Dr.WEB

Anti-virus for Windows Servers

Administrator Manual

© Doctor Web, 2024. All rights reserved

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

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

Trademarks

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

Disclaimer

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

Dr.Web Anti-virus for Windows Servers
Version 12.0
Administrator Manual
6/7/2024

Doctor Web Head Office

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

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

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

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

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

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

Table of Contents

1. Introduction 7
   1.1. Document Conventions and Abbreviations 7
2. About the Product 9
   2.1. Protection Components and Management Modules 9
   2.2. Detection Methods 10
   2.3. System Requirements 16
   2.4. Testing the Anti-Virus 17
3. Installing, Removing, or Changing Dr.Web 19
   3.1. Installing the Product 19
   3.2. Configuring Components 24
   3.3. Removing and Reinstalling the Product 25
4. Licensing 27
   4.1. License Activation 29
      4.1.1. Activation Using Serial Number 30
      4.1.2. Activation Using Key File 31
   4.2. Renewing License 34
   4.3. Key File 35
5. Program Menu 36
6. Security Center 38
7. Updating of Virus Databases and Program Components 40
8. Notification Feed 45
9. Program Settings 47
   9.1. General Settings 47
      9.1.1. Program Settings Password Protection 48
      9.1.2. Selecting Interface Color Theme 49
      9.1.3. Selecting Program Language 51
      9.1.4. Managing Dr.Web Settings 52
      9.1.5. Dr.Web Operation Logging 52
      9.1.6. Quarantine Settings 55
      9.1.7. Automatic Deletion of Statistics Records 56
   9.2. Notification Settings 57
   9.3. Update Settings 61
   9.4. Network 65

9.5. Self-Protection 66
9.6. Dr.Web Cloud 68
9.7. Remote Access to Dr.Web 69
9.8. File Scan Options 70
10. Files and Network 74
10.1. Real-Time File System Protection 75
10.2. Computer Scan 81
10.2.1. Scan Start and Scan Modes 81
10.2.2. Neutralizing Detected Threats 83
10.2.3. Additional Options 85
11. Preventive Protection 88
11.1. Ransomware Protection 89
11.2. Behavior Analysis 93
11.3. Exploit Prevention 101
12. Devices and Personal Data 104
12.1. Data Loss Prevention 105
12.2. Device Blocking 112
12.2.1. Bus and Device Class Blocking 115
12.2.2. Allowed Devices 120
13. Tools 124
13.1. Quarantine Manager 124
13.2. Anti-Virus Network 126
13.3. License Manager 128
14. Exclusions 131
14.1. Files and Folders 132
14.2. Applications 134
15. Statistics on Component Operation 138
16. Technical Support 143
16.1. Assistance in Resolving Problems 143
16.2. About 146
17. Appendix A. Additional Command-Line Parameters 147
17.1. Scanner and Console Scanner Parameters 147
17.2. Dr.Web Updater Command-Line Parameters 153
17.3. Return Codes 156
18. Appendix B. Computer Threats and Neutralization Methods 157

18.1. Types of Computer Threats 157
18.2. Actions Applied to Threats 161
19. Appendix C. Naming of Viruses 162
20. Appendix D. Main Terms and Concepts 166

1. Introduction

This manual describes how to install the Dr.Web Anti-virus for Windows Servers 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 Anti-virus for Windows Servers components (with default settings).

The Appendices contain some general information and additional parameters for Dr.Web Anti-virus for Windows Servers setting-up.

1.1. Document Conventions and Abbreviations

Conventions

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

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

Abbreviations

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

- Dr.Web—Dr.Web Anti-virus for Windows Servers
- 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
- UNC—Uniform Naming Convention
- URL—Uniform Resource Locator

2. About the Product

Dr.Web Anti-virus for Windows Servers 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 Anti-virus for Windows Servers 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. 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 Anti-virus for Windows Servers 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.

2.1. Protection Components and Management Modules

Dr.Web Anti-virus for Windows Servers contains the following protection components and management modules:

Component/module	Description
SplDer Guard	A component that constantly resides in memory. SplDer Guard scans processes and files on their launch and creation and detects any malicious activity.
Behavior Analysis	A component that controls application access to critical system objects and provides exploit prevention and integrity of running applications.
Exploit Prevention	A component that blocks malicious objects that use application vulnerabilities.
Ransomware Protection	A component that provides protection against ransomware.
Scanner	A scanner with a graphical interface that launches on demand or as scheduled and scans your computer for viruses and other malicious software.
Console Dr.Web Scanner	A command-line version of Dr.Web Scanner.
Dr.Web Updater	A module that allows registered users to receive and automatically install updates for virus databases and Dr.Web modules.

Component/module	Description
SpIDer Agent	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 constantly updated Dr.Web cloud service, along with the information on malware behavior, it determines whether the program is dangerous and then takes necessary measures to neutralize the threat. 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).

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

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

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.
- If it belongs to the black or white list on Dr.Web Cloud service.

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.
- If it belongs to the black or white list of applications that is stored on Dr.Web Cloud service.

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. Large amounts of data are processed faster thanks to the connection to the cloud service, and continuous training of the system provides preventive protection from the latest threats. At that, the technology can function even without a constant connection to the cloud.

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

Cloud-based threat detection technologies

Cloud-based detection methods allow scanning any object (file, application, browser extension, etc.) by its hash value. Hash is a unique sequence of numbers and letters of a given length. When analyzed by a hash value, objects are scanned using the existing database and then classified into categories: clean, suspicious, malicious, etc. Objects detected using Cloud-based technologies are indicated with the `CLOUD` prefix added to their names.

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

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

2.3. 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
Operating system	For 32-bit platforms: • Windows Server 2003 with Service Pack 1 • Windows Server 2008 with Service Pack 2 or later For 64-bit platforms: • Windows Server 2008 with Service Pack 2 or later • Windows Server 2008 R2 with Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Free RAM	Minimum 512 MB
Screen resolution	Recommended 1024x768 or higher
Cloud and virtualization environment support	Operation of the program is guaranteed in the following environments: • VMware • Hyper-V • Xen • KVM

As Microsoft has stopped supporting SHA-1 hashing algorithm, please ensure that your operating system supports SHA-256 hashing algorithm before installing Dr.Web Anti-virus for Windows Servers on 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 Anti-virus for Windows Servers of 12.0 version is compatible with Dr.Web products of 12.0 version only:

- Dr.Web for Microsoft Exchange Server
- Dr.Web for IBM Lotus Domino for Windows

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

Purpose	Direction	Port numbers
Receive updates (if the `update using https` option is enabled)	outgoing	443
To update	outgoing	80
To send email notifications		25 or 465 (or depending on the settings of email notifications)
To connect to Dr.Web Cloud	outgoing	443 (TCP), 2075 (including UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

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.

Testing the Anti-Virus with CloudCar file

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

To check Dr.Web Cloud operation

1. Make sure the usage of the Dr.Web Cloud service is enabled.
2. Download the test file. For that, go to http://kettle.dev.drweb.com/public/cloudcar.exe (EXE, 7 KB).
3. If the SpIDer Guard is installed and enabled, Dr.Web automatically moves the file to quarantine after the file is saved to the computer. If the SpIDer Guard component is not installed or disabled, scan the downloaded file. For that, right-click on the file name and select the **Check with Dr.Web** option in the context menu.
4. Check that the test file is processed by Dr.Web as `CLOUD:AMTSO.Test.Virus`. The `CLOUD` prefix in the threat name indicates correct Dr.Web Cloud operation.

3. Installing, Removing, or Changing Dr.Web

Before installing Dr.Web Anti-virus for Windows Servers, 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 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 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.
>
> Dr.Web is not compatible with other anti-virus software (including other versions of Dr.Web anti-virus programs). Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have another anti-virus software installed then it is necessary to uninstall it using the installation file or standard tools of the OS.

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

- Command line mode
- Wizard mode

3.1. Installing the Product

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

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 **Cancel**.

To install the program

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

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

2. At the first step of installation process, you are prompted to connect to Dr.Web cloud services that allow scanning using the newest information on threats. The information is updated in real-time mode. The option is disabled by default.

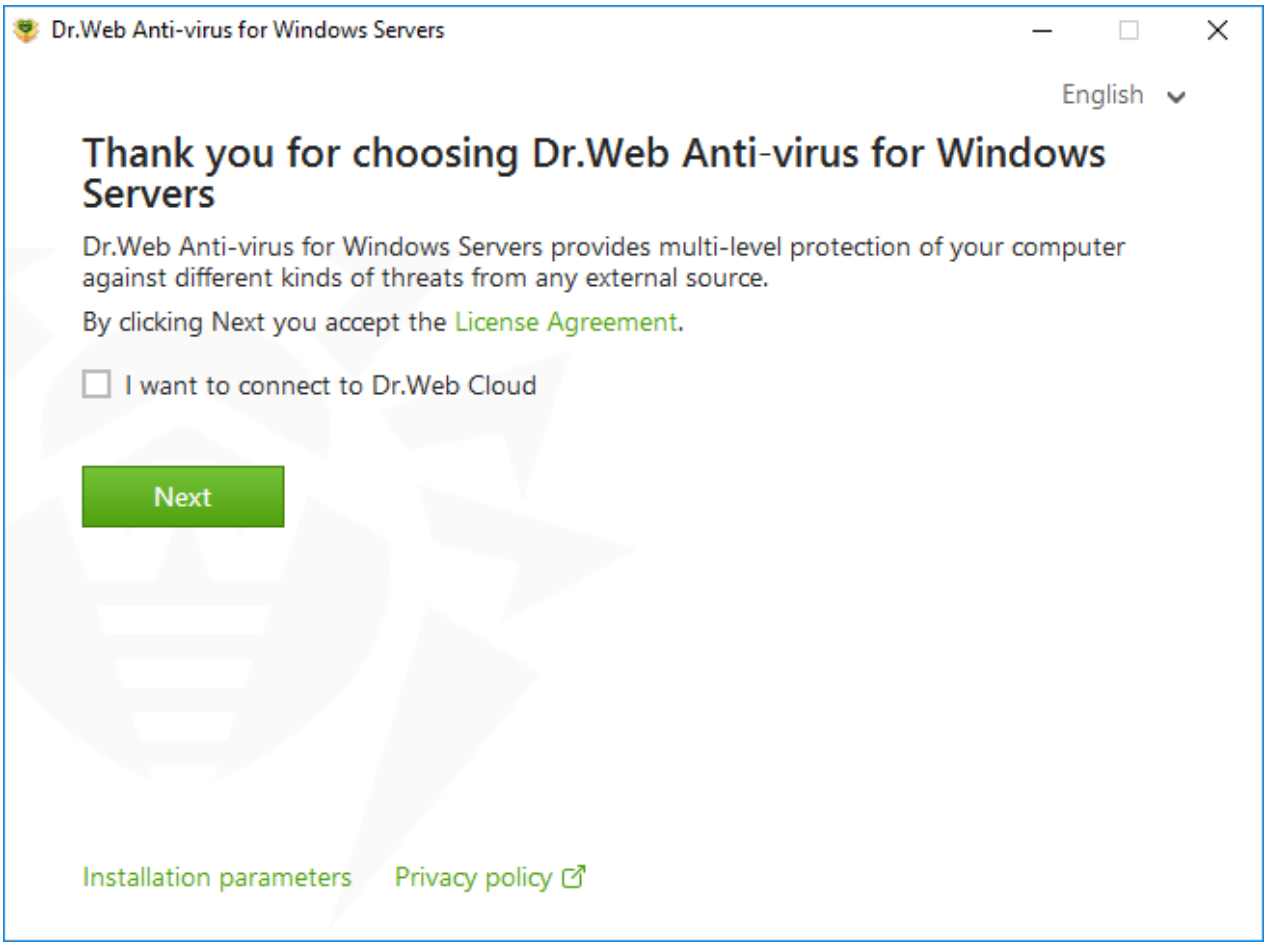

Figure 1. Installation Wizard

3. If you want to use default installation settings, go to the next step. To select components you want to install, specify the installation path and configure other settings, click **Installation parameters**.

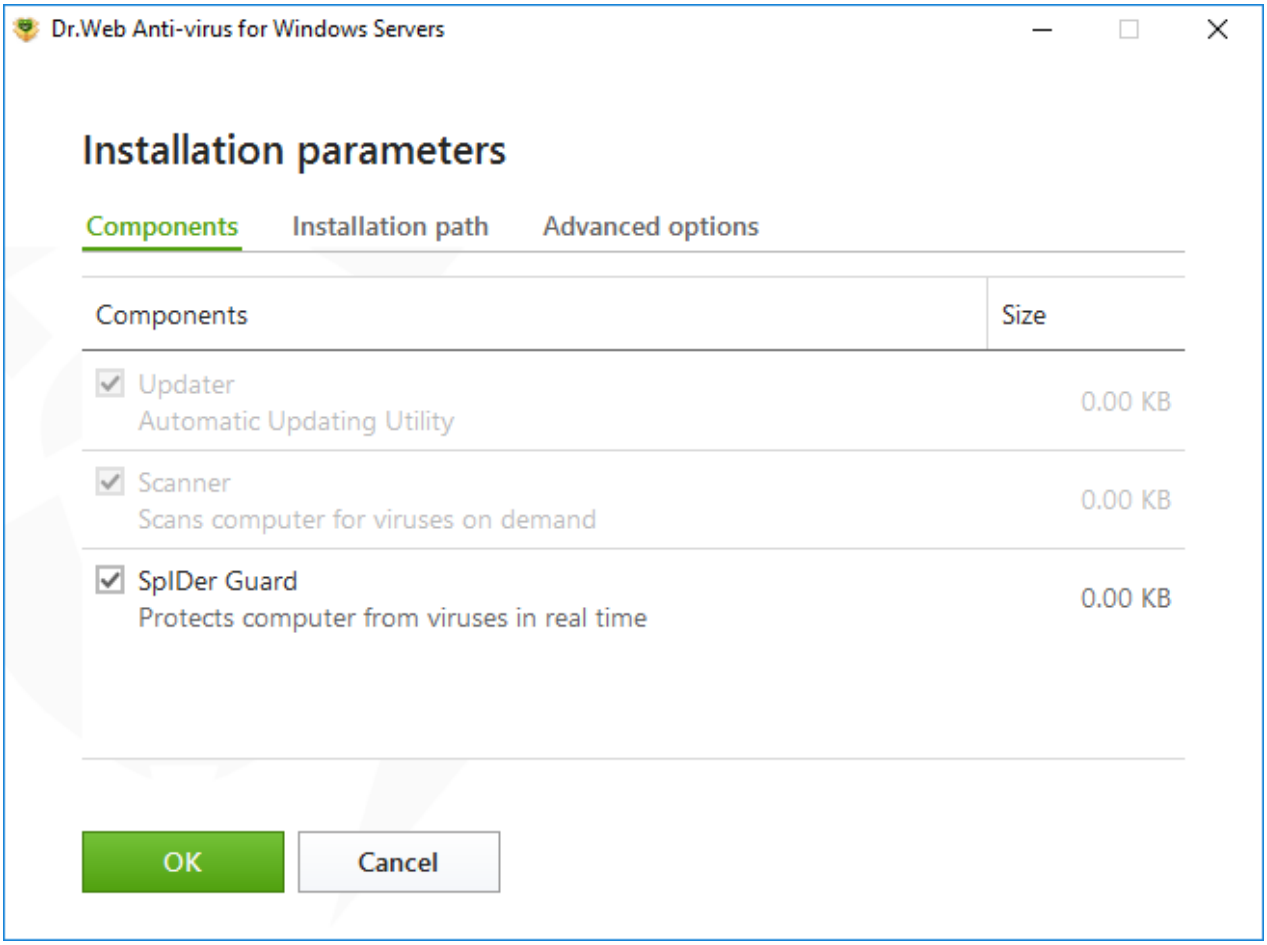

Figure 2. Installation parameters

The option is meant for experienced users.

- On the first tab, you can specify the components you want to install. Select the check boxes next to those components that you want to install.
- On the second tab, you can change the installation path. By default, it is installed into the `DrWeb` folder in the `Program files` folder on the system disk. To change the installation path, click **Browse** and specify the necessary folder.
- The third tab of the window allows you to enable the **Update during installation** option to download updates to virus databases and other program components. Enable the **Enable compatibility with screen readers** option to use such screen readers as, for example, JAWS and NVDA for reading aloud the information on Dr.Web interface elements. This option makes Dr.Web interface accessible for disabled people.

