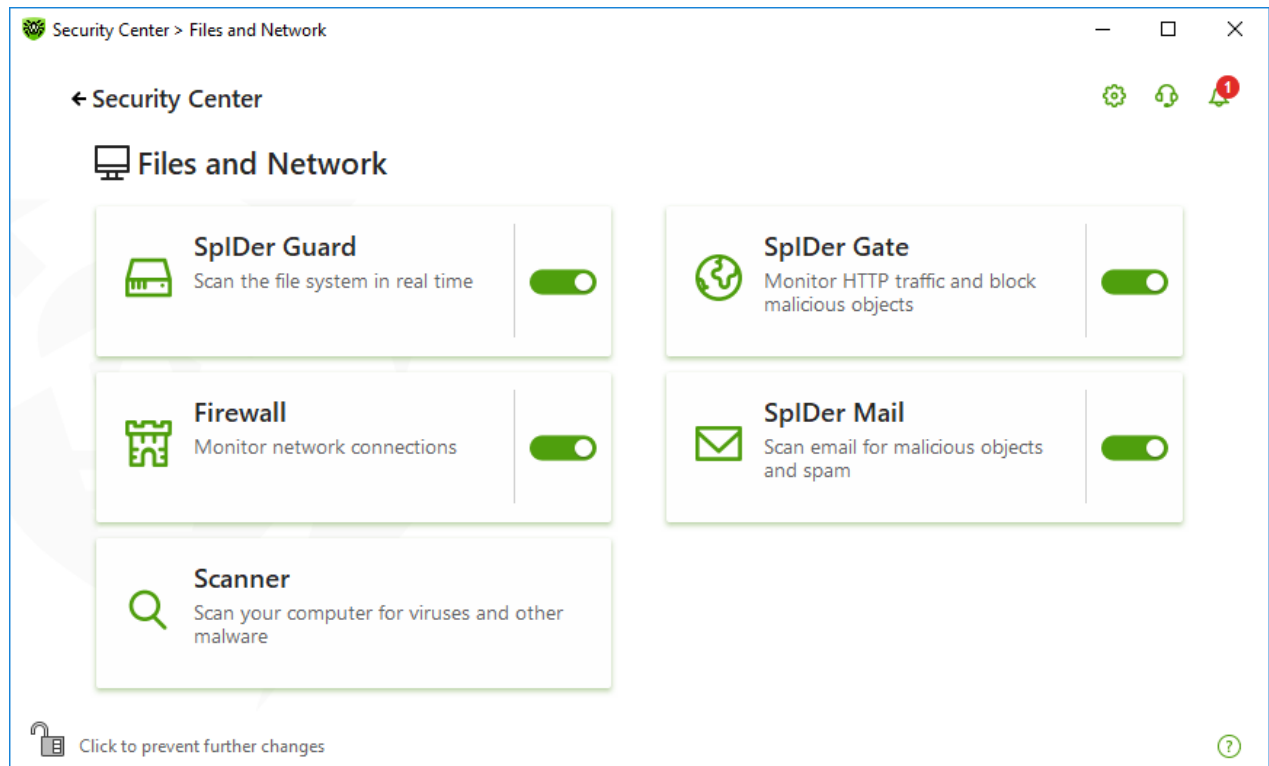




Figure 30. The Files and Network window

### Enable and disable protection components

Enable or disable the necessary component by using the switcher .

### To open the component parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the tile of a necessary component.


In this section:

- [The file system monitor SpIDer Guard](#) is a component that scans files when they are being opened, launched, or changed, and processes that are being launched, in real time.



- [The internet monitor SpIDer Gate](#) is a component that scans HTTP traffic.
- [The email anti-virus SpIDer Mail](#) is a component that scans email for malicious objects and spam.
- [Firewall](#) is a component that monitors connections and data transfer via the internet and blocks suspicious connections both on network and application levels.
- [Scanner](#) is a component that scans object on user demand or according to schedule.
- [Dr.Web for Microsoft Outlook](#) is a module for Microsoft Outlook.





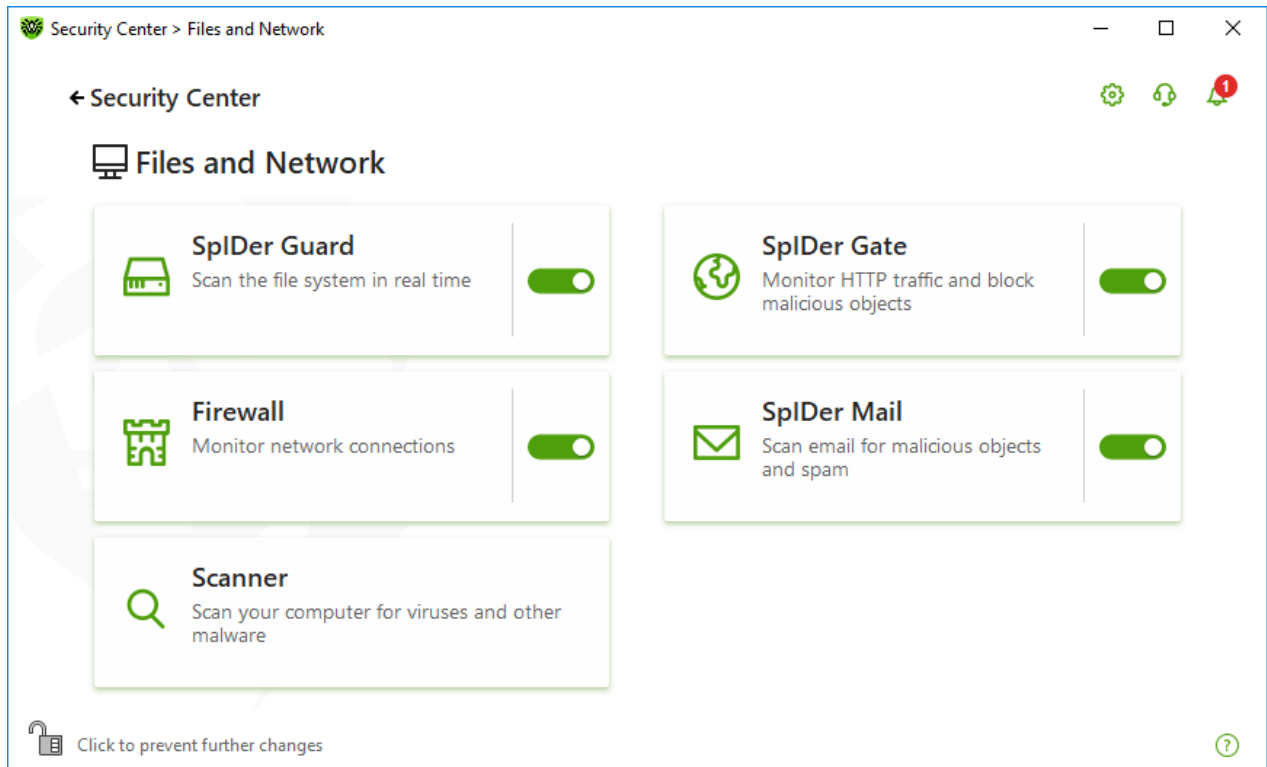
To *disable* any component, Dr.Web should operate in the administrator mode. For that, click the lock  at the bottom of the program window.

## 8.1. Real-Time File System Protection

The file system monitor SpIDer Guard protects your computer in real time and prevents infecting of your computer. SpIDer Guard automatically launches upon Windows startup and scans file when they are opened, run, or edited. SpIDer Guard also monitors actions of launched processes.

### To enable or disable the file system monitor

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Enable or disable the file system monitor SpIDer Guard by using the switcher .



**Figure 31. Enabling/Disabling SplDer Guard**

In this section:

- [SplDer Guard operation peculiarities](#)
- [Removable media scan](#)
- [Actions for detected threats](#)
- [Selecting the scan mode by SplDer Guard](#)
- [Advanced settings](#)

See also

- [Excluding files and folders from scanning](#)
- [Excluding applications from scanning](#)

## SplDer Guard operation peculiarities

With the default settings, SplDer Guard 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, SplDer Guard constantly monitors running processes for virus-like activity and, if such is detected, blocks malicious processes.



SplDer Guard does not scan files within archives, email archives, and file containers. If a file within an archive or email attachment is infected, a threat will be detected on the archive extraction, when a computer cannot be infected.



By default, SplDer Guard loads automatically when Windows starts and cannot be unloaded during the current Windows session.



Incompatibility between Dr.Web and Microsoft Exchange Server is possible. If any problem occurs, add Microsoft Exchange Server databases and transaction log to the [exclusion list](#) of SplDer Guard.

## SplDer Guard file system monitor parameters

If infected objects are detected, SplDer Guard applies actions according to the specified parameters. The default settings are optimal for most cases. Do not change them unnecessarily.

### To open SplDer Guard parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the **SplDer Guard** tile. A component parameters window opens.

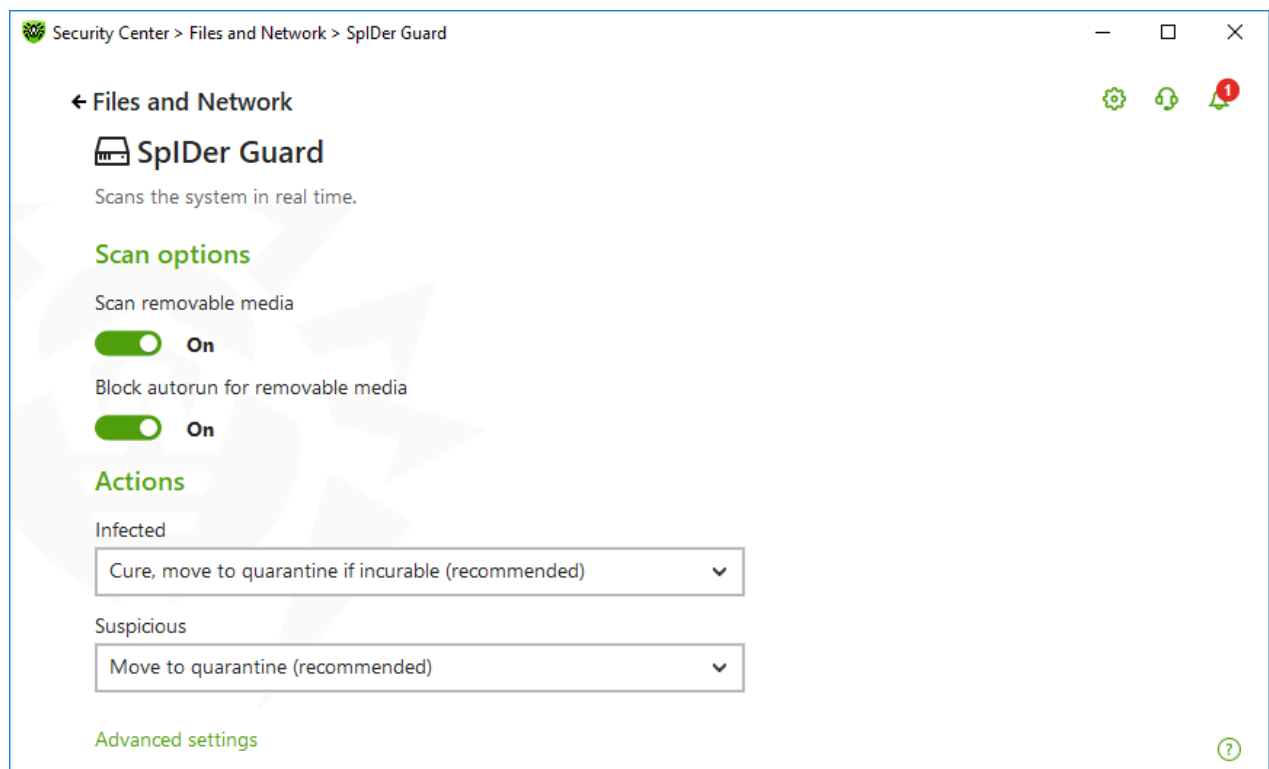


Figure 32. The file system monitor parameters

## Removable media scan


By default, SplDer Guard 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, as well as blocking the automatic startup of their active content. This method prevents your computer from getting



infected through removable media, as SplDer Guard monitors your file system accesses in the real-time mode and blocks the execution of malicious code.



Operating system may register some removable media as hard drives (for example, portable USB hard drives). In this case, the Safely Remove Hardware and Eject Media icon is not displayed in the Windows notification area. Unless in paranoid scan mode, SplDer Guard does not perform scanning when reading a file from such a disk. Scan such devices with Dr.Web Scanner when you connect them to the computer.

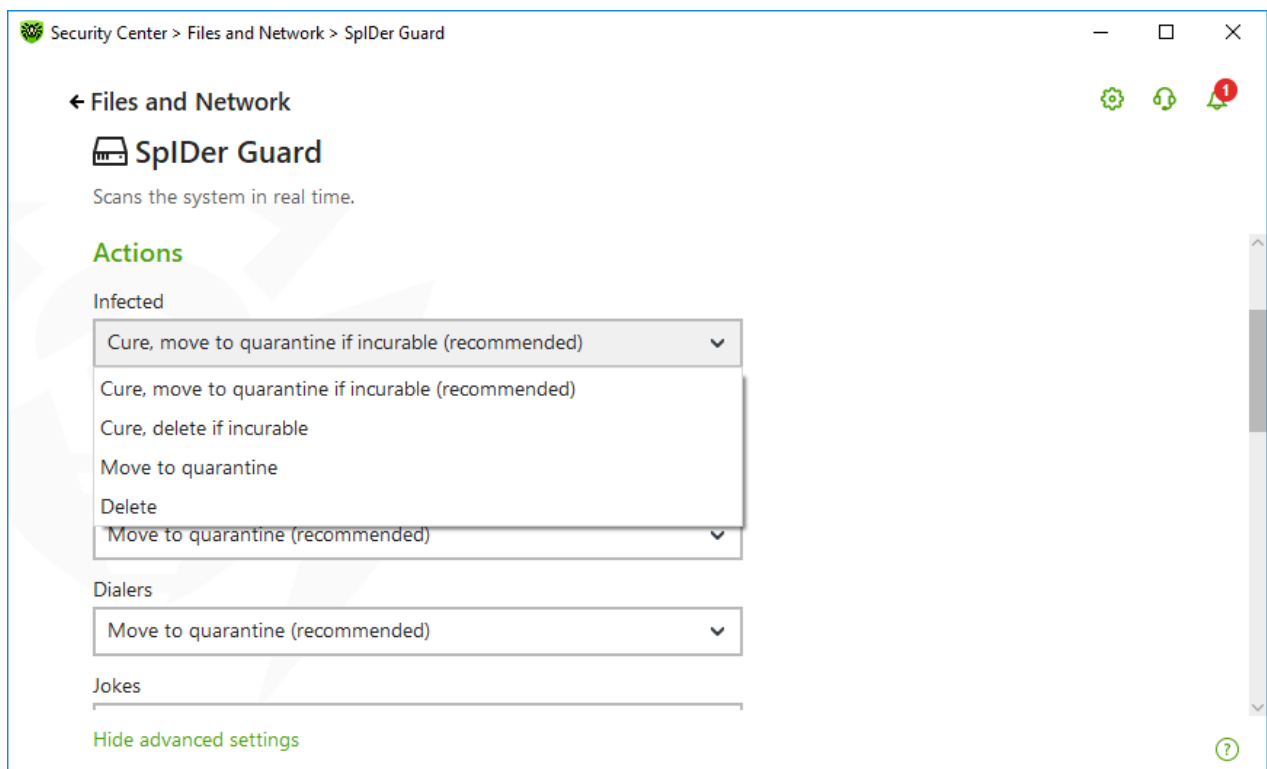
You can enable or disable the **Scan removable media** and **Block autorun for removable media** options by using the switcher  in the **Scan options** setting group.



If any problem occurs during installation with the autorun option, it is recommended that you temporary disable the **Block autorun for removable media** option.

## Actions for detected threats

In this group, you can configure actions that Dr.Web will apply to threats detected by the file system monitor SplDer Guard.



**Figure 33. Configuring actions applied to threats**

The actions are set separately for each type of malicious and suspicious objects. These actions vary for different object types. The recommended actions are set by default for each type of objects. Copies of all processed objects are stored in [Quarantine](#).



## Possible actions

The following actions can be applied to 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 incurable	<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 <a href="#">Quarantine</a>.</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>
Report	<p>Instructs to display a notification and skip the object without performing any actions.</p> <p>The action is available only for suspicious objects and malware.</p>

## SpIDer Guard scan mode

To access this and following sections, click the **Advanced settings** link.

In this setting group, you can select the file scan mode of the SpIDer Guard monitor.

Mode	Description
Optimal, used by default	In this mode, SpIDer Guard scans objects only when one of the following actions is traced:



Mode	Description
	<ul style="list-style-type: none"><li>• 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.</li><li>• For objects on removable media, an attempt to access file or boot sectors in any way (write, read, execute).</li></ul> <p>It is recommended that you use this mode after a thorough <a href="#">scan</a> of all hard drives by Dr.Web Scanner. With this mode activated, SplDer Guard prevents possibility of 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.</p>
Paranoid	<p>In this mode, SplDer 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> <p>This mode ensures maximum protection but considerably reduces computer performance.</p>

## Additional options

The settings of this group allow you 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, Windows 11)

## 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 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.



## 8.2. Checking Web Traffic

SpIDer Gate scans HTTP traffic and blocks malicious objects. HTTP is used by browsers, download managers, and other applications which work with the internet. SpIDer Gate does not check data transmitted over cryptographic protocols, such as HTTPS.

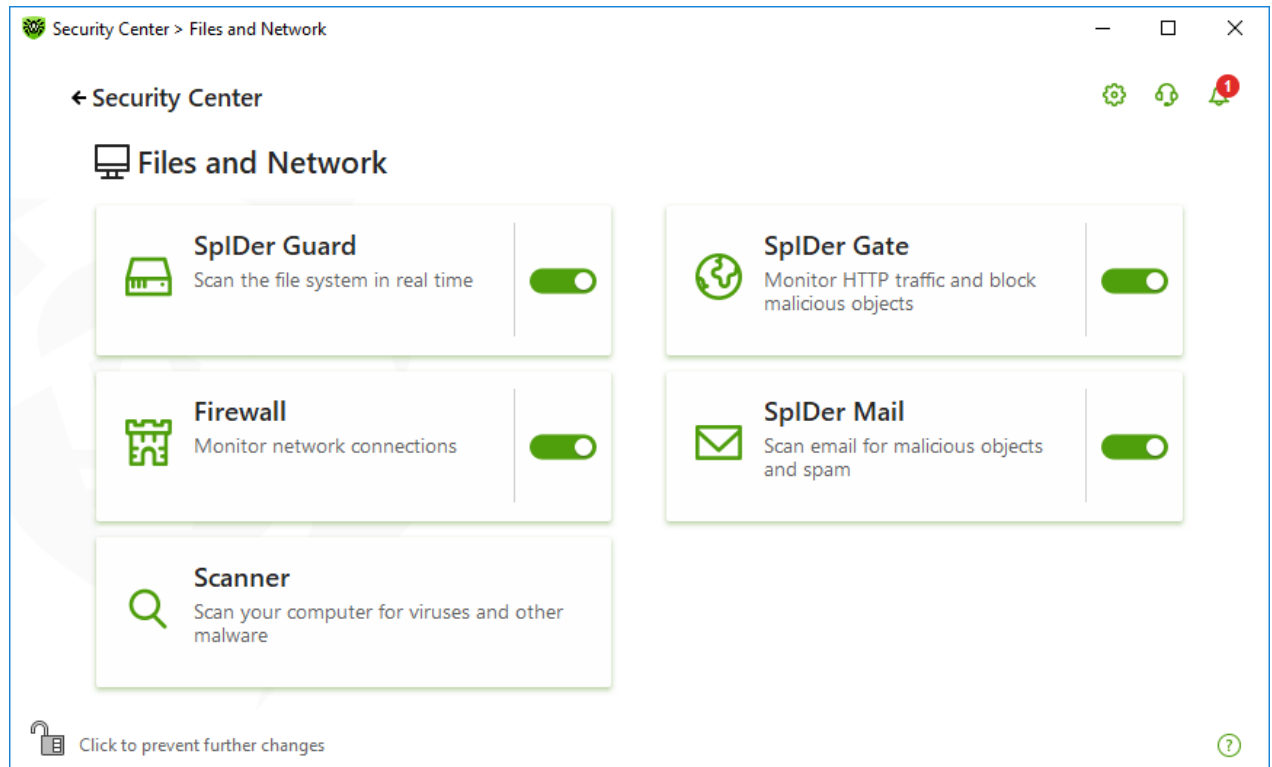
By default, SpIDer Gate filters non-recommended websites and websites known as infection sources.

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

### To enable or disable traffic scan and non-recommended websites filter

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Enable or disable SpIDer Gate by using the switcher .





**Figure 34. Enabling/Disabling SplDer Gate**

In this section:

- [Traffic and URLs in IM clients scan](#)
- [Blocking parameters](#)
- [Block programs](#)
- [Block unchecked and corrupted objects](#)
- [Check archives and installation packages](#)
- [Use system resources during the checks](#)
- [Traffic direction](#)

See also:

- [Exclude websites from scan](#)
- [Excluding applications from scanning](#)

## Traffic check options



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



The component parameters can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.



## To open SplDer Gate parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the **SplDer Gate** tile. A component parameters window opens.

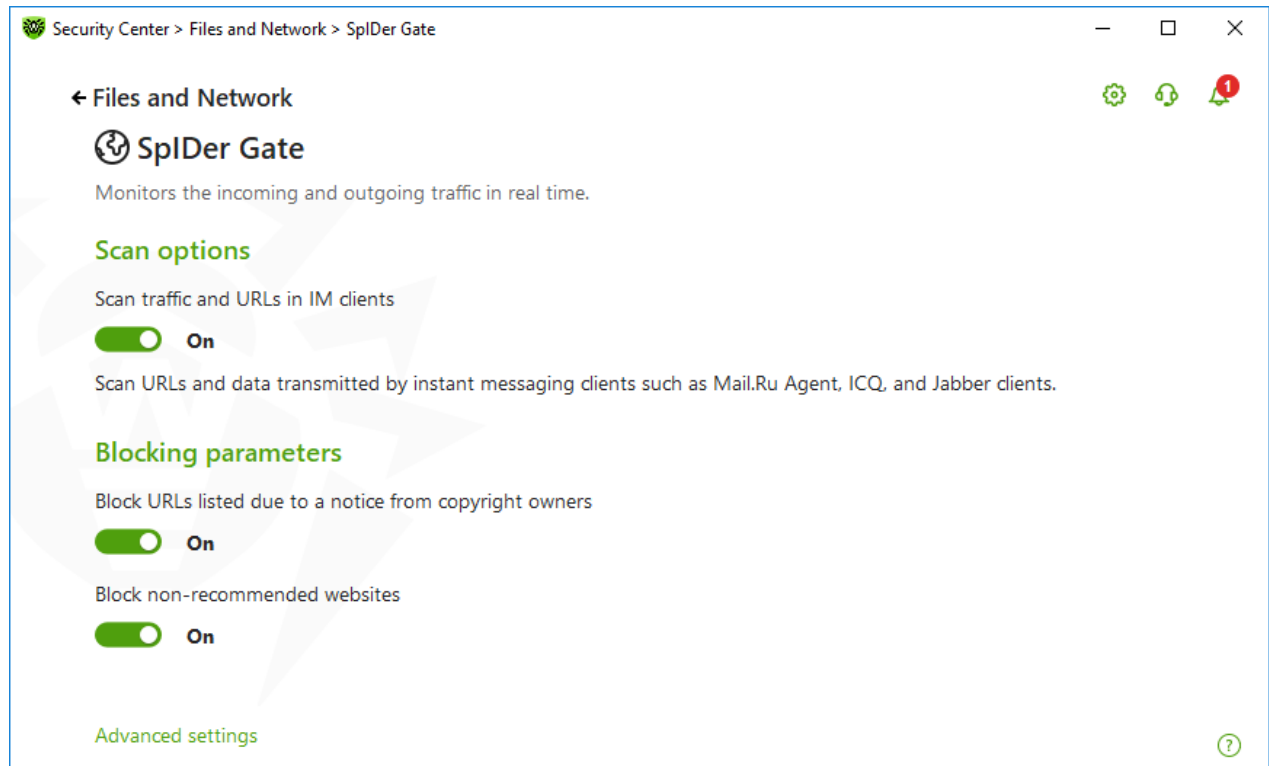


Figure 35. HTTP traffic check parameters

## Traffic and URLs in IM clients scan

In the **Scan options** group, you can enable scanning of URLs and files transmitted by instant messaging clients, such as Mail.ru Agent, ICQ, and Jabber clients. Only incoming traffic is checked. By default, the option is enabled.



The following actions are applied to the found threats:

Object	Action
<b>URL scan</b>	
Websites known as infection sources	Blocked automatically.
Non-recommended websites and URLs listed due to a notice from the copyright owner	Blocked according to settings in the <b>Blocking parameters</b> group.
<b>File scan</b>	
Viruses	Blocked automatically.
Malware: <ul style="list-style-type: none"><li>• Suspicious</li><li>• Riskware</li><li>• Dialers</li><li>• Hacktools</li><li>• Adware</li><li>• Jokes</li></ul>	Blocked according to parameters in the <b>Block programs</b> group.

When SpIDer Gate scans URLs in messages, the [websites](#) and [applications](#) excluded from scan have an effect.

## Blocking parameters

In the **Blocking parameters** group, you can enable automatic blocking of URLs listed due to a notice from copyright owners and blocking unreliable websites. For this, enable the corresponding option.

To allow access to necessary websites [specify exclusions](#) in the **Exclusions** group.



By default, SpIDer Gate blocks access to the websites known as infection or malware sources except the [list of websites excluded from scan](#).

## Block programs

To access this and following sections, click the **Advanced settings** link.

SpIDer Gate can block the following malware:

- Suspicious
- Riskware



- Dialers
- Hacktools
- Adware
- Jokes

To enable blocking of malware, click the **Advanced settings** link and enable the corresponding switchers in the **Block programs** group. By default, SpIDer Gate blocks suspicious programs, adware and dialers.

## Block objects

SpIDer Gate can block unchecked and corrupted objects. By default, these settings are disabled. To open the settings, click the **Advanced settings** link.

## Advanced settings

**Scan archives** and **Scan installation packages**. The settings are disabled by default.

**Level of system resource consumption.** In some cases Dr.Web cannot determine the final file size for example when loading the file. In this case, the file is sent for the scan in parts. It requires the use of computer resources. You can configure the resource use level and determine the frequency of sending files with unknown size. If you select a high resource use level, files will be sent more frequently and will be scanned faster. However, frequent scans increase processor load.



**Traffic scan mode.** By default, SpIDer Gate scans incoming traffic only. If necessary, you can select HTTP traffic type to scan.

During the traffic scanning, the SpIDer Gate parameters, the [white list](#), and the [list of applications excluded from scan](#) have an effect.

## 8.3. Email Scan

SpIDer Mail scans your email. Email anti-virus SpIDer Mail is installed by default. It resides in memory and runs automatically at OS startup. SpIDer Mail can also scan messages for spam using Dr.Web Anti-spam. SpIDer Mail cannot scan encrypted email traffic.

### To enable or disable email scan

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Enable or disable the email anti-virus SpIDer Mail by using the switcher .

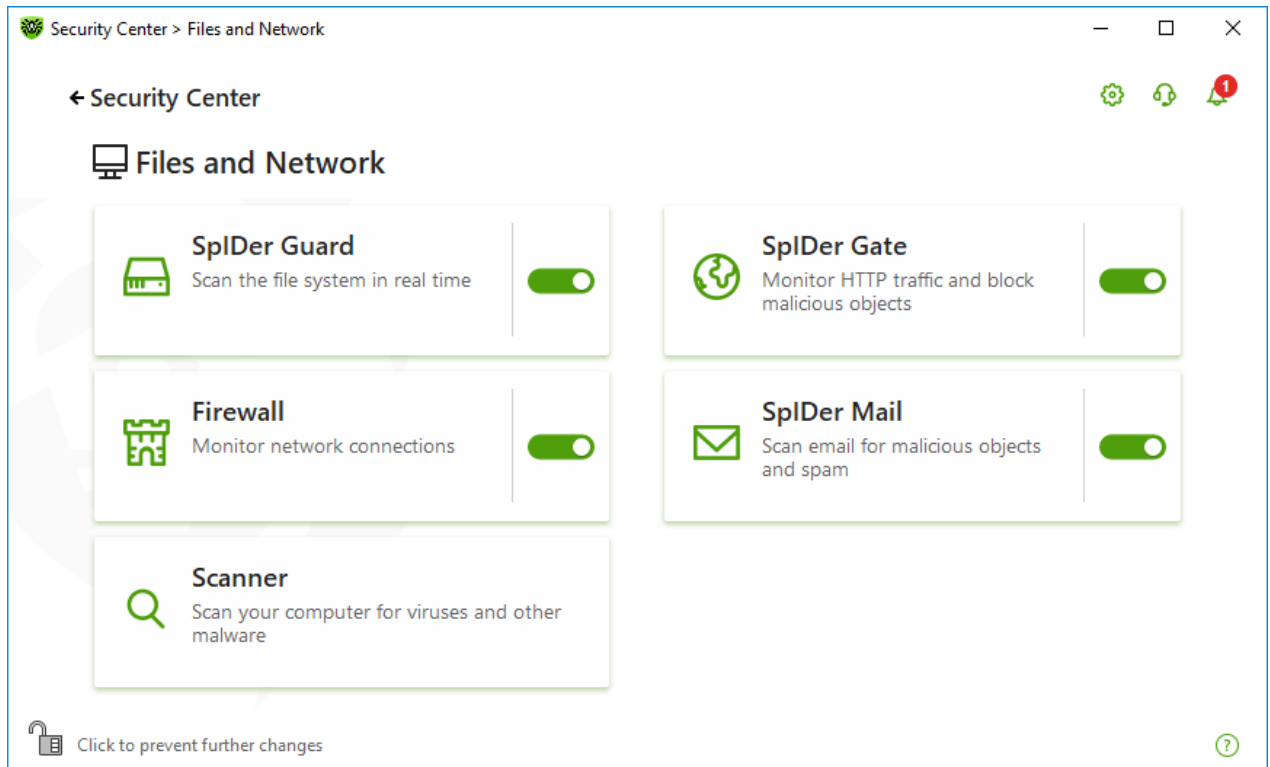


Figure 36. Enabling/Disabling SpliDER Mail

In this section:

- [Message processing](#)
- [Scanning messages by other components](#)

See also:

- [Configuring message scan](#)
- [Anti-spam parameters](#)

## Message processing

SpliDER Mail intercepts any incoming messages and scans them before they are received by mail clients. If no threats are detected, messages are passed on to the email client as if they have been received directly from the server. Similar procedure is applied to outgoing messages before they are sent to a server.

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

Message type	Action
Infected messages	Removes malicious content from the messages. Then the messages are delivered as usual. This action is called <i>curing</i> the message.



Message type	Action
Messages with suspicious objects	Moves the messages to <a href="#">Quarantine</a> as separate files. The email client receives a notification about this. This action is called <i>moving</i> the message. All moved messages are deleted from the POP3 or IMAP4 mail servers.
Safe messages and messages that have not been scanned	Passes the messages on to the mail client ( <i>skips</i> ).

Infected or suspicious *outgoing messages* are not sent to the server. The user is notified that a message will not be sent (usually the email client saves such a message).

## Scanning messages by other components

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.
- Scanner does not check mailboxes at the moment of the mail receipt, but either on user demand. Furthermore, this action is resource consuming and may take a lot of time.

### 8.3.1. Configuring Message Scan

By default, SpIDer 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](#). Other messages are transmitted unchanged by SpIDer Mail (*skipped*). The default message scan parameters are optimal for most cases. Do not change them unnecessarily.

In this section:

- [Actions for detected threats](#)
- [Configuring message scan parameters](#)
- [Scanning archives](#)




## Configuring message scan

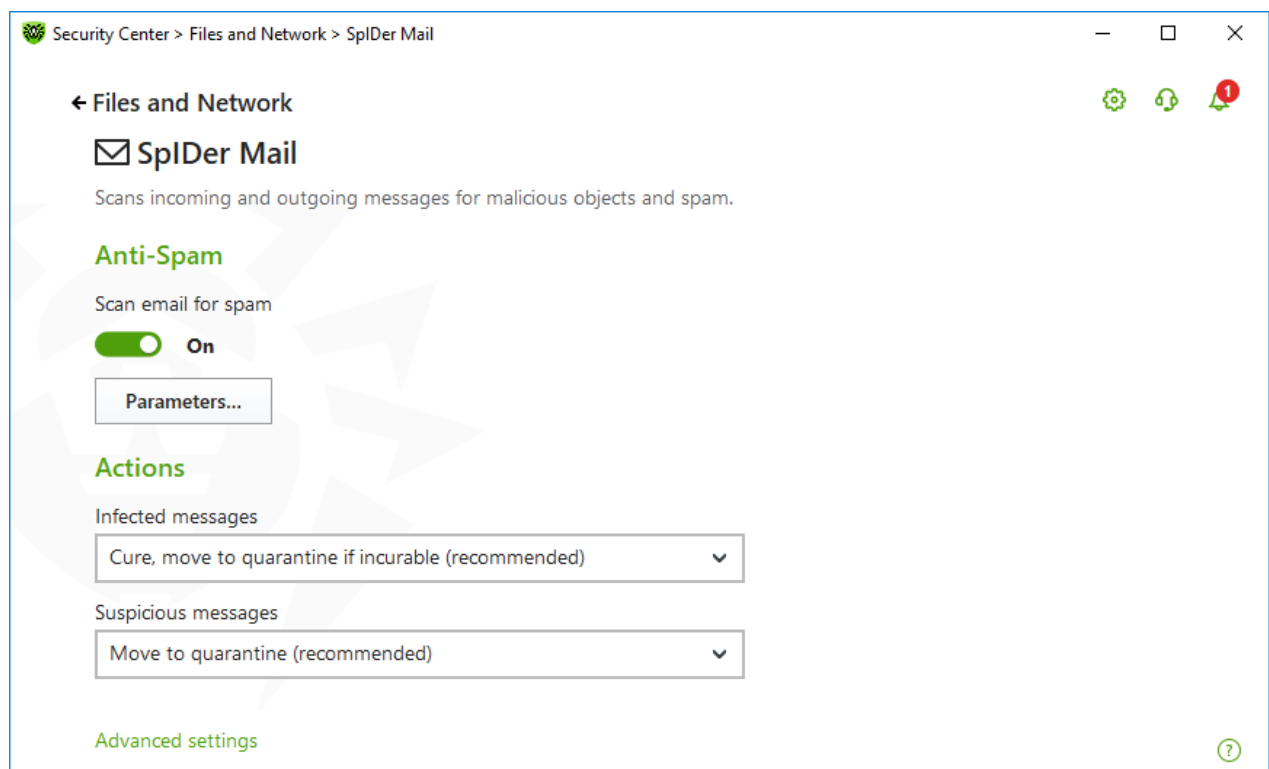
The default SpIDer Mail settings are optimal for recent users, provide maximum protection and require minimum user actions. However, by default SpIDer Mail may block some features of email programs (for example, sending a message to multiple addresses might be considered as mass distribution, incoming mail is not scanned for spam). Useful information from safe text part of infected messages also becomes unavailable in case of automatic deletion.



The component parameters can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.