To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**.

4. Click **Next**. Please note that by clicking the Next button you accept the terms of the License agreement.
5. In **Registration Wizard** window select one of the following options:
   - If a key file is present on the hard drive or removable media, select **Specify path to an available valid key file**. Click **Browse** and select the key file in dialog box. More information can be found in Activation Using Key File section.

- To continue installation without a key file, select **Receive license later**. If you select this option, none of the program components will operate until you get a valid key file. You will be able to purchase a license and get a valid key file after the installation.

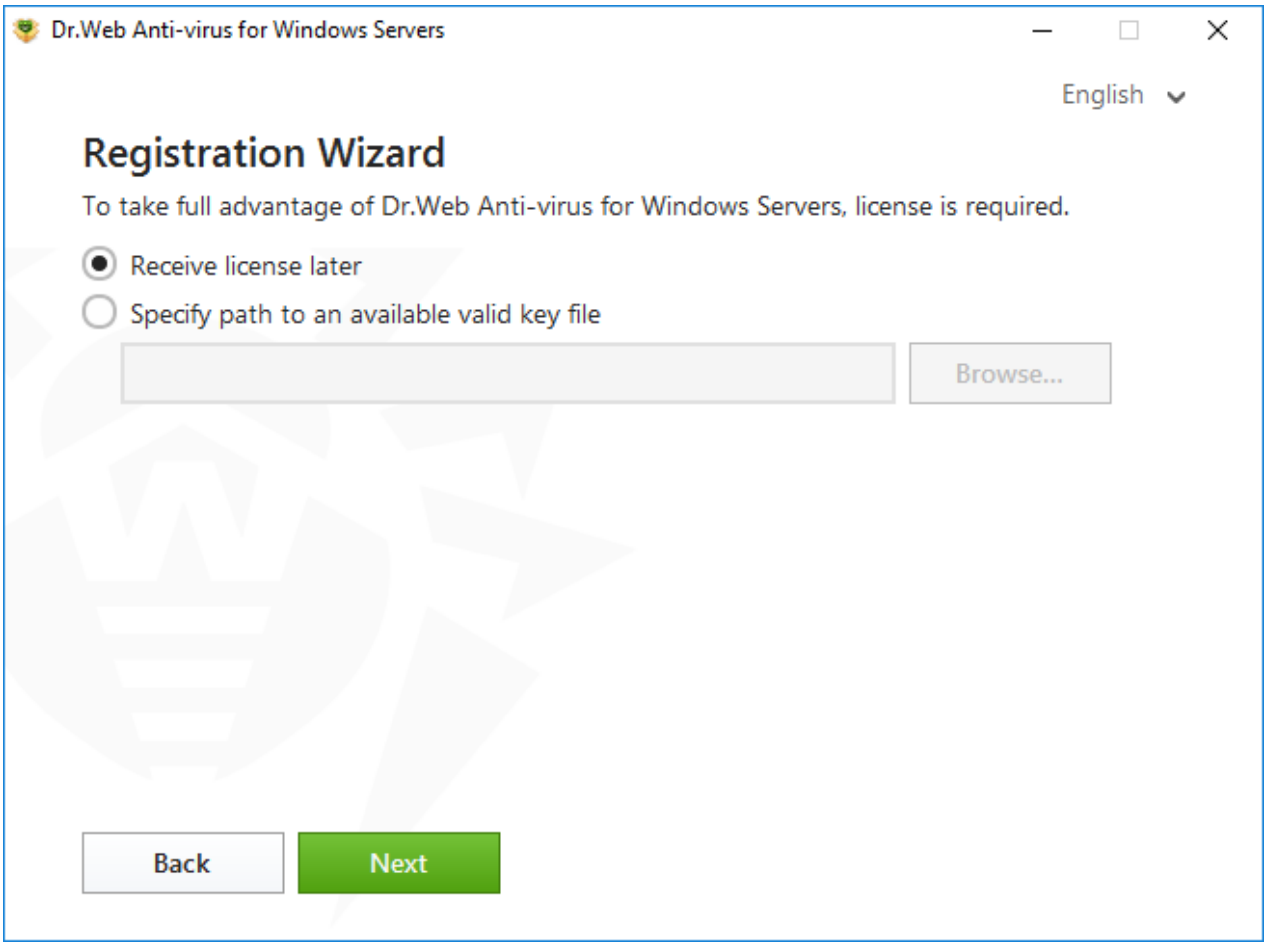

Figure 3. Registration Wizard

Click **Next**.

6. If you need to configure a proxy server, enable the option **Specify proxy server IP and port manually**. Click **Install**.
7. If you have specified a valid key file and have not cleared the **Update during installation** check box, the Wizard updates virus databases and other Dr.Web components. Updating starts automatically and does not require any additional actions.
8. To complete installation, restart your computer.

Installation via the command line

To start the installation of Dr.Web in the background mode, enter the executable file name and specify necessary parameters in the command line:

Parameter	Value
`lang`	Language used for the installation. The value of this parameter is language in ISO 639-1 format, e.g., `/lang en`.
`reboot`	Restart the computer automatically after installation is completed. Can take the value `yes` or `no`.
`silent`	Installation in the background mode. Can take the value `yes` or `no`.
`blockEmulateUserActions`	Enable the **Block user activity emulation** option during the installation. Can take the value `yes` or `no`.
`allowUiAccessibility`	Enable the compatibility with screen readers option during the installation. Can take the value `yes` or `no`.
`importSettings`	Import settings from the file (the maximum file size is 20 MB). You need to specify the path to the file.
`enableDebugLogs`	Enable debug logging. Can take the value `yes` or `no`. Debug logging is enabled for SpIDer Guard, SpIDer Mail, SpIDer Gate, Scanner, Dr.Web Updater and Dr.Web Service. Logging is disabled when you restart your computer after the installation is completed.

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

```
drweb-12.0-av-win-server.exe /silent yes /reboot yes
```

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 an error, do the following:

1. Scan the system using CureIt! utility by Doctor Web. You can download CureIt! from Doctor Web website: https://free.drweb.com/download+cureit+free/.
2. Enable or restart BFE service. 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.

3.2. Configuring Components

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 Anti-virus for Windows Servers**.
  3. Click **Change**.

To delete or add components

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

Figure 4. 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**.
4. The **Disabling Self-Protection** window opens. Enter the confirmation code that is displayed.
5. 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.

3.3. Removing and Reinstalling the Product

Removing Dr.Web

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

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

1. To remove Dr.Web Anti-virus for Windows Servers, run Windows removal component.
2. In the list select the line with the program name.
3. Click **Delete**.
4. 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** and **Dr.Web Anti-virus for Windows Servers settings**—are selected. Click **Next**.
5. The **Disabling Self-Protection** window opens. Enter the displayed confirmation code and click **Remove program**.
6. 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.

Reinstalling Dr.Web

1. Download the latest installation package of the program from the official Dr.Web website. For this, enter a valid serial number in the corresponding field.

2. Uninstall the program, as described above.
3. Restart your computer.
4. Using the downloaded executable file (`drweb-12.0-av-win-server.exe`), reinstall the program. While installing, specify the path to the key file.
5. Restart your computer.

4. Licensing

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

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

License activation methods

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

- during the installation via the Installation Wizard,
- at any moment after the installation via the License Manager,
- on the official Doctor Web website at https://products.drweb.com/register/.

License activation via the Registration Wizard is available using the key file only. License activation via the License Manager is available using the serial number or the key file.

For the detailed information on license activation, refer to the Activation using serial number and Activation using key file sections.

If you have questions on licensing, read the FAQ section on Doctor Web website.

Possible questions

How to transfer a license to another computer?

You are entitled to transfer your license for commercial use using the key file or serial number.

To transfer a license to another computer

- using the serial number:
  1. Copy the serial number from the computer of license origin.
  2. Remove Dr.Web from the computer of license origin or activate another license on this computer.
  3. Activate the current license on the target computer. To do this, use the License Manager after the installation (see Activation using serial number).

- using the key file:
  1. Copy the key file from the computer of origin. By default, the key file is stored in the Dr.Web installation folder and has the `.key` extension.
  2. Remove Dr.Web from the computer of license origin or activate another license on this computer.
  3. Activate the current license on the target computer. To do this, use the Registration Wizard during the product installation or the License Manager after the product is installed (see Activation Using Key File).

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

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

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

How can I change the registration email?

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

Why are some components missing in my product?

- Not all the components, that are included in your license, were installed.

  To enable missing components

  1. Go to Windows Control Panel, click Programs.
  2. In the list of installed programs, select the line with the program name.
  3. Click **Change** button, Uninstall/Change Wizard launches.
  4. Select the **Change components** option.
  5. Select the components you want to enable from the list of components and click **Apply**.

  Other option is to run the installation file `drweb-12.0-av-win-server.exe`. Select the **Change components** option in the open window. Go to step 5.

4.1. License Activation

To get access to all product functions and components, activate the license. License activation is available using:

- Serial number
- Key file

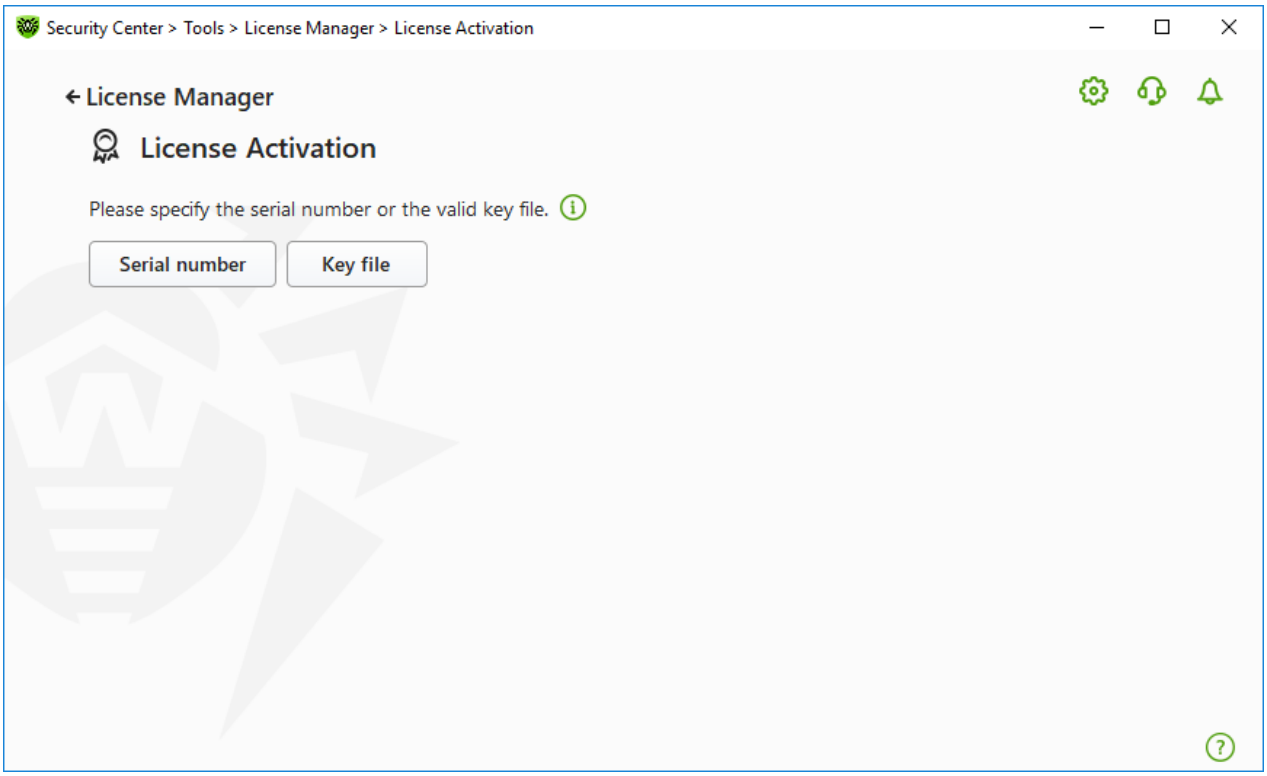

Figure 5. License Activation

Windows Server 2003 users can activate the license using the key file only.

> If you are already a Dr.Web user, you are eligible for extension of your new license.

License activation on Windows Server 2003

Users of Windows Server 2003 can activate their licenses using the key file only. If you have a serial number without the key file, it is necessary to register it on the Doctor Web website. After the registration is over, the link for downloading the key file becomes available. Use this key file for license activation during the installation or in any moment after the installation via the Registration Wizard included in the License Manager:

1. In the Dr.Web menu, select **License**. The License Manager opens. Click **Activate**.
2. In the open window, click **Browse** to specify the path to the key file.
3. Click **OK** to close the window and go to the License Manager.

Reactivating license

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

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

When you reinstall the product or install it on several computers, if the license allows that, reactivation of the key file is not required.

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

4.1.1. Activation Using Serial Number

If you have a serial number, you can:

- activate the license via the License Manager:
  1. In the Dr.Web menu, select **License**. The License Manager opens. Click **Activate**.
  2. The License Activation window opens. Click **Serial number**.