### To start editing email scan parameters

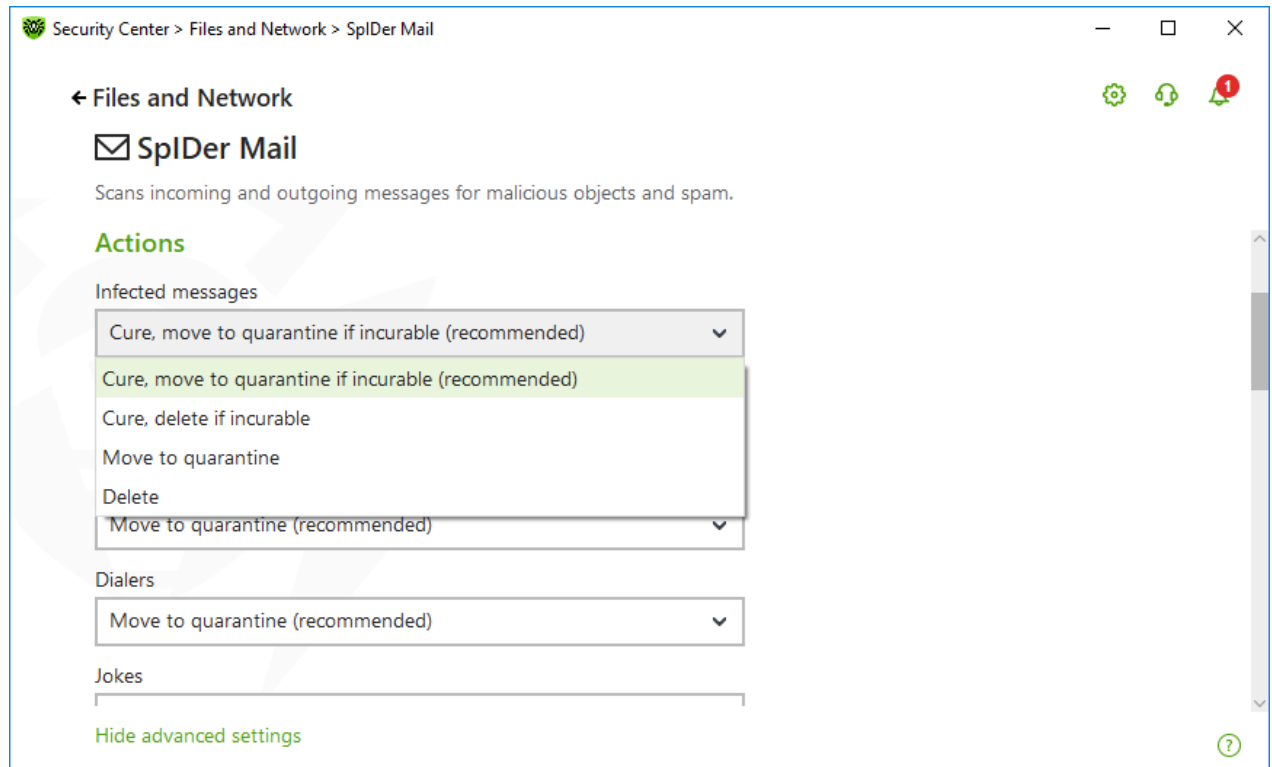
1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Click the **SplDer Mail** tile. A component parameters window opens.



**Figure 37. Email scan parameters**

### Actions for detected threats

In this group, you can configure actions that Dr.Web will apply to messages if Dr.Web detects a threat in them.



**Figure 38. Configuring actions for messages**

## Possible actions

The following actions can be applied to 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> <p>Results in failure to send the message.</p>
Cure, delete if incurable	<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 deleted.</p> <p>Results in failure to send the message.</p>
Delete	<p>Instructs to delete the message. The message is not sent to the recipient; the mail client receives a notification about this.</p> <p>Results in failure to send the message.</p>





Action	Description
Move to Quarantine	Instructs to move the message to the special <a href="#">Quarantine</a> folder. The message is not sent to the recipient; the mail client receives a notification about this.  Results in failure to send the message.
Ignore	Instructs to pass the message to the mail client as usual, that is, without performing any action.

You can increase security above the default level. For this, click the **Advanced settings** link and select **Move to quarantine** action for **Not scanned**. It is recommended that you scan the moved file with Dr.Web Scanner after that.



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

## Configuring message scan parameters

To access the parameters of message scan, click the **Advanced settings** link.

### 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	This option is enabled by default.  Instructs SpIDer Mail to add scan results and information on Dr.Web version to message headers after processing. You cannot edit data format.
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.

### Scan optimization

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 scanning the message.



## Scanning archives

Enable the **Scan archives** option if you want SpIDer Mail to scan archived files transferred via email. If necessary, enable the following options and configure scan parameters for archives:

- **Maximum file size to extract.** If an archive size exceeds the specified value (by default, 30,720 KB), SpIDer Mail does not unpack and scan 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.



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

## Additional options

The following settings allow you to configure additional email 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.




## Notification settings

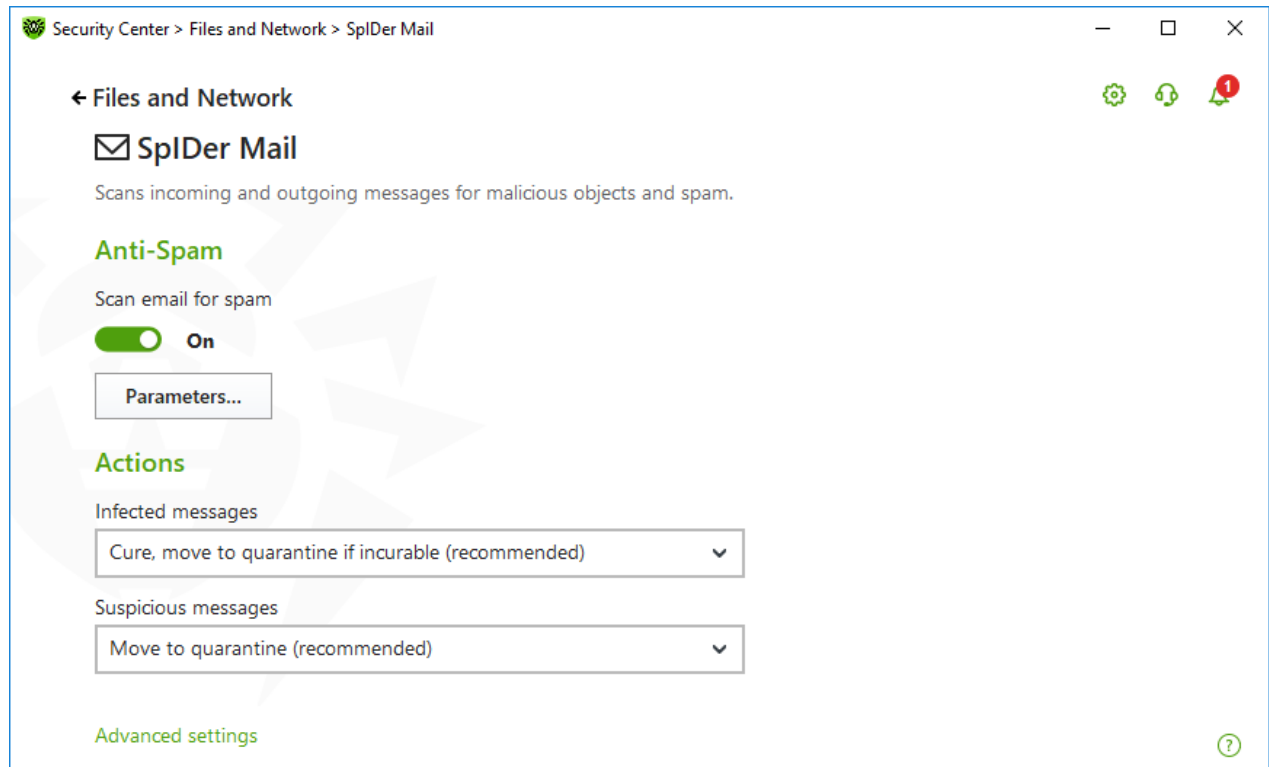
After performing the action you configured, SpIDer Mail can display a notification in the notification area. If necessary, you can [configure](#) desktop.

### 8.3.2. Anti-Spam Parameters


The default SpIDer Mail settings, including Anti-Spam settings, are optimal for most cases. Do not change them unnecessarily.

#### To enable or disable email scan for spam

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Click the **SpIDer Mail** tile. A component parameters window opens.

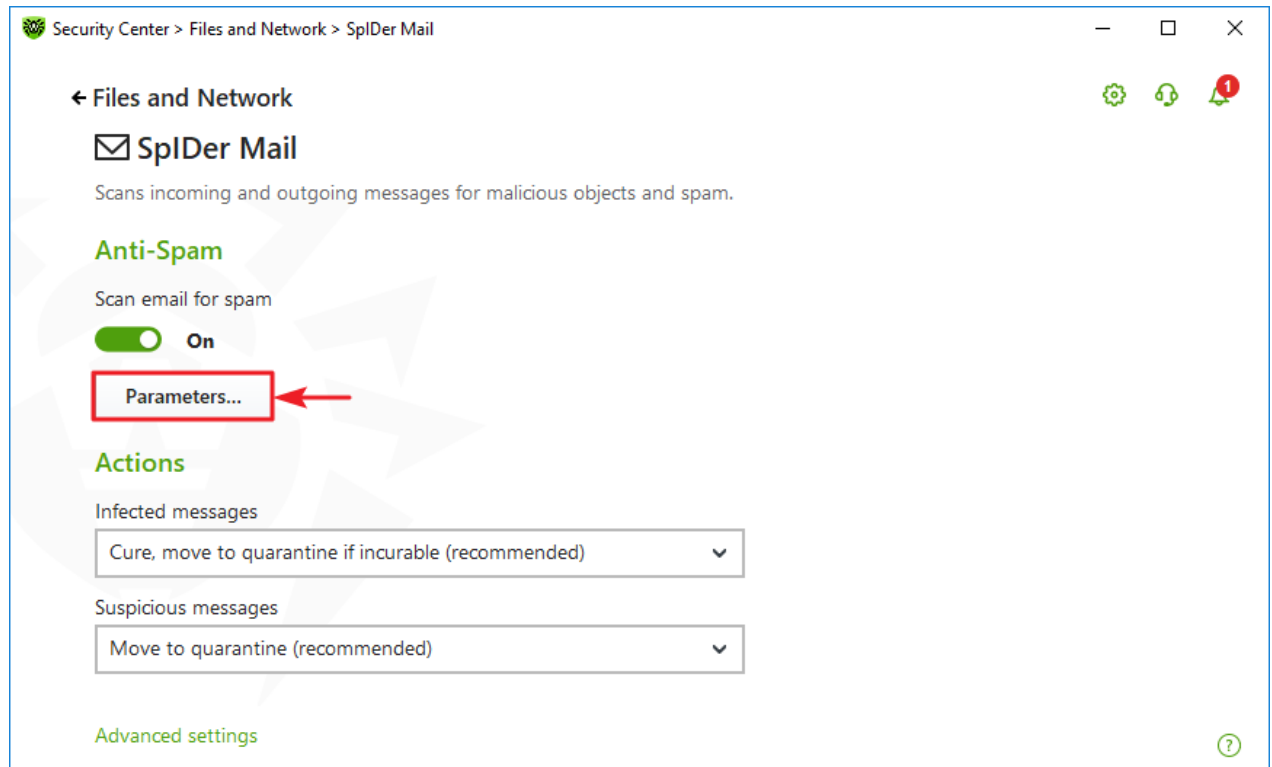


**Figure 39. Email scan parameters**

5. In the **Anti-Spam** section, enable or disable mail scan for spam using a corresponding switcher .

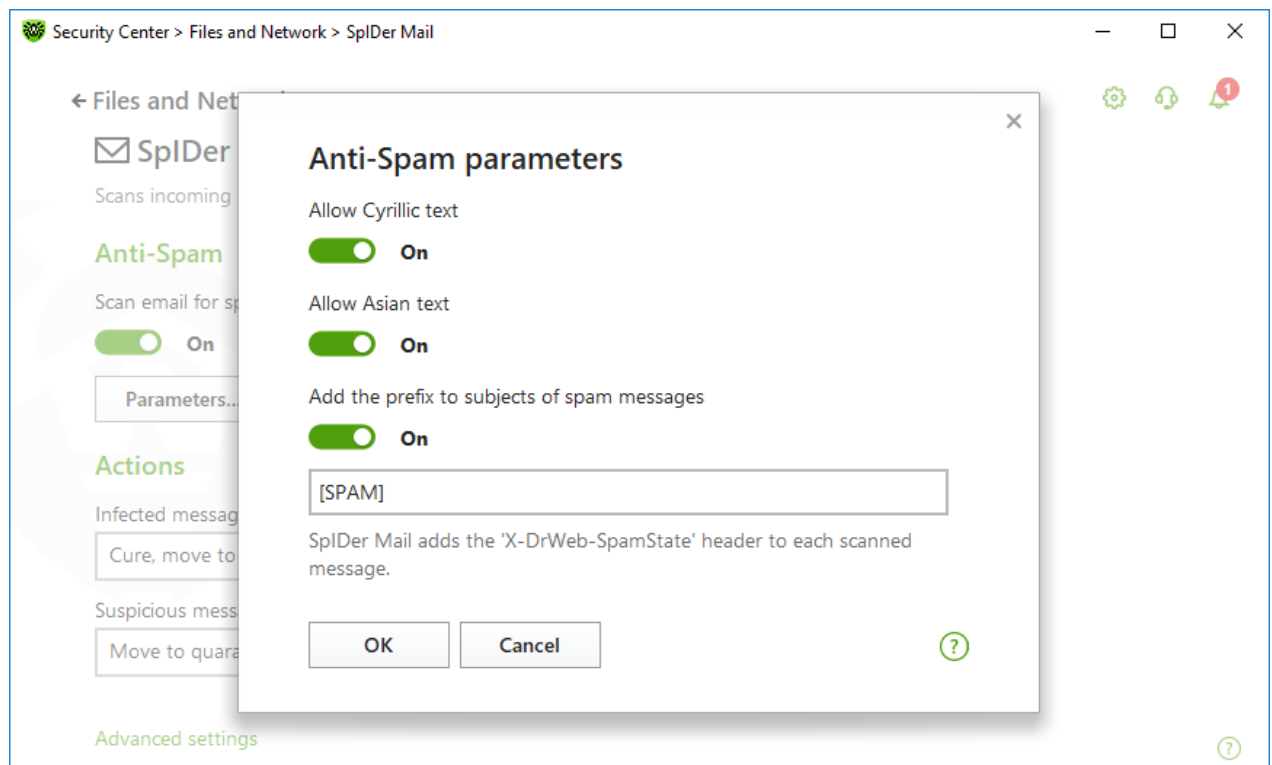
## Configuring Anti-spam parameters

1. In the **Anti-Spam** group, click **Parameters**.



**Figure 40. Changing Anti-spam parameters**

2. In the open **Anti-Spam parameters** window, enable or disable the necessary options.



**Figure 41. Anti-Spam parameters**



Available scan settings (enabled by default)

Option	Description
Allow Cyrillic text	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.
Allow Asian text	Select this check box to prevent SpIDer Mail from marking emails with the most spread Asian encodings as spam without prior analysis. Otherwise, such emails are most likely to be marked as spam.
Add the prefix to subjects of spam messages	<p>By default, SpIDer Mail adds the [SPAM] prefix to the Subject field of all spam messages. You can change this prefix.</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>

3. To save the settings, click **OK**.

## Additional information

### Anti-spam technologies

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

- **Heuristic analysis**—a technology that empirically analyzes all parts of a message: header, message body, and attachments, if any.
- **Detection of evasion techniques**—a technology that detects evasion techniques adopted by spammers to bypass anti-spam filters.
- **HTML signature analysis**—a technology that compares messages containing HTML code 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**—a technology that compares the words and phrases of a message (both visible to the human eye and hidden) with words and phrases typical for spam using a special dictionary.
- **Anti-scamming**—a technology that filters scam and phishing messages including so-called “Nigerian” scams, loan scams, lottery and casino scams, and false messages from banks and credit organizations.
- **Technical spam**—a technology that detects bounces that are delivery-failure messages sent by a mail server. Such messages are also sent by a mail worm. The bounces are detected as unwanted.



## 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.

---

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

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

## Spam detection errors

If you find an error in the spam filter:

1. Create a new email and attach the message that was processed incorrectly. Messages included in the email body are not analyzed.
2. Send the message with the attachment to the anti-virus network administrator.

## 8.4. 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.

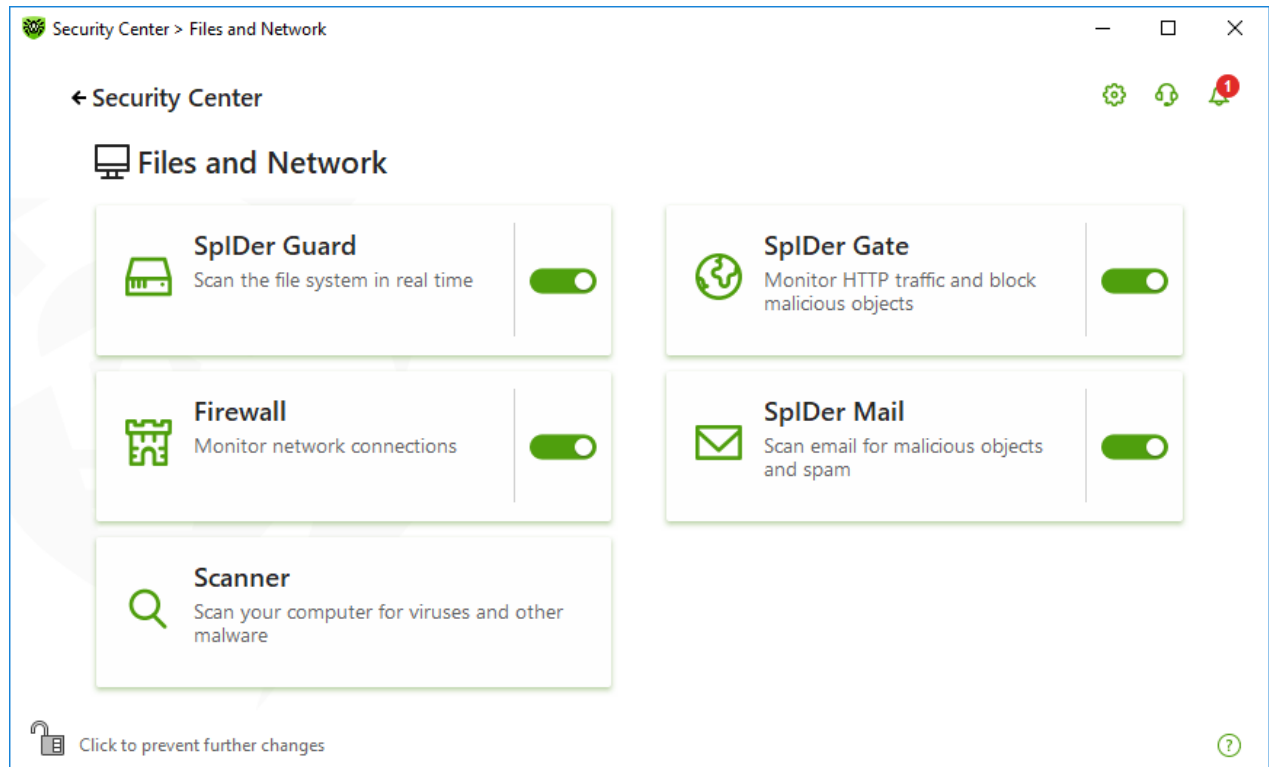
Firewall provides you with the following features:

- 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



## To enable or disable Firewall

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Enable or disable Firewall by using the switcher .



**Figure 42. Enabling/Disabling Firewall**

In this section:

- [Configuring Firewall](#)
- [Parameters for applications](#)
- [Application rules](#)
- [Configuring parameters for application rules](#)
- [Parameters for networks](#)
- [Packet filter](#)
- [Set of rules for filtering packets](#)
- [Filtering rules](#)

### 8.4.1. Configuring Firewall

You can configure the following Firewall options:

- [Select the operation mode](#)
- [List authorized applications](#)



- [Configure parameters for the known networks](#)



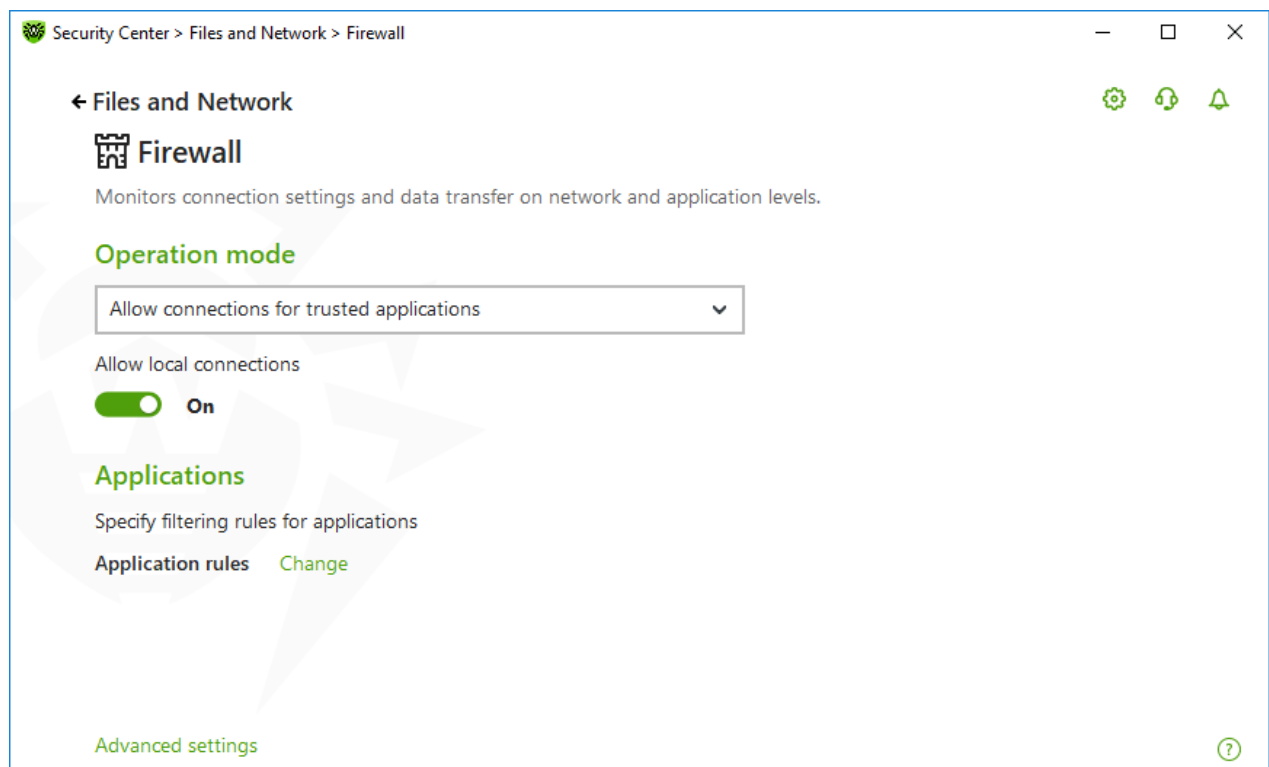
To access the Firewall parameters, you are prompted to enter the password if you have enabled the **Protect Dr.Web settings with a password** option in the [settings](#).

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.

### To select an operation mode and open Firewall parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the **Firewall** tile. A component parameters window opens.



**Figure 43. Firewall parameters**

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.





## Selecting an operation mode

Select one of the following operation modes:

Operation mode	Description
<b>Allow connections for trusted applications</b>	<p>This mode is used by default.</p> <p>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 with a valid digital signature. Rules for such applications are not displayed in the rule list. For other applications, Firewall prompts you to allow or block once the unknown connection manually, as well as <a href="#">create a new rule for it</a>.</p> <p>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 <a href="#">create a rule</a> to be applied each time this type of connection is detected.</p>
<b>Allow unknown connections</b>	<p>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.</p>
<b>Interactive learning mode</b>	<p>In this mode, you have total control over Firewall reaction to the detection of unknown connections.</p> <p>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 <a href="#">create a rule</a> to be applied each time this type of connection is detected.</p>
<b>Block unknown connections</b>	<p>In this mode, Firewall automatically blocks all unknown connections to network resources, including the internet.</p> <p>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.</p>



## Parameters for Applications

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).






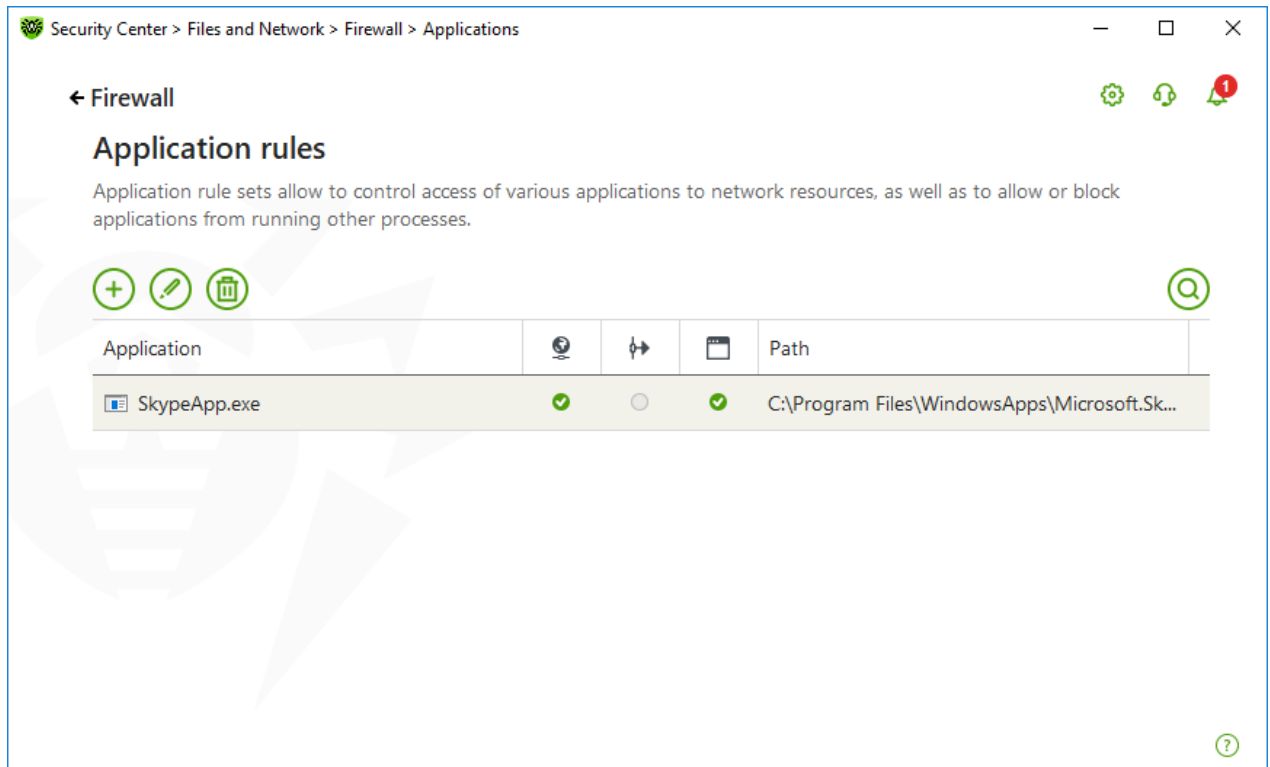
Firewall allows you to create no more than one set of rules per each application.

If you create a blocking rule for a process or set Block unknown connections mode and then disable the rule or change the work mode, the process is blocked till it will be restarted and will attempt to establish connection again.




## Application Rules

### To open Application rules window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ) . Otherwise, click the lock .
4. Click the **Firewall** tile. A component parameters window opens.
5. In the **Application rules** section click **Edit**. A window with a list of applications opens. For these applications, rules have been set.



**Figure 44. Application rules**

6. To start creating a new rule set or editing an existing one, click  or select an application and click . To search for a necessary rule, click .

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.

## Editing of an existing rule set or creating a new rule set

You can configure access to network resources as well as enable or disable launch of other applications in the **New application rule set** (or **Edit rule set for <application name>**) window.



New application rule set

Specify the process or application to create a rule set for:

Browse...

☒ Require confirmation on object change (recommended)

Launching network applications:

Not specified

Access to network resources:

Allow all

OK Cancel

?

Figure 45. Creating a new rule set

### 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"><li>• <b>Block packets</b>—block the connection.</li><li>• <b>Allow packets</b>—allow the connection.</li></ul>
Rule name	The rule name.
Connection type	The direction of the connection: <ul style="list-style-type: none"><li>• <b>Inbound</b>—the rule is applied when someone from the network attempts to connect to an application on your computer.</li><li>• <b>Outbound</b>—the rule is applied when an application on your computer attempts to connect to the network.</li><li>• <b>Any</b>—the rule is applied regardless of packet transfer direction.</li></ul>
Description	User description of the rule.

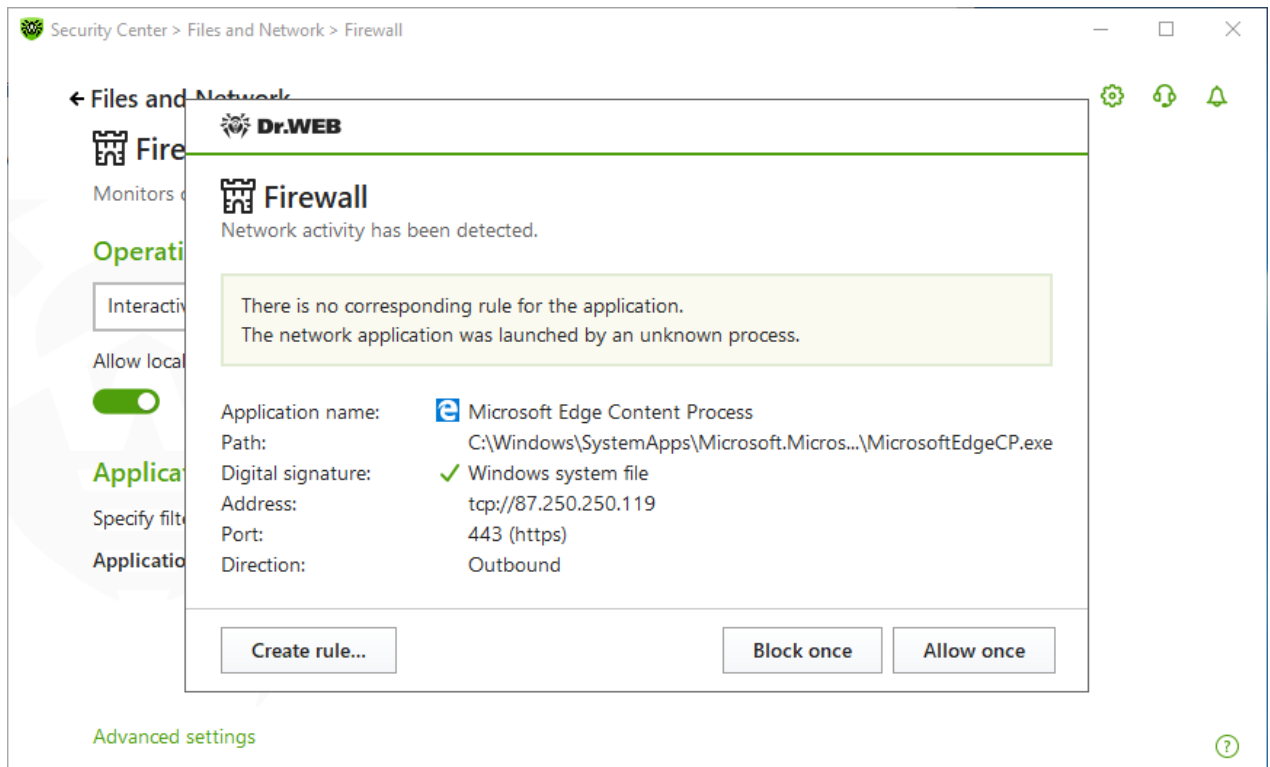
3. If necessary, edit the predefined rule set or create a new one.
4. If you select to create a new rule set or edit an existing one, [adjust the settings](#) in the open window.
5. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to cancel them. When shifting to another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



## Creating application rules from the Firewall notification window

When Firewall is operating in the interactive mode or in the Allow connections for trusted applications mode, you can start creating a new rule directly from the window with notification on an unknown connection attempt.



**Figure 46. Example of a notification on a network connection attempt**



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.

### To add application rules

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

Field	Description
Application name	The name of the application. Ensure that the path to the application executable, specified in the <b>Path</b> entry field, corresponds to the file location.
Path	The full path to the application executable file and its name.
Digital signature	Digital signature of the application.



Field	Description
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 application access using this port once, select **Block once**.
  - To allow application access by this port 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 identifying 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 that can access using the specified port, allow this connection.

If 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.



## Rule Settings

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

### To add or edit a rule

1. In **Access to network resources** section select the **User-defined** mode.
2. In **Edit rule set for** window press  button to add a new rule or select the rule from the list and press the  button to edit the rule.
3. Configure the following parameters:

Parameter	Description
<b>General</b>	
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"><li>• <b>Block packets</b>—block the connection.</li><li>• <b>Allow packets</b>—allow the connection.</li></ul>
State	Rule status: <ul style="list-style-type: none"><li>• <b>Enabled</b>—the rule is applied for all matching connections.</li><li>• <b>Disabled</b>—the rule is temporary not applied.</li></ul>
Connection type	The direction of the connection: <ul style="list-style-type: none"><li>• <b>Inbound</b>—the rule is applied when someone from the network attempts to connect to an application on your computer.</li><li>• <b>Outbound</b>—the rule is applied when an application on your computer attempts to connect to the network.</li><li>• <b>Any</b>—the rule is applied regardless of packet transfer direction.</li></ul>
Logging	Logging mode: <ul style="list-style-type: none"><li>• <b>Enabled</b>—register events.</li><li>• <b>Disabled</b>—do not log rule information.</li></ul>
<b>Rule settings</b>	
Protocol	The network and transport level protocols used for the connection attempt.  The following protocols of the network level are supported:





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

4. Click **OK**.

## Parameters 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

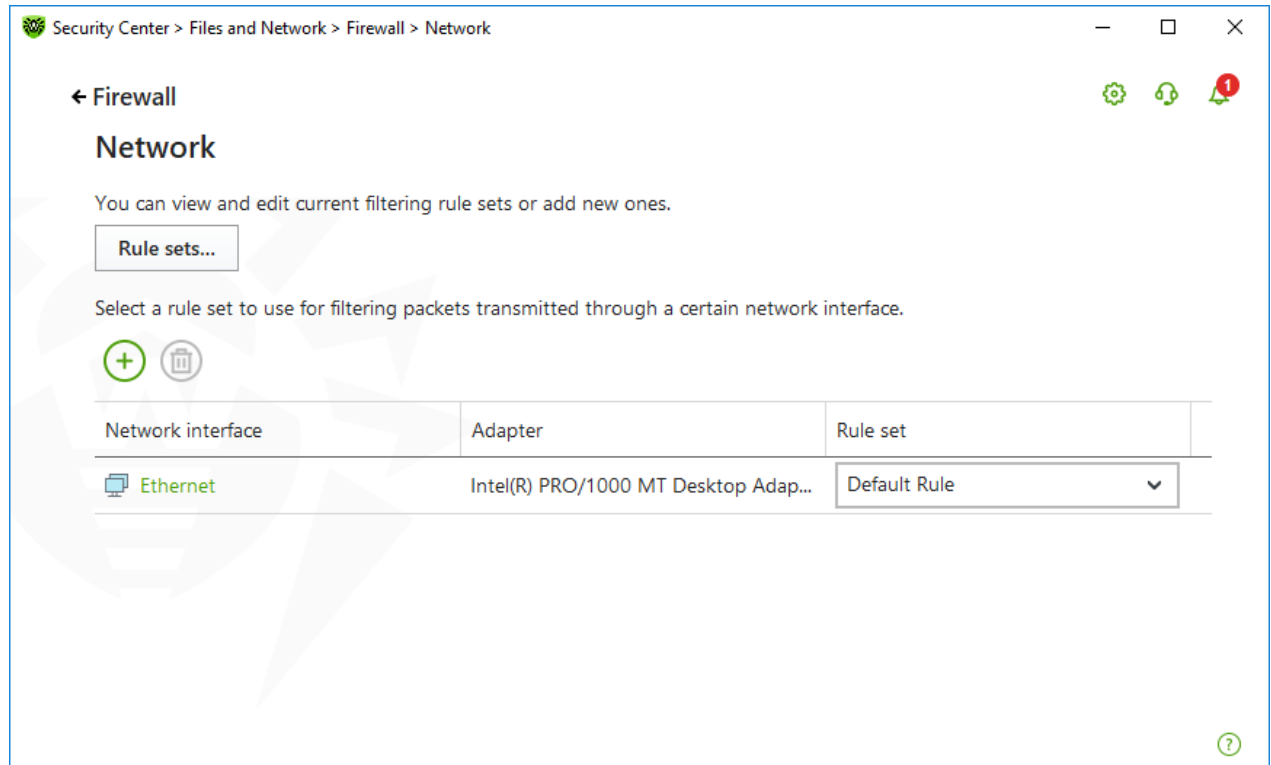
In the **Network** window, you can create a set of rules for filtering packets transmitted through a certain interface.

### To open Network window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, select the **Files and Network** section.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .



4. Click the **Firewall** tile. A component parameters window opens.
5. Expand the **Advanced settings** group.
6. In the **Application rules** section click **Edit**. A window with a list of network interfaces opens. For these network interfaces, rules have been set.




**Figure 47. Sets of rules for network interfaces**


7. For the required interface, select the appropriate rule set. If the appropriate rule set does not exist, you can [create it](#).

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 clicking .

To access the interface parameters, click on the interface name.



## 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.

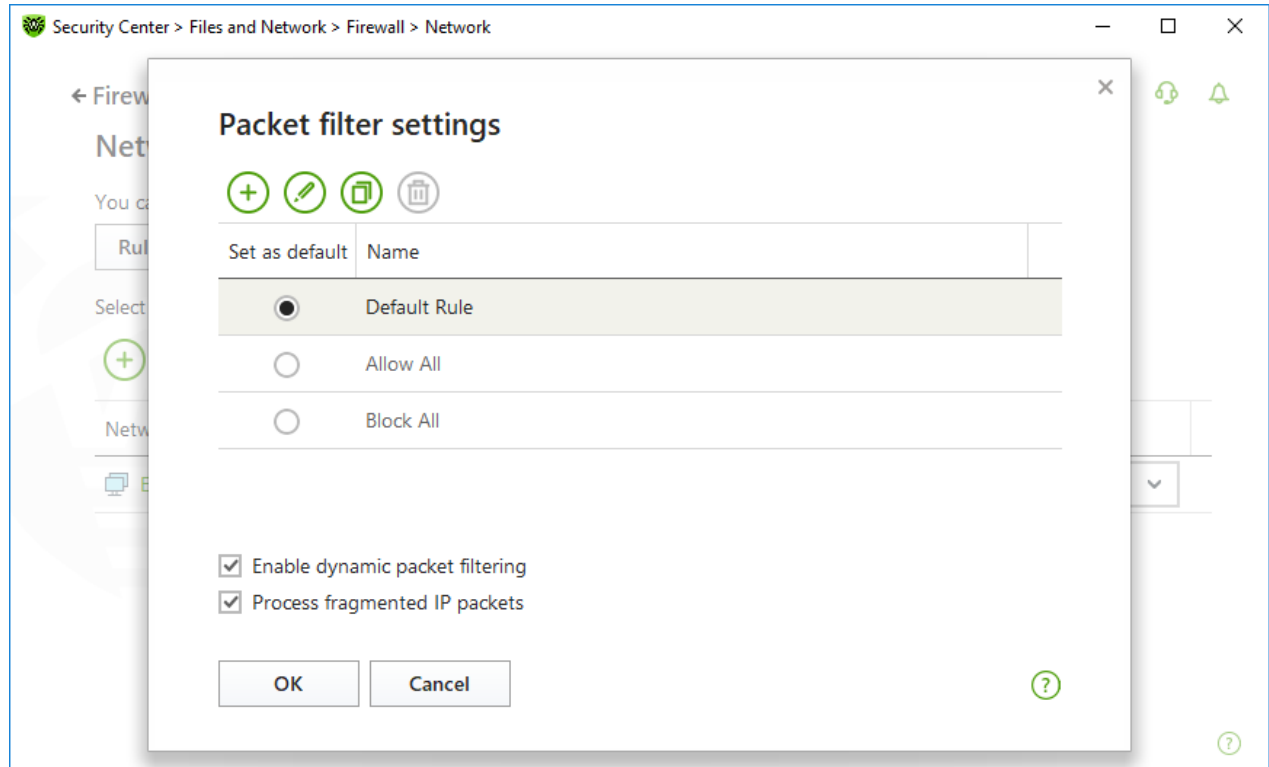






Figure 48. Packet filter settings

On this page you can:

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

## Configuring 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

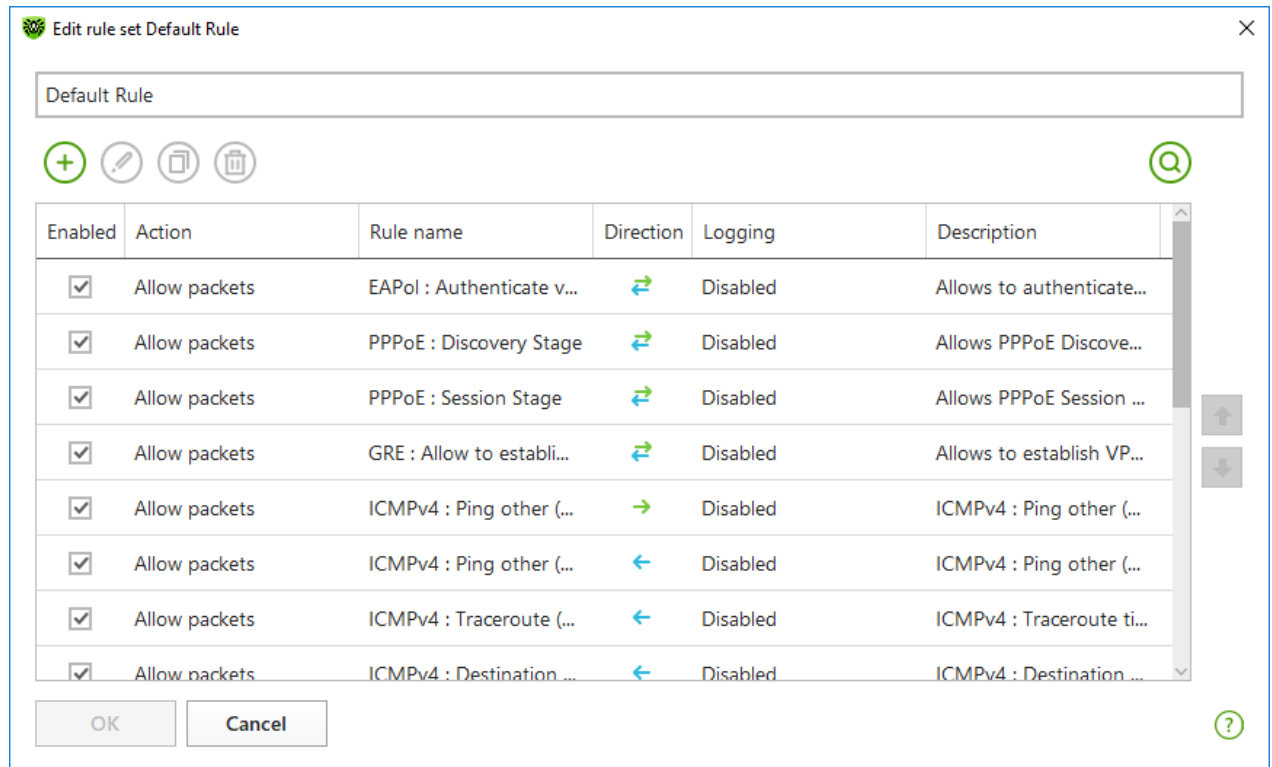
In the **Packet filter settings** window, you can select the following options:

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 that you enable stateful packet filtering when using complex data transfer protocols (FTP, SIP, etc.).</p> <p>Clear this check box to filter packets without regard to the TCP session state.</p>
Management of fragmented IP packets	<p>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.</p> <p>Clear this check box to process fragmented packets independently.</p>

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

## Rule Sets for Filtering Packets

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.








**Figure 49. Rule set for filtering packets**

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"><li>• <b>Block packets</b>—block a packet;</li><li>• <b>Allow packets</b>—allow a packet.</li></ul>
Rule name	The rule name.
Direction	The direction of the connection: <ul style="list-style-type: none"><li>•  —the rule is applied when a packet is received from the network.</li><li>•  —the rule is applied when a packet is sent into the network from your computer.</li><li>•  —the rule is applied regardless of packet transfer direction.</li></ul>
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log: <ul style="list-style-type: none"><li>• <b>Headers only</b>—log packet headers only.</li><li>• <b>Entire packet</b>—log the whole packet.</li><li>• <b>Disabled</b>—do not log packet information.</li></ul>
Description	The rule description.



### To edit or create a rule 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 .
  - To search for a necessary rule, click .
3. If you have 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.

## Filtering Rule Settings

### To add or edit a filtering rule

1. In the packet filter rule set creation or modification window, click  or . This opens a rule creation or rule modification window.



Add packet rule

×

Rule name:

New rule set

Description:

Rule description

Action:

Allow packets

▼

Direction:

Inbound

▼

Logging:

Disabled

▼

Filtering criteria

You can add filtering criteria to this rule.

Add criterion...

OK

Cancel

?

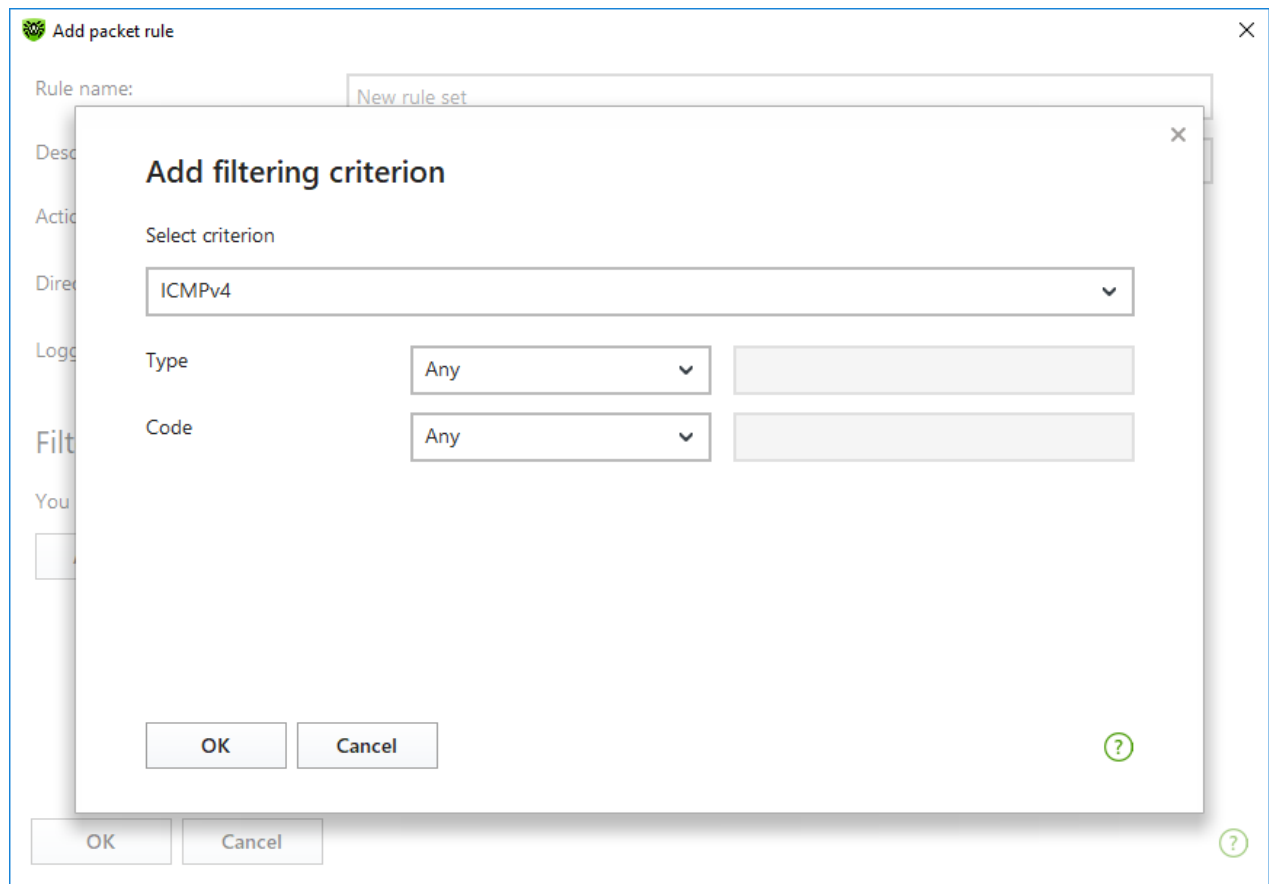
Figure 50. Adding filtering rule

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"><li>• <b>Block packets</b>—block a packet;</li><li>• <b>Allow packets</b>—allow a packet.</li></ul>
Direction	The direction of the connection: <ul style="list-style-type: none"><li>• <b>Inbound</b>—the rule is applied when a packet is received from the network.</li><li>• <b>Outbound</b>—the rule is applied when a packet is sent into the network from your computer.</li><li>• <b>Any</b>—the rule is applied regardless of packet transfer direction.</li></ul>
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log: <ul style="list-style-type: none"><li>• <b>Entire packet</b>—log the whole packet.</li><li>• <b>Headers only</b>—log packet headers only.</li><li>• <b>Disabled</b>—do not log packet information.</li></ul>



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



**Figures 51. 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.





## 8.5. Computer Scan

The Scanner component performs anti-virus scan of the computer. Scanner checks boot sectors, memories, and both separate files and objects enclosed within complex structures (archives, containers, or email attachments). Dr.Web uses all [detection methods](#) during computer scan.

On detection of a malicious object, Scanner only informs you about the threat. Report on all infected or suspicious objects is displayed in the table where you can [select a necessary action](#). You can apply default actions to all detected threats or select the necessary action to certain objects.

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

See also:


- [File Scan Options](#)
- [Scan Start and Scan Modes](#)
- [Neutralizing Detected Threats](#)

### 8.5.1. Scan Start and Scan Modes

#### To start scan of the files



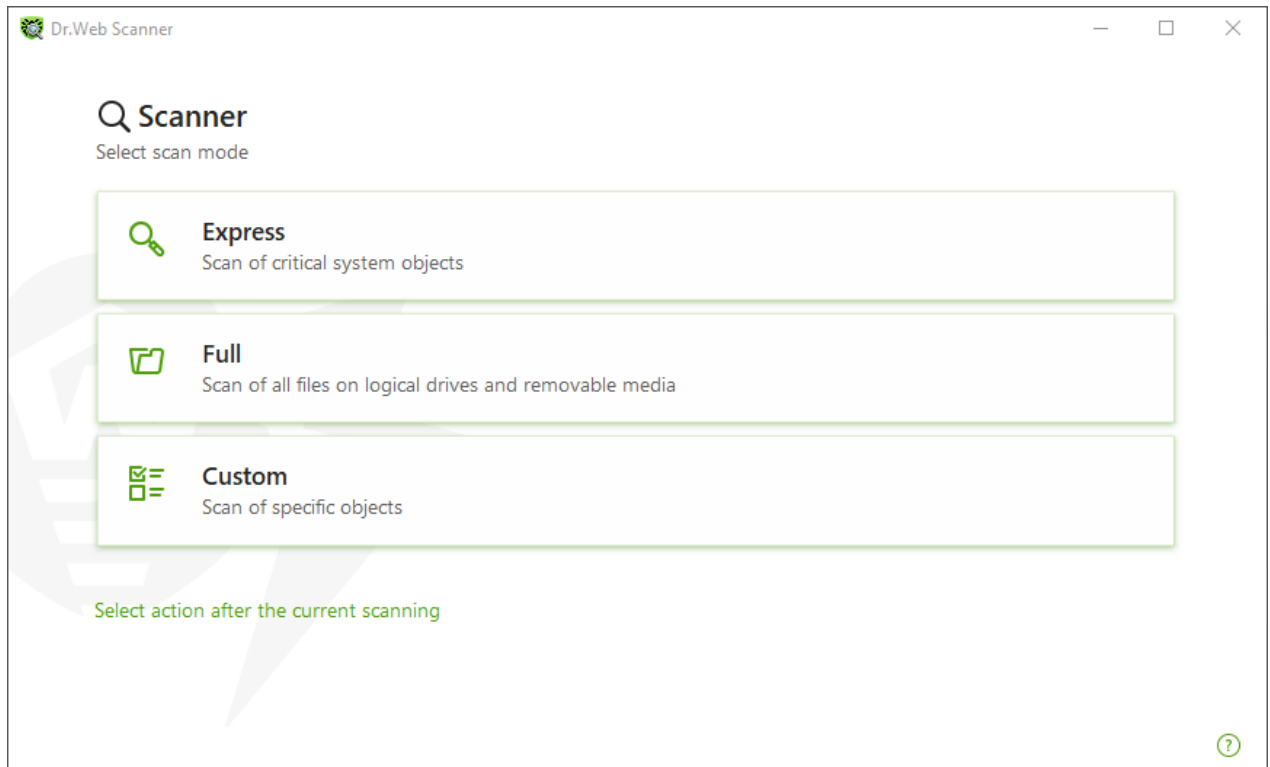
When using Windows Vista, Windows Server 2003 or later operating systems, it is recommended running Scanner with administrative privileges. Otherwise, all folders and files (including system folders) that are not accessible to an unprivileged user will not be scanned.

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Files and Network** tile, then **Scanner** tile.



You can also start the file scan from **Start** menu. For this, expand the application group **Dr.Web** and then select **Dr.Web Scanner**.

3. Choose the needed scan mode:
  - **Express** item to scan only critical Windows objects.
  - **Full** to scan all files on logical drives and removable media.
  - **Custom** item to scan only selected objects. The Scanner window opens.



**Figure 52. Selecting the scanning mode**

You can also select an action after the current scanning. For this, click the corresponding link at the bottom of the window. The action does not depend on the action selected in the [Scanner settings](#) and does not affect general settings.

4. The scanning starts. To pause scanning, click **Pause**. To stop scanning, click **Stop**.



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

When the scan is completed, Scanner informs you about detected threats and recommends that you [neutralize](#) them.



### To scan a certain file or folder

1. Open shortcut menu of the file or folder (on your desktop or in Windows Explorer).
2. Select **Check with Dr.Web**. The file or folder will be scanned according to the default settings.

## Scan modes

Scan mode	Description
<b>Express</b>	In this mode, Scanner checks the following: <ul style="list-style-type: none"><li>• Boot sectors of all disks</li></ul>



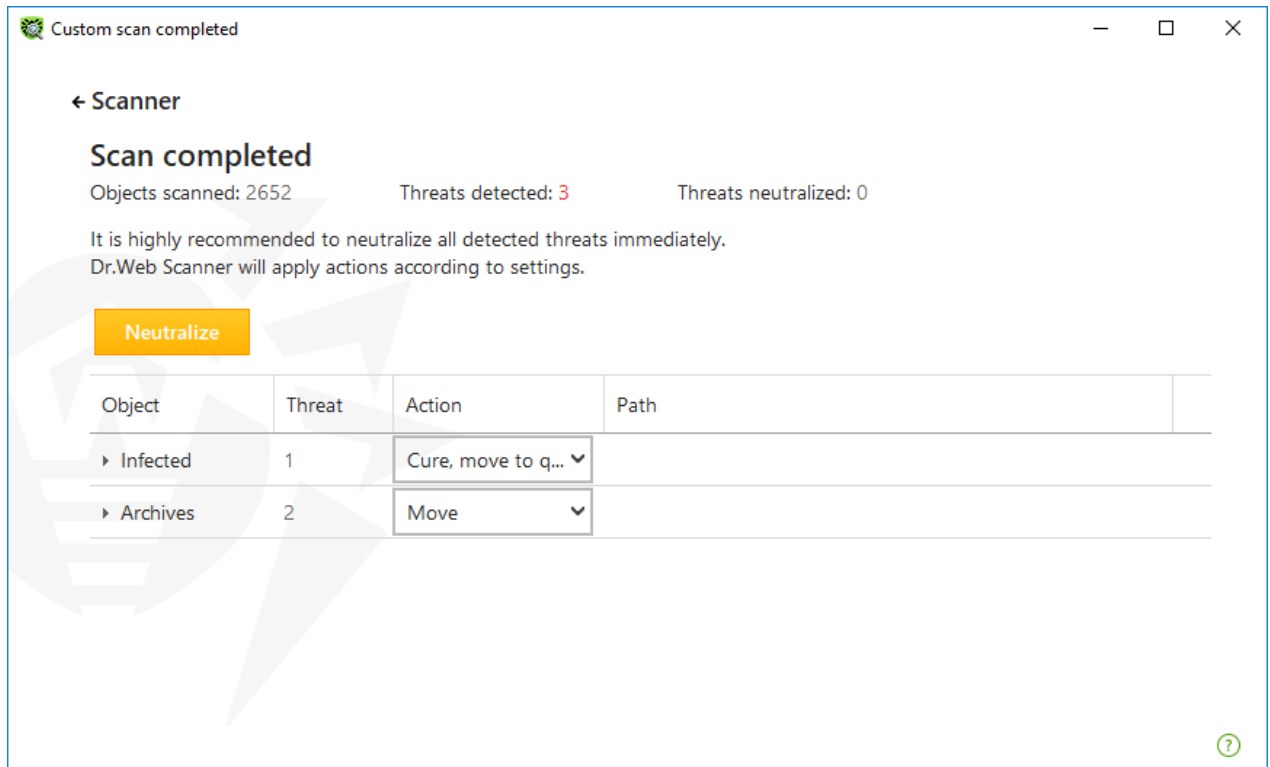
Scan mode	Description
	<ul style="list-style-type: none"><li>• Random access memory</li><li>• Boot disk root folder</li><li>• Windows system folder</li><li>• User documents folder ("My Documents")</li><li>• Temporary files</li><li>• System restore points</li><li>• Presence of rootkits (if the process is run with administrative privileges)</li></ul> <div> Scanner does not check archives and email files in this mode.</div>
<b>Full</b>	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.
<b>Custom</b>	In this mode, you can scan any files or folders and such objects as random access memory, boot sectors, and so on. To select objects, click  .

## 8.5.2. Neutralizing Detected Threats

When the scan is completed, Scanner informs you about detected threats and recommends that you neutralize them.



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



**Figure 53. Selecting an action after a scan**

The table with scan results contains the following information:

Column	Description
Object	This table column contains the name of an infected or suspicious object (either a file name if a file is infected, or <b>Boot sector</b> if a boot sector is infected, or <b>Master Boot Record</b> if an MBR of the hard drive is infected).
Threat	The names of viruses or <a href="#">virus modifications</a> as per the internal classification of Doctor Web. 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	The action recommended for the detected threat according to the <a href="#">Scanner settings</a> . To apply the action for the selected threat, use the drop-down list options.
Path	The full paths to the corresponding files.

### Neutralizing all the threats in the table

An action is specified for each threat according to the [Scanner settings](#). To neutralize all the threats by applying actions that are specified in the table, click **Neutralize**.

### To change the action for the threat specified in the table

1. Select an object or a group of objects.



2. In the **Action** column, select a necessary action from the drop-down list.
3. Click **Neutralize**. Scanner starts neutralizing all the threats listed in the table.

### Neutralizing selected threats

You can also neutralize selected threats separately. To do so:

1. Select an object, several objects (by pressing the CTRL key) or a group of objects.
2. Open a shortcut menu and select a necessary action. Scanner starts neutralizing the selected threat (threats).

### Restrictions on neutralizing 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 action applies to the whole file.

### Scanner report

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

## 8.5.3. Additional Options

This section contains information about the additional Scanner options:

- [Command-Line Scanning Mode](#)
- [Console Scanner](#)

### Command-Line Scanning Mode

You can run Scanner in the command-line mode. This allows you to specify settings of the current scanning session and the list of objects for scanning as additional parameters.

The launching command syntax is as follows:

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

*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.



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

## 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;
- 12—Scanning Engine did not start;
- 255—scanning was aborted by user request.

## 8.6. 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
- 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 you with an access to the following program functions:

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

### 8.6.1. 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 you to specify program reaction to detection of infected or suspicious files and malicious objects in email attachments.

To configure virus scan 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 scanned objects and also for the scan failure. You can also enable or disable scan 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 unwanted software of the following types:
  - Adware
  - Dialers
  - Jokes
  - Hacktools
  - Riskware
- The **If check failed** drop-down list allows you to configure actions if the attachment cannot be scanned, that is, if the attached file is corrupted or password protected.
- The **Check archives (recommended)** check box allows you to enable or disable scan of attached archived files. Select this check box to enable scanning; clear this check box to disable scanning.





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.
- **Delete**—delete the object.
- **Move to quarantine**—move the object to the special [Quarantine](#) folder.
- **Ignore**—skip the object without performing any action or displaying a notification.

## 8.6.2. 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 **Anti-spam filter**. The [Anti-spam filter](#) window opens.



The **Anti-spam filter** window is available only for users with administrative privileges.

For Windows Vista and later operating systems, after clicking **Anti-spam filter**:

- 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.

## Anti-Spam Filter Settings

**To configure Anti-spam filter parameters:**

1. Select the **Check for spam** check box to enable the anti-spam filter.
2. 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\***.
3. 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.
4. 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 your anti-virus network administrator.



## 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 [Anti-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 in 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

If the sender's address is in the white list, the message is not 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.



### 8.6.3. 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
- Parameters of program modules: scanner, engine, virus databases (information is logged on program startup and module update)
- Information on threat detection

#### 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:

- 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

#### To configure the program 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, we recommend that you 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.

### To open the text log

1. On the **Dr.Web Anti-virus** tab, click **Log**. The window with logging settings opens.
2. Click **Show in folder**. The folder with the log opens.

## 8.6.4. 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 objects and messages.
- **Infected**—total number of infected objects attached to the messages.
- **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 objects and messages that 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.
- **Ignored**—number of objects skipped without changes.
- **Spam messages**—number of objects detected as spam.

By default, statistics is saved to the `drwebforoutlook.log` 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.



## 9. Preventive Protection

In this group, 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.

### To open the Preventive Protection group of settings

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.

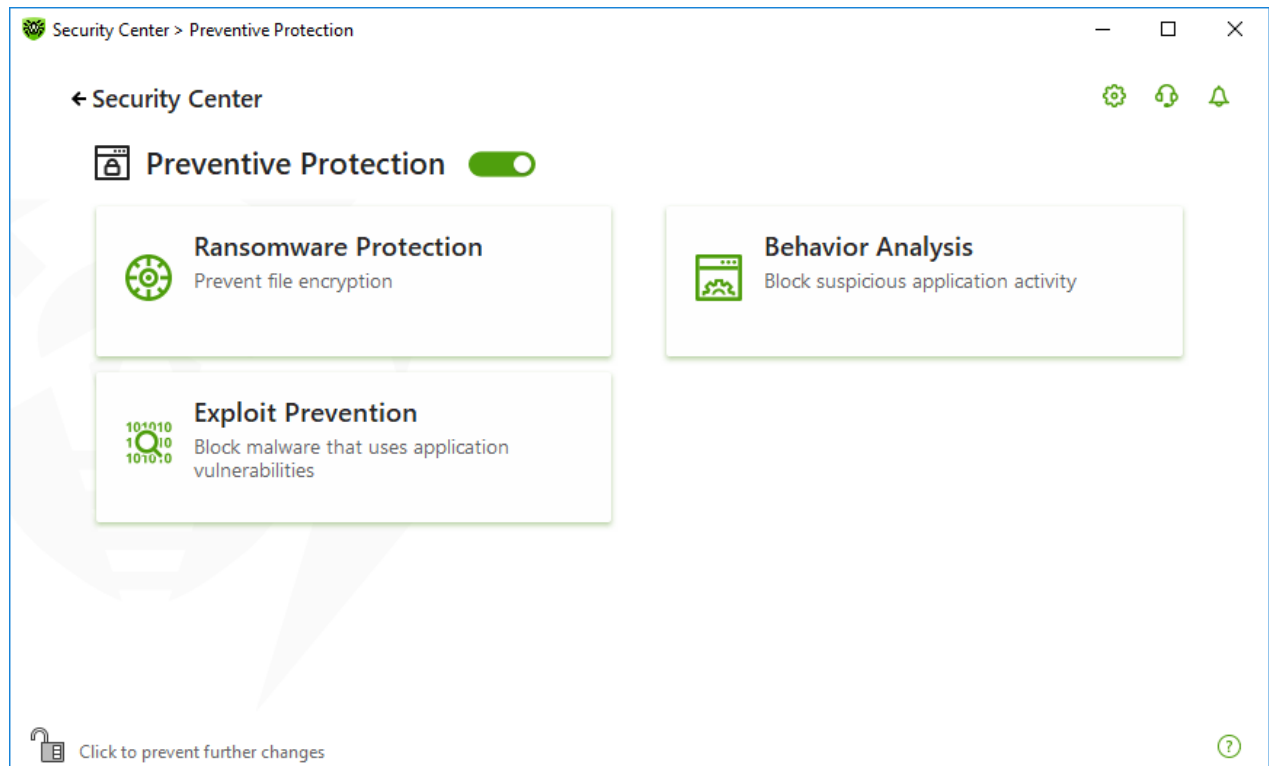




Figure 54. Preventive Protection window

### Enable and disable Preventive Protection

Enable or disable the Preventive Protection by using the switcher .

### To open the component parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the tile of a necessary component.



Enabling and disabling Preventive Protection and changing the component parameters is available if the administrator of the central protection server, to which Dr.Web is connected,




enables this option.

In this section:

- [Behavior Analysis](#)—configure application access to the system objects.
- [Ransomware Protection](#)—prevent user files encryption.
- [Exploit Prevention](#)—block the usage of application vulnerabilities.






To *disable* Preventive Protection, Dr.Web should operate in administrator mode. For that, click the lock  at the bottom of the program window.

## 9.1. Ransomware Protection

Ransomware Protection allows detection of processes that attempt to encrypt user's files using known algorithm that defines processes as a security threat. *Ransomware* is one of these processes. When entering a computer such malicious programs block access to user data and then demand ransom for decryption. They are considered among the most common malicious programs and cause great annual losses both to companies and ordinary users. The most common way of getting infected are bulk emails containing malicious files or a link to malware.

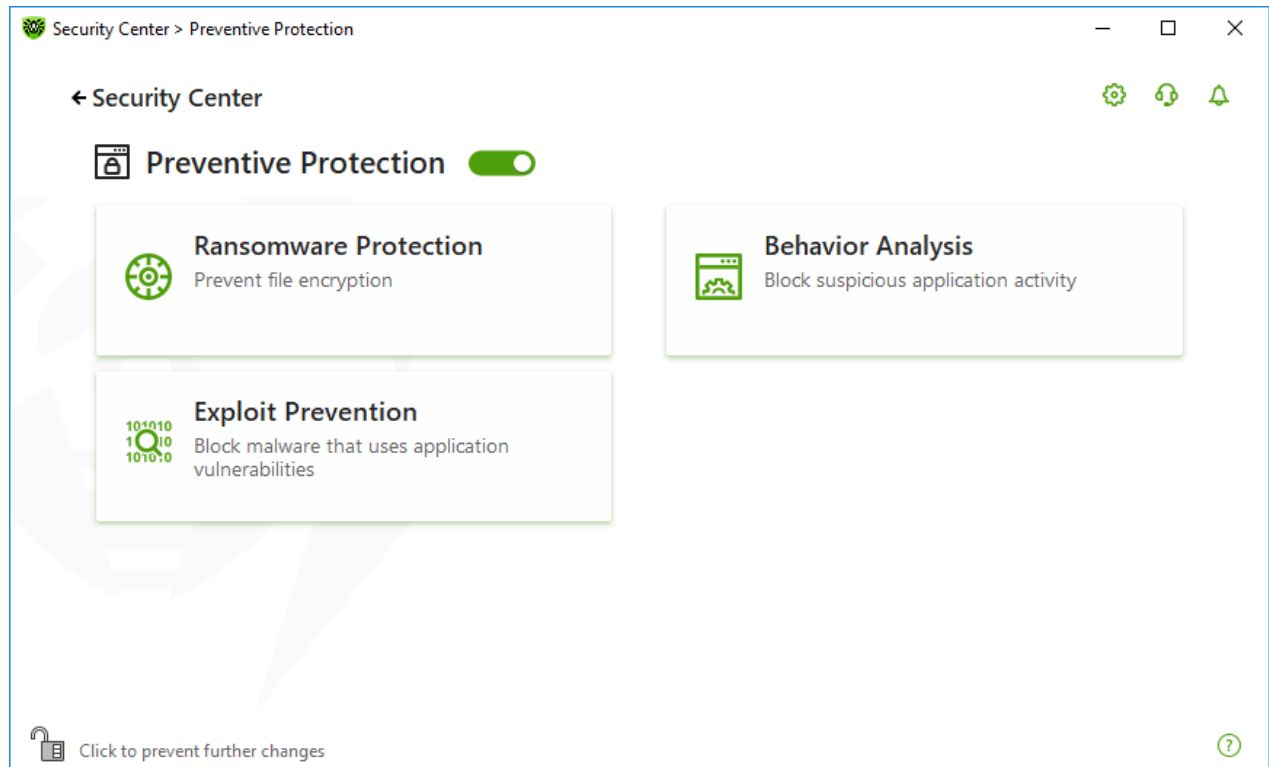
According to Doctor Web statistics, probability of restoring files compromised by encryption ransomware is only 10%, that is why the most efficient way of fighting it is to prevent the infection. Recently the number of users that have suffered such infection has decreased. However, the number of Dr.Web technical support requests for decryption reaches 1000 every month.

### To open the Ransomware Protection window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Click the **Ransomware Protection** tile.



The component parameters can be adjusted if the the administrator of the central protection server, to which Dr.Web is connected, enables this option.





**Figure 55. Access to the Ransomware Protection component**

In this section:

- [Configuring reaction to application attempts to encrypt files](#)
- [Separate rules for certain applications](#)

## Dr.Web reaction to application attempts to encrypt a file

### To configure Ransomware Protection parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the **Ransomware Protection** tile. A component parameter window opens.
3. In the drop-down menu, select an action to be applied to all applications.