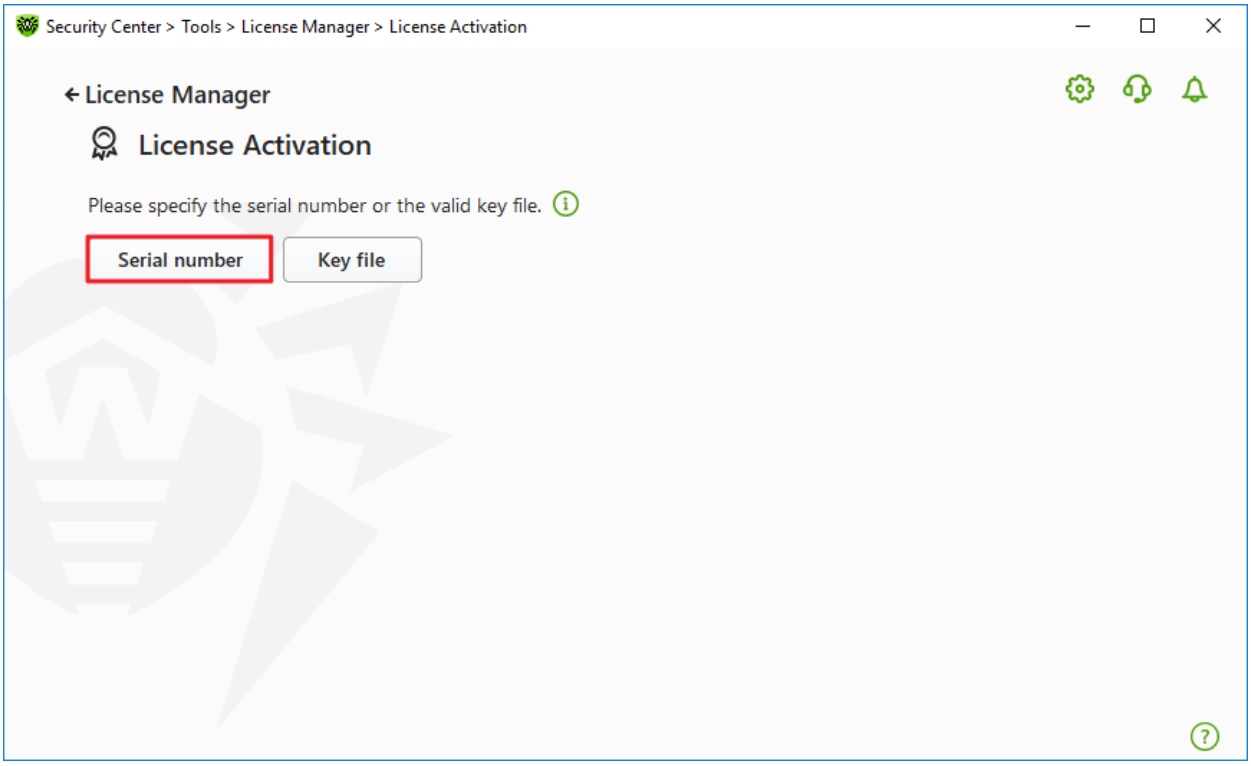

Figure 6. Access to the serial number specification window

  3. In the additional window enter your serial number and click **Activate**.

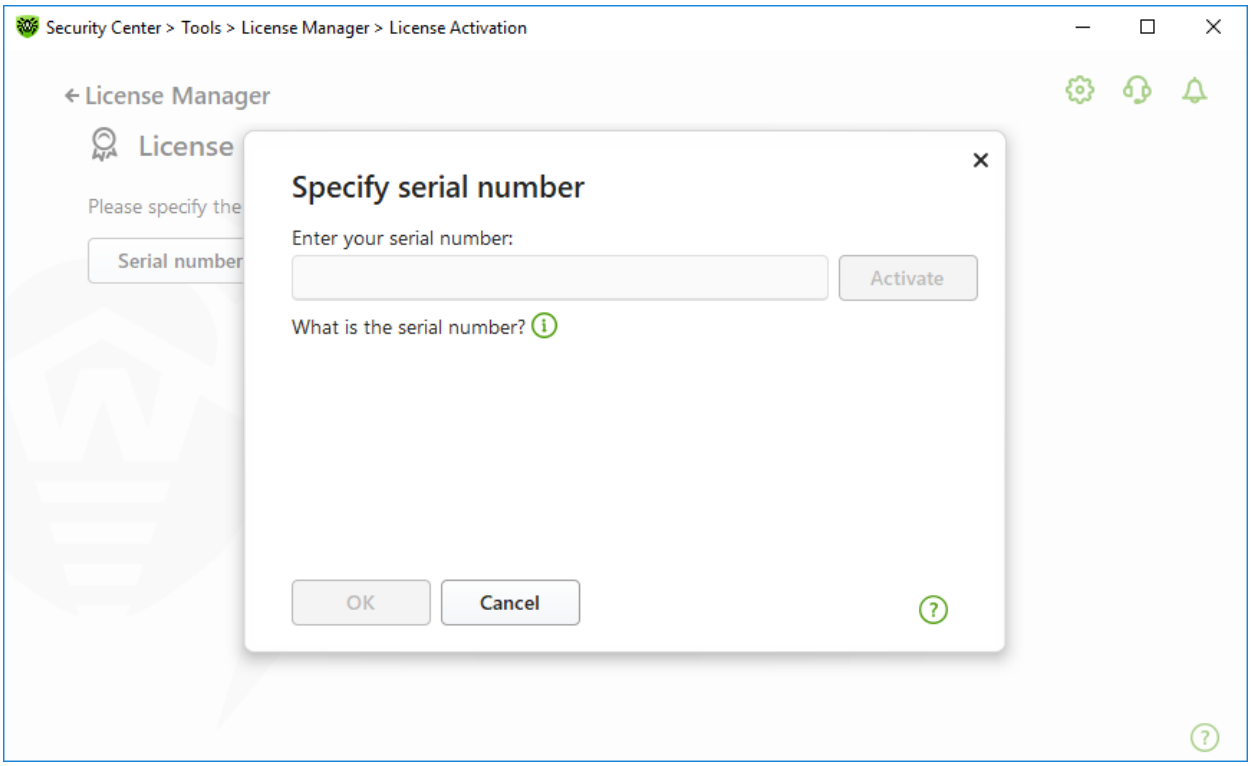

Figure 7. Activation using a serial number

4. The Doctor Web official website page opens where you can enter your registration data. Follow the instructions on the website to complete the registration.

   After long standby, the window will automatically close and an error message will be displayed.

   Do not close the activation window before completing the serial number registration. If a window is closed, the license can only be activated with a key file.

5. The link to register your serial number is sent to the specified email address. Follow the link to complete the license activation.
6. If activation is successful, the program window shows detailed information about the license. Click **OK** to close the window and go to the License Manager.

If the license activation has failed, an error message displays. Check internet connection parameters and click **Retry**.

- register your serial number on the Doctor Web website and get a key file to activate your license.

4.1.2. Activation Using Key File

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

- during the installation via the Registration Wizard:

1. Run product installation. At step 5 of the installation, select **Specify path to an available valid key file**. Click **Next**.

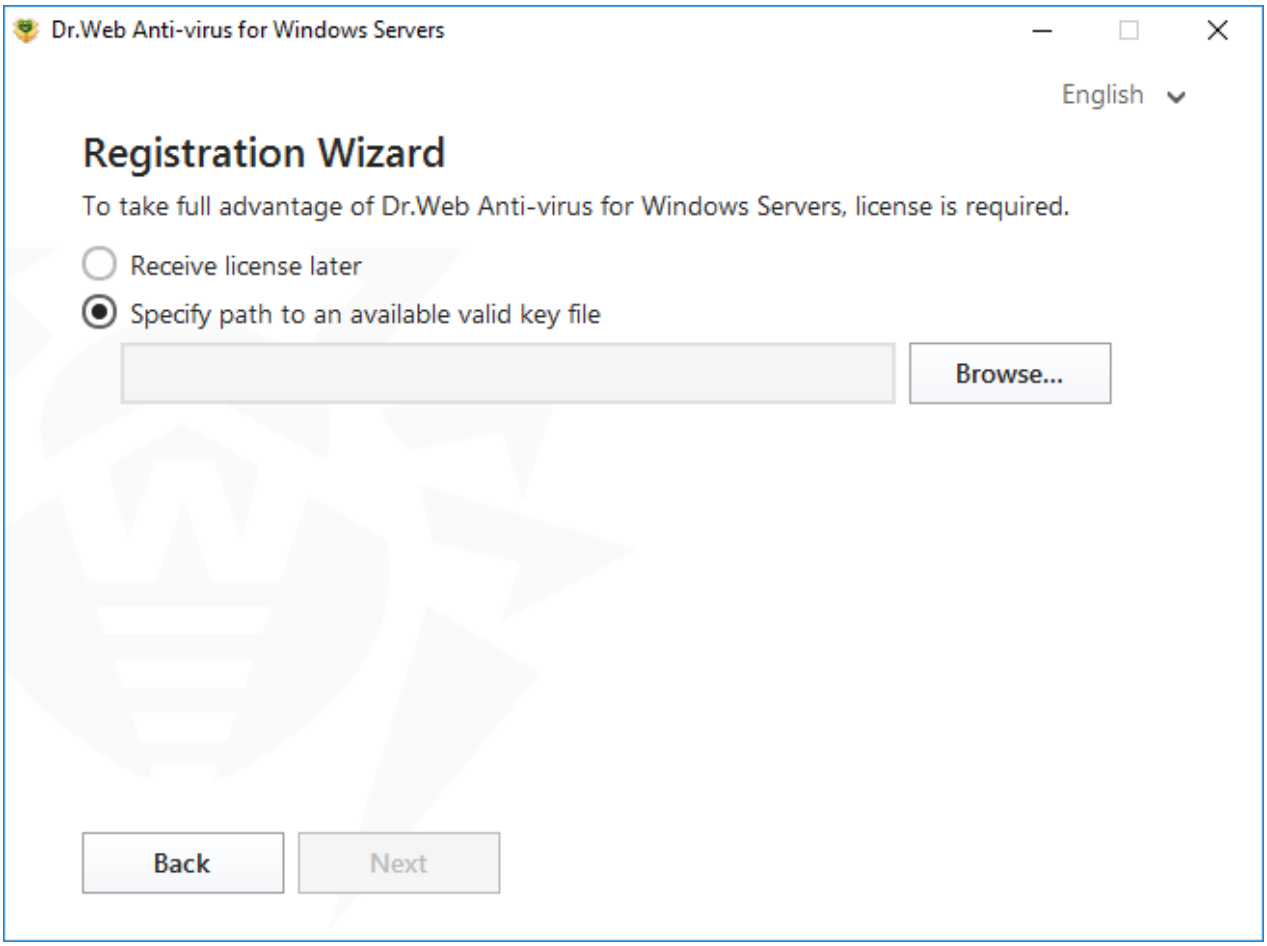

Figure 8. Installation. Registration Wizard

2. Continue product installation following the instructions of the Installation Wizard.

- at any moment after the installation via the License Manager:
  1. In the Dr.Web menu, select **License**. The License Manager opens. Click **Activate**.
  2. The License Activation window opens. Click **Key file**.

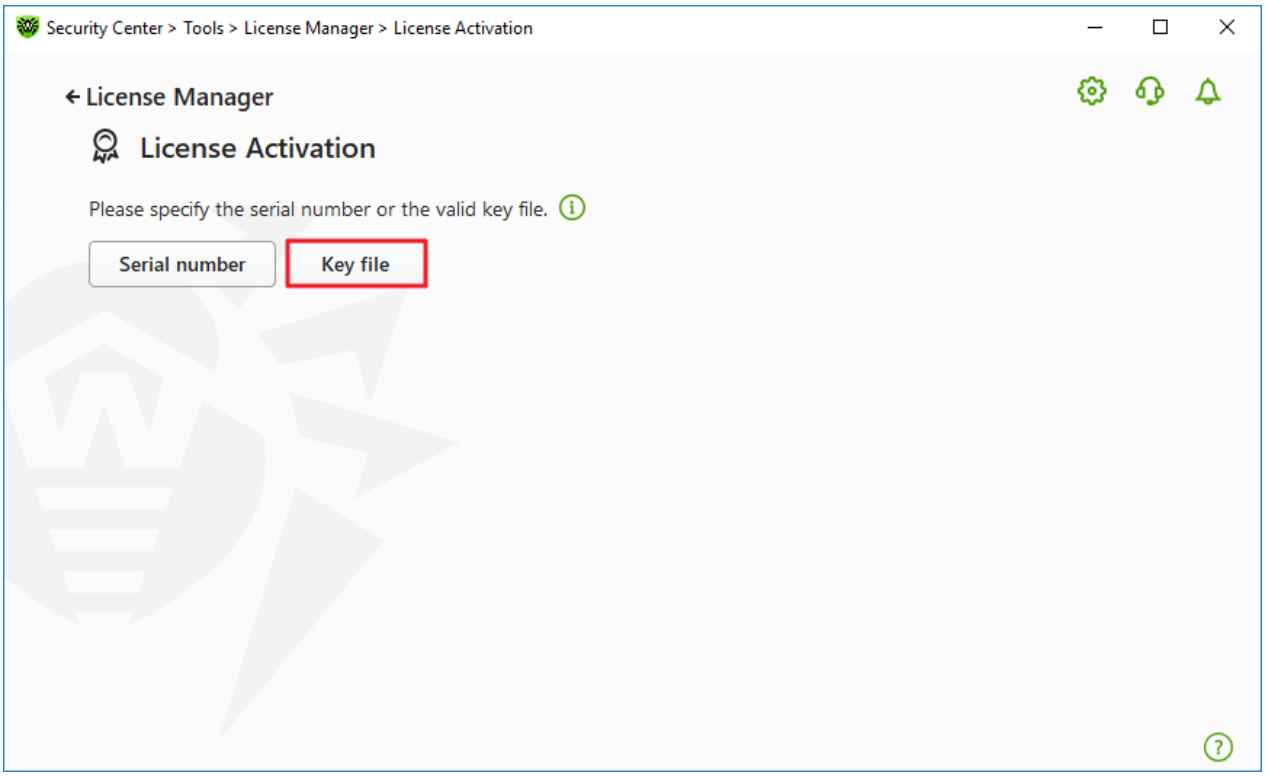

Figure 9. Access to the key file specification window

3. In the open window, click **Browse** to specify the path to the key file.

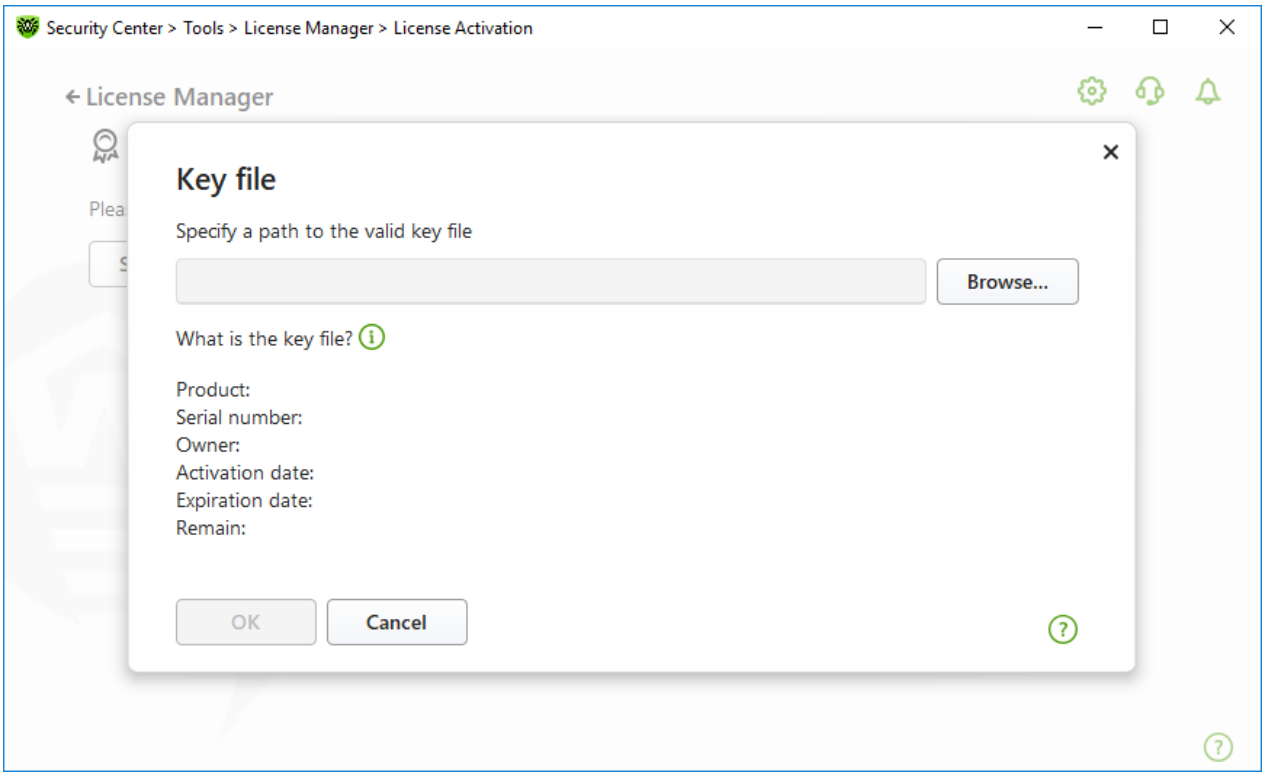

Figure 10. Activation using a key file

4. Click **OK** to close the window and go to the License Manager.

4.2. Renewing License

You can renew the current license using Renewal Wizard on the Doctor Web website.

To renew the current license using License Manager

1. Open Dr.Web menu, then select **License**.
2. In the License Manager window, click **Buy**. A page on the Doctor Web website where you can renew your license with a discount will open.

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

> After long standby, the window will automatically close and an error message will be displayed.
>
> Do not close the activation window before the renewal process is completed. If a window is closed, the license can only be activated with a key file.

If license activation has failed, an error message displays. Check internet connection parameters and click **Retry**.

To activate a license

1. Open License Manager by selecting **License** in Dr.Web menu. Click **Activate**.
2. In the open window, click **Serial number** or **Key file**. Enter the product serial number or specify the path to the key file. Windows Server 2003 users can activate the license using the key file only.

The detailed information on license activation is available in the Activation using serial number and Activation using key file sections.

If the license you want to renew has expired, Dr.Web will start using the new license.

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

If you have questions on license renewal, read the FAQ section on Doctor Web website.

Possible questions

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

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

It is recommended that you remove the previous license from the product. To remove the license:

1. In Adiminstator mode, in Dr.Web menu, select **License**. The License Manager opens.
2. Click **Details** to open the License Information window.
3. In the drop-down menu select the license, on which behalf the extension was made, then click .

4.3. Key File

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

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

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

> By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.
>
> If no valid key file is found, all Dr.Web components are blocked.

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

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

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

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

5. 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**.

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

To access the component parameters and open your personal webpage My Dr.Web, 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 technical support.