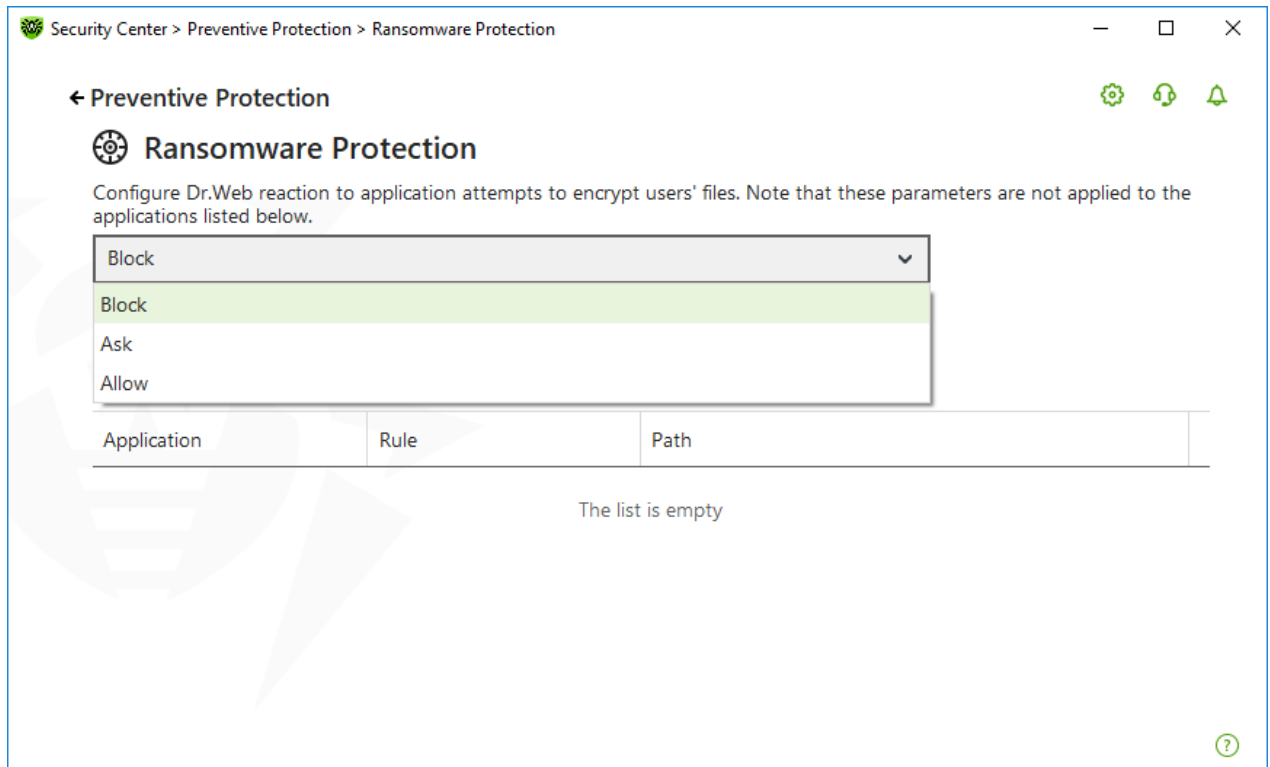


Figure 56. Selecting Dr.Web reaction

- **Allow**—all the applications are allowed to modify user's files.
- **Block**—all the applications are not allowed to encrypt user's files. This mode is enabled by default. When an application attempts to encrypt user's files the following notification will be shown:

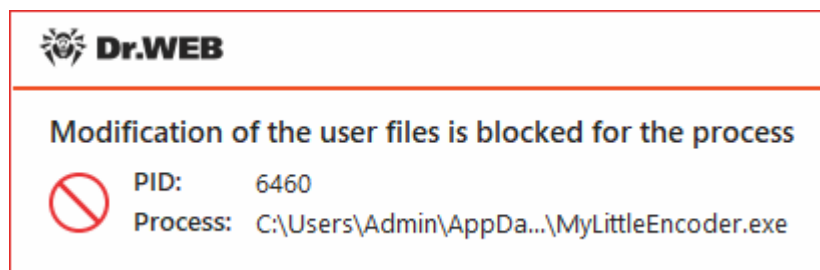
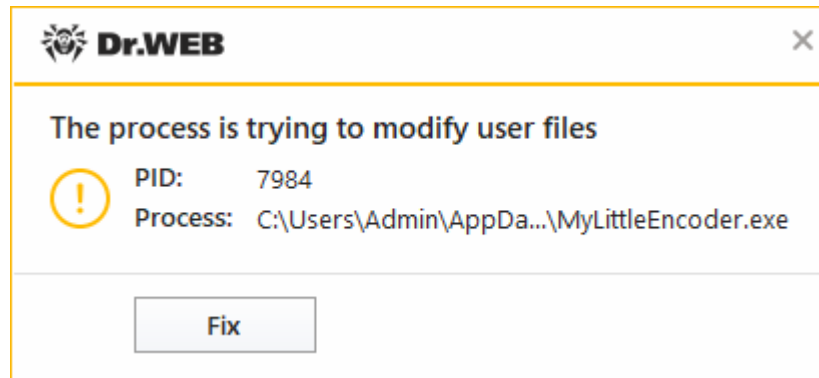


Figure 57. Notification example with a blocked application attempt to modify user's files

- **Ask**—when an application attempts to encrypt a user's file, a notification appears, where you can prevent the encryption or ignore it:



**Figure 58. Notification example with an application attempt to modify user's files**

- When clicking **Fix** button the process is blocked and moved to quarantine. Even if the application is restored from the quarantine it cannot be launched until the computer restart.
- If you close the notification window, the application will not be neutralized.

## Receiving notifications



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

See also:

- [Notifications](#)

## Separate rules for certain applications

You can configure Ransomware Protection reaction on actions of certain applications. For this, add applications to the list and select a necessary reaction of the component. The following management elements are available to work with objects in the list:

- The  button—add the application to the list of applications with separate rules.
- The  button—delete the application from the list of applications with separate rules.

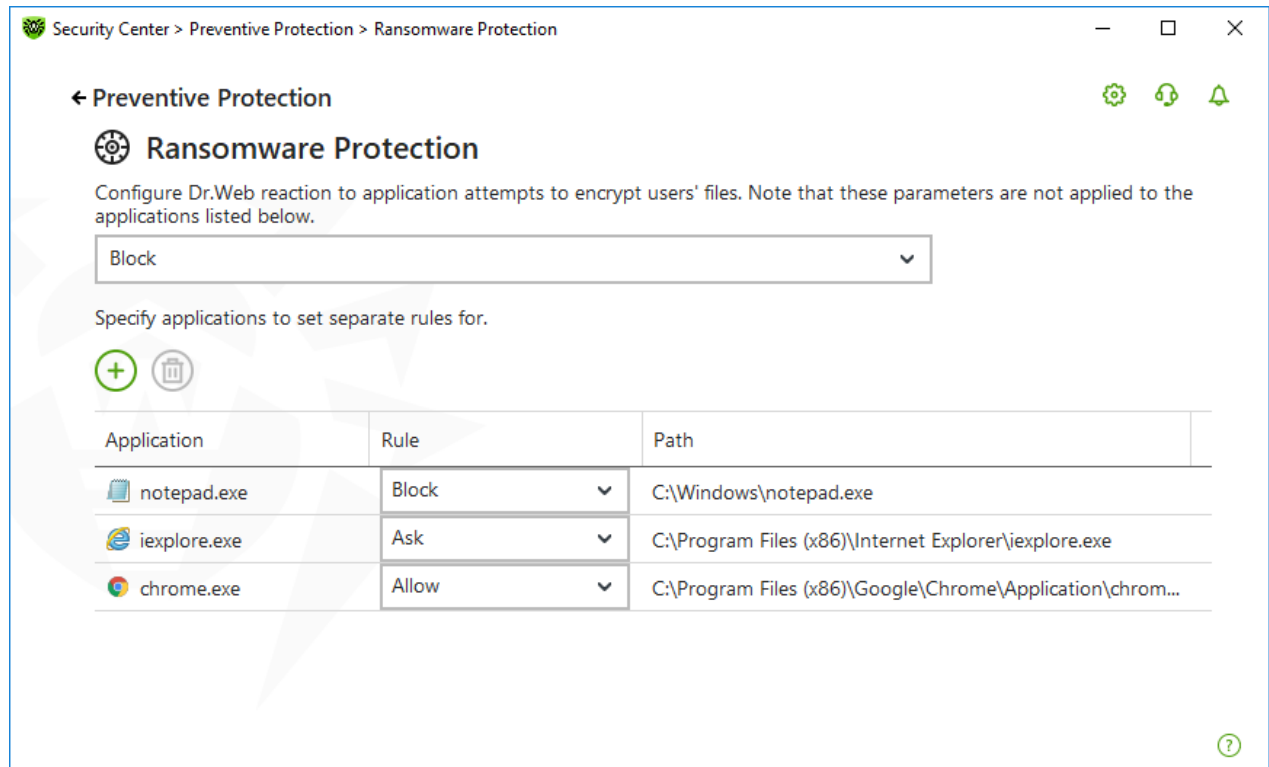

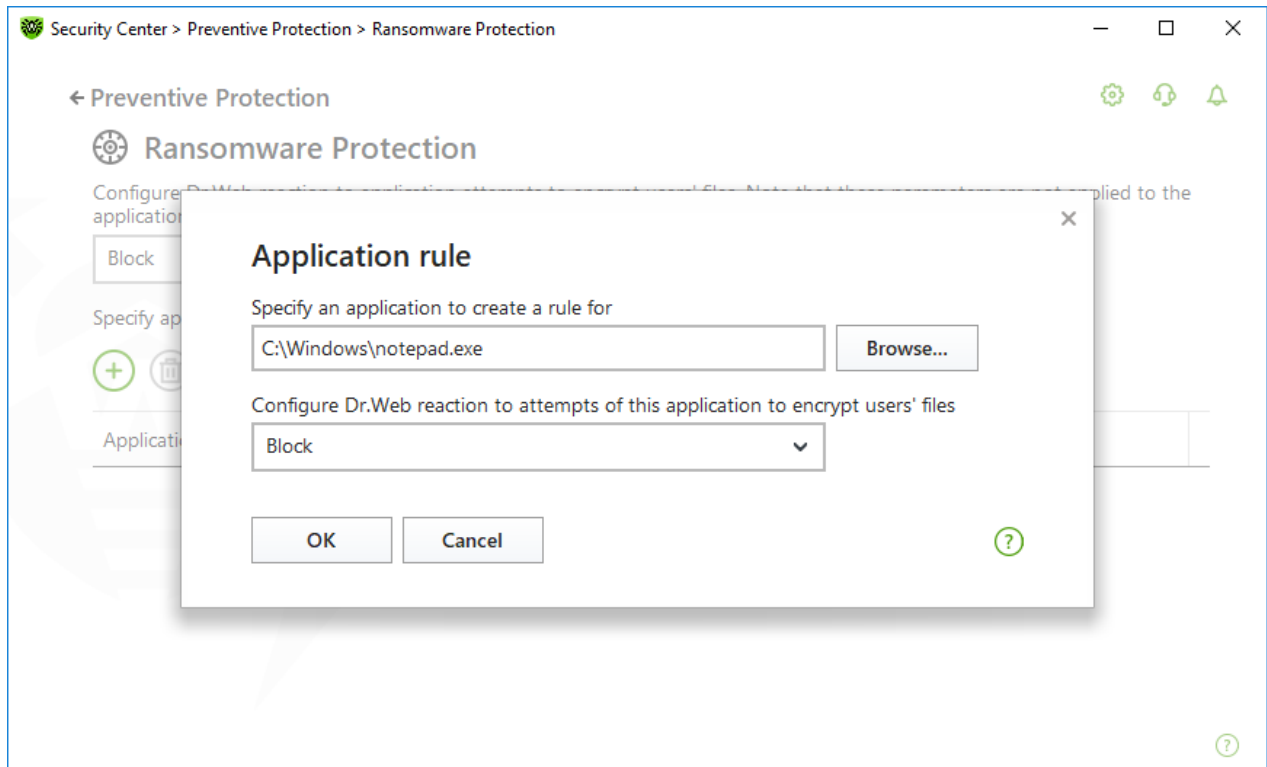


Figure 59. Applications not covered by component general rule

### To add an application to the list

1. Click .
2. In the open window, click **Browse** and specify the path to the application executable file.



**Figure 60. Selecting a rule for a certain application**

3. Select a necessary component reaction from the drop-down list.
4. Click **OK**.

You can also change previously selected rule.

### To change the Dr.Web reaction for applications with rules set

1. On the [main window](#) of the Ransomware Protection component, select the required application.
2. In the corresponding line in the **Rule** column select from the drop-down list the required reaction on application attempts to encrypt user's files.

## 9.2. Behavior Analysis

The Behavior Analysis component allows you to configure Dr.Web reaction on third-party application actions that are not trusted and may result in infecting your computer, e.g., attempts to modify the HOSTS file or to change the critically important system registry keys. When the Behavior Analysis component is enabled, Dr.Web blocks automatic changing of system objects, if such modification explicitly signifies a malicious attempt to harm the operating system. Behavior analysis protects the system against previously unknown malicious programs that can avoid detection by traditional signature-based and heuristic analyses.

### To access the Behavior Analysis window

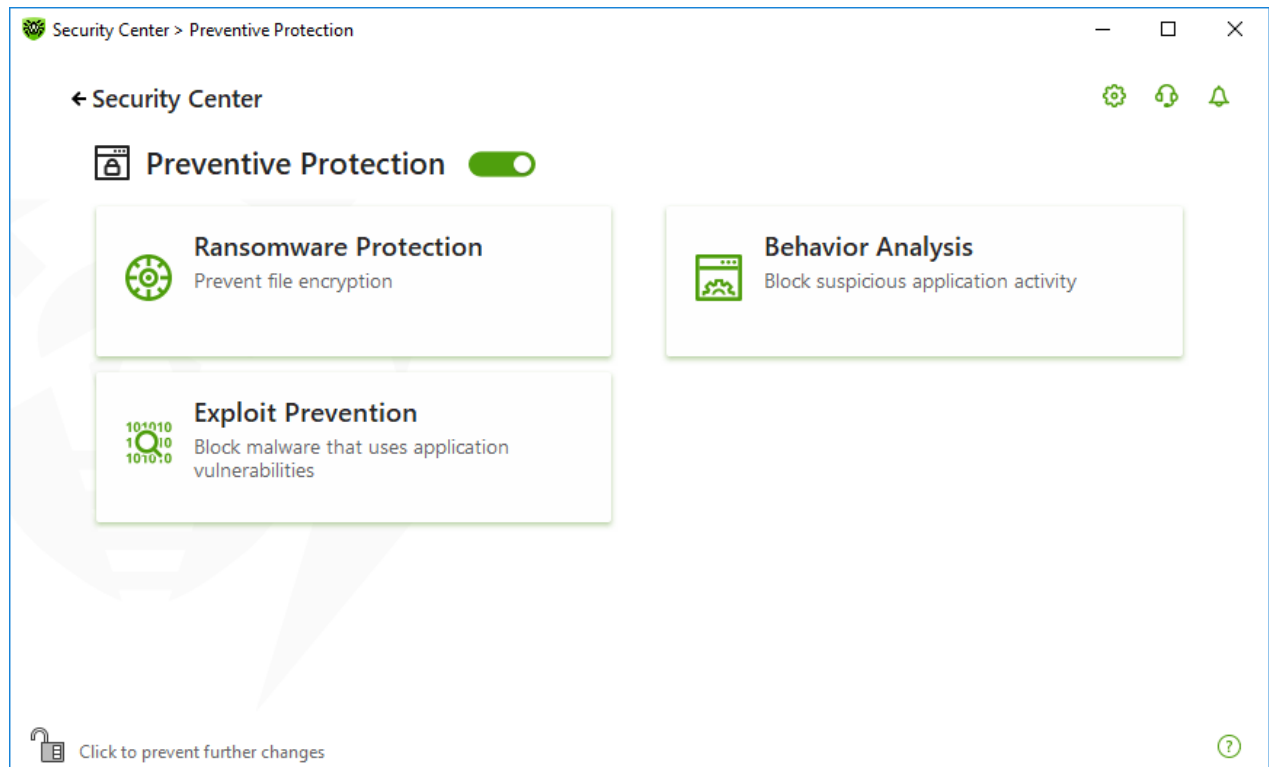
1. Open Dr.Web [menu](#) , then select **Security Center**.



2. In the open window, click **Preventive Protection** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Click the **Behavior Analysis** tile.



The component settings can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.



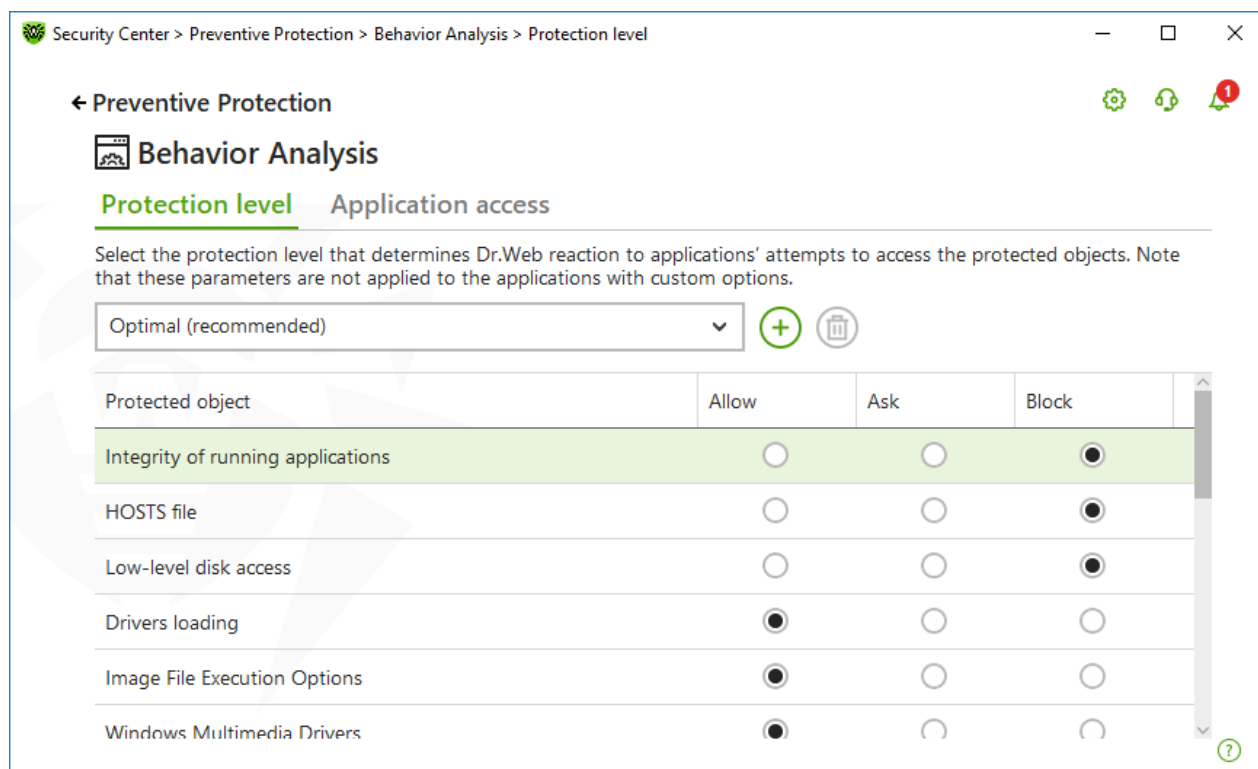
**Figure 61. Access to the Behavior Analysis component**

In this section:

- [Component operation modes](#)
- [Creating and editing necessary application rules](#)
- [Protected object description](#)



## Behavior Analysis parameters

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

**Figure 62. Behavior Analysis parameters**

You can configure a separate protection level for particular objects and processes or set a general level which settings will be applied to all other processes. To set a general protection level, select it from the drop-down list on the **Protection level** tab.

## Protection levels

Protection level	Description
<b>Optimal (recommended)</b>	<p>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 application access to disk and protects the HOSTS file from modification, if it explicitly signifies a malicious attempt to harm the operating system.</p> <div> Only actions by the applications that are not trusted, are blocked.</div>
<b>Medium</b>	<p>If there is a high risk of your computer getting infected, you can increase protection by selecting this mode. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.</p> <div> Using this mode may lead to compatibility problems with legitimate software that uses the protected registry</div>



	branches.
<b>Paranoid</b>	When required to have total control of access to critical Windows objects, you can select this mode. In this mode, Dr.Web also provides you with interactive control over loading of drivers and automatic running of programs.
<b>User-defined</b>	With this mode, you can set a custom protection level for various objects.

## User mode

All changes are saved in the User mode. In this window, you can also create a new protection level for saving necessary settings. The protected objects will be available for reading at all component settings.

You can choose one of the Dr.Web reactions to application attempts to modify the protected objects:

- **Allow**—the access to a protected object will be allowed for all the applications.
- **Ask**—if an application attempts to modify a protected object the notification will be displayed:

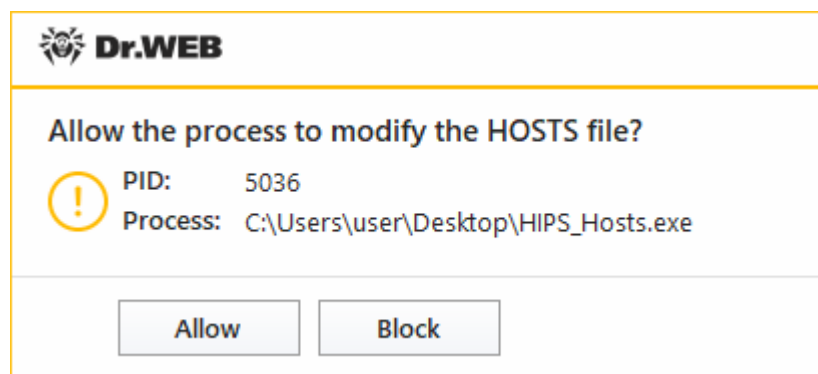


Figure 63. Notification example with an access to a protected object request

- **Block**—if an application attempts to modify a protected object the access will be blocked. Herewith, the notification will be displayed:

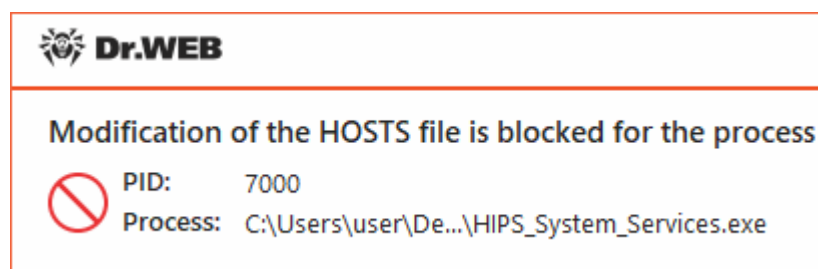




Figure 64. Notification example with a blocked access to a protected object



### To create a new protection level

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

### To delete a protection level

1. In the drop-down menu, select a protection level created earlier that you want to delete.
2. Click the  button. Predefined profiles cannot be deleted.
3. To confirm the deletion, click **OK**.

## Receiving notifications

If necessary, you can [configure](#) desktop notifications on Behavior Analysis actions.

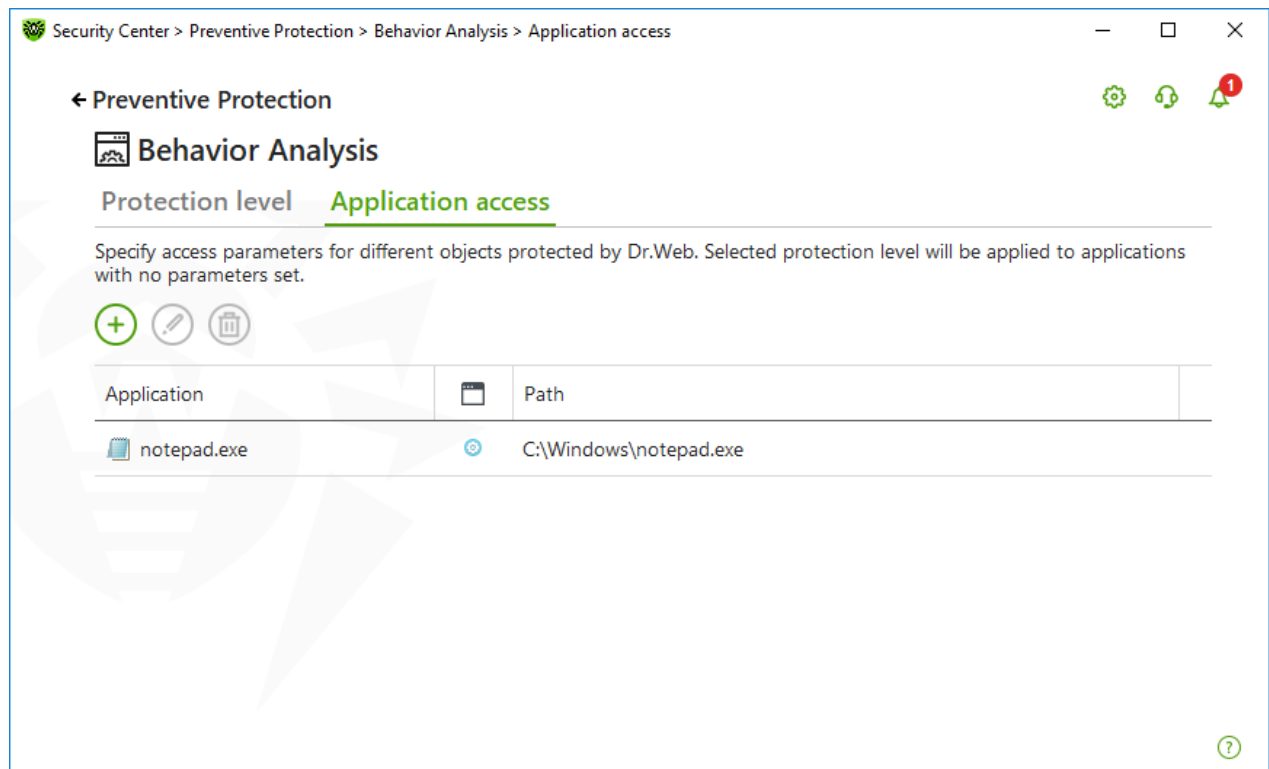
See also

- [Notifications](#)

## Application access

To add custom access parameters for certain applications, go to the **Application access** tab. On this tab, you can add a new application rule, edit or delete an existing one.





**Figure 65. Application access parameters**

The following management elements are available to work with objects in the table:

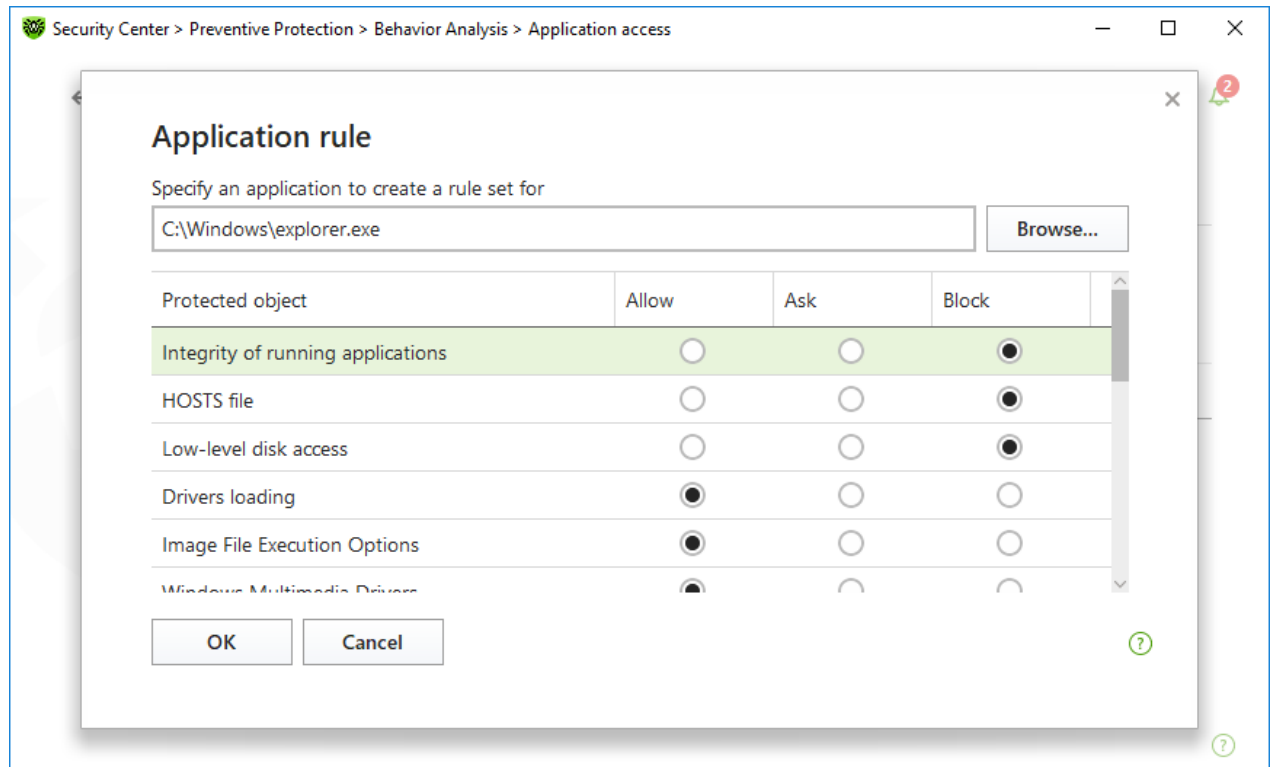
- The button—adding a rule set for the application.
- The button—editing existing rule sets.
- The button—deleting a rule set.

In the (**Rule type**) column you can see three rule types:

- —the **Allow all** rule is set for all protected objects.
- —different rules are set for protected objects.
- —the **Block all** is set for all protected objects.

### To add an application rule

1. Click .
2. In the open window, click **Browse** and specify the path to the application executable file.



**Figure 66. Adding a rule set for an application**

3. Look through default settings and, if necessary, edit them.
4. Click **OK**.

## Protected 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.
HOSTS file	The operating system uses the HOSTS file when connecting to the internet. Changes to this file may indicate virus infection.
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 the users' profiles).</p> <p>Image File Execution Options</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options</li></ul> <p>Windows Multimedia Drivers:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Drivers32</li></ul>



Protected object	Description
	<ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers</li></ul> <p>Winlogon registry keys:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL</li></ul> <p>Winlogon notifiers:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify</li></ul> <p>Windows registry startup keys:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadApplnit_DLLs, Load, Run, IconServiceLib</li></ul> <p>Executable file associations:</p> <ul style="list-style-type: none"><li>• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)</li><li>• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys)</li></ul> <p>Software Restriction Policies (SRP):</p> <ul style="list-style-type: none"><li>• Software\Policies\Microsoft\Windows\Safer</li></ul> <p>Browser Helper Objects for Internet Explorer (BHO):</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects</li></ul> <p>Autorun of programs:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Run</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServices</li><li>• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce</li></ul> <p>Autorun of policies:</p> <ul style="list-style-type: none"><li>• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run</li></ul> <p>Safe mode configuration:</p> <ul style="list-style-type: none"><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal</li><li>• SYSTEM\ControlSetXXX\Control\SafeBoot\Network</li></ul> <p>Session Manager Parameters:</p> <ul style="list-style-type: none"><li>• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows</li></ul> <p>System services:</p> <ul style="list-style-type: none"><li>• System\CurrentControlSetXXX\Services</li></ul>






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

## 9.3. Exploit Prevention

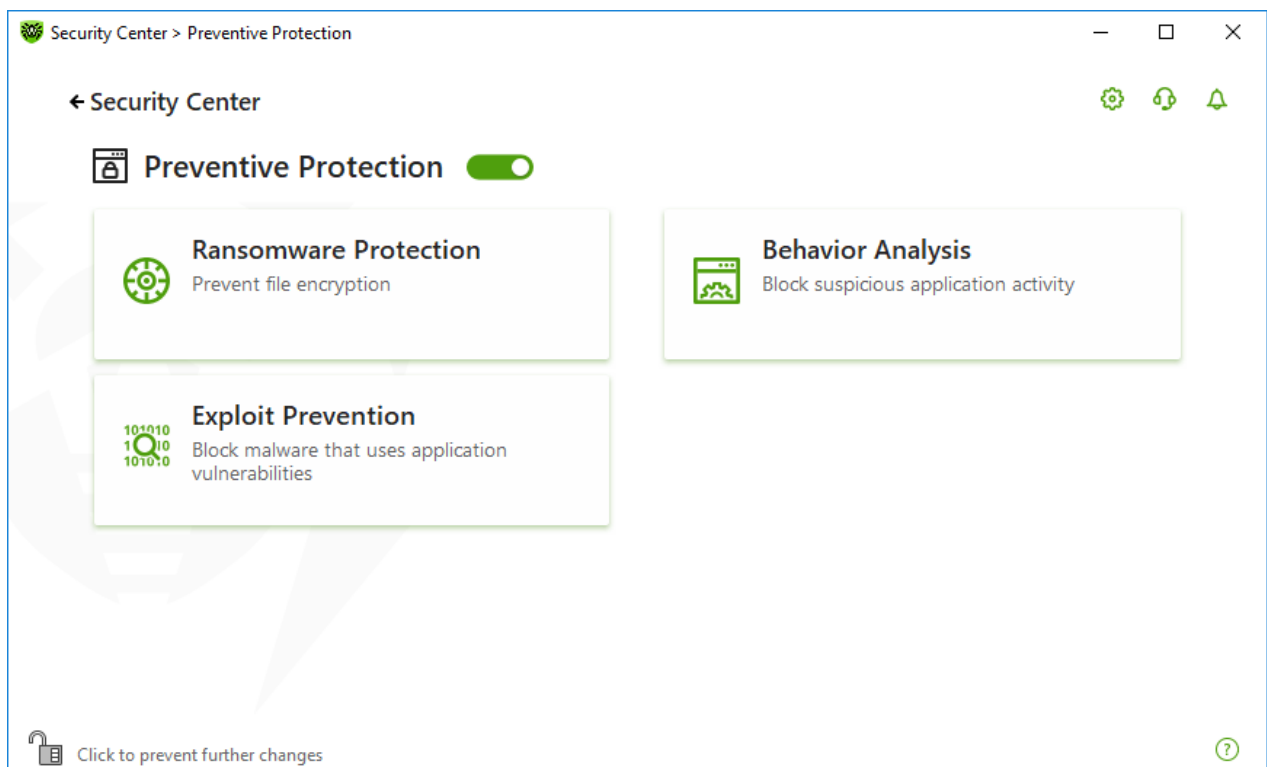
The Exploit Prevention component allows you to block malicious programs that use vulnerabilities of well-known applications.

### To open Exploit Prevention parameters

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.
3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Click the **Exploit Prevention** tile. A component parameter window opens.

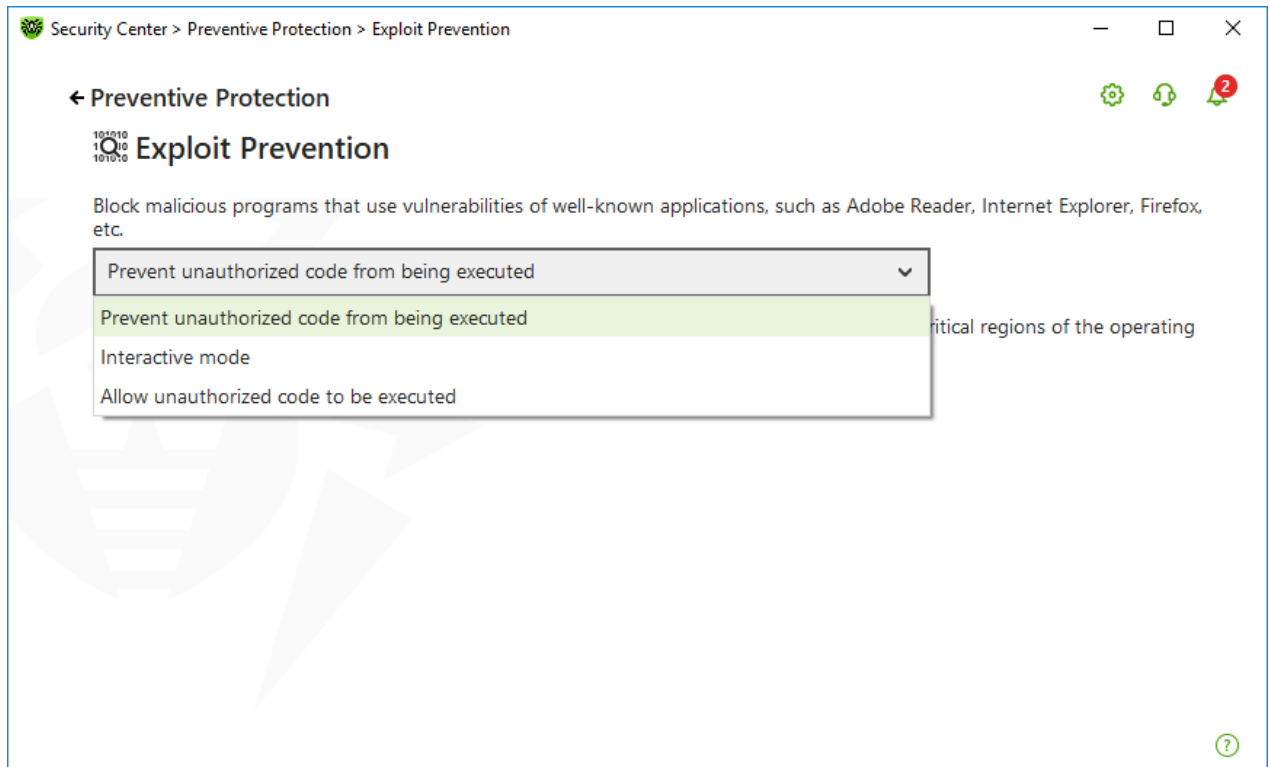


The component parameters can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.



**Figure 67. Access to the Exploit Prevention component**

In the window of component parameters, from the corresponding drop-down list, select the required level of protection against exploits.

**Figure 68. Selecting protection level**

## Protection levels

Protection level	Description
Prevent unauthorized code from being executed	If an attempt of a malicious object to exploit software vulnerabilities in order 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 in order 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 in order to get access to critical regions of the operating system is detected, it will be allowed automatically.

## Receiving notifications

If necessary, you can [configure](#) desktop notifications on Exploit Prevention actions.

See also

- [Notifications](#)






## 10. Devices

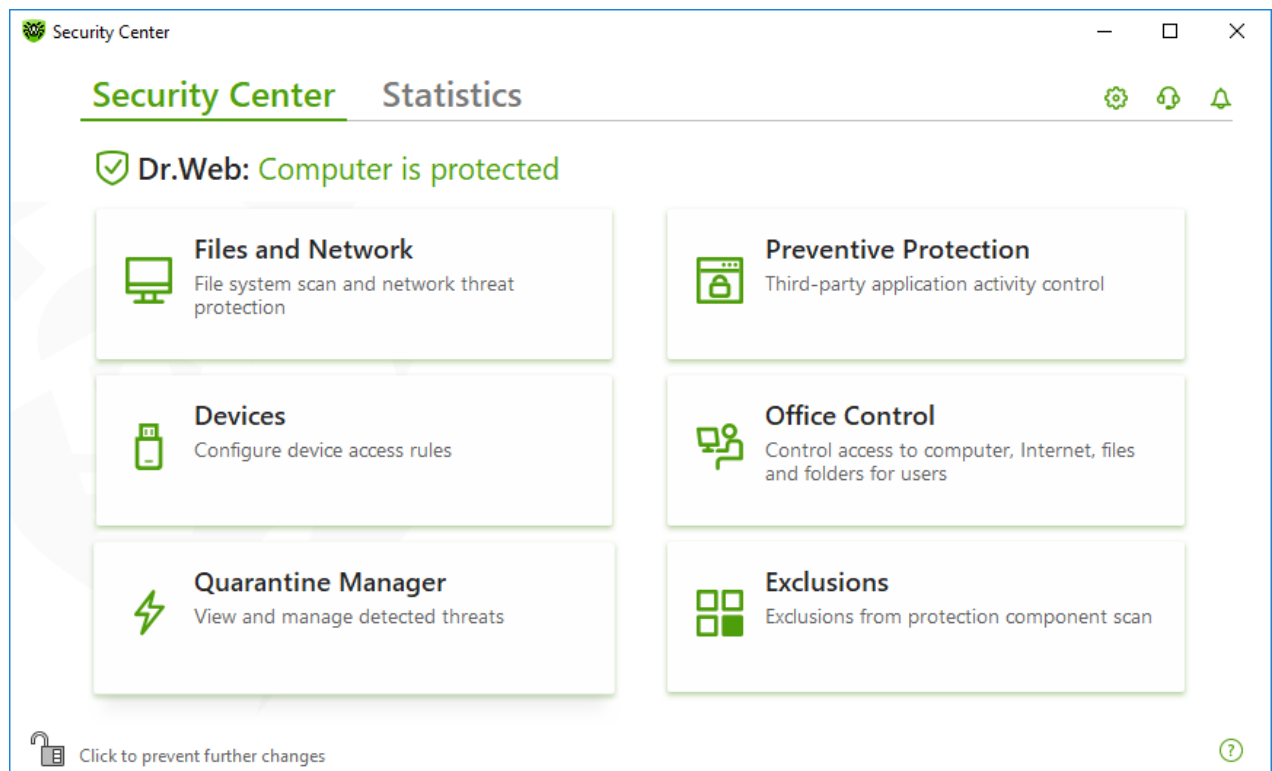
In the **Devices** window you can restrict access to certain devices or buses and configure the list of allowed devices.



Device access parameters are applied for all Windows accounts.

### To open the Devices window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
3. Click the **Devices** tile.



**Figure 69. Access to the Devices window**

In this section:

- [General blocking parameters](#)
- [Device classes and buses blocking](#)
- [Configuring the list of allowed devices](#)



## General parameters

You can enable the corresponding settings to:

- Block sending jobs to printers.
- Block data transfer via local networks and the internet.

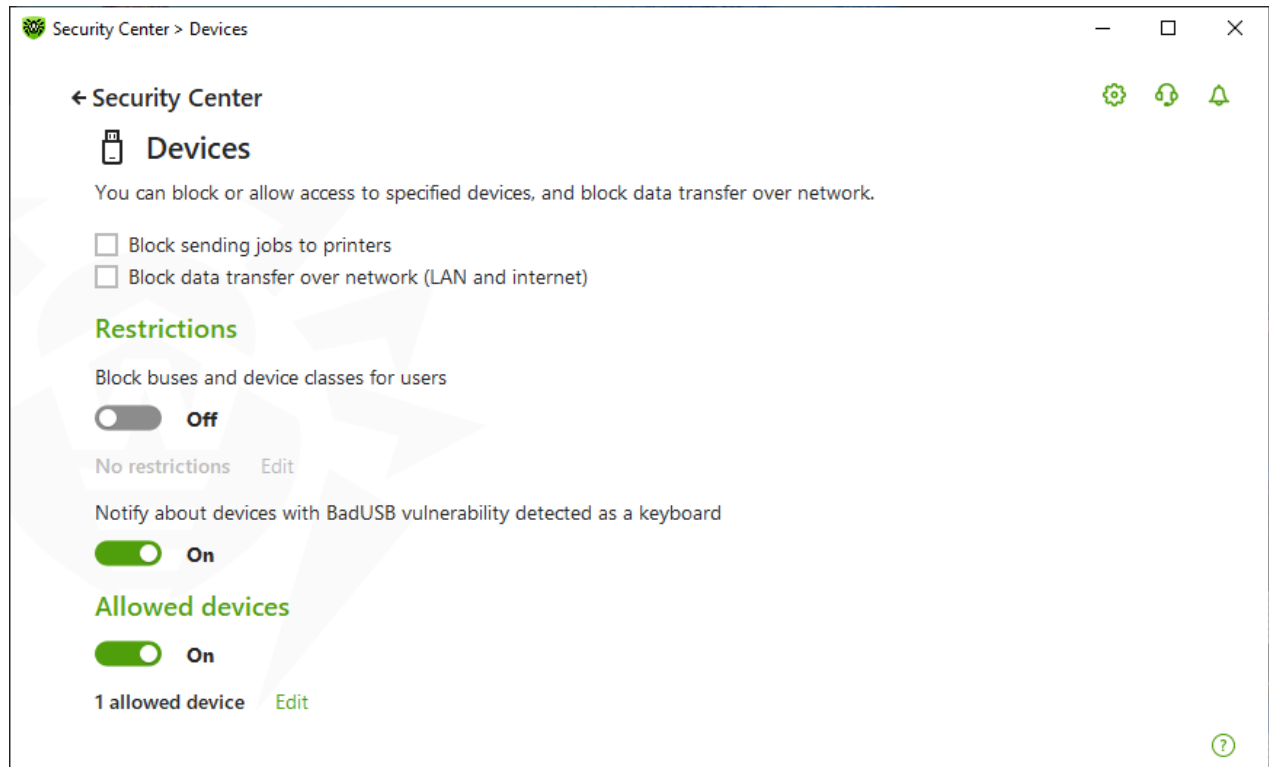


Figure 70. Device blocking parameters

All options are disabled by default.



The **Block removable media** option is only available to the users who had it enabled before the product components were updated on 2/2/2022. If you were not using this option or are installing the product for the first time, use the **Block device classes and buses for users** option to prevent access to data on removable media.


## Restrictions

### Device blocking parameters

The function of device blocking allows you 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). *Buses* are communication subsystems for transferring data between functional units of the computer (for example, the USB).



### To block access to the selected device classes or buses

1. Enable the **Block device classes and buses for users** option by using the switcher .
2. Click **Edit** link.
3. In the open window, you can [select device classes or buses](#) that you want to restrict access to.

### Notification on BadUSB vulnerable devices

Some of the 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 about devices with BadUSB vulnerability detected as a keyboard** option. In this case, when a keyboard is connected, you are prompted to press the specified keys.

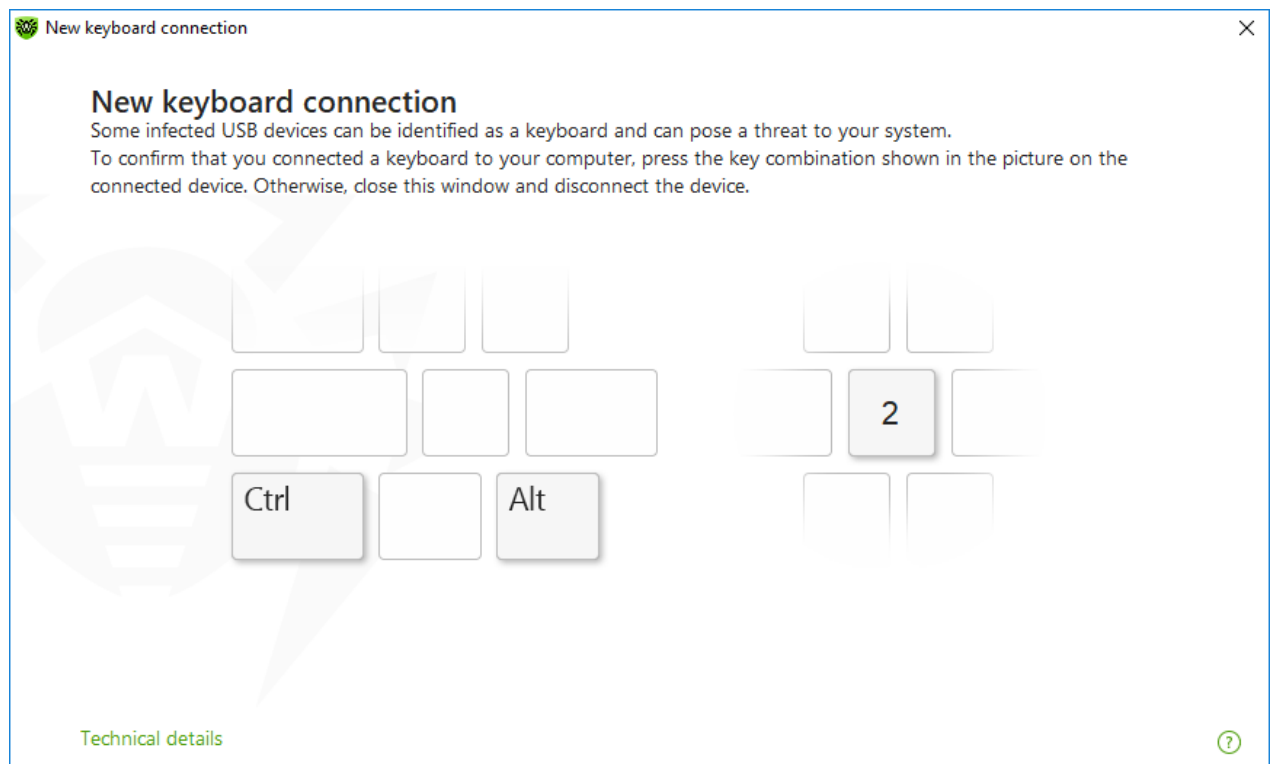


Figure 71. Keyboard unblock window

When you click the **Technical details** link, a window with a detailed information on the device opens.


### Allowed Devices

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







### To add a device to the list of allowed devices

1. Enable the **Allowed devices** option by using the switcher .
2. Click **Edit** (the button is available if any restrictions are set).
3. In the open window, you can [generate a list of devices](#) to which the access restrictions are not applied.

## 10.1. Bus and Device Class Blocking

### To open the Device classes and buses window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Devices** tile.
3. In **Restrictions** setting group, enable the **Block device classes and buses for users** option by using the switcher .
4. Click **Edit**.
5. In the open window, you can select device classes or buses that you want to restrict access to.

The window contains a table with the information on blocked buses and device classes. By default, the table is empty. After adding buses or classes to the block list, they are displayed in the table. The line with the blocked bus displays all blocked classes on this bus.

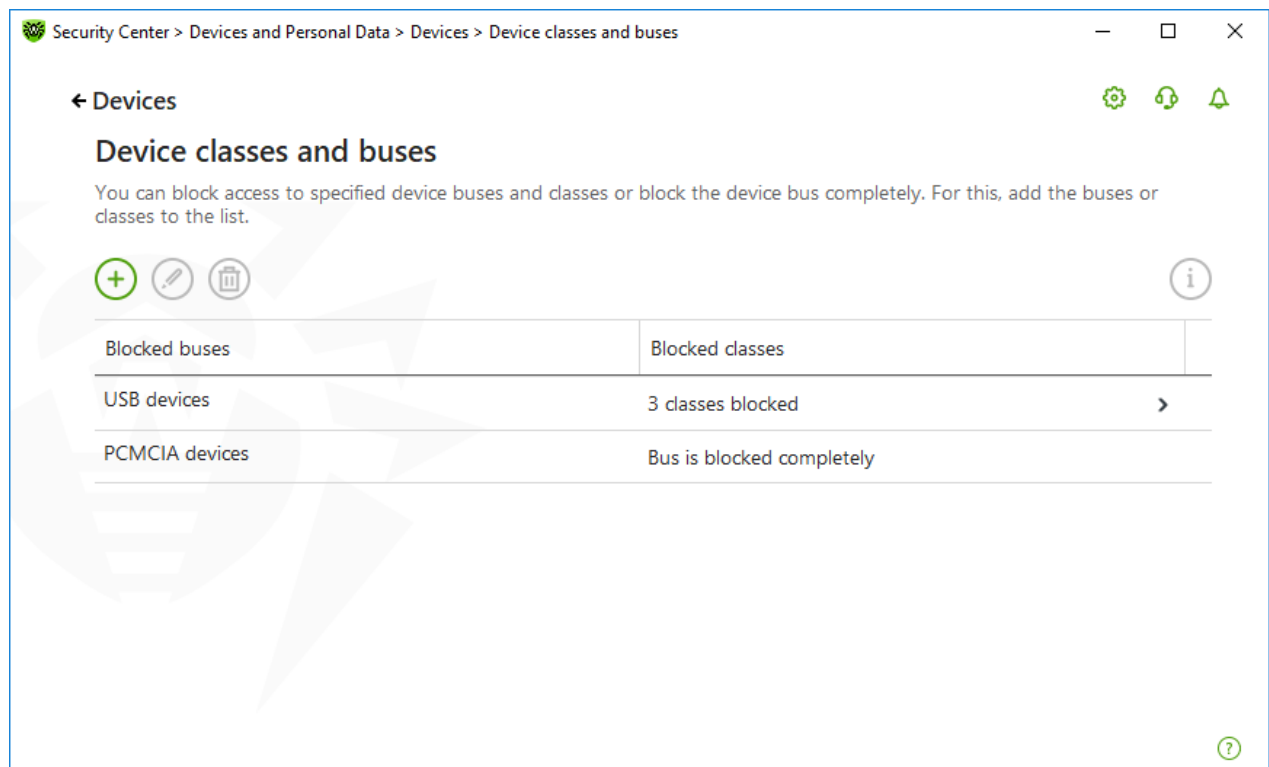





Figure 72. Blocked classes and classes




In the **Blocked classes** column, you can see the number of blocked classes on the corresponding bus. If several classes are blocked on a bus, they are displayed as a drop-down menu.


Class blocked on all buses is grayed out.

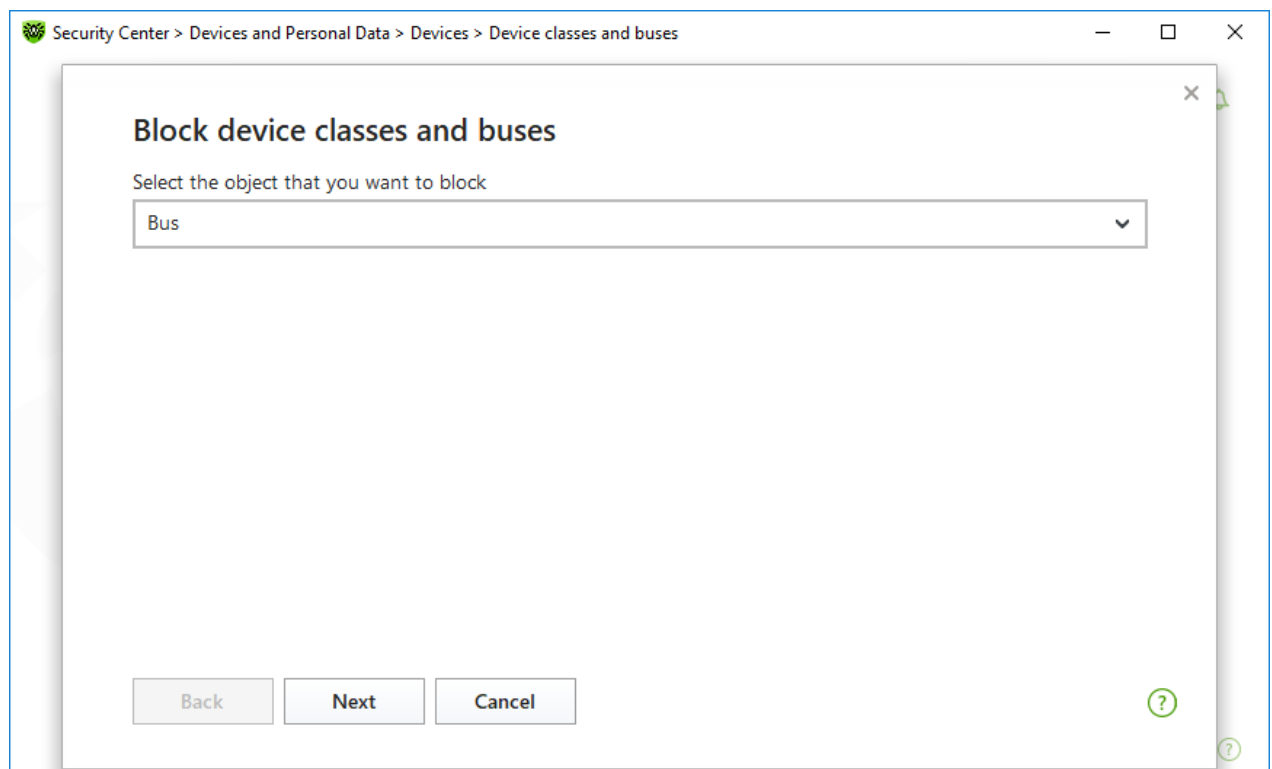
The following management elements are available to work with objects in the table:

- The  button—adding an object to the block list.
- The  button—editing the settings for the selected object in the table.
- The  button—removing the selected object from the block list.

You can view detailed information on the blocked bus and blocked classes on it. For that, select the necessary line and click .

## Bus blocking

1. To block the entire bus or some devices on a certain bus click .
2. Select an object to be blocked from the drop-down menu: **Bus**. Click **Next**.



**Figure 73. Selecting an object to be blocked**

3. Select the bus type. Click **Next**.

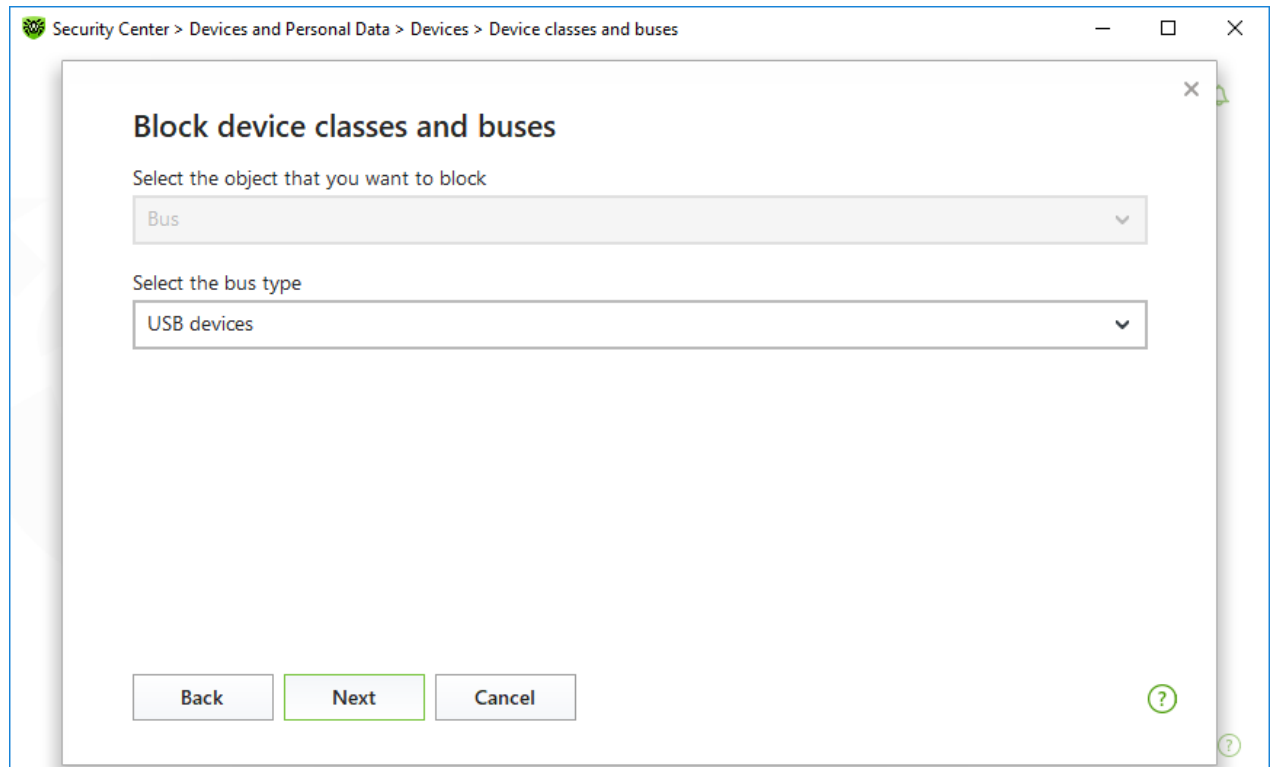


Figure 74. Selecting the bus type

4. Select the blocking type and click **Next**:

- **Completely**—to block all device classes on the selected bus;
- **Partially**—to open a window where you can select device classes to be blocked on the selected bus.

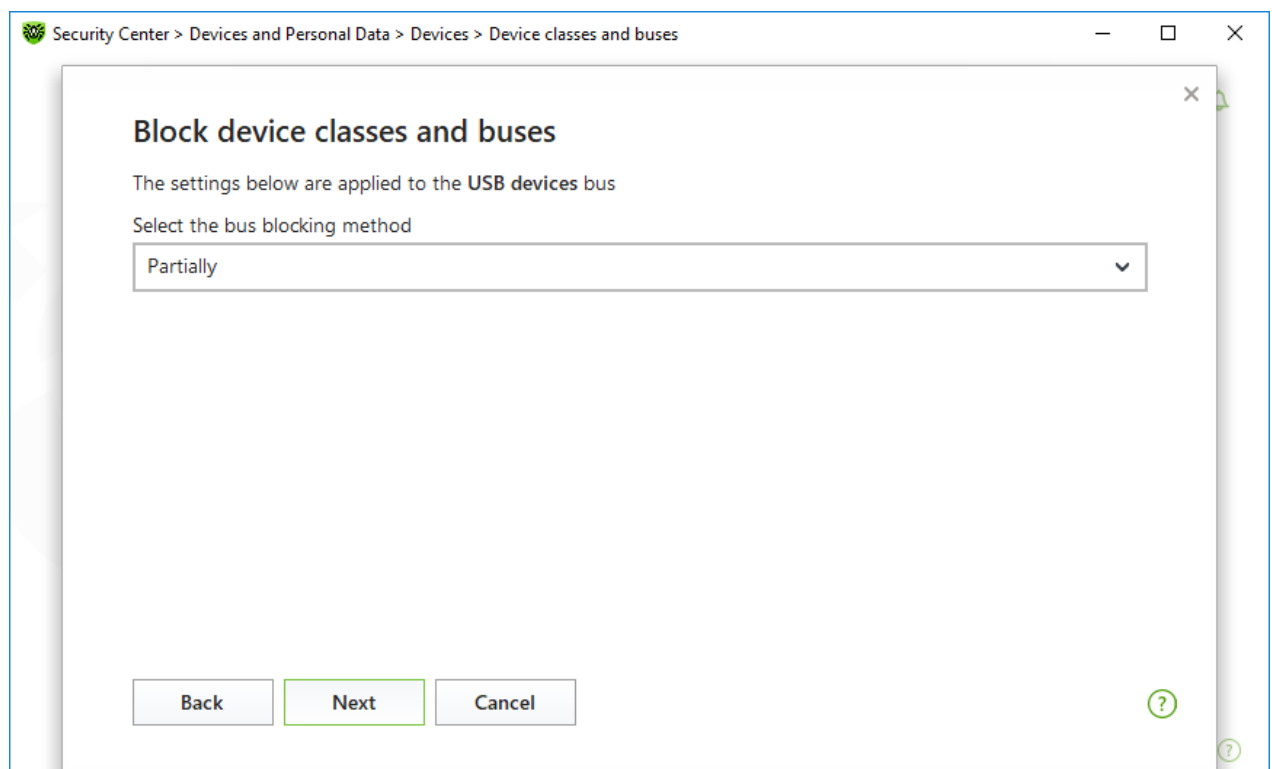
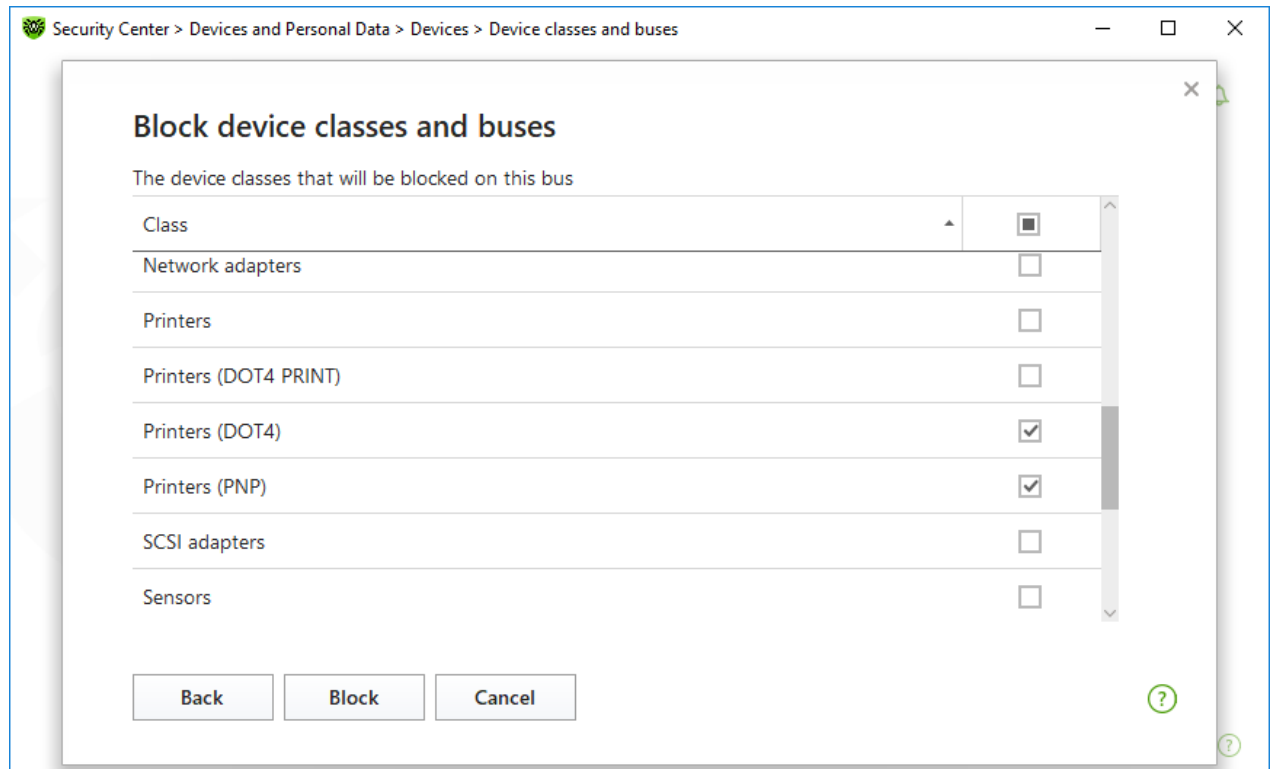


Figure 75. Selecting a bus blocking method




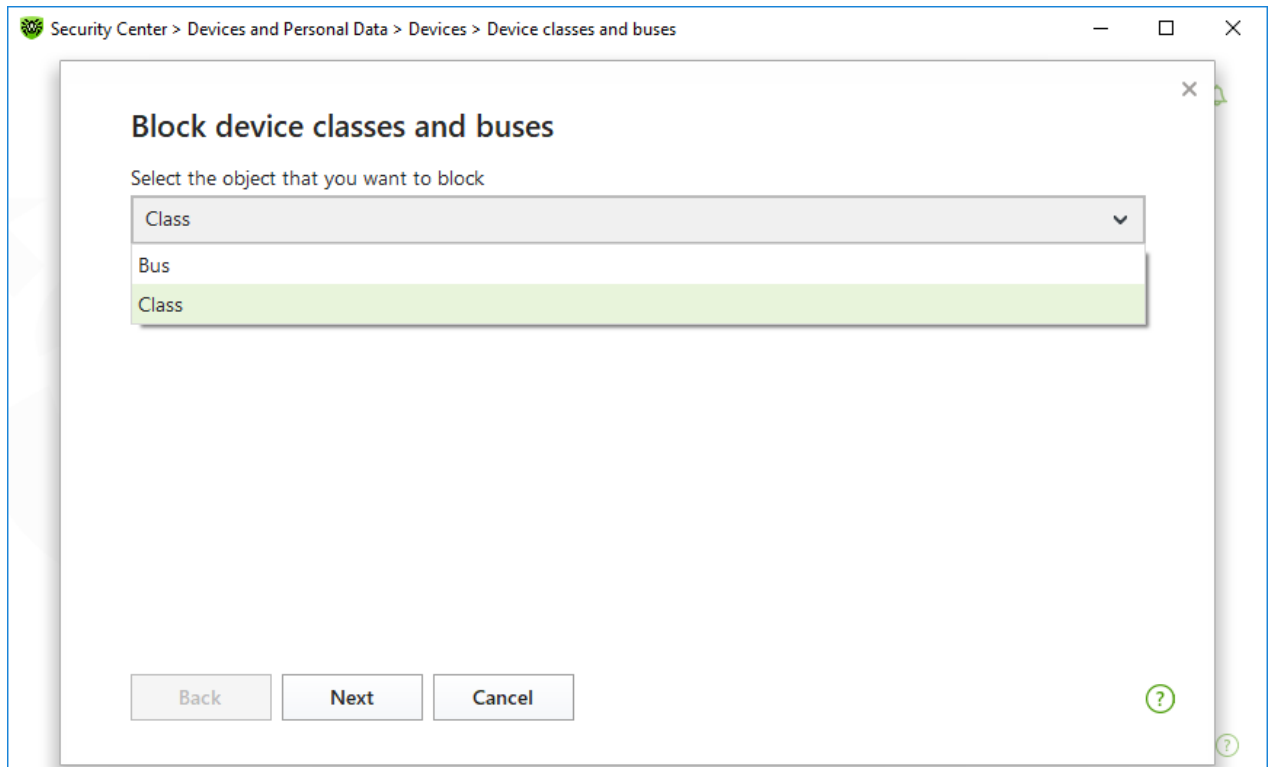
5. If you have selected the **Partially** option, in the open window check the classes on the list to be blocked. Click **Block**.



**Figure 76. Selecting device classes on a bus**

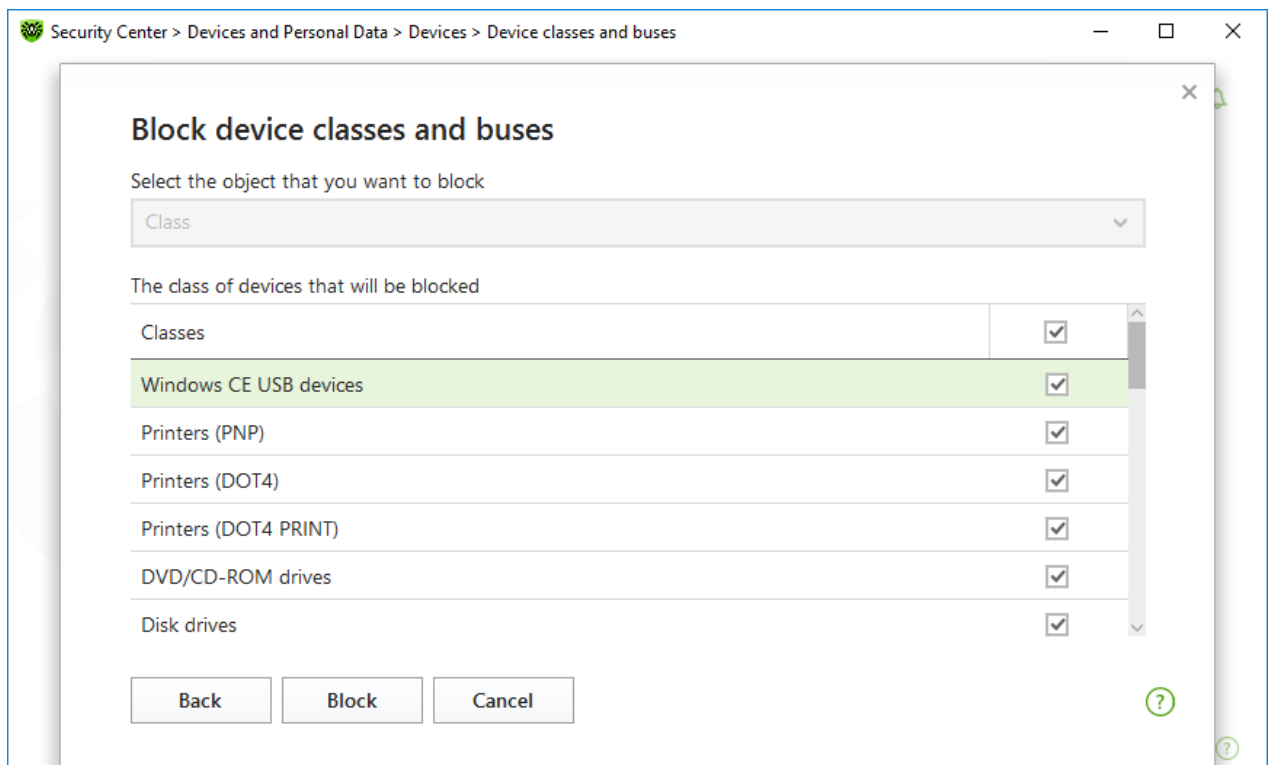
## Device class blocking

1. To block one or several classes, click .
2. Select an object to be blocked in the drop-down menu: **Class**. Click **Next**.



**Figure 77. Selecting an object to be blocked**

3. Check the classes on the list to be blocked. Click **Block**.



**Figure 78. Selecting device classes**



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.


If you block the USB bus, the keyboard and the mouse are added to the exclusions.