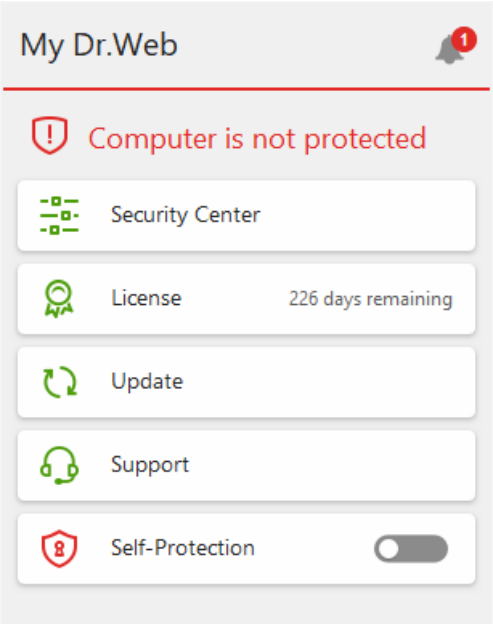

Figure 11. Program menu

Menu items

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

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, and exclusions.

License. Information on the amount of days remaining until the license expires. Opens License Manager.

Update . Information about the actuality of virus databases and last update date. Launches the update of program components and virus databases.

Support. Opens support window.

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

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.
	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. Enable Self-Protection or the disabled component.
	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. Check that you have a valid key file and, if required, install it.

6. 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**.

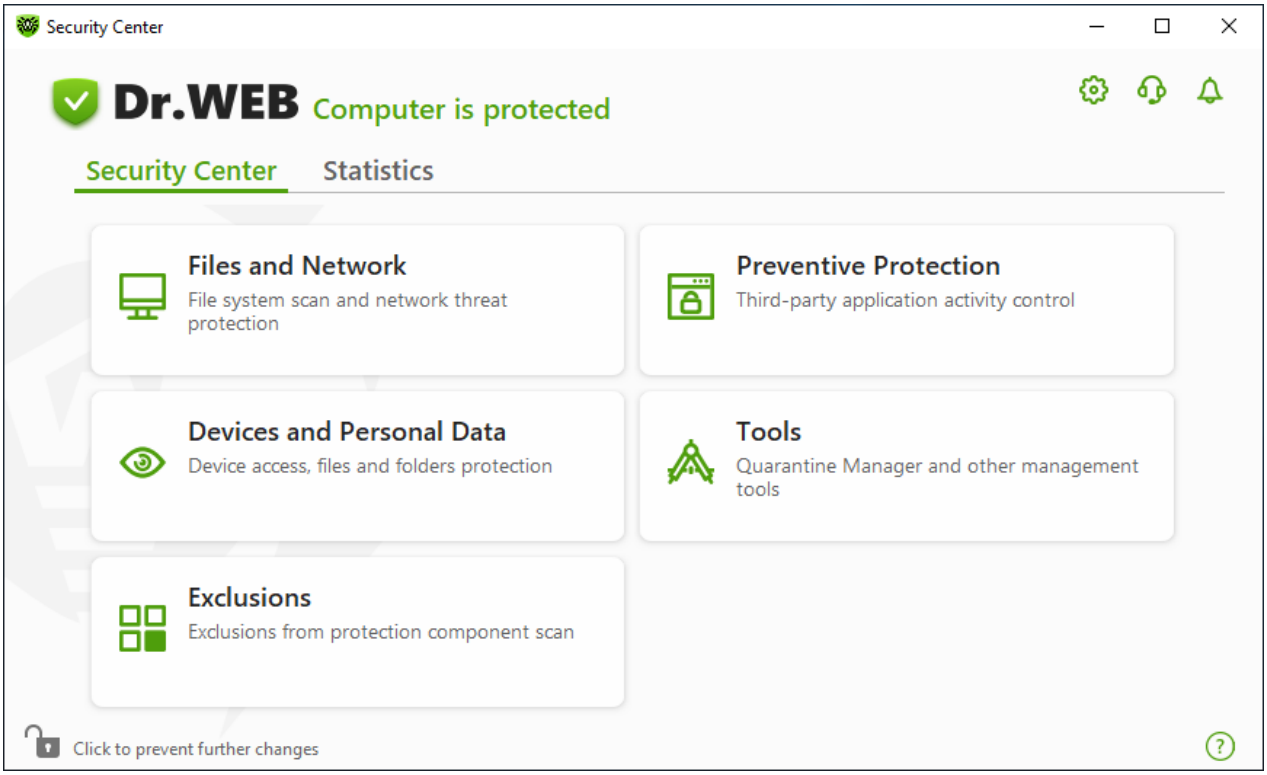

Figure 12. Security Center window

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 and Personal Data

  - Tools;
  - 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 control 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 **Tools** group of settings 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, control the component parameters and change program settings, you need to switch to the administrative mode.

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.
- **License expires**. Starts to display when 7 days are left before the license expires. Displayed in yellow color. To renew the license, go to License Manager.

7. Updating of Virus Databases and Program Components

To detect malicious objects, Dr.Web products use virus databases that contain information about all known malicious programs. Regular updates of databases allow the detection of previously unknown viruses, blocking their distribution, and in some cases curing previously incurable infected files. Virus databases are considered outdated after 24 hours since the last successful update. Besides virus databases, Dr.Web software components and help documentation are updated as well.

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

Update relevance check

To check the relevance of virus databases and program components, open Dr.Web menu. If updates are relevant, the **Update** item is highlighted in green:

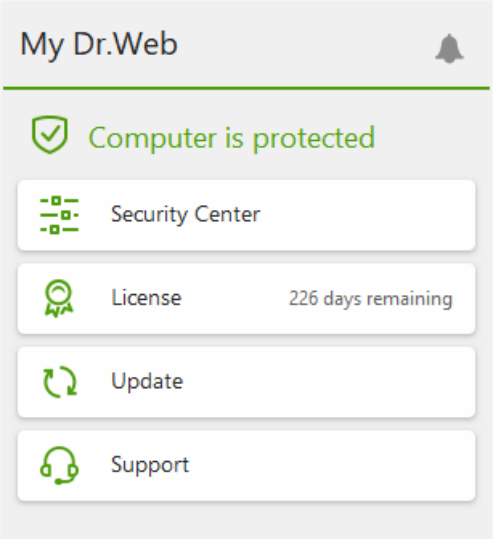

Figure 13. Dr.Web menu

If updates are required, the **Update is required** highlighted in red appears:

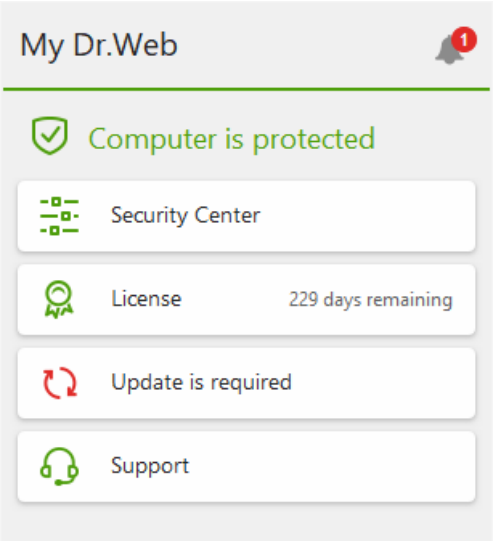

Figure 14. Update required

Starting update

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

> After an update of executable files, drivers, or libraries, a restart may be required. In such cases, an appropriate warning displays. You can set any convenient time for the restart or pick a time for the next reminder.

To start update from Dr.Web menu

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

To start update from the command line

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

Update and statistics logs

To view update history on Statistics tab

1. Open Dr.Web menu.

2. Select **Security Center**.
3. Open the **Statistics** tab.
4. Click the **Detailed Report** tile.

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

How to set update of databases and components without internet access?

If the computer is connected to the local network, you can choose to update the virus databases and components using the update mirror created on another computer with Dr.Web product installed (Security Space, Anti-virus for Windows or Anti-virus for Windows Servers). The computer on which the update mirror is created should have the internet connection. The product version should be the same.

More information on how to create an update mirror

You can set the update from the update mirror in two ways:

To set the update when the computer is connected to the anti-virus network

1. Enable remote control of Dr.Web product in Anti-virus network section of settings window.

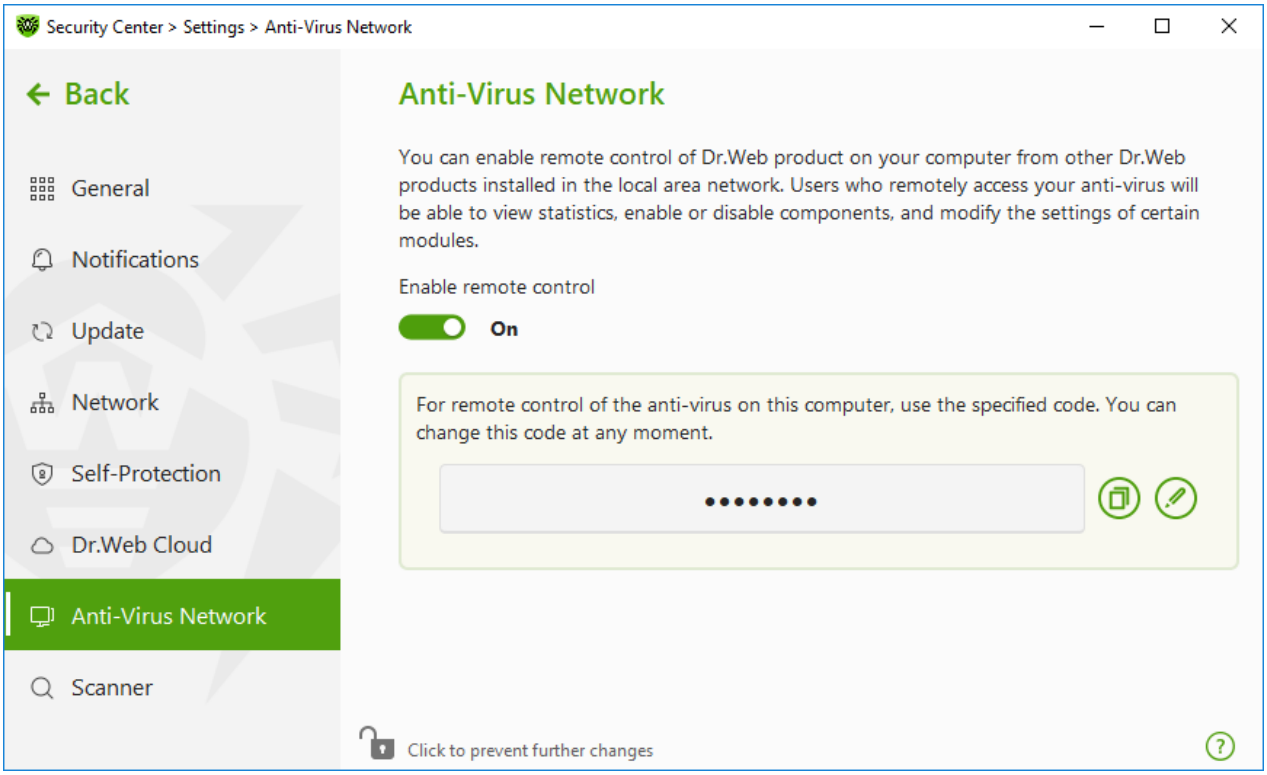

Figure 15. Switching on the remote access

2. Go to **Settings** → **Update** window.

3. In the **Update source** section, click **Edit** and then select **Anti-Virus Network** from the drop-down list.

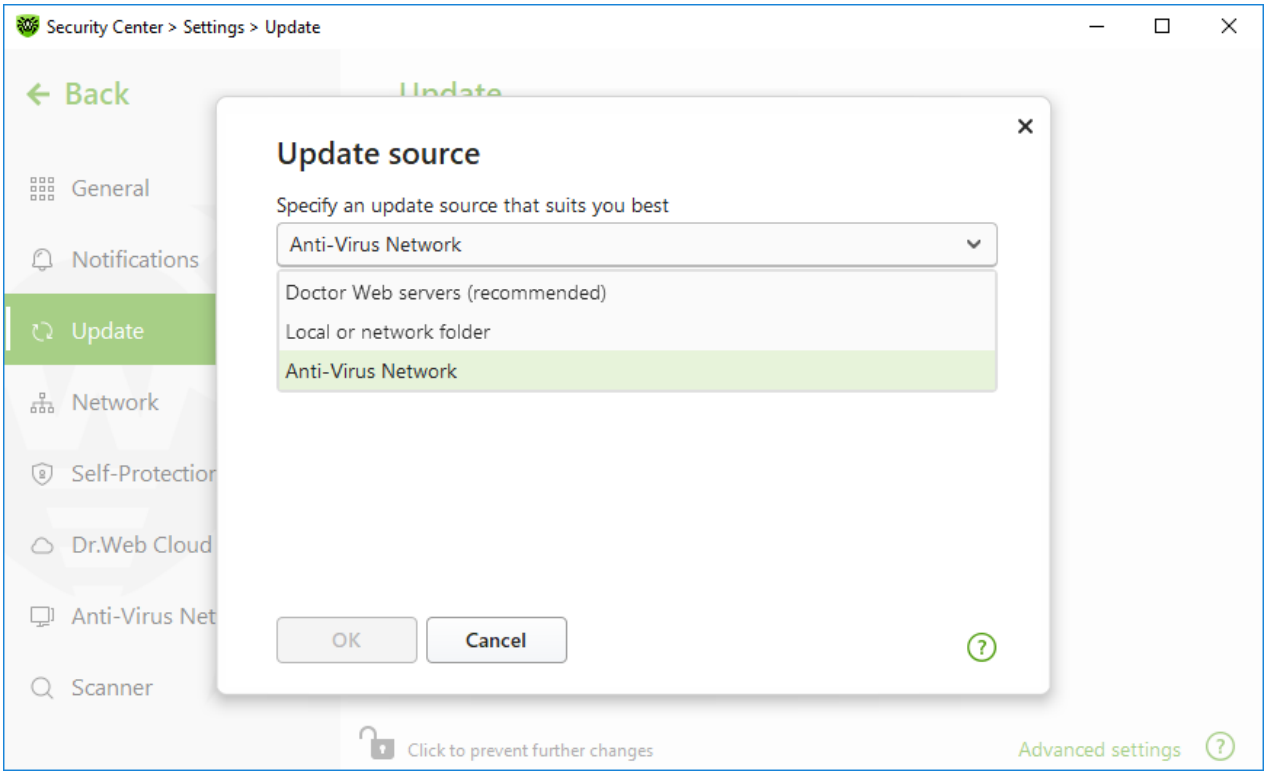

Figure 16. Selecting the update source

4. Select the computer that will be used to update program virus databases and components.
5. Click **OK**.

To set the update from local or network folder

1. Go to **Settings** → **Update** window.
2. In the **Update source** section, click **Edit** and then select **Anti-Virus Network** from the drop-down list.