## Receive notifications

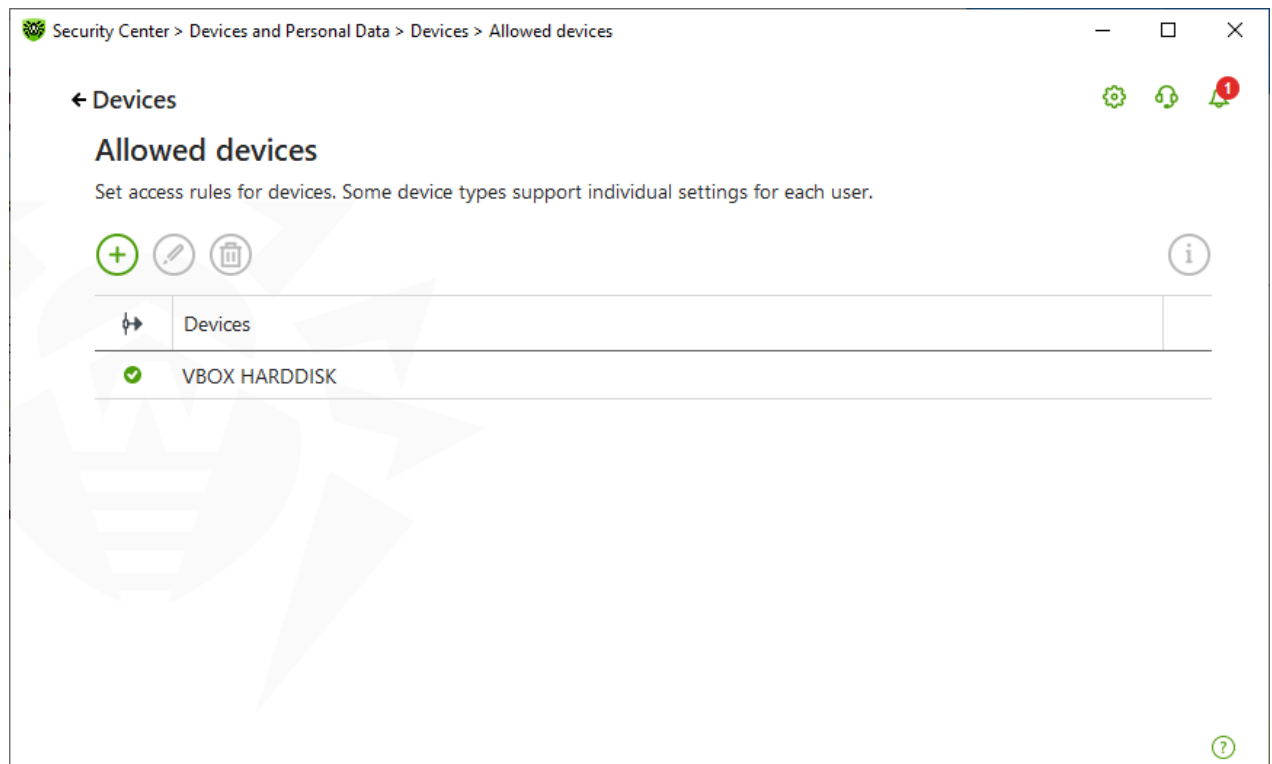
You can [configure](#) displaying pop-ups on blocking a device.

## 10.2. Allowed Devices

### To open the Allowed devices window


1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Devices** tile.
3. In the **Allowed devices** group, click **Edit**.

The **Allowed devices** window contains information on all the devices added to the list of allowed devices. This information is in the table:






**Figure 79. Allowed Devices**


The following management elements are available to work with objects in the table:

- The  button—adding a rule set for the device.




- The  button—editing a rule set for the device.
- The  button—deleting a rule set for the device.

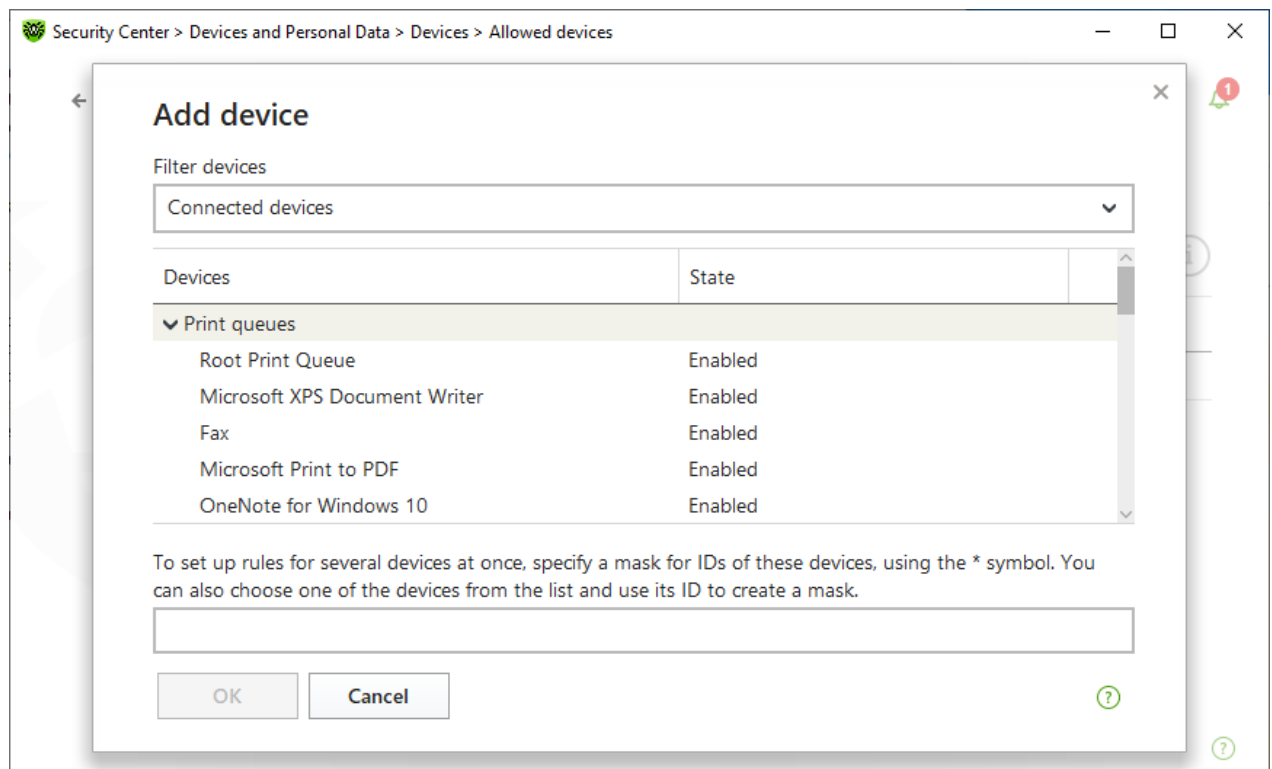
You can view detailed information on a device added to the list of allowed devices. For that, select the necessary line and click .

In the  (**Rule type**) column, you can see two rule types:



- —the **Allow all** rule is set.
- —the **Read-only** rule is set.

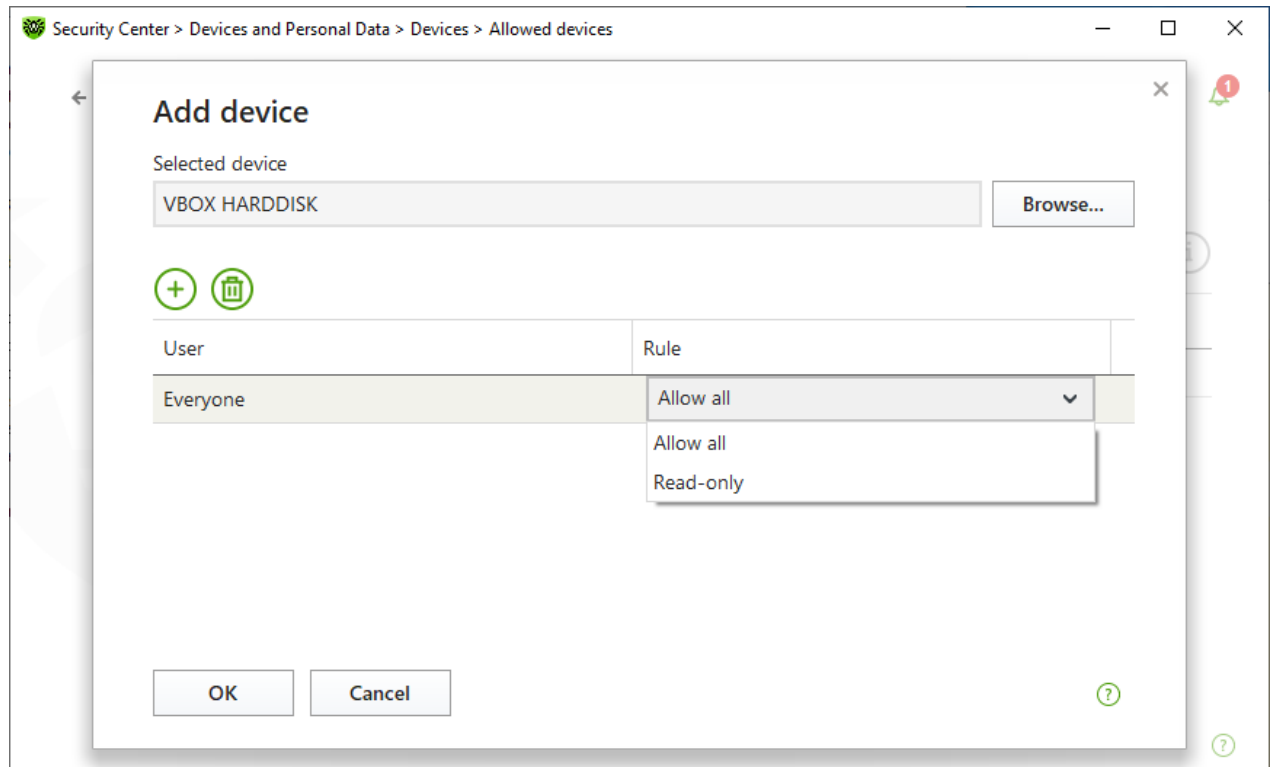
### To add a device to the list of allowed devices

1. Make sure that the device is connected to the computer.
2. 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**.



**Figure 80. Adding a device to the list of allowed devices**

3. 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 .



**Figure 81. Selecting a rule for a certain user**

4. To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**. You will return to the list of allowed devices.






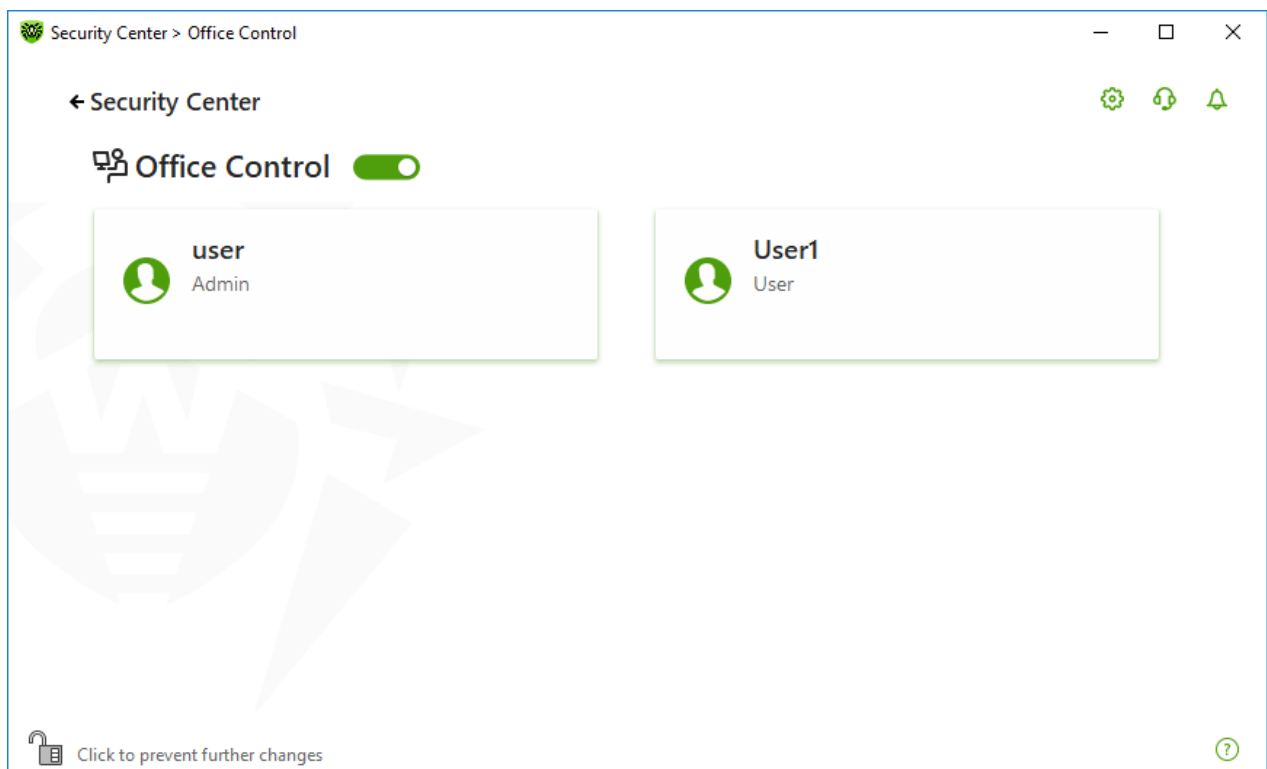
## 11. Office Control

The Office Control component allows you to manage the access to websites, files, and folders. You can also set time limits on internet and computer usage.




By default, Office Control is enabled and operates in the **No restrictions** mode.

### To enable or disable Office Control

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Office Control** tile. The **Office Control** window opens.



**Figure 82. Office Control**

3. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
4. Enable or disable Office Control using a corresponding switcher .



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

### Configuring Office Control for a certain user

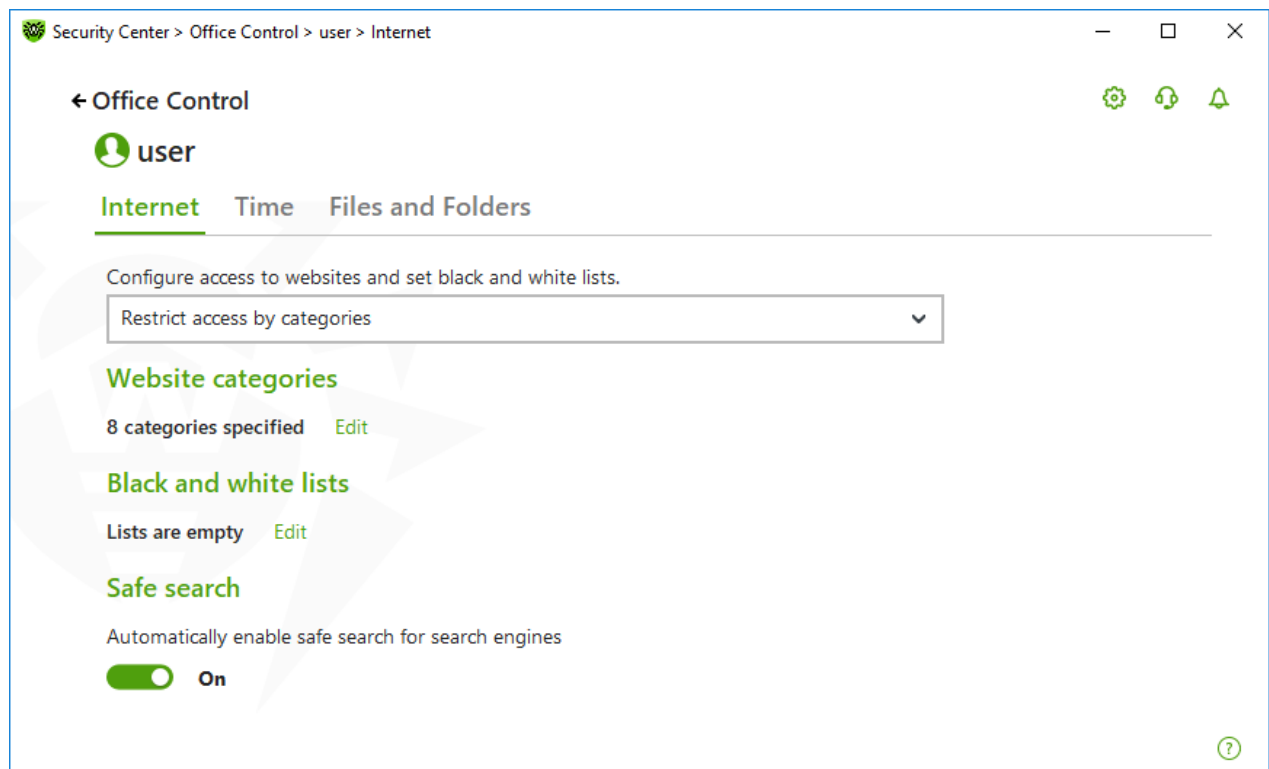
Before setting restrictions for a user, make sure that this user does not have administrative privileges. Otherwise, the user could change the Office Control component parameters and disable the access restrictions.



The component settings can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enables this option.

## To open Office Control parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. In the Office Control window (see figure [Office Control](#)), click the tile with the user name for whom you want to configure Office Control. A window with Office Control parameters opens for the selected user.



**Figure 83. Configuring Office Control**

3. Select a necessary tab to configure Office Control.
  - **Internet**—configure access to internet resources. The tab allows you to restrict users from visiting unwanted websites (pages on violence, gambling, etc.) or allow access only to certain websites. See the [Access to internet Resources](#) section.
  - **Time**—configure access to the computer and the internet. The tab allows you to set time limits on use of your computer and the internet on selected time and days of the week. See the [Time limits](#) section.
  - **Files and Folders**—configure access to the file system. The tab allows you to restrict access to certain files or folders (on local drives and removable media). See the [Access to files and folders](#) section.



If the user has a Windows account with administrator rights, you should change its type to Standard User.

## How to change the user's account type

### On Windows XP

1. Open the **Start** menu, then click **Control Panel** and select **User accounts**.
2. Select the account which type you would like to change and click **Change account type**.
3. Select the user's account type: **Limited account**.
4. Click **Change account type** to save the changes.

### On Windows Vista and Windows 7

1. Open the **Start** menu, then click **Control Panel** and select **User accounts**.
2. To change the account type, click **Manage another account**.
3. Select the account which type you would like to change and click **Change account type**.
4. Select the user's account type: **Standard User**.
5. Click **Change account type** to save the changes.

### On Windows 8

1. Open **Control Panel** and select **User Accounts and Family Safety**.
2. Click **Manage another account** button.
3. Select the account which type you would like to change and click **Change account type**.
4. Select the user's account type: **Standard User**.
5. Click **Change account type** to save the changes.

### On Windows 8.1

1. Point to the lower-right corner of the screen, move the mouse pointer up, click **Settings**, and then click **Change PC settings**.
2. Click **Accounts**, and then click **Other accounts**.
3. Select the account which type you would like to change and click **Change account type**.
4. Select the user's account type: **Standard User**.
5. Click **OK**.




## On Windows 10

1. Select the **Start** button, then select **Settings**.
2. In the open window, select **Accounts**.
3. On the left side of the window, select **Family & other people**.
4. Click the icon of an account which type you would like to change and click **Change account type**.
5. Select the user account type: **Standard User**.
6. Click **OK**.

## On Windows 11

1. Select the **Start** button, then select **Settings**.
2. In the open window, select **Accounts**.
3. In the center of the window, select **Family & other users**.
4. Click the icon of an account which type you would like to change and click **Change account type**.
5. Select the user account type: **Standard User**.
6. Click **OK**.

If there is only one account in the system, you cannot change its type to Standard User. For more information, please refer to [Microsoft technical support](#)  website.

## Receiving notifications

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

## 11.1. Access to Internet Resources

On the **Internet** tab, you can restrict users from visiting unwanted websites (pages on violence, gambling, etc.) or allow access only to certain websites. By default, the **No restrictions** mode is set for all users. The following modes are also available:

- **Restrict access by categories**
- **Allow access only to websites from the white list**

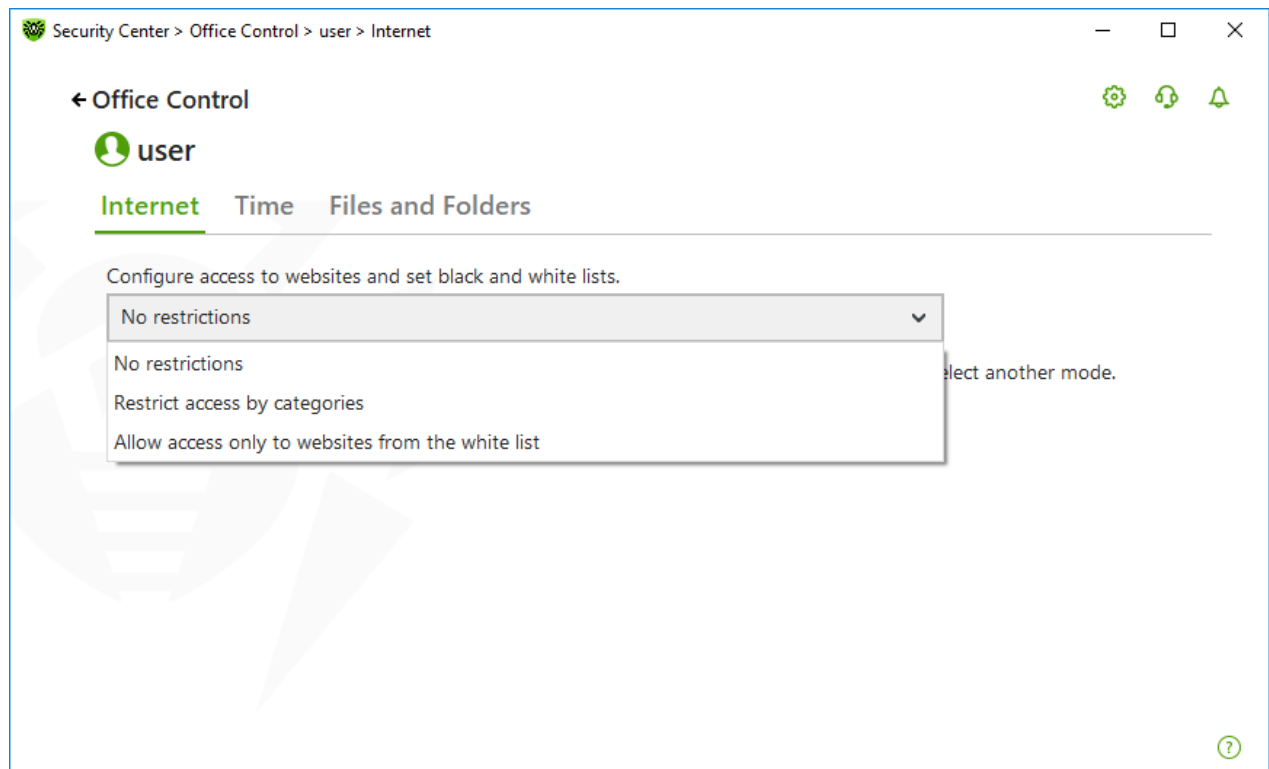


Figure 84. Selecting the mode of Office Control

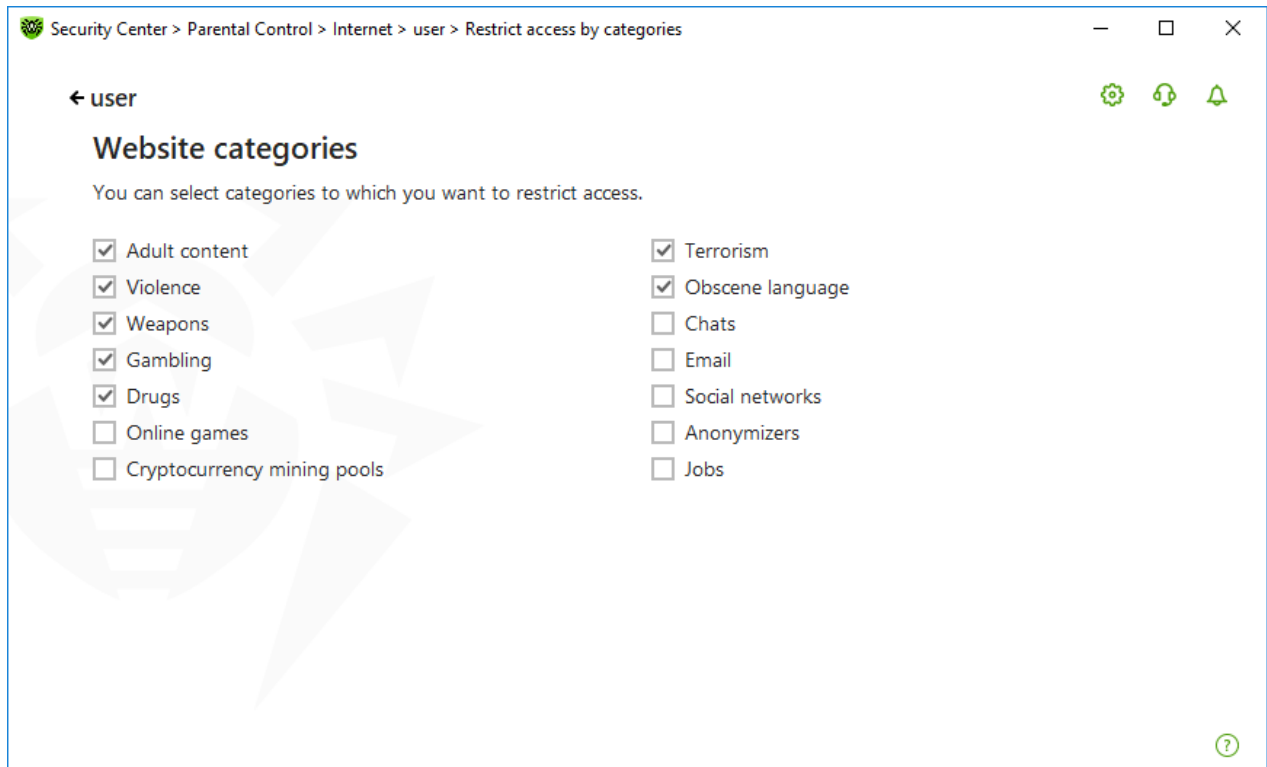
### Restrict access by categories mode

In the mode, you can specify website categories to block. The same website can be assigned to several different categories. In this case, Office 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 also add websites to block or allow access to the resources regardless of other restrictions. To do so, use [black and white lists](#).

#### To allow or block access to websites of a certain category

1. In the **Website categories** group, click **Edit**. The window with blocking categories parameters opens.



**Figure 85. Categories of websites to block**

2. Select or clear the check box to allow or block access to websites of a certain category.

### Categories of internet resources

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.



Category	Description
Email	Websites that offer the possibility of free registration of a web mailbox.
Social networks	Different social networks: 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.
Jobs	Websites that are used to post job vacancies and search for jobs.

## Allow access only to websites from the white list mode

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



If selecting the **Allow access only to websites from the white list** mode, such websites can be displayed incorrectly. Banners and other site elements integrated with external resources will not be displayed.

## Black and white lists

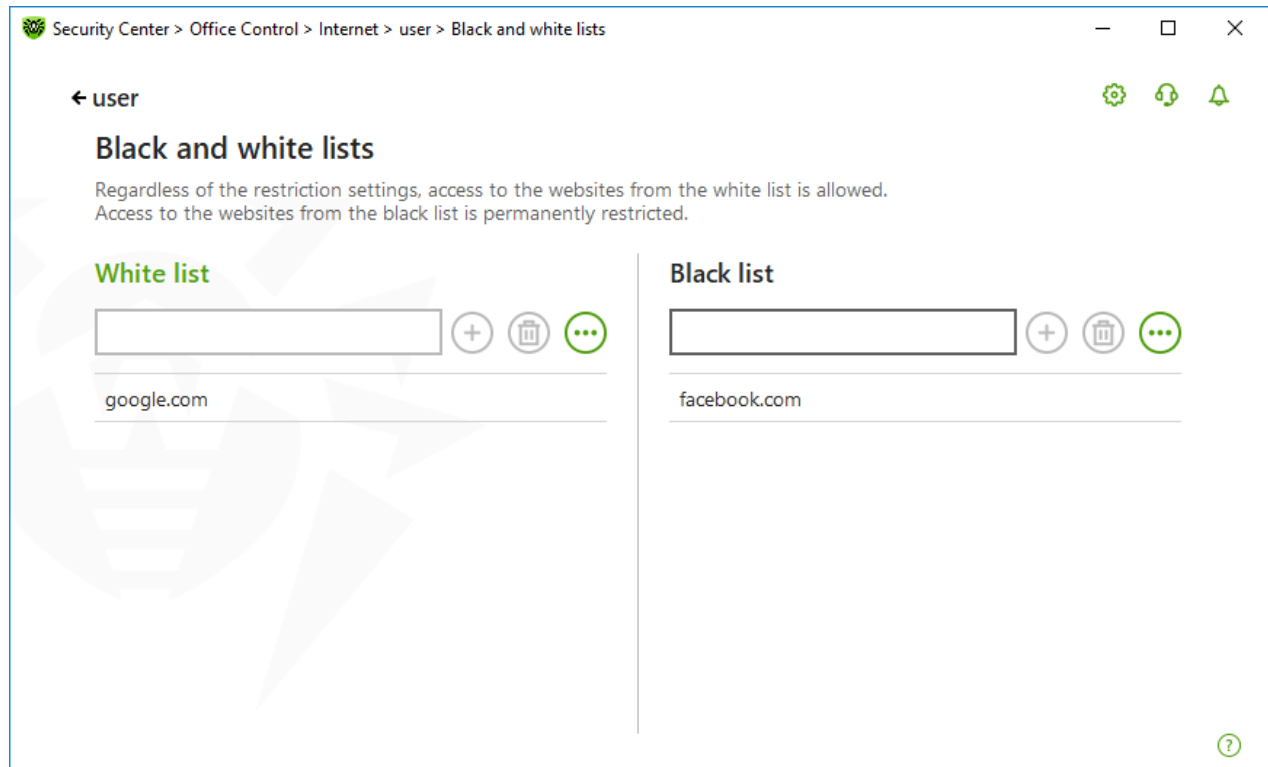
You can set black and white lists of websites access to which is allowed or blocked regardless of other Office Control parameters.



Before adding a site to the black or the white list, clear the browser cache if the site has been previously opened in this browser.

## Configuring black and white lists of Office Control

1. In the **Black and white lists** group, click **Edit**. The window with black and white list settings opens.



**Figure 86. Configuring black and white lists of Office Control**

2. Enter a domain name or a part of a domain name for the website in the **White list** or **Black list** field:
  - To add a certain website, enter its URL (for example, `www.example.com`). This allows access to all the 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 dot (.) character. This allows access to all the 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.

Example: if you enter `example.com/test`, SplDer 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/`—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 will be transformed into `www.example.com`.

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

## Safe search

The **Safe search** option affects results of search engines. This option allows you to exclude unwanted webpages from search results by using the search engine tools.

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

## 11.2. Time Limits on Computer and Internet Use

On the **Time** tab, you can set time limits on use of your computer and the internet. By default, the **No restrictions** mode is set for all users.

You can set time limits using a table with timeslots.



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

### Table of time limits on computer and internet use

The table is available in the Office Control **No restrictions** mode. If the table is changed, the **No restrictions** mode is switched to **User-defined** automatically.

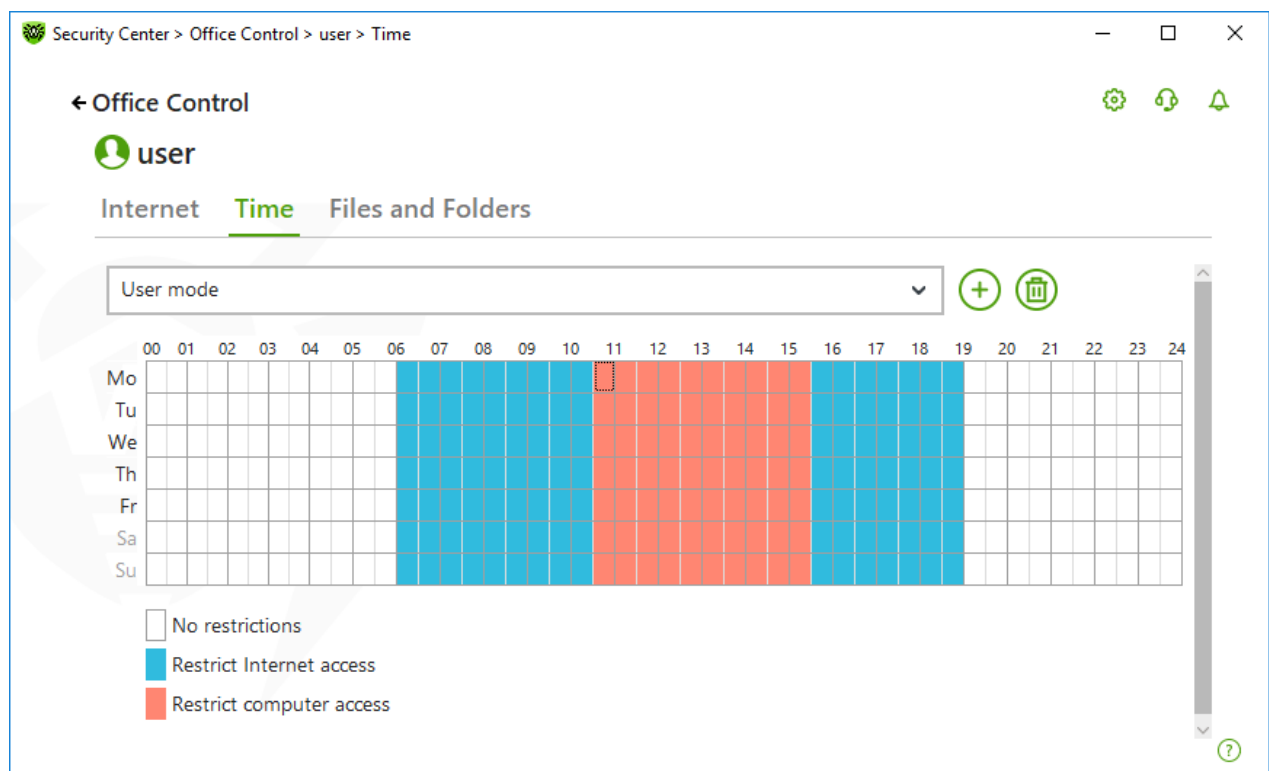
Using the table, you can specify hours and days of the week when the user is allowed to use the computer or the internet. When comes the time of computer access restriction, the user will be logged off automatically. While the restriction for a specific user's account is in effect, this user cannot log in to it. When internet use restriction is in effect, all internet content stops to download.

You can check the time remaining until access restrictions activation in the Dr.Web [menu](#) by clicking the tile **Time Limits**.



### To set time limits in the table mode

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



**Figure 87. Table of computer and internet use**

You can also create different setting profiles for one user. This option allows you to easily switch between existing setting profiles.

### Creating and removing a setting profile

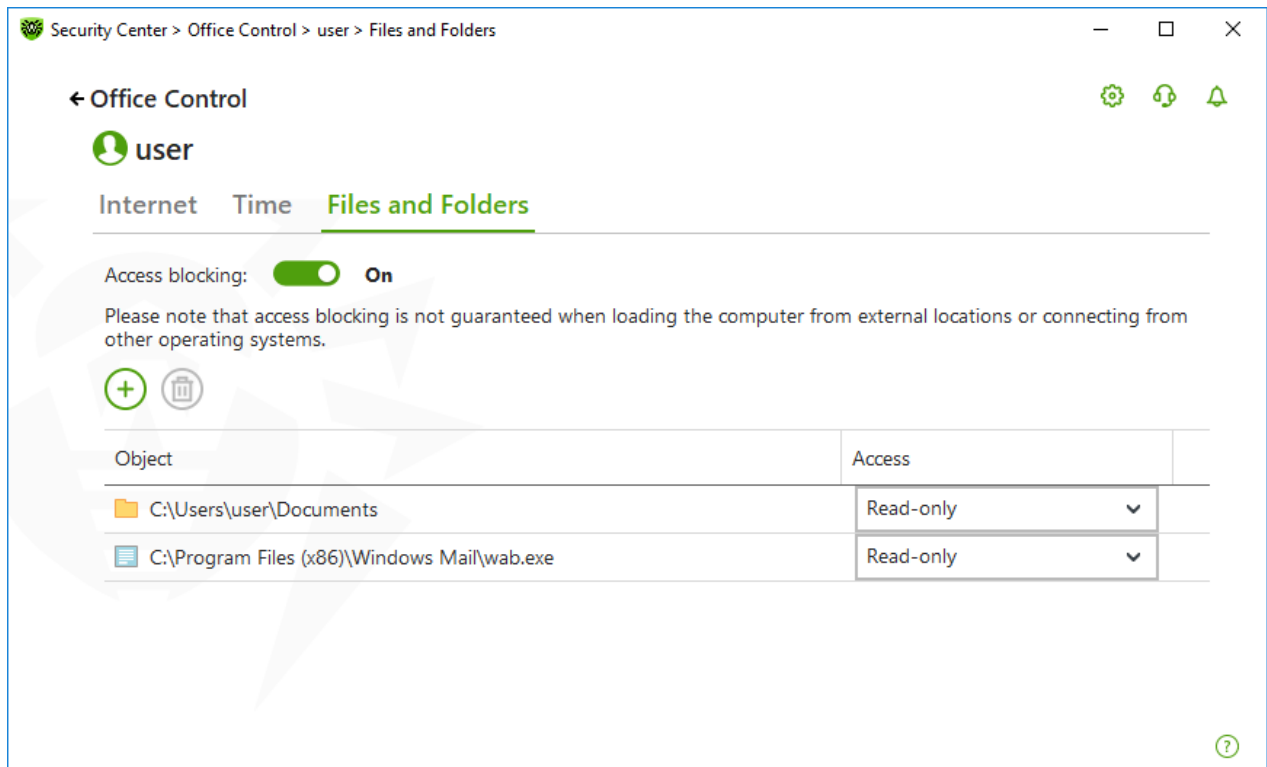
- To create a setting profile, click . The current table settings are saved. If you change the settings, the settings will be saved to the profile automatically.
- To remove a setting profile, click .