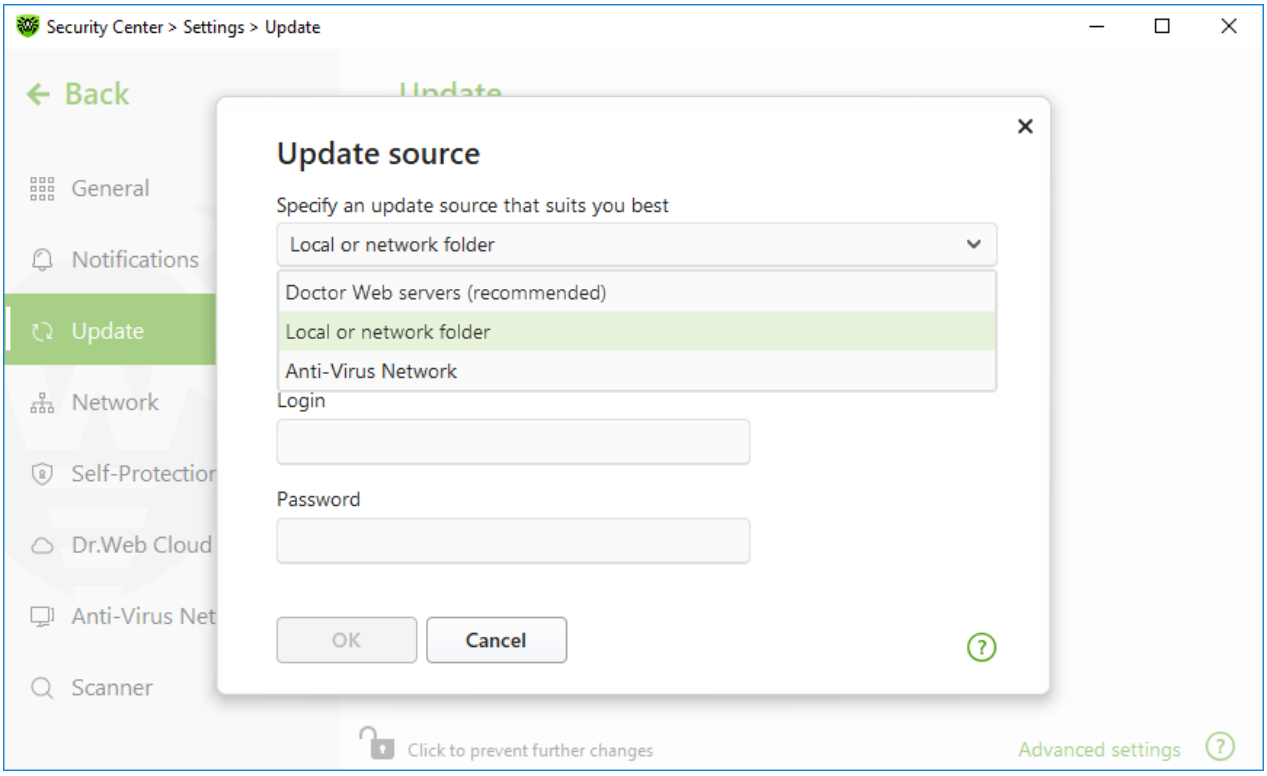

Figure 17. Selecting the update source

3. In the **Path to the update mirror** field, specify the folder that contains files of the created update mirror. For this, click **Browse** button and select the required folder, or enter the path manually using UNC.
4. Enter the **Login** and **Password** to the folder you try to connect, if necessary. **Login** is the user name of the account on the computer that contain network folder. Login requires the computer name in the local network and full path to the folder. **Password** is the account password.
5. Click **OK**.

8. 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. A window with the event notifications opens.

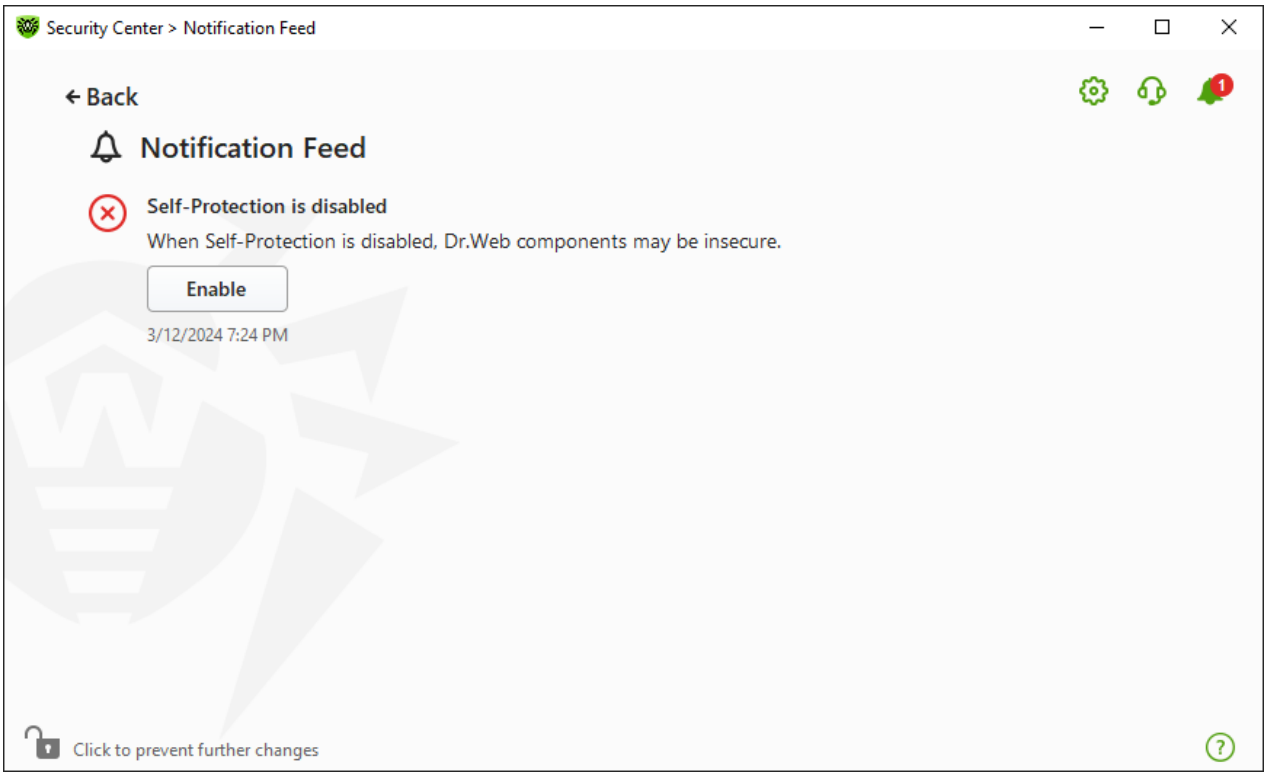

Figure 18. Notification Feed window

Notification retention period

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

Notification types

Critical notifications	
License	• The valid license is not found. • The current license is blocked.
Threats	• Threat is detected. • The reboot is required to neutralize the threats. • Virus databases are out of date.
Blocked access to the objects and devices	• Device is blocked according to settings.
Major notifications	
License	• License expires. • The current license is blocked.
Update	• The restart is required to complete the update.
Not important informative notifications	
New version	• New version is available.

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.

9. 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.

> 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, and import or export settings.
- Notifications—configure parameters to display pop-ups and to receive notifications by email.
- Update—change source or frequency of updates and create an update mirror.
- Network—configure the proxy server connection.
- Self-Protection—configure advanced security parameters.
- Dr.Web Cloud—configure access to the Doctor Web cloud services.
- Anti-Virus Network—configure remote access to Dr.Web installed on your computer.
- File Scan Options—configure Scanner parameters.

9.1. General Settings

You can find the following features among general settings:

- Program settings password protection
- Selecting interface color theme
- Selecting program language
- Managing program settings (import and export settings or restore defaults)
- 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.

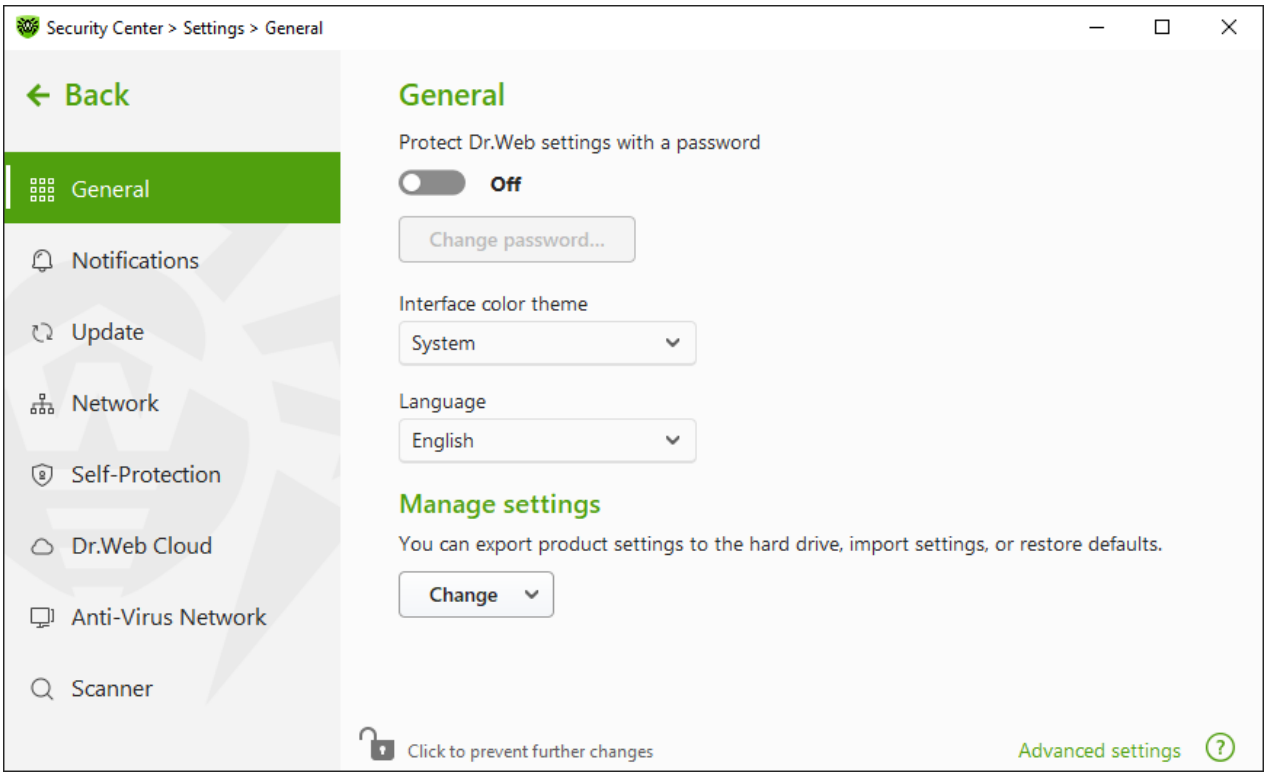

Figure 19. General Settings

9.1.1. Program Settings Password Protection

You can restrict access to Dr.Web settings on your computer by using a password. A password can be any length, and can include any combination of letters, numbers, and special characters. For better protection, use a password consisting of 10 or more different characters. 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.

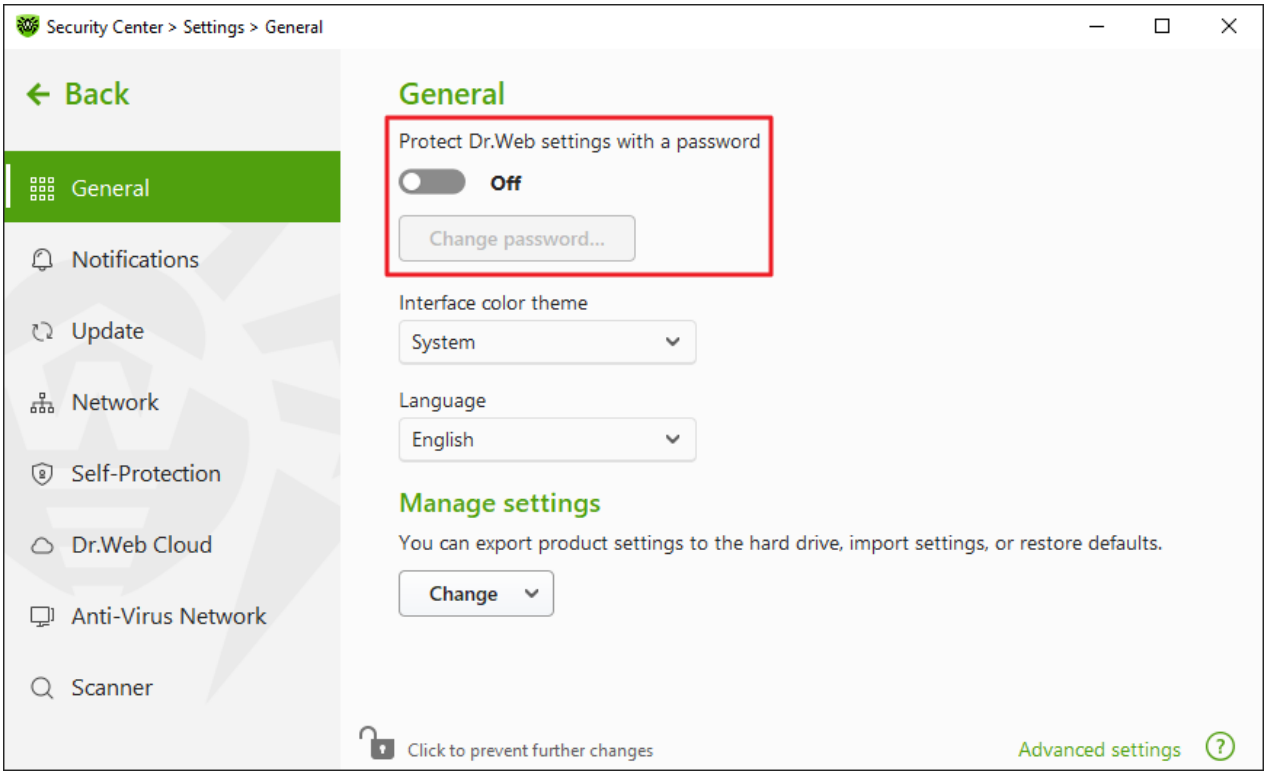

Figure 20. Settings password protection

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

> If you have forgotten your password for the product settings, reinstall Dr.Web program without saving the current settings.

9.1.2. 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.

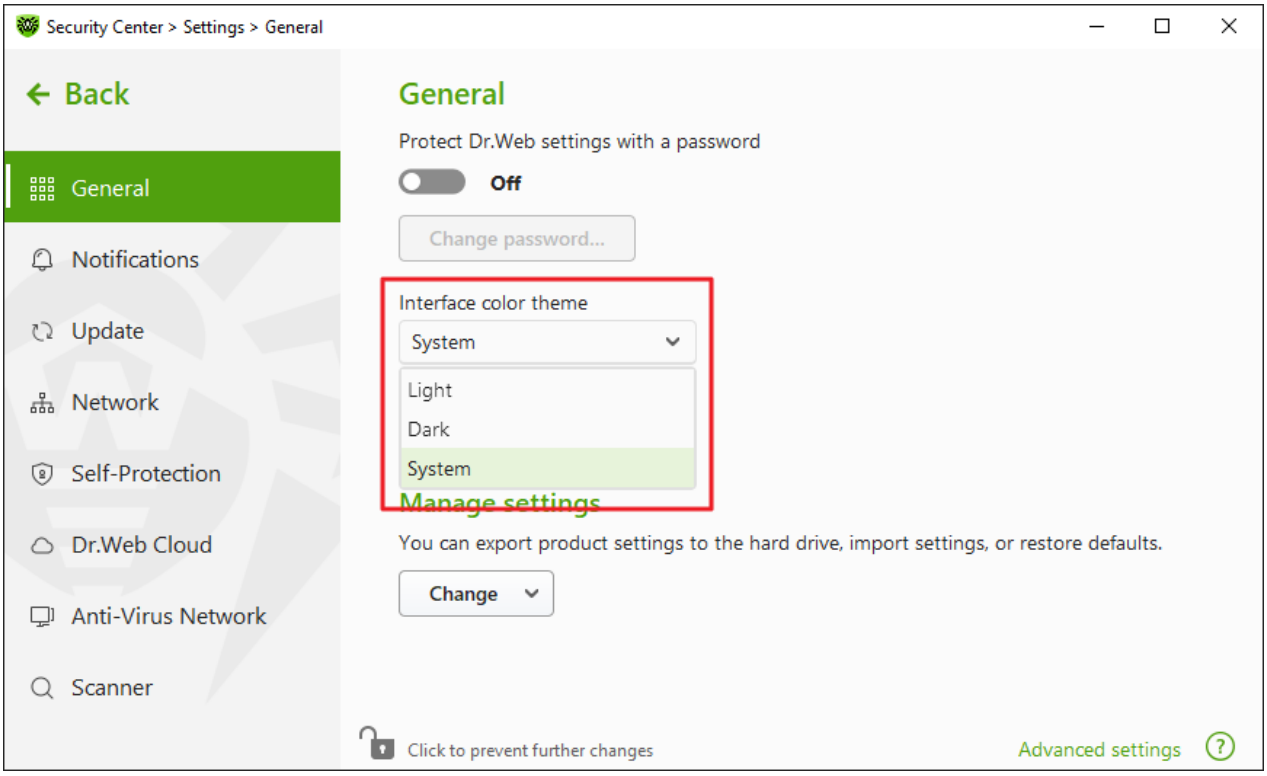

Figure 21. Selecting interface color theme

The dark color theme is available for computers running 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.

9.1.3. 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.

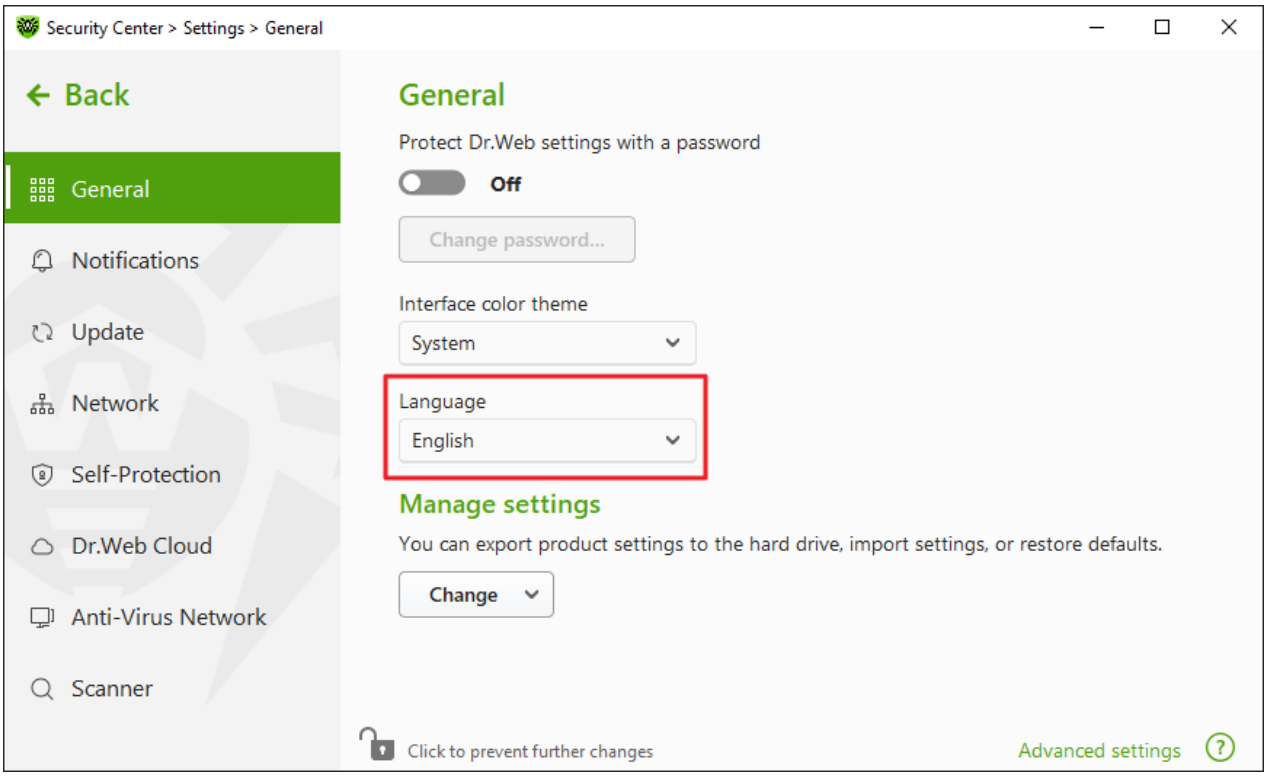

Figure 22. Selecting program language

9.1.4. Managing Dr.Web Settings

To manage settings, select one of the following actions in the drop-down menu of the **Manage settings** setting group:

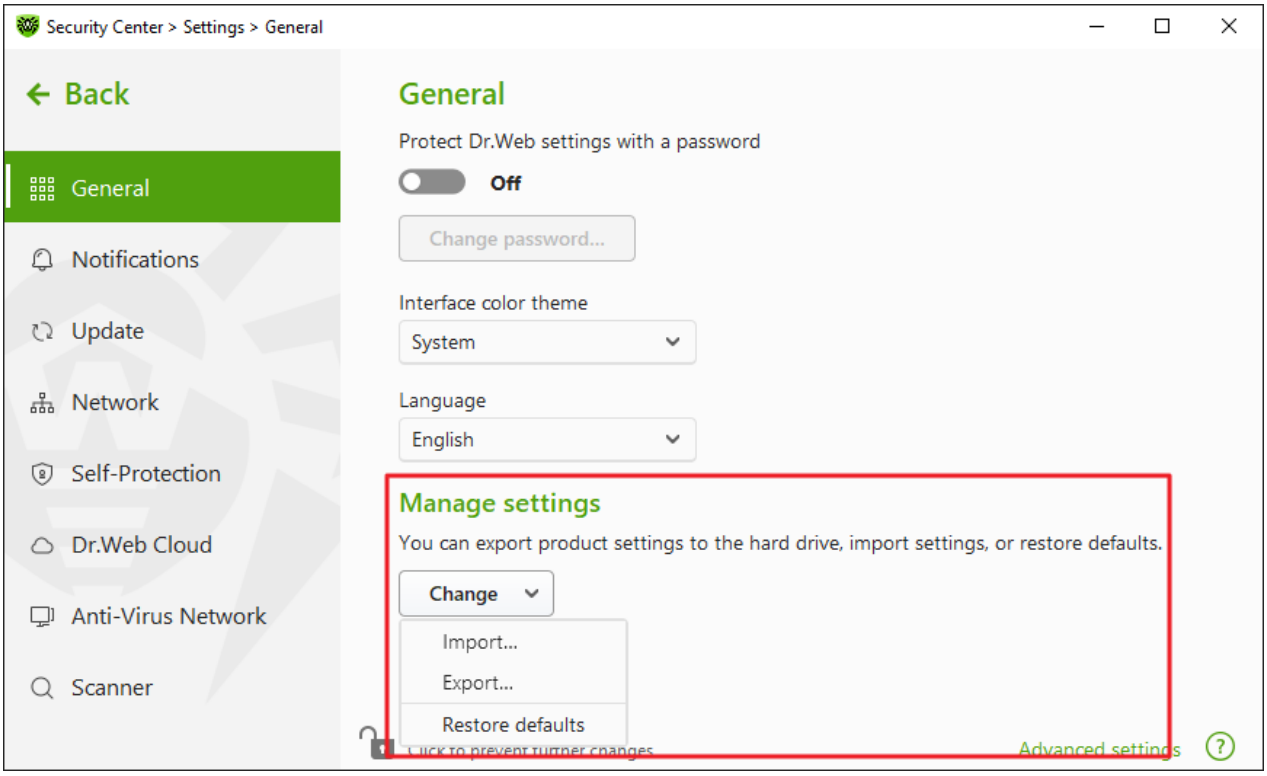

Figure 23. Managing settings

- **Restore defaults** to restore default settings.
- **Import**, if you want to use settings of the anti-virus that you already configured on another computer.
- **Export**, if you want to use your settings on other computers. Then, use the import feature on another computer.

9.1.5. Dr.Web Operation Logging

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

To change operation logging settings

1. Click **Advanced settings** link.
2. In the **Log** section click **Edit**.

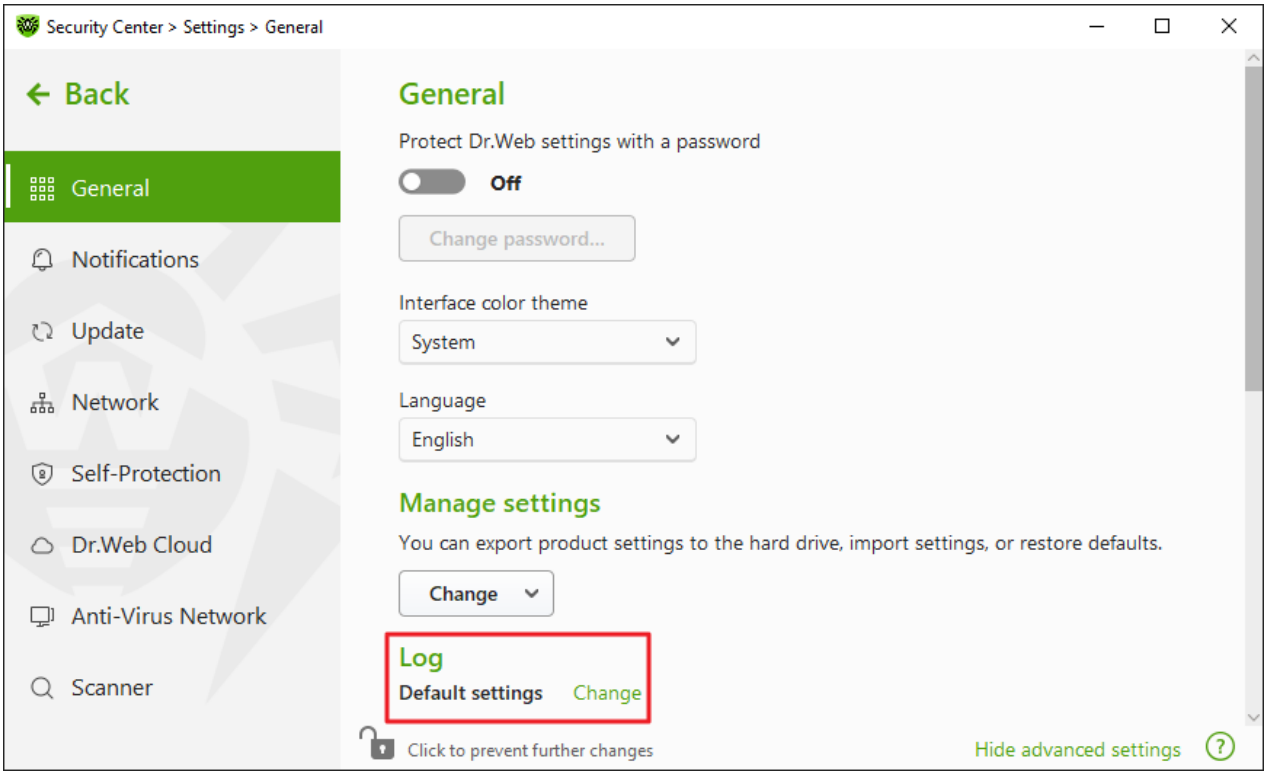

Figure 24. General Settings. Log

The window with detailed logging settings opens:

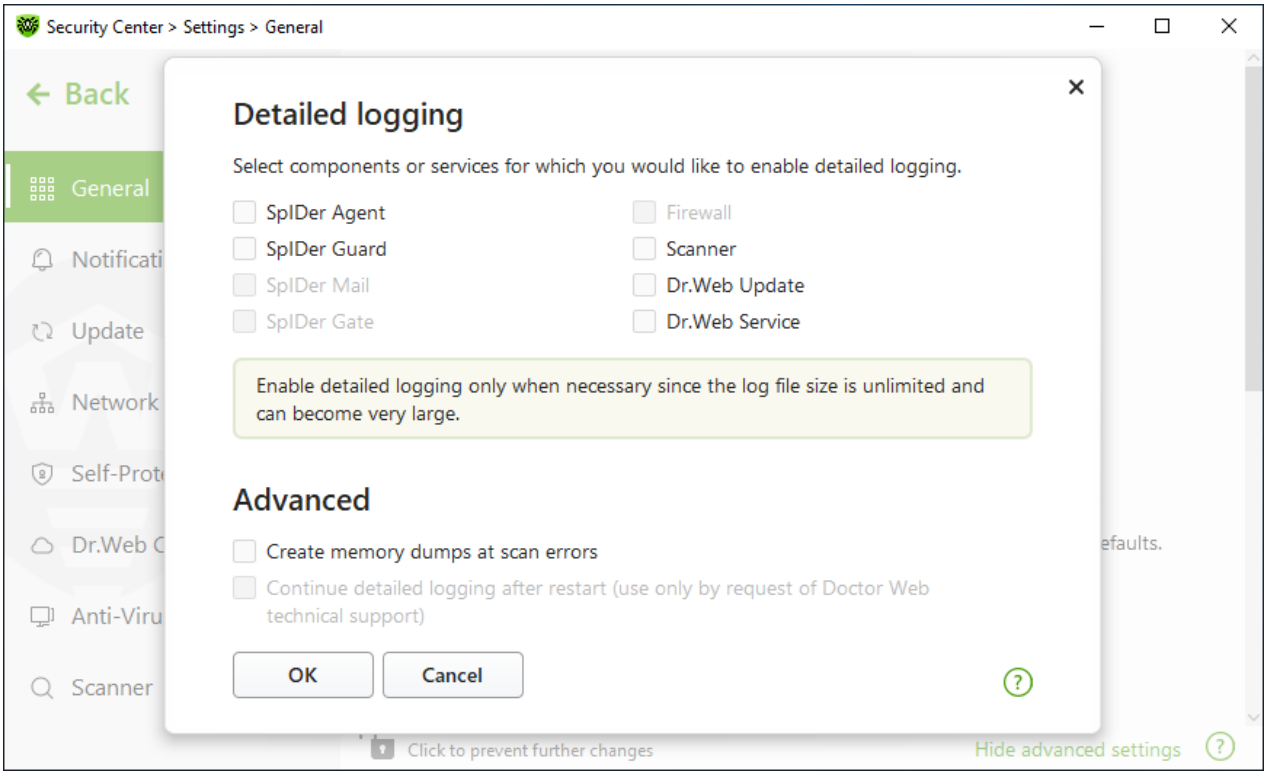

Figure 25. Operation logging settings

3. Select components, modules or services for which you would like to enable detailed logging. By default, the standard logging mode is enabled for all the Dr.Web components and the following information is logged:

Component	Information
SpIDer Agent	Time of updates and SpIDer Agent starts and stops, virus events, connections to anti-virus network, license events, Dr.Web component status, settings management (import, export), error notifications, and system reboot notifications. It is recommended that you use this mode to get detailed information about the sources of errors in the program operation.
SpIDer Guard	Time of updates and SpIDer Guard starts and stops, virus events, data on scanned files, names of packers, and content of scanned complex objects (archives, email attachments, file containers). It is recommended that you use this mode to determine the most frequent objects scanned by SpIDer Guard file monitor. If necessary, add these objects to the list of exclusions in order to increase computer performance.
Scanner	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.
Dr.Web Update	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.
Dr.Web Service	Information on Dr.Web components, changes in their settings, component starts and stops, preventive protection events, connections to anti-virus network.

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 Doctor Web technical support.

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

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

> Size of a log file is restricted to 10 MB by default (and 100 MB for SplDer Guard). If the log file size exceeds the limit, the content is reduced to:
>
> - Specified size if the current session information does not exceed the limit.
> - Size of the current session if the session information exceeds the limit.

9.1.6. 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.

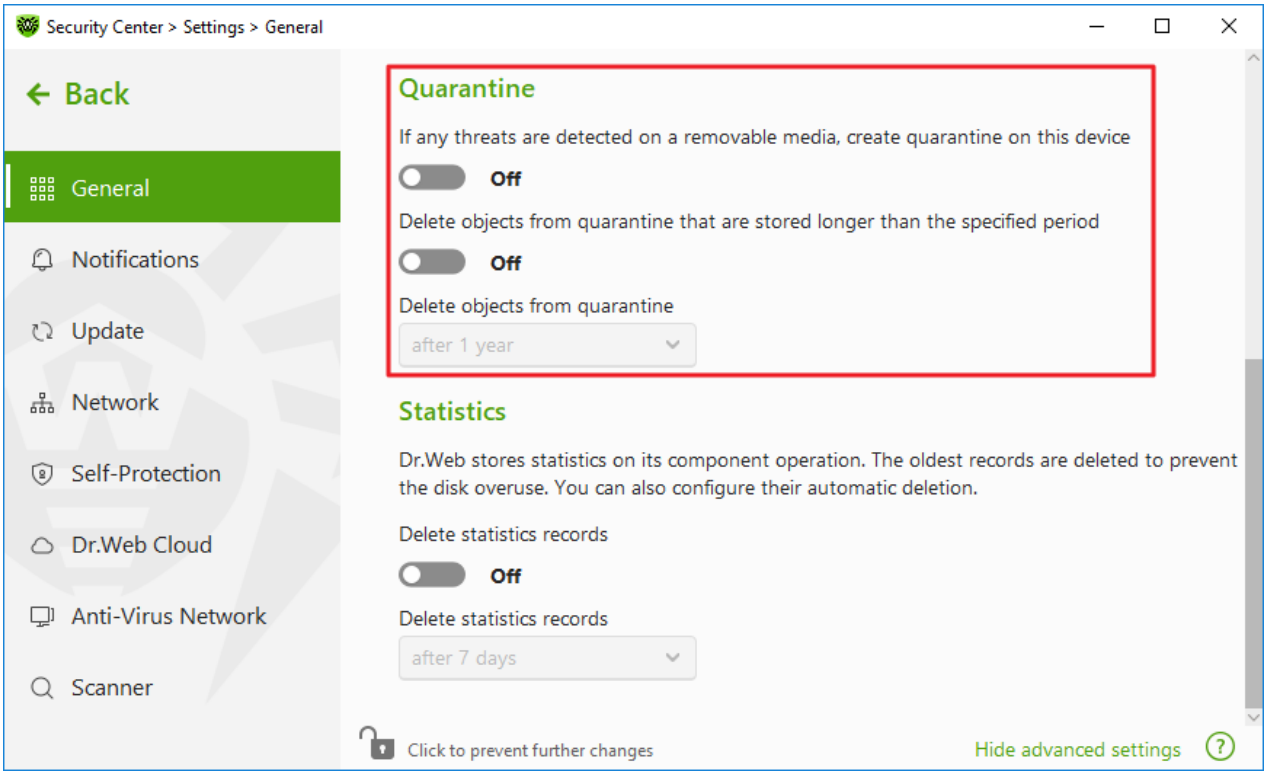

Figure 26. Quarantine settings

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.