## 11.3. Access to Files and Folders

On the **Files and Folders** tab, you can restrict access to files and folders. By default, no restrictions are set.

To enable or disable access restriction to files and folders for a user, use switcher .






**Figure 88. Managing the access to files and folders**



Access restriction is not guaranteed when loading the computer from removable media or addressing the objects from other operating systems installed on your computer.

### To restrict access to files and folders

1. Enable restriction of access to files and folders using the switcher .
2. To add an object to the list, click  and select a file or a folder.
3. Select an access mode for the added object:
  - **Blocked** to block access to the selected object completely.
  - **Read-only** (selected by default) to allow reading of the object (for example, viewing a document or an image, starting an executable file). The object is not allowed to be deleted, removed, and modified.


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



## 12. Quarantine Manager

Quarantine Manager is an instrument that allows you to manage isolated files. The quarantine contains files where the malicious objects were detected. Quarantine also stores backup copies of files processed by Dr.Web. With Quarantine Manager, you can remove, scan again, and restore isolated files.

### To open the Quarantine Manager window

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. Click the **Quarantine Manager** tile.

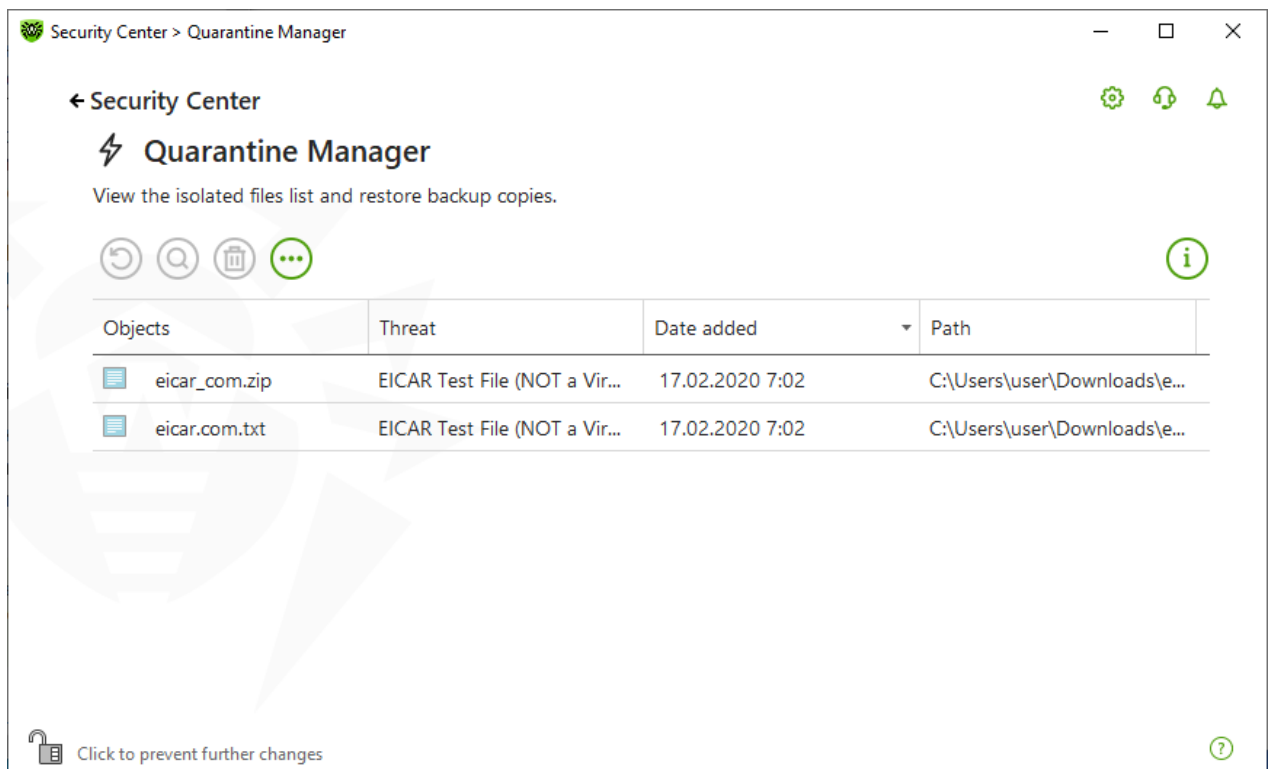


Figure 89. Objects in Quarantine


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:


- The  (**Restore**) button—move one or several objects to the selected folder.



Use this action only if you are sure that the object is safe.

- The  (**Rescan**) button—scan the file in quarantine again.
- The  (**Delete**) button—delete one or several objects both from quarantine and 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** in the drop-down list.

## Advanced


To configure storage and automatic deletion of quarantine records, go to the [Quarantine Manager settings](#).



## 13. Exclusions

In this group, you can configure exclusions from SplDer Guard, SplDer Gate, SplDer Mail and Scanner scans, as well as add sender addresses to black or white lists not to scan the messages for spam.

### To open the Exclusions group of settings

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Exclusions** tile.

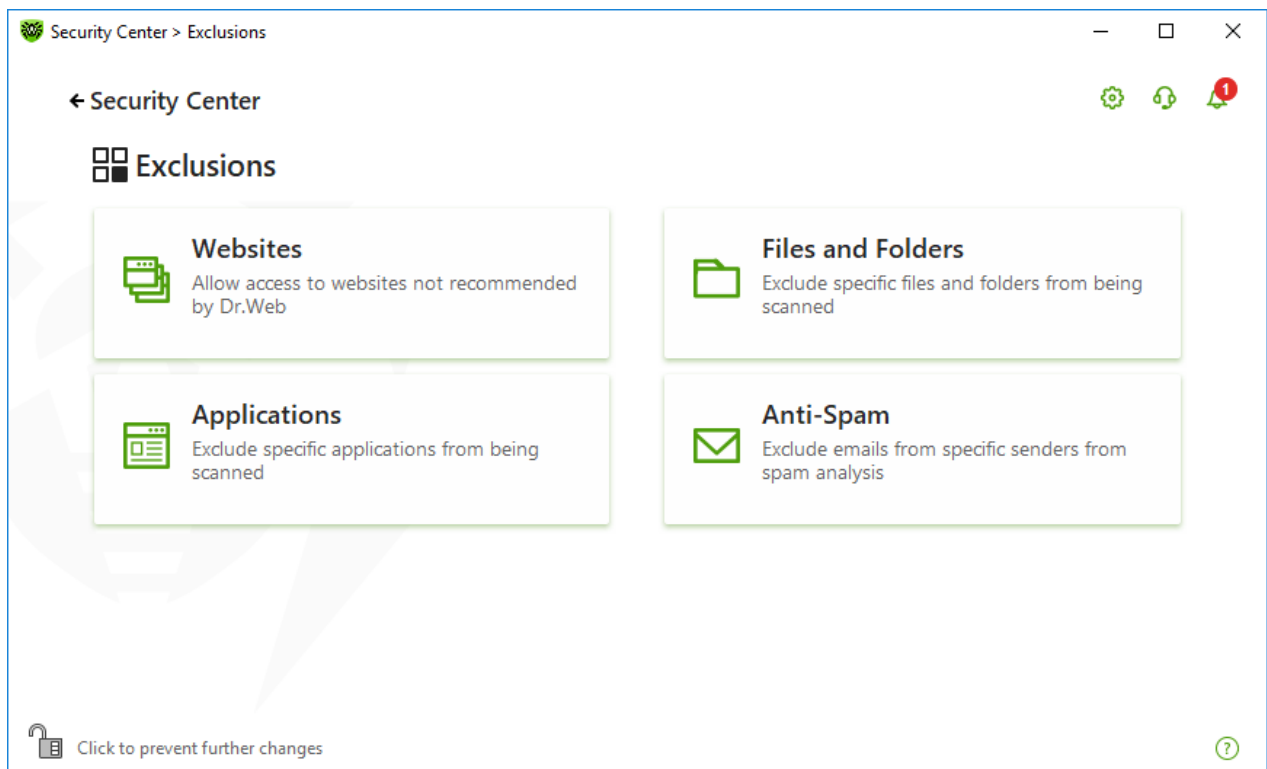




Figure 90. Exclusions

### To open exclusion parameters

1. Make sure Dr.Web operates in [administrator mode](#) (the lock at the bottom of the program window is open ). Otherwise, click the lock .
2. Click the tile of the corresponding section.



Note that the settings could be locked by your anti-virus network administrator.

In this section:

- [Websites](#)—configure access to websites that are not recommended by Doctor Web.




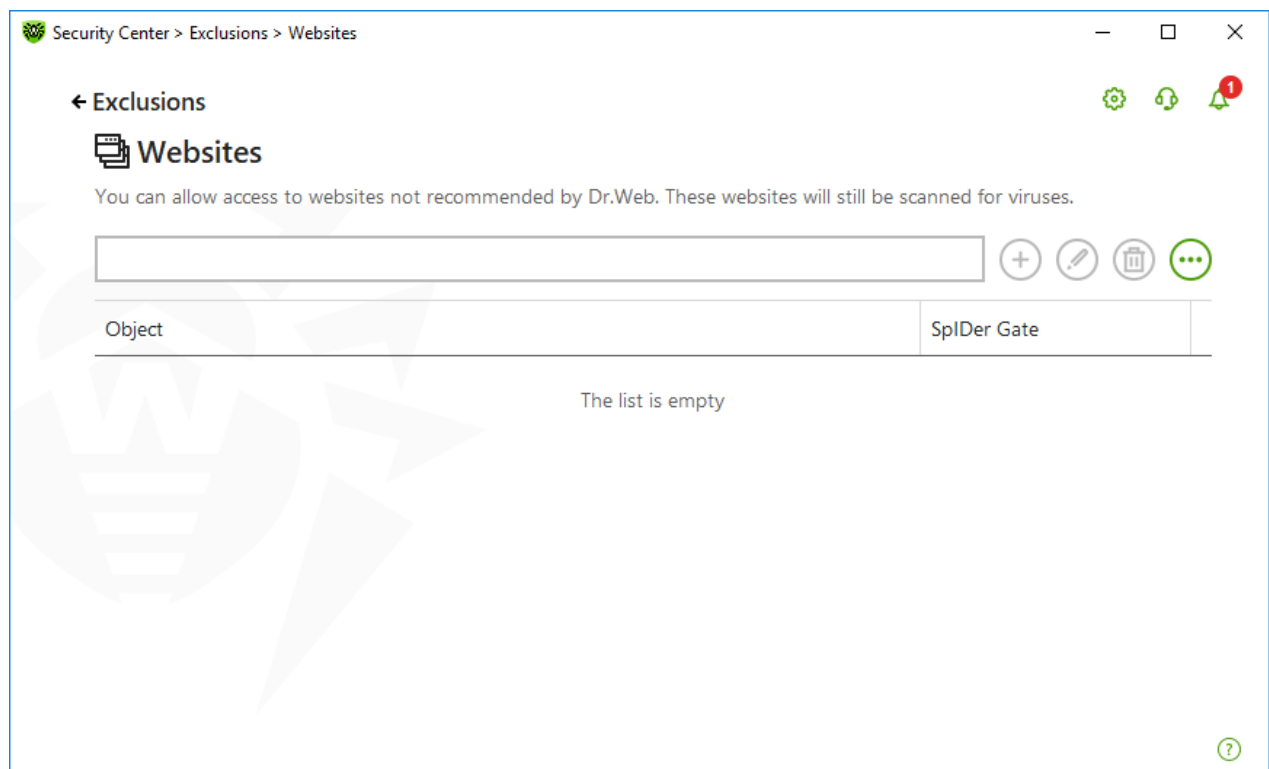
- [Files and Folders](#)—exclude certain files and folders from SplDer Guard and Scanner scans.
- [Applications](#)—exclude specific processes from SplDer Guard, SplDer Gate,, and SplDer Mail scans.
- [Anti-Spam](#)—configure SplDer Mail message scan for spam.

## 13.1. Websites

You can configure list of websites access to which is allowed regardless of the SplDer Gate HTTP traffic scan parameters. If the **Block non-recommended websites** option is enabled in SplDer Gate parameters, you can allow access to specific websites by adding them to the exclusion list. Access to the websites on the list is allowed, however the websites are still scanned for viruses.

### To configure the list of websites access to which is allowed

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Exclusions** tile.
3. Click the **Websites** tile.



**Figure 91. Excluded website list**

By default, the list is empty. If you add a website to the list of exclusions, users will be able to access it regardless of other SplDer Gate parameters. Please note that if this website is added both to the black list of Office Control and to the exclusions, access will be blocked.



## To add domain names to the list

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`). It allows access to all the webpages located on this website.
- To allow access to the 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 dot (.) 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 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 `.com` domain websites, whose names consist of three characters or less.

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

2. Click the  button or press ENTER on the keyboard. The specified address appears on the list.
3. To add other addresses, repeat steps 1 and 2.



## Managing listed objects

The following management elements are available to work with objects in the table:

- The  button—adding an address to the exclusion list. The button becomes available if a text field contains any symbol.
- The  button—editing the selected website address in the exclusion list.






- The  button—removing the selected website address from the exclusion list.
- Click  to access the following options:
  - **Export**—allows you to save the created list of exclusions to be used on another computer where Dr.Web is installed.
  - **Import**—allows you to use the list of exclusions created on another computer.
  - **Clear all**—allows you to remove all objects from the list of exclusions.

You can also remove or edit an object by right-clicking the selected object or several selected objects.

## 13.2. Files and Folders

You can manage the list of files and folders to be excluded from system anti-virus scans by the SpIDer Guard and Scanner components. You can exclude Dr.Web quarantine folders, working folders of some programs, temporary files (paging file), and so on.

### To configure the list of excluded files and folders

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Exclusions** tile.
3. Click the **Files and Folders** tile.

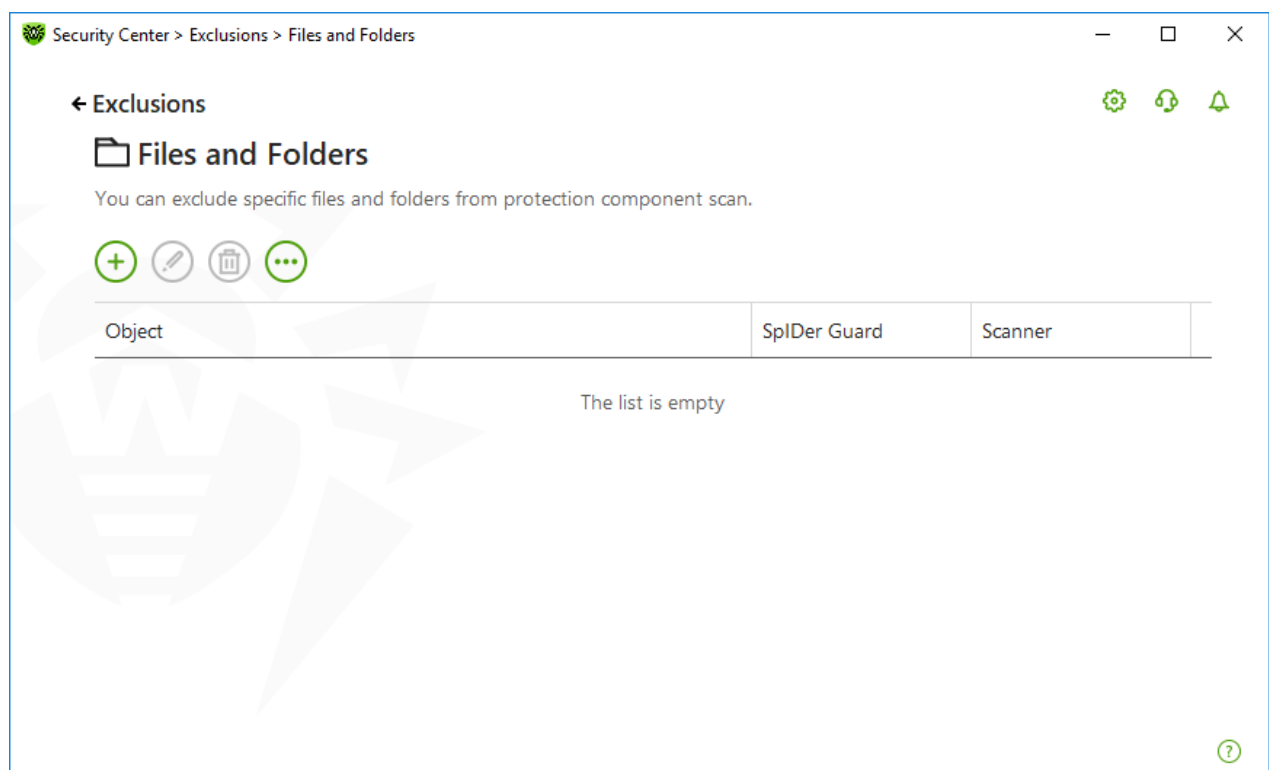



Figure 92. Files and folders exclusion list



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

### To add files and folders to the exclusion list

1. To add a file or folder to the exclusion list, do one of the following:

- To add an existing file or folder, click the  button. In the open window, click the **Browse** button to select a file or a folder. 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 the `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 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 window of adding a file or a folder, specify the components that should not scan the selected object.
  3. Click **OK**. The file or folder will appear on the list.
  4. To add other files and folders, repeat steps 1–3.

## Managing listed objects

The following management elements are available to work with objects in the table:

- The  button—adding an object to the exclusion list.
- The  button—editing the selected object in the exclusion list.
- The  button—removing the selected object from the exclusion list.


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

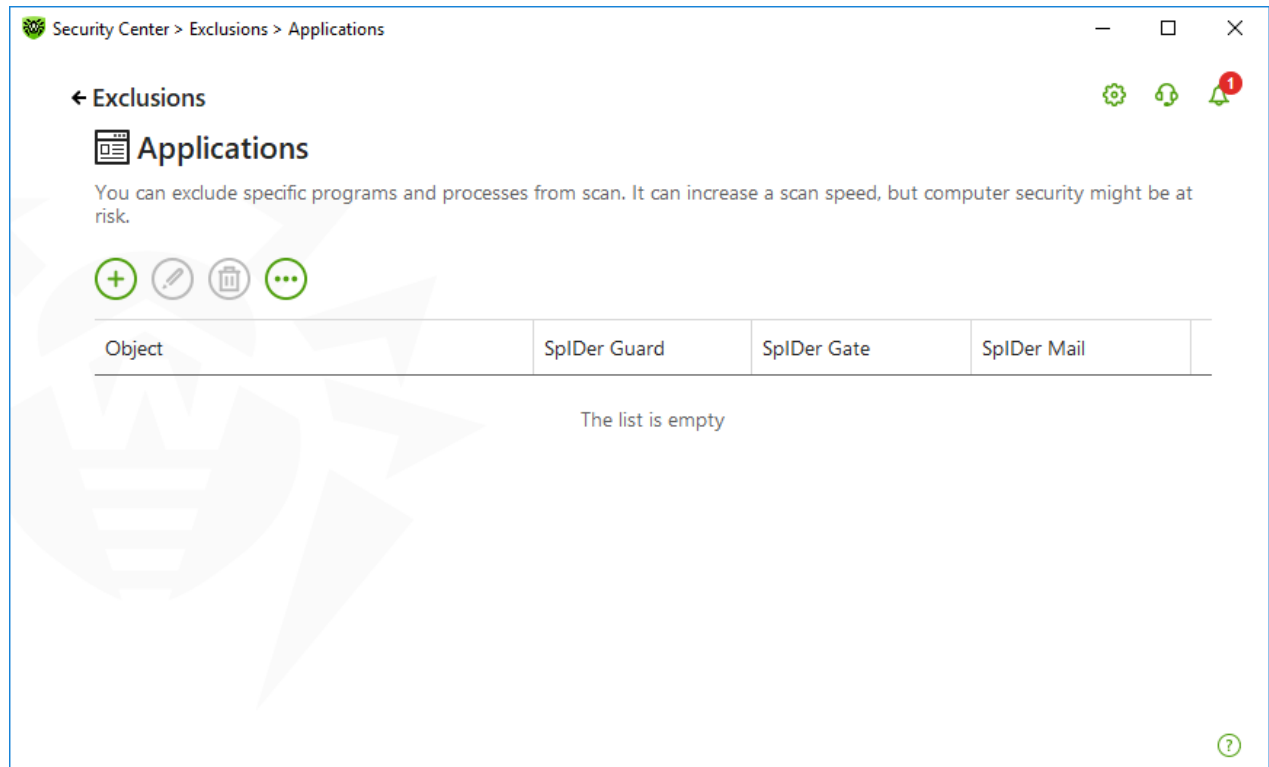
- Click  to access the following options:
  - **Export**—allows you to save the created list of exclusions to be used on another computer where Dr.Web is installed.
  - **Import**—allows you to use the list of exclusions created on another computer.
  - **Clear all**—allows you to remove all objects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

## 13.3. Applications

You can specify a list of programs and processes which activity will be excluded from scanning by the file monitor SpIDer Guard, the internet monitor SpIDer Gate, and the mail anti-virus SpIDer Mail. The objects that are changed as a result of the activity of these applications are excluded.

### To configure the list of excluded applications


1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Exclusions** tile.
3. Click the **Applications** tile.



**Figure 93. Excluded applications list**

The list is empty by default.

### To add applications to the list

1. To add a program or a process to the exclusion list, click . Do one of the following actions:

- In the open window, click the **Browse** button to select an application. You can also enter the full path to the application manually, for example:

`C:\Program Files\folder\example.exe`

- To exclude an application from scan, enter its name in the field. The full path to the application is not required, for example:

`example.exe`

- To exclude applications from scan, enter the defining 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 scan by the name of a variable if the name and a value of this variable are specified in the system variable settings.. For example:

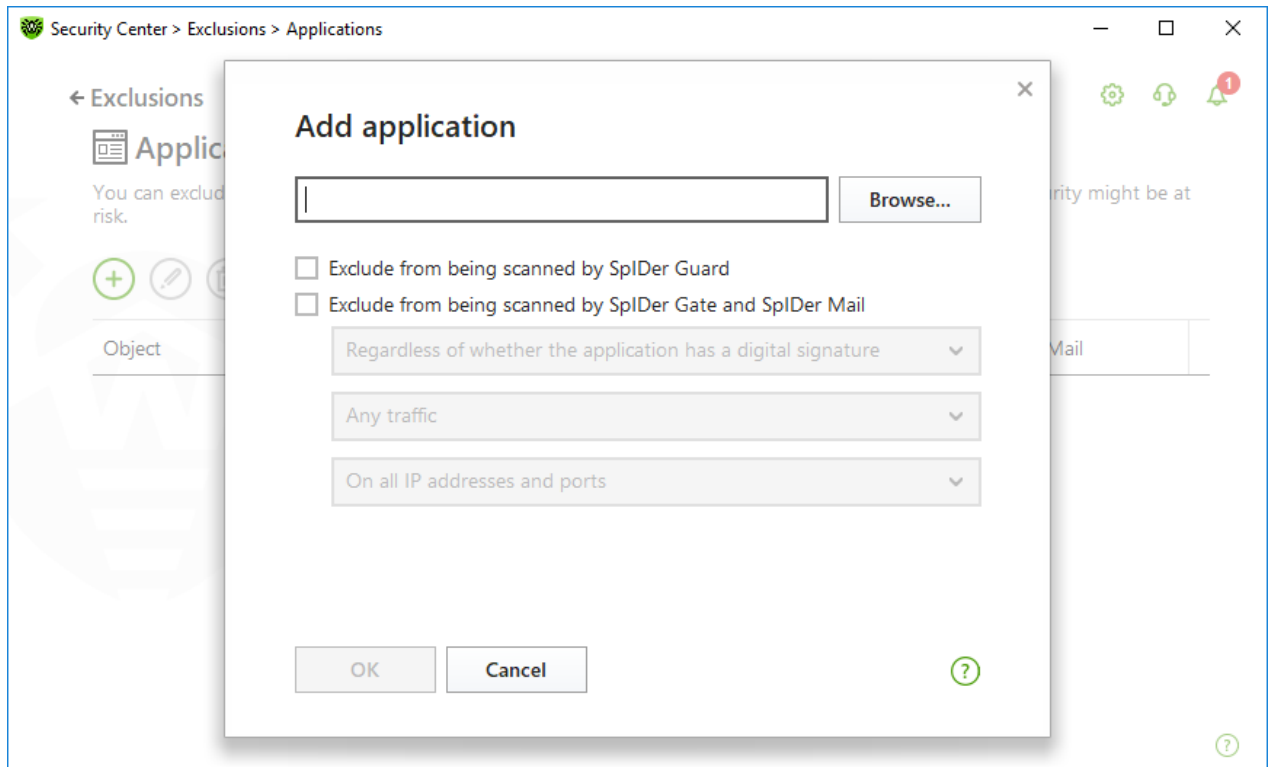
`%EXAMPLE_PATH%\example.exe` – excludes an application by the name of a system variable. A name of a system variable and its value can be specified in the operating system settings.

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 scan the selected application.



**Figure 94. Adding applications to the exclusions**

3. For objects, excluded from scans by the SpliDer Gate and SpliDer Mail components, specify additional conditions.

Parameter	Description
Regardless of whether the application has a digital signature	Select this parameter to exclude the application from scan 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 scan only if it has a valid digital signature. Otherwise, the application will be scanned by the components.
Any traffic	Select this parameter to exclude encrypted and non-encrypted application traffic from scan.
Encrypted traffic	Select this parameter to exclude only encrypted application traffic from scan.
On all IP addresses and ports	Select this parameter to exclude traffic on all IP addresses and ports from scan.
On specific IP addresses and ports	Select this parameter to exclude specific IP addresses and ports from scan. Traffic from other IP addresses and ports will be scanned (unless specified otherwise).






Parameter	Description
To specify addresses and ports	<p>To configure exclusion settings follow the guidance below:</p> <ul style="list-style-type: none"><li>• To exclude a specific domain corresponding to a particular port from scan, enter <code>site.com:80</code>, for example.</li><li>• To exclude scanning of traffic on a custom port (for example, 1111), enter <code>*:1111</code>.</li><li>• To exclude scan of traffic on any port, enter <code>site:*</code>.</li></ul>


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

## Managing listed objects

The following management elements are available to work with objects in the table:

- The  button—adding an object to the exclusion list.
- The  button—editing the selected object in the exclusion list.
- The  button—removing the selected object from the exclusion list.


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

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

## 13.4. Anti-Spam

You can configure lists of senders whose messages will be excluded from spam scan.

### To configure black and white lists

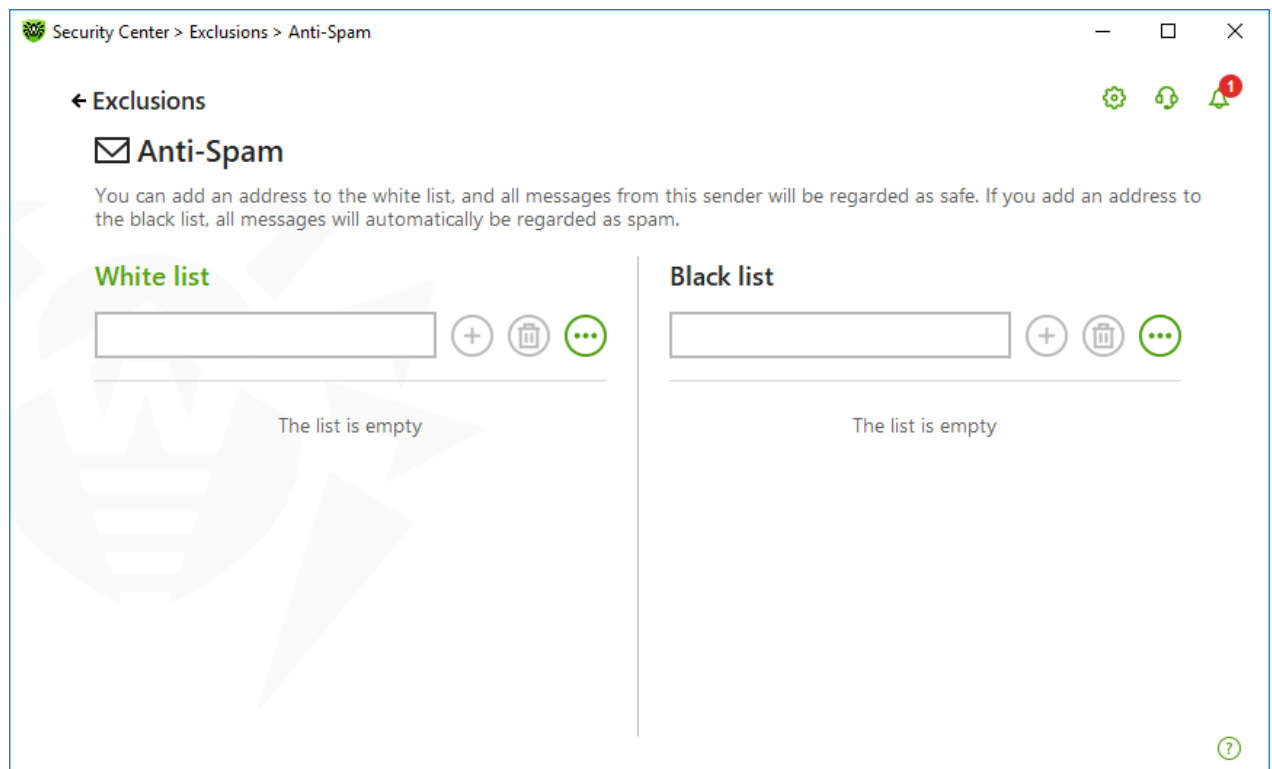
1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Exclusions** tile.
3. Click the **Anti-Spam** tile.

The SpIDer Mail component reaction on messages from senders from black and white lists:

- If you add an address to the white list, messages from this sender are considered to be safe and are not scanned for spam.




- If you add an address to the black list, messages from this sender are automatically considered as spam.



**Figure 95. Black and white lists**

By default, both lists are empty.

### To add email addresses to the exclusions




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`, SplDer 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  or press ENTER on the keyboard.
3. To add other addresses, repeat steps 1 and 2.





## Managing listed objects

The following management elements are available to work with objects in the table:

- The  button—adding an email address to the list. The button becomes available if a text field contains any symbol.
- The  button—removing the selected email address from the list of exclusions.
- Click  to access the following options:
  - **Edit**—allows you to edit the selected email address on the list.
  - **Export**—allows you to save the created list of exclusions to be used on another computer where Dr.Web is installed.
  - **Import**—allows you to use the list of exclusions created on another computer.
  - **Clear all**—allows you to remove all objects from the list of exclusions.


You can also remove or edit an object by right-clicking the selected object or several selected objects.

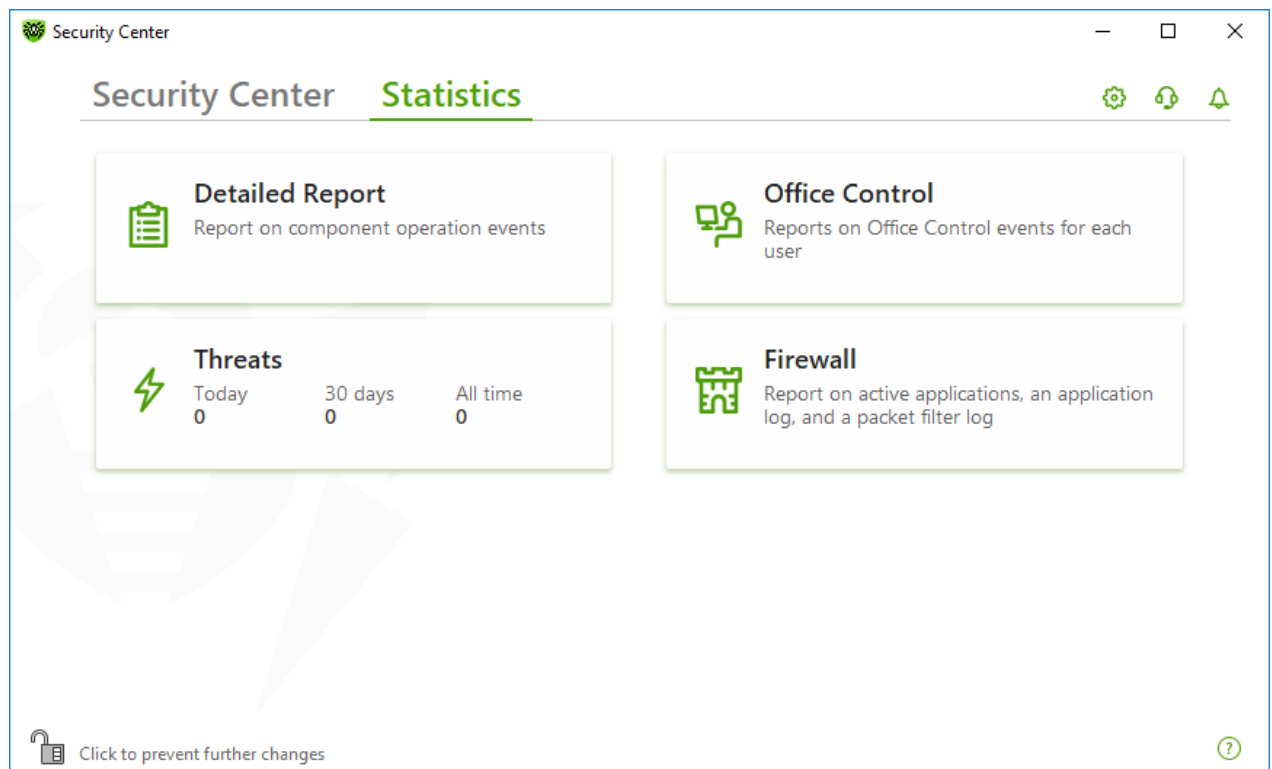


## 14. Statistics on Component Operation

You can review the statistics on operation of the main Dr.Web components.

### To open the statistics on important events of protection component operation

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, select **Statistics** tab.
3. The **Statistics** page opens where reports for the following groups are available:
  - [Detailed Report](#)
  - [Office Control](#)
  - [Threats](#)
  - [Firewall](#)



**Figure 96. Statistics on component operation**

4. Select a group to review the reports.

### Detailed Report

In this window, the detailed information on all the program operation events is collected.



Security Center > Statistics > Detailed Report

← Statistics

Detailed Report

Date	Component	Event
10.09.2019 8:56	Updater	Update completed
10.09.2019 8:18	Updater	Update completed
10.09.2019 7:39	Updater	Update completed
10.09.2019 7:00	Updater	Update completed
10.09.2019 6:22	Updater	Update completed
10.09.2019 5:43	Updater	Update completed
10.09.2019 5:05	Updater	Update completed
10.09.2019 4:27	Updater	Update completed
10.09.2019 3:49	Updater	Update completed

Click to prevent further changes

Figure 97. Detailed report window

The following information is logged in the report:

- **Date**—date and time of an event.
- **Component**—the component or module that caused the event.
- **Event**—a brief description of the event.

By default, all events for all the time are displayed.

The [management elements](#) , ,  are used to work with objects in the table.

You can use [additional filters](#) to select certain events.

## Office Control

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



Date	Blocked resource	Reason for blocking
3/21/2019 3:57 AM	www.facebook.com	Social networks
3/21/2019 3:57 AM	www.facebook.com	Social networks
3/21/2019 3:57 AM	www.facebook.com	Social networks
3/21/2019 3:57 AM	www.facebook.com	Social networks
3/21/2019 3:57 AM	vk.com	Adult content
3/21/2019 3:57 AM	vk.com	Adult content

**Figure 98. The Office control statistics window**

The following information is logged in the report:

- **Date**—date and time of blocking.
- **Blocked resource**—the link to the blocked resource.
- **Reason for blocking**—the category or exclusion list that the blocked resource belongs to.