9.1.7. 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.

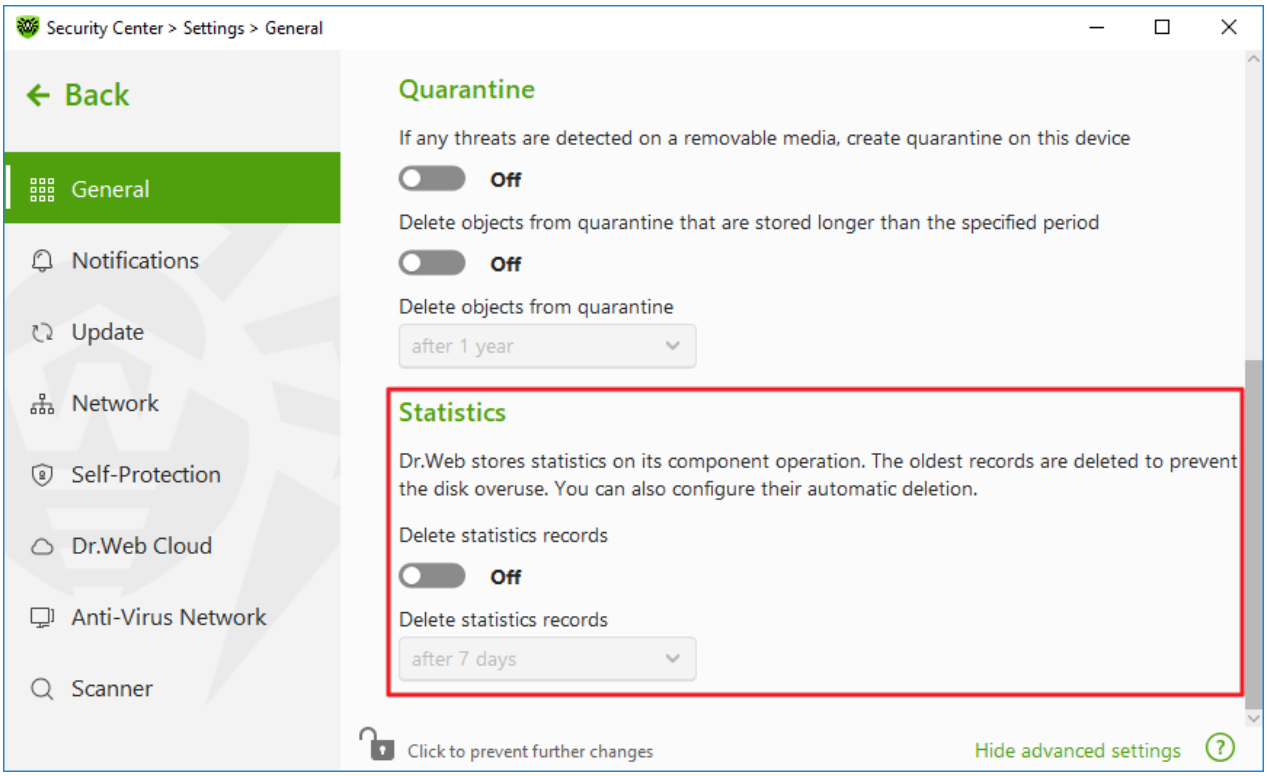

Figure 27. Statistics settings

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.

9.2. Notification Settings

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

In this section:

- Configuring notification parameters
- Configuring showing notifications on the desktop
- Configuring email notifications

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.

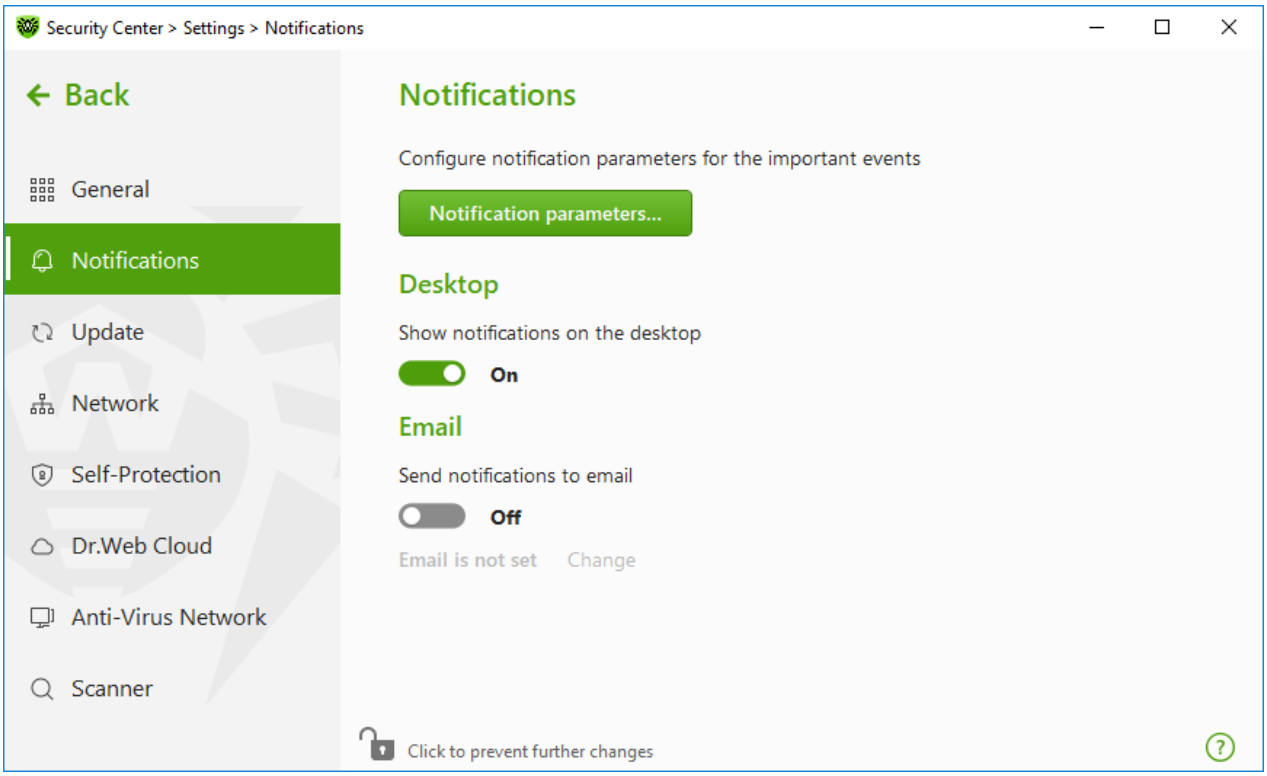

Figure 28. Notification settings

To configure notification parameters

1. Click **Notification parameters**.
2. Select notifications that you want to receive.
   - To display the notifications on the desktop, select a corresponding option in the **Desktop** column.
   - To receive email notifications, select check boxes in the **Email** column.

   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. By default, these notifications are enabled.
Major notifications	Important notifications on the following issues: • Virus databases are out of date. • Device is blocked. • Attempt to change system date and time is blocked. • Access to the protected object is blocked by Behavior Analysis. • Access to the protected object is blocked by Exploit Prevention. • Access to the protected object is blocked by Ransomware Protection. • Information about product updates and support

Notification type	Description
Minor notifications	Minor notifications on the following issues: • Successful update. • Update error. • Modification of the folder contents is blocked for the process. By default, these notifications are disabled except the notification on blocking an attempt of a process to modify folder contents.
License	Notifications on the following issues: • License expires. • The valid license is not found. • The current license is blocked.

3. If necessary, configure additional parameters:

Option	Description
Do not show notifications in full-screen mode	Hide notifications when an application is running in full-screen mode on your computer (e.g., a game or a movie). Clear this check box to display notifications regardless of the mode.

4. If you select one or more email notifications, configure sending emails from your computer.

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

- Priority updates installed and restart is required.
- To finish neutralizing threats, restart the computer.
- Automatic restart.
- Request for allowing a process to modify an object.
- Successful connection to a remote computer in the Anti-virus Network.
- New keyboard connected.

Pop-up notifications

In the notification settings window, enable the appropriate option to get pop-up notifications above Dr.Web icon in the Windows notification area.

Email notifications

To receive email notifications about events

1. In the notification settings window, enable the **Send notifications to email** option.
2. Specify the email address that you want to use for receiving notifications in the appeared window. You will need to confirm this email address at step 7.

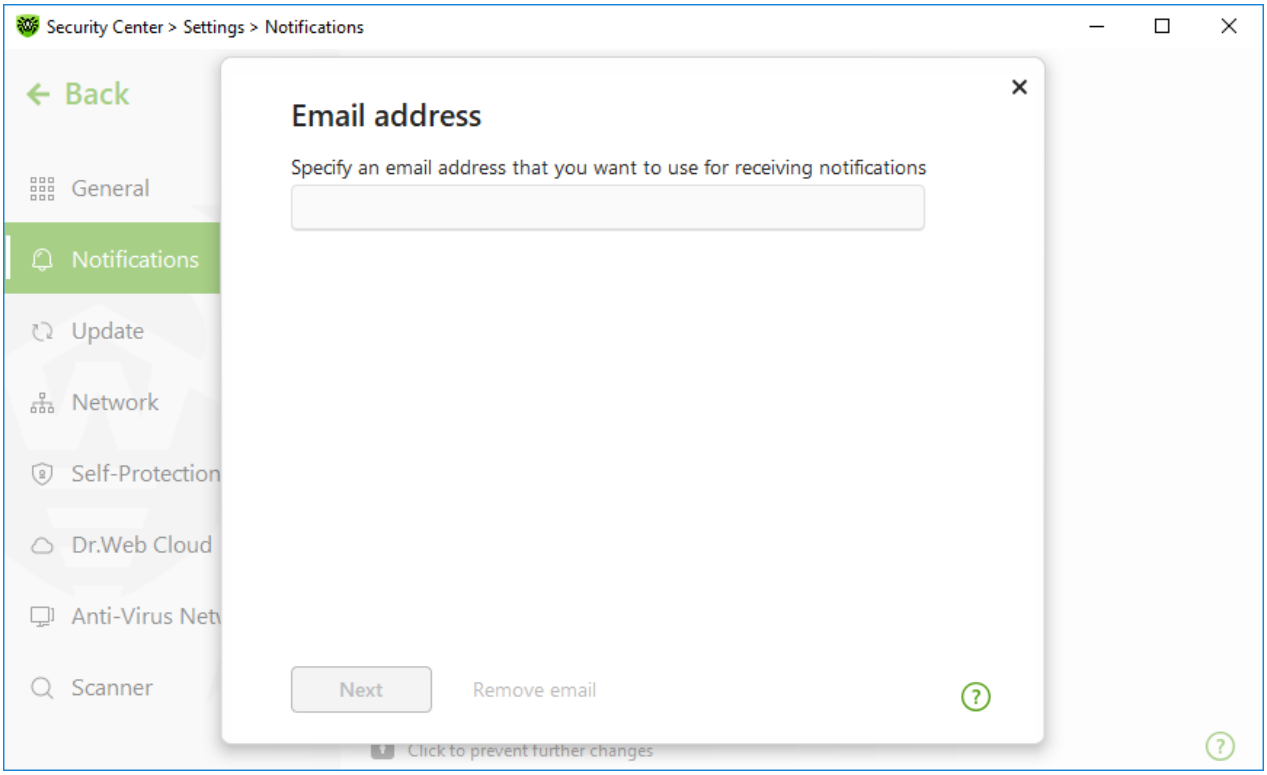

Figure 29. Specifying address for email notifications

3. Click **Next**.
4. In the open window, specify the data of the account that will be used to send notifications.
   - Select the mail server from the list and enter your account login and password.
   - If the required mail server is not on the list, select **Set manually**. In the open window, fill in the following fields:

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

Option	Description
Password	Enter the password for the login to be used when connecting to the mail server.
Use SSL/TLS	Select this check box to use SSL/TLS encryption when sending messages.
NTLM authentication	Select this check box to use NTLM authentication when connecting to the mail server.

5. Click **Send a test message** link to make sure that all the details are specified correctly. The message is forwarded to the email address that will be used to send notifications (specified at step 4).
6. Click **Next**.
7. Enter the conformation code that was sent to the email address specified at step 2. If you do not receive the message within 10 minutes, click **Send the code again**. If you do not enter the code, notifications to this email address will not be sent.

To change the email address and other parameters, in the notification settings window (see Figure Notification settings), click **Edit** and repeat all the actions starting from step 2.

9.3. Update Settings

Set the period for receiving updates and the source of updates for virus databases and components. You can also create an update mirror to receive updates on another computer.

You can configure the following Dr.Web update parameters:

- Update frequency
- Update source
- Updating components
- Update mirror

To open update 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 **Update** at the left of the window.

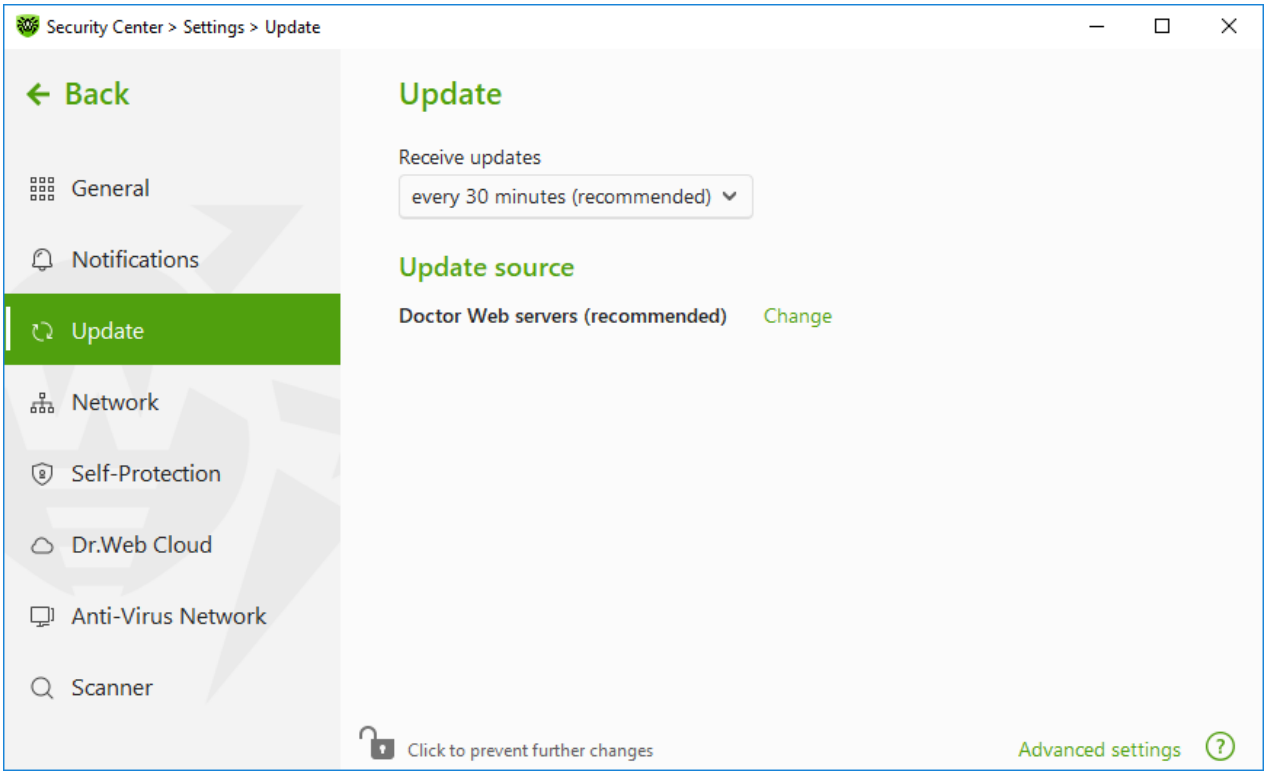

Figure 30. Update settings

Update frequency

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

Automatic update is performed in the background mode. You can also select the option **Manually** from the drop-down menu. In this case, you will have to manually run the Dr.Web update.