By default, all events for all the time are displayed.

The [management elements](#) , ,  are used to work with objects in the table.

You can use [additional filters](#) to select certain events.



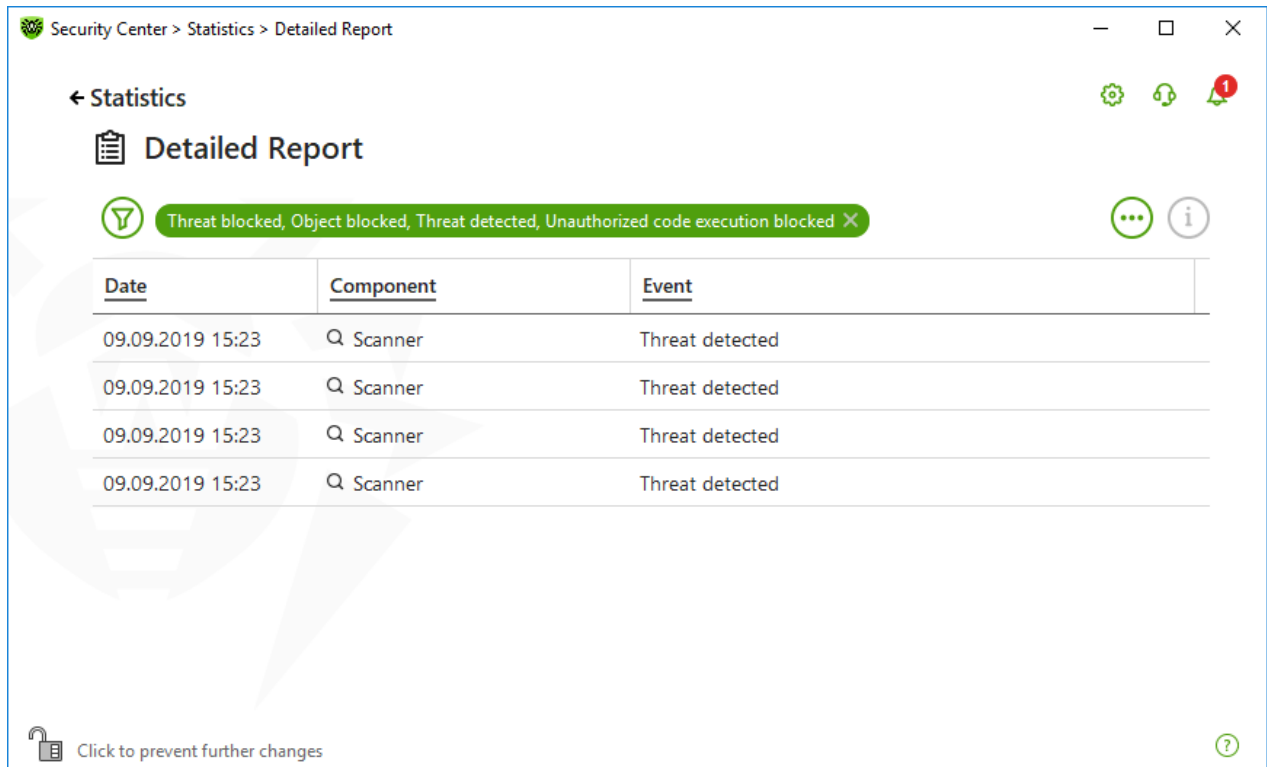
The statistics also includes the information on external resources integrated with other webpages, such as embedded widgets. Having such resources in the statistics does not mean that the user has tried to visit these websites intentionally.

## Threats

On the **Threats** tile on the main statistics window, the information on the total number of threats for a certain period of time is shown.



When choosing this option, the **Detailed Report** window with predefined filters for all the threats will open.



**Figure 99. Statistics on threats window**

The following information is logged in the report:

- **Date**—date and time of the threat detection.
- **Component**—the component that has detected the threat.
- **Event**—a brief description of the event.

By default, all events for all the time are displayed.

The [management elements](#) , ,  are used to work with objects in the table.

You can use [additional filters](#) to select certain events.

## 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.



Security Center > Statistics > Firewall > Active applications

← Statistics

Firewall

Active applications

Name	Direction	Protocol	Local address	Remote address	Sent	Received
wininit.exe...	2 connections					
SYSTEM:4	5 connections					
svchost.e...	2 connections					
	Listening	TCPv6	:::135	:::0	0 bytes	0 bytes
	Listening	TCPv4	0.0.0.0:135	0.0.0.0:0	0 bytes	0 bytes
svchost.e...	2 connections					
svchost.e...	8 connections					
svchost.e...	2 connections					

Click to prevent further changes

**Figure 100. Statistics on network activity window**

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

You can block one of the current connections or allow previously blocked connection. For this, select a required connection and right-click. Only one option is available, depending on the connection status.

The application log shows the following information:

- Application start time
- Application name
- Application processing rule name
- Direction
- Action
- Endpoint

To enable the application logging, go to **Firewall** page and then open Add or Edit application rule window. For the detailed information, refer to the [Application rule settings](#) section.




Packet Filter Log shows the following information:

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

To enable packet filter logging, go to **Firewall** page and then open Add or Edit packet filter rule window. For the detailed information, refer to the [Rule sets for filtering packets](#).




When clicking at one of the columns, the events are arranged in ascending or descending order.

## 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 by clicking . You can also create custom event filters.



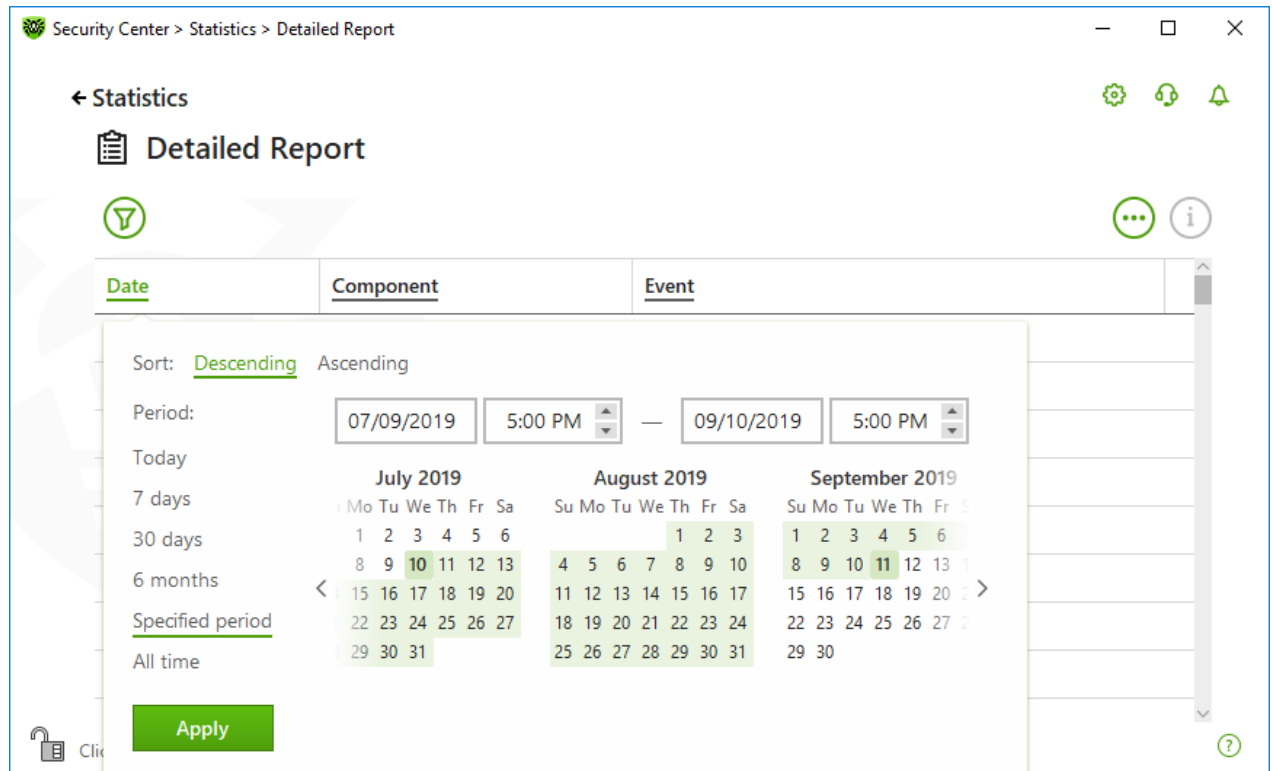
The buttons to manage table elements:

- Click  to access the following options:
  - To select the predefined filter for the set period of time or the filter for the update event.
  - To save the current custom filter. It is also possible to delete previously saved custom filter.
  - To delete all the current filters.
- Click  to access the following options:
  - **Copy selected**—allows you to copy the selected entry (entries) to the clipboard.
  - **Export selected**—allows you to export the selected entry (entries) to the specified folder in .csv format.
  - **Export all**—allows you to export all the entries of the table to the specified folder in .csv format.
  - **Delete selected**—allows you to delete the selected event(s).
  - **Delete all**—allows you to delete all the events from the table.
- Clicking the  button, the detailed information about the event is displayed. Available when one of the entries is selected. Clicking this button again will hide the detailed information on the event.

### To set custom filter

1. To filter by a specific parameter, click on the heading of the required column:
  - Filter by date. You can select one of the predefined periods specified in the left part of the window, or specify your own. To set the required period, select the start date and the end date of the period in the calendar, or specify the dates in the **Period** field. Filtering by date is also available in ascending or descending order.






**Figure 101. Data sorting**

- Filter by component. You can check the components the information on which will be included in the report, or arrange the entries by ascending or descending order.
- Filter by event. You can check the events to be shown in the report, or arrange the entries by ascending or descending order.

For Office control statistics, in addition to the date filter, the following options are available:

- Filter by blocked resource. You can sort entries in ascending or descending order only.
  - Filter by reason for blocking. You can check the reasons for blocking to be shown in the report, or arrange the entries by ascending or descending order.
2. Once the filter parameters selected, click **Apply**. Selected items will be displayed above the table.
  3. To save the filter, click  and select **Save filter**.
  4. In the open window, enter a name for the new filter. Click **Save**.

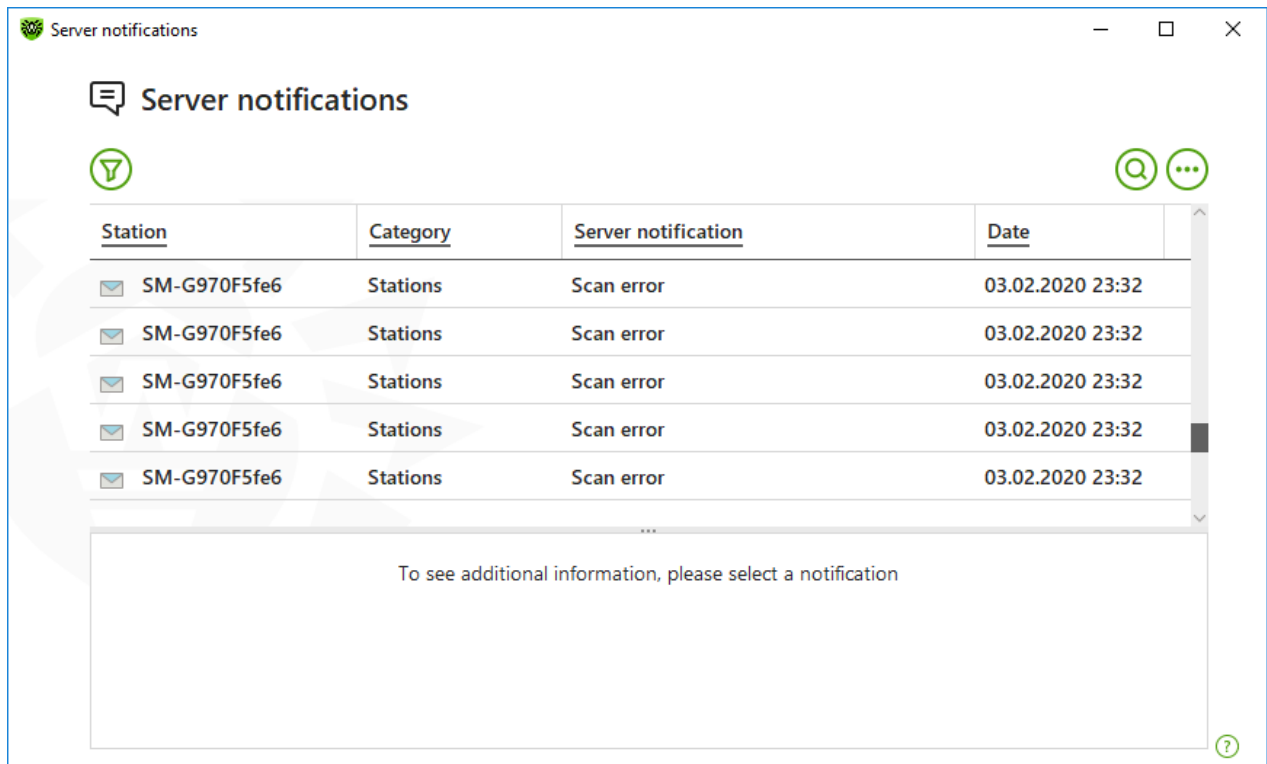


## 15. Server Notifications

The network administrator may enable server notifications on any station. This feature can be necessary for the administrator while working at one of the stations.

### To open Server Notifications window


1. Open Dr.Web [menu](#) .
2. Select **Server Notifications**.




**Figure 102. Server Notifications window**

All the notifications received are shown in the upper side of the window. To see the information on the notification, click it.



### Filters

To view a list of only those notifications that correspond to specific parameters, use filters. By clicking  only default filter is available. Its settings are the same as set on the server. You can also create custom notification filters.

The buttons to manage table elements:

- Click  to access the following options:
  - To select the default filter.



- To save the current custom filter. It is also possible to delete previously saved custom filter.
- To delete all the current filters.
- Click  to access the following options:
  - **Copy selected**—allows you to copy the selected entry (entries) to the clipboard.
  - **Export selected**—allows you to export the selected entry (entries) to the specified folder in .csv format.
  - **Export all**—allows you to export all the entries of the table to the specified folder in .csv format.
  - **Delete selected**—allows you to delete the selected notification(s).
  - **Mark as read**—allows you to mark all the notifications as read.
  - **Delete all**—allows you to delete all the notifications from the table.
- Click  to search through all the notifications.


### To set custom filter

1. To filter by a specific parameter, click on the heading of the required column:
  - Filter by station. You can sort entries in ascending or descending order only.
  - Filter by category. You can check the categories the information on which will be included in the report, or arrange the entries by ascending or descending order. You can filter notifications by the following categories:
    - Administrators
    - Stations
    - Licenses
    - Newbies
    - Repository
    - Installations
    - Other
  - Filter by server notification. You can sort entries in ascending or descending order only.
  - Filter by date. You can select one of the predefined periods specified in the left part of the window, or specify your own. To set the required period, select the start date and the end date of the period in the calendar, or specify the dates in the **Period** field. Filtering by date is also available in ascending or descending order.



The screenshot shows a window titled 'Server notifications'. Inside, there's a table with columns: Station, Category, Server notification, and Date. The 'Station' column lists multiple 'ubuntu16' entries. A filter dialog box is open, showing options for sorting (Descending, Ascending), period (Today, 7 days, 30 days, 6 months, Specified period, All time), and a date range (02/12/2019 to 04/09/2019). The dialog also displays a calendar view for February, March, and April 2019. An 'Apply' button is visible at the bottom of the dialog.

**Figure 103. Data sorting**

2. Once the filter parameters selected, click **Apply**. Selected items will be displayed above the table.
3. To save the filter, click  and select **Save filter**.
4. In the open window, enter a name for the new filter. Click **Save**.



## 16. 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/](https://support.drweb.com/show_faq/).
- Browse the Dr.Web official forum at <https://forum.drweb.com/index.php>.

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.

### 16.1. Assistance in Resolving Problems

When contacting your anti-virus network administrator, you may need to generate a report on your operating system and Dr.Web operation.

#### To generate a report using the Report Wizard

1. Open Dr.Web [menu](#) , then select **Security Center**.
2. In the open window, click **Go to Report Wizard**.

You can also access this window by clicking the  button in the upper right side of the **Security Center** window.

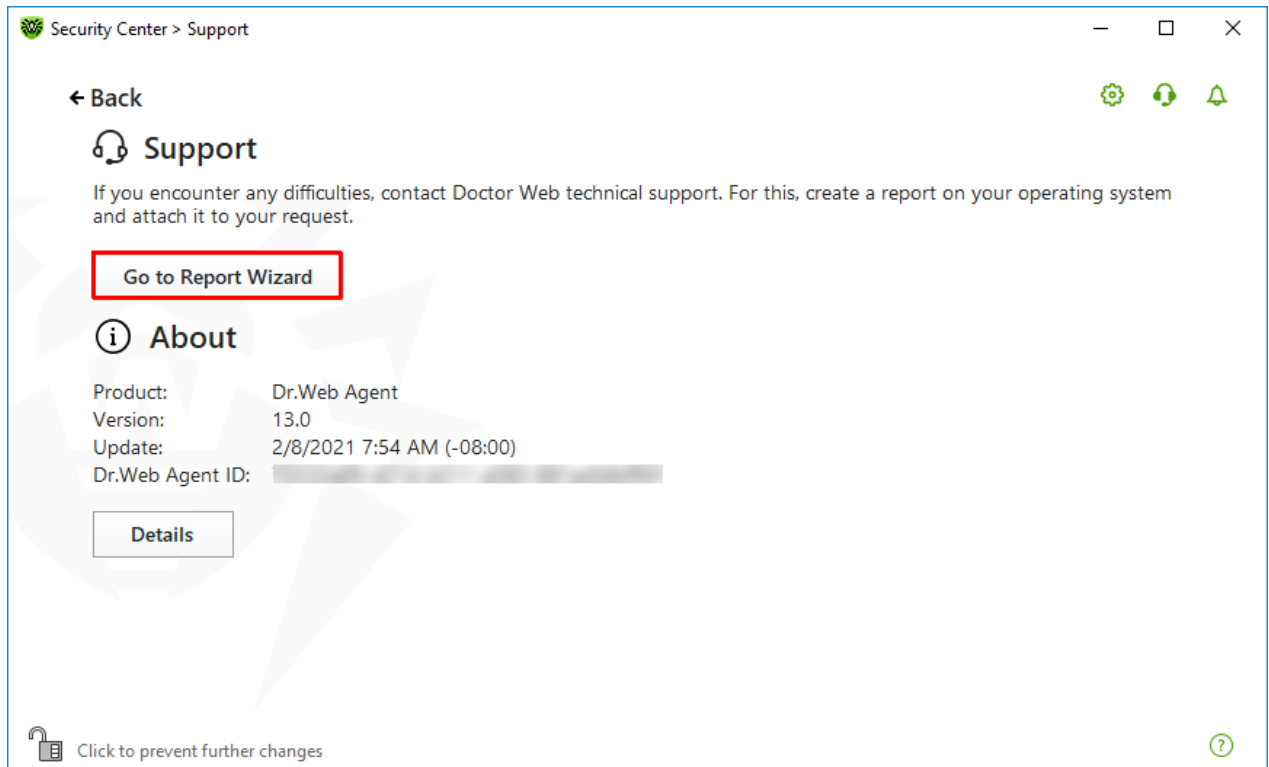


Figure 104. Support

3. In the open window, click **Create report**.

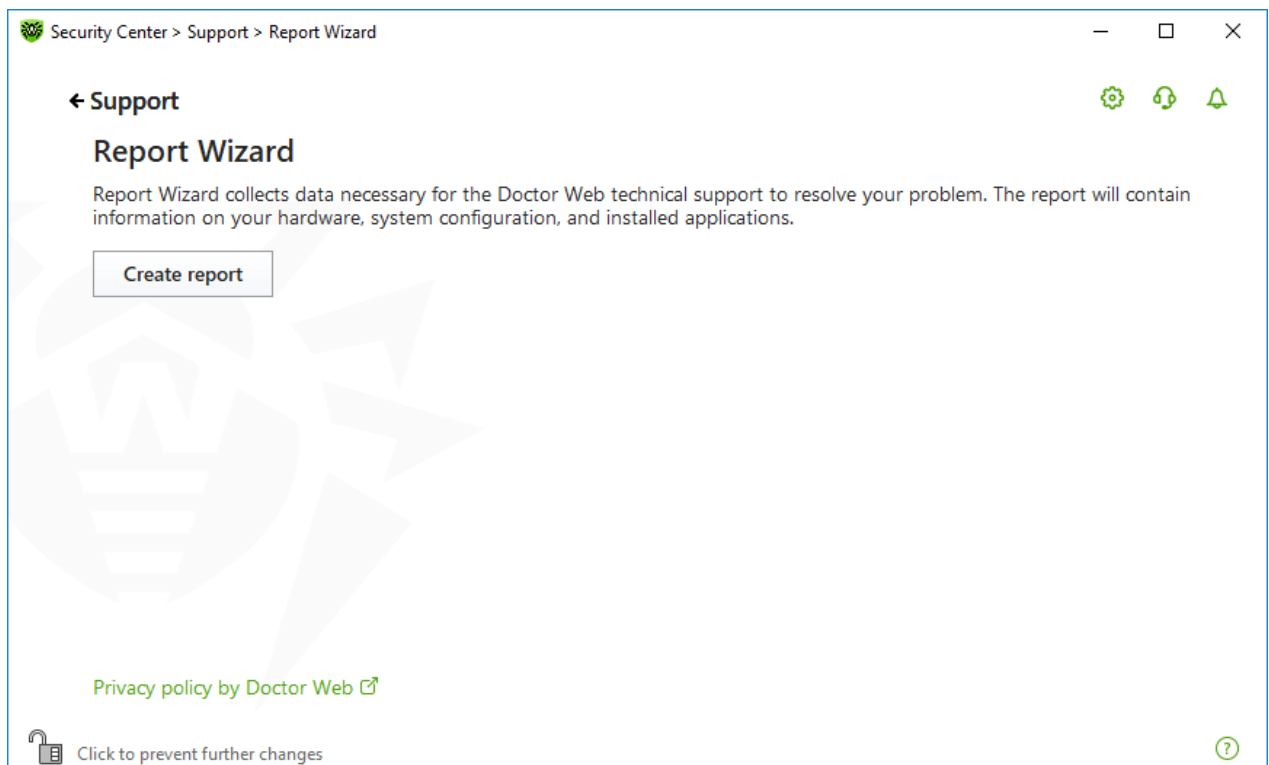


Figure 105. Generating a report for technical support

4. Generating a report starts.



## Report generation from command line

To generate a report, use the following command:

```
/auto For example: dwsysinfo.exe /auto
```

You can also use the command:

```
/auto /report:[<full path to the archive>]. For example:  
dwsysinfo.exe /auto /report:C:\report.zip
```

The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% folder. You can access the archive by clicking the **Open folder** button after the archive has been created.

## The information included in the report

The report will include the following information:

1. Technical information about the operating system:
  - General information about your computer
  - Information on running processes
  - Information on scheduled tasks
  - Information on services, drivers
  - Information on default browser
  - Information on installed applications
  - Information on policies
  - Information on HOSTS file
  - Information on DNS servers
  - System event log
  - System directories
  - Registry branches
  - Winsock providers
  - Network connections
  - Dr. Watson logs
  - Performance index
2. Information on installed Dr.Web product:
  - Type and version of Dr.Web product
  - Information on installed components and Dr.Web modules
  - Information on settings and configuration parameters of Dr.Web product



- License information
- Dr.Web Operation Logging

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

## 16.2. About


The **About** section provides information on:

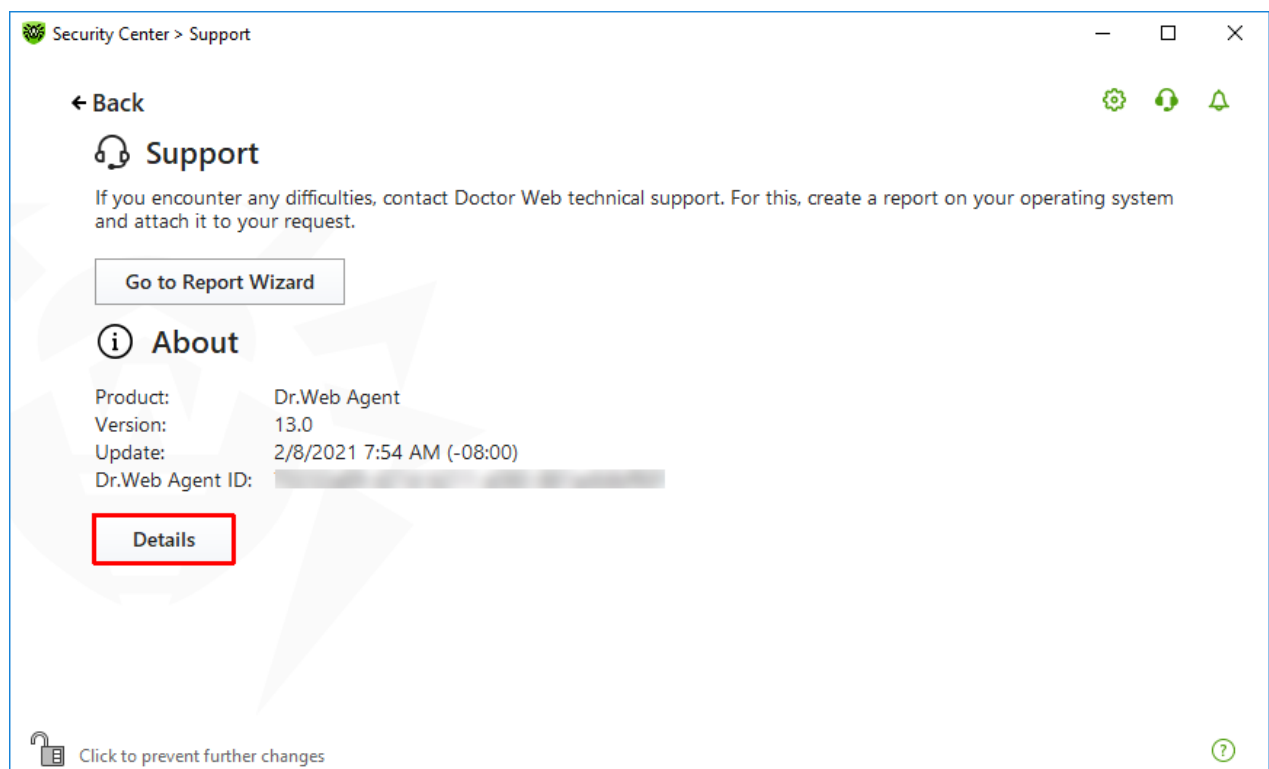
- Product version
- Date and time of the last update
- Dr.Web Agent ID

The **About Dr.Web** window provides you with the information on the version of installed components and update date of virus databases.

### To access this window

1. Open Dr.Web menu Dr.Web icon, then select **Support**.
2. In the open window, click **Details**.

You can also access this window by clicking the  button in the upper right side of the **Security Center** window.



**Figure 106. Access to the About Dr.Web window**





## 17. 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 and Console Scanner. 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.

### 17.1. 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.)
/DCT	Do not display estimated scan time. (For Console Scanner only.)
/DR	Scan folders recursively (scan subfolders). Option is enabled by default.



Switch	Description
/E: <number_of_threads>	Perform scanning in specified number of threads.
/FAST	Perform an <a href="#">express scan</a> 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: <regex>	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.
/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.



Switch	Description
/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:  O—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.
/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 completed 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 (when running Scanner in the command-line mode).
/REP	Follow symbolic links while scanning. Option is disabled by default.



Switch	Description
/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 (when running Scanner in the command-line mode).
/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.
/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.)



Switch	Description
/X:S[:R]	Set one of the following states for the computer to enter once scanning is completed: 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)
/AES:<action>	action for exploitable software (possible: IR)
/AHT:<action>	action for hacktools (possible: DQIR)
/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 is enabled or disabled by default or has been 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`.

## 17.2. Installation Packages Parameters

`/compression <mode>`—compression mode of the traffic with the central protection server. The `<mode>` parameter may take one of the following values:

- `yes`—use compression.
- `no`—do not use compression.
- `possible`—compression is possible. The final decision depends on the settings on the Server side.

If the switch is not set, the `possible` value is used by default.

`/encryption <mode>`—encryption mode of the traffic with the central protection server. The `<mode>` parameter may take one of the following values:

- `yes`—use encryption.
- `no`—do not use encryption.
- `possible`—encryption is possible. The final decision depends on the settings on the Server side.

If the switch is not set, the `possible` value is used by default.

`/excludeFeatures <components>`—the list of components that will be excluded from installation. To specify several components, use the `'` sign as a divider. Available components are as follows:

- `scanner`—Dr.Web Scanner,
- `spider-mail`—SpIDer Mail,
- `spider-g3`—SpIDer Guard,
- `outlook-plugin`—Dr.Web for Microsoft Outlook,
- `firewall`—Dr.Web Firewall,
- `spider-gate`—SpIDer Gate,



- `parental-control`—Office Control,
- `antispam-outlook`—Dr.Web Anti-spam for the Dr.Web for Microsoft Outlook component,
- `antispam-spidermail`—Dr.Web Anti-spam for the SpIDer Mail component.

Components that are not specified directly will have their default installation status.

`/id <station_id>`—identifier of a station on which Dr.Web Agent will be installed.

The parameter is set with the `/pwd` switch for manual authorization on the Server. If authorization parameters are not set, the final authorization decision depends on the settings on the Server side.

`/includeFeatures <components>`—the list of components that must be installed. To specify several components, use the `'` sign as a divider. Available components are as follows:

- `scanner`—Dr.Web Scanner,
- `spider-mail`—SpIDer Mail,
- `spider-g3`—SpIDer Guard,
- `outlook-plugin`—Dr.Web for Microsoft Outlook,
- `firewall`—Dr.Web Firewall,
- `spider-gate`—SpIDer Gate,
- `parental-control`—Office Control,
- `antispam-outlook`—Dr.Web Anti-spam for the Dr.Web for Microsoft Outlook component,
- `antispam-spidermail`—Dr.Web Anti-spam for the SpIDer Mail component.

Components that are not specified directly will have their default installation status.

`/installdir <folder>`—installation folder.

If the switch is not set, default installation folder is the `Program Files\DrWeb` folder on the system drive.

`/instMode <mode>`—installer launch mode. The `<mode>` parameter may take the following value:

- `remove`—remove the installed product.

If the switch is not set, by default, installer automatically defines the launch mode.

`/lang <language_code>`—the language of the installer and installed product. The language code is specified in the ISO-639-1 format.

If the switch is not set, the system language is used by default.

`/pubkey <path>`—full path to the Server certificate or public key file.



If the certificate or the public key is not specified, after the launch of the local installation, installer automatically uses the certificate (with `.pem` extension) or public key (`drwcsd.pub`) from its own launch folder. If the certificate or the public key file is located in the folder other than the installer launch folder, you must manually specify the full path to the certificate or the public key file.

If you launch the installation package generated in Control Center, the certificate or the public key is included into the installation package and additional specifying of the public key file in the command-line switches is not required.

`/pwd <password>`—the Dr.Web Agent password to access the Server.

The parameter is set with the `/id` switch for manual authorization on the Server. If authorization parameters are not set, the final authorization decision depends on the settings on the Server side.

`/regagent <mode>`—defines whether Dr.Web Agent will be registered in the list of installed programs. The `<mode>` parameter may take one of the following values:

- `yes`—register Dr.Web Agent in the list of installed programs.
- `no`—do not register Dr.Web Agent in the list of installed programs.

If the switch is not set, the `no` value is used by default.

`/retry <number>`—number of attempts to locate the Server by sending multicast requests. If the Server does not respond after the specified number of attempts has been reached, it is assumed that the Server has not been found.

If the switch is not set, 3 attempts to find the Server are performed.

`/server "[<protocol>/]<server_address>[:<port>]"`—the Server address from which Dr.Web Agent will be installed and to which Dr.Web Agent connects after the installation.

If the switch is not set, by default, the Server is searched by sending multicast requests.

`/silent <mode>`—defines whether the installer will be run in the background mode. The `<mode>` parameter may take one of the following values:

- `yes`—launch the installer in the background mode.
- `no`—launch the installer in the graphical mode.

If the switch is not set, Dr.Web Agent installation is performed in the graphical mode by default.

`/timeout <time>`—waiting time limit of each reply when searching for the Server. Defined in seconds. Receiving of response messages continues while the response time is less than the timeout value.

If the switch is not set, 3 seconds are used by default.





## 17.3. 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.
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.



## 18. 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.

### 18.1. Types 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 also become threats under certain circumstances.

#### 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.
- *Macro viruses* infect documents used by Microsoft Office (or other programs supporting macro commands written for example, 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.
- *Stealth viruses* (invisible viruses) perform certain actions to disguise their activity and to conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these “dummy” characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the language they are written in (most viruses are written in Assembly but there are also viruses written in 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 programs can replicate themselves however they do not infect other objects. A worm infiltrates a computer from a network (usually, as an email attachment or from the internet) 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).
- *Chat worms* use protocols of popular instant messengers and chat programs (ICQ, IM, IRC, etc.).

## Trojan programs (Trojans)

These programs cannot replicate themselves. Trojans substitute a frequently-used program and perform its functions (or imitate its operation). Meanwhile, they perform some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or make it possible for hackers to access the computer without permission, for example, to harm the computer of 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.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are attributed to Trojans only. Here are some Trojan types which Doctor Web distinguishes as separate classes:

- *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.
- *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).
- *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 DDoS attacks.
- *Proxy Trojans* provide cybercriminals with anonymous internet access via the victim's computer.



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).

## 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 are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

## Riskware

These 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. Please move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.

## 18.2. Actions Applied to Threats

There are many methods of neutralizing computer threats. Products of Doctor Web company 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.
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. We recommend that you 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**—this action can also be used for neutralizing malicious programs. In this case, the copies of such programs are kept in the file system. All access attempts to or from the file are blocked.



## 19. 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/7/8/8.1/10 programs
- **Win32**—32-bit Windows 95/98/Me and NT/2000/XP/Vista/7/8/8.1/10 programs
- **Win64**—64-bit Windows XP/Vista/7/8/8.1/10/11 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.



## 20. Appendix D. Main Terms and Concepts

### A

*Administrative mode* is a Dr.Web mode in which the user has an access to all the security components parameters and to the program settings. To switch to the administrative mode, click the lock .

*Anti-virus Network* is a complex of computers with Dr.Web product installed (Dr.Web Anti-virus for Windows, Dr.Web Anti-virus for Windows Servers, or Dr.Web Security Space) that are connected to one local network.

### B

*Bus* is a communication subsystem for transferring data between functional units of the computer (for example, the USB).

### D

*Device classes* are the devices that perform the same functions (e.g., printing devices).

*Digital signature* is an attribute of a digital document that is meant to protect the document from forgery. It is generated by cryptographic transformation of information with a use of a private key of digital signature and allows to identify the owner of the certificate private key and to verify that the transmitted digital document was not altered.

### E

*Emulation* is an imitation of a system operation by means of another system without the loss in functionality and distortion of results throughout the use of special computer programs.

*Exploit* is a program, code fragment or a sequence of commands that use software vulnerabilities to attack the system.

### H

*Hash value* is a unique file identifier i.e. sequence of numbers and letters of a given length. Hash is used to verify data integrity.

*Heuristic* is an assumption, the statistical significance of which is confirmed experimentally.



## M

*Modification of a 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.

## S

*Signature (virus entry)* is a finite continuous sequence of bytes that is necessary and sufficient to identify a specific virus.

## T

*Trusted applications* are those applications whose digital signatures have been added to the list of trusted signatures in drwbase.db. the list of trusted applications includes the popular software such as Google Chrome, Firefox, Microsoft applications and so on.

## U

*Update mirror* is a folder to which the update files are copied. The update mirror can be used as a Dr.Web update source for other computers of the local network that are not connected to the Internet.