Configuring update source

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

To specify the update source that suits you best

1. In the update settings window (see Figure Update settings) , in the **Update source** group, click the **Edit** link. The update source settings window opens.

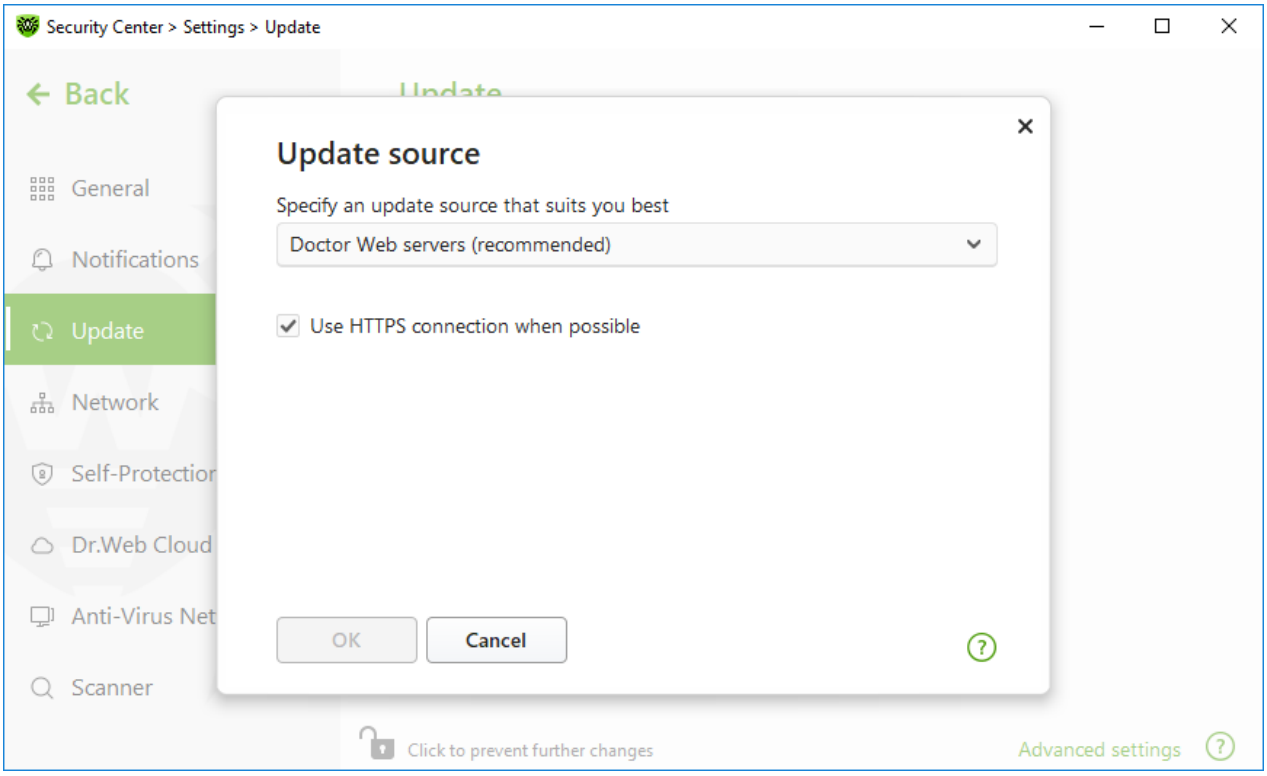

Figure 31. Configuring update source

2. Select an update source that suits you best from the drop-down list.
   - **Doctor Web servers (recommended)**. Updating from Doctor Web servers via the internet. If you want to download updates via a secure protocol when it is possible, select the **Use HTTPS connection when possible** check box.
   - **Local or network folder**. Updating from local or network folder to which the updates have been copied. Specify the path to the folder (by clicking **Browse** button or by entering the path manually using UNC), enter the user name and password if necessary.
   - **Anti-Virus Network**. Updating from a local network using a computer with Dr.Web product installed and an update mirror created. Select the computer that will be used as an update source.
3. To save the changes, click **OK**.

> If Dr.Web product of 12.0 version is already installed on the computer, do not select a computer with previous Dr.Web product versions installed as an update source as it may lead to critical operation issues.

Advanced settings

To open advanced settings, click the **Advanced settings** link in the **Update** window (see Figure Update settings).

Configuring updating components

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

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

Creating update mirror

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

To set your computer as an update mirror

1. In the update settings window (see Figure Update settings), click the **Advanced settings** link and enable the update mirror using the switcher. The update mirror settings window opens.

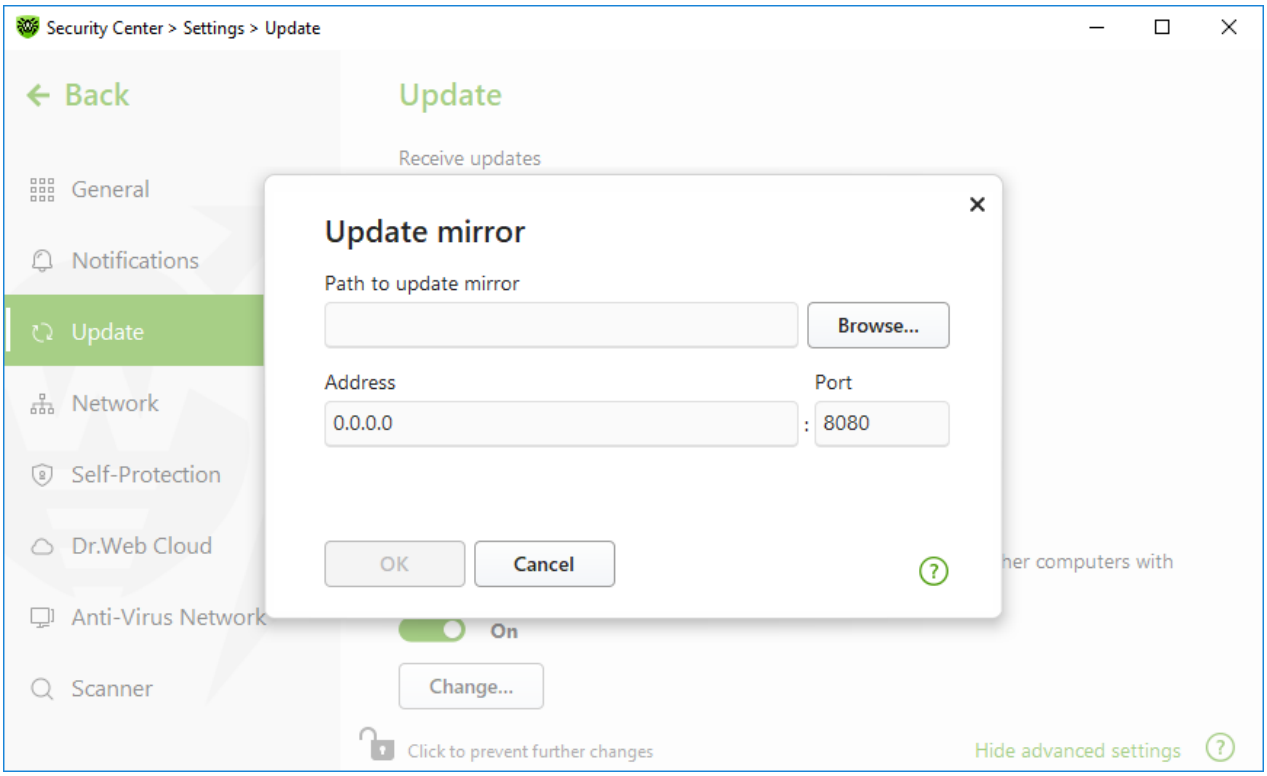

Figure 32. Configuring update mirror

2. Click **Browse** and select a folder to copy updates into. Please select an empty folder or create a new one. If the selected folder is not empty, all its contents will be deleted. You can also specify the path to the folder in UNC format.

3. If your computer is connected to several subnets, you can specify the IP address available to computers of only one subnet. You can also specify the port for HTTP server to receive connection requests.
   - In the **Address** field, specify the host name or IP address in Ipv4 or Ipv6 formats.
   - In the **Port** filed, specify any free port.
4. To save the changes, click **OK**.

The frequency of the mirror updates corresponds to the value selected in **Receive updates**.

9.4. Network

You can configure the parameters of connection to the proxy server.

In this section:

- Proxy server connection settings

To open network 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 **Network** at the left of the window.

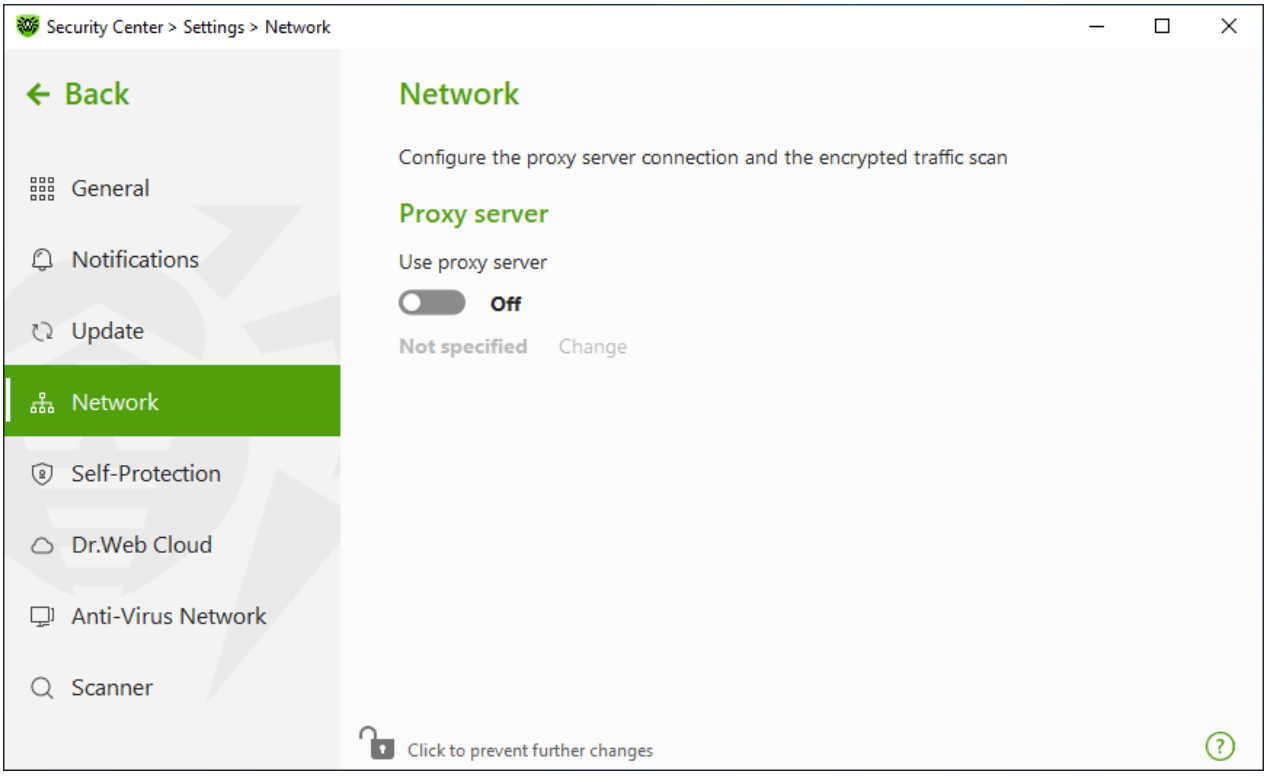

Figure 33. Connecting to proxy server

Proxy server usage

By default, all components use direct connection mode. If necessary, you can enable use of a proxy server and specify its connection settings. For this:

1. Enable **Use proxy server** option by using the switcher .
2. Click **Edit** to specify the following proxy server parameters:

Option	Description
Type	Select the protocol to connect to the proxy server.
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 (for HTTP only).

9.5. 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.

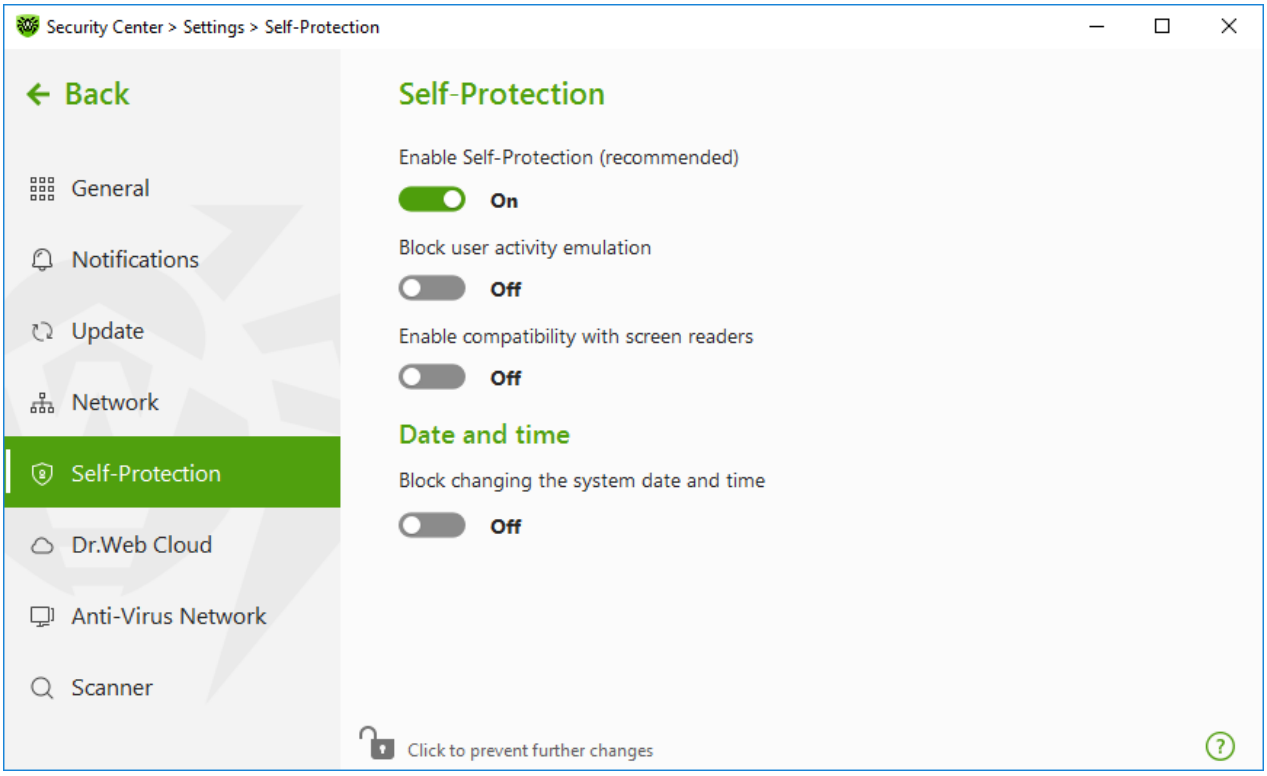

Figure 34. Dr.Web self-protection parameters

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, license removal 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. You can configure notification parameters to be informed on an attempt to change the system time.

9.6. Dr.Web Cloud

You can connect to the Doctor Web cloud service and take part in the Dr.Web quality improvement program. The cloud service collects information on last threats detected on user stations, ensuring virus databases are constantly updated and the newest threats are neutralized effectively. Moreover, data is processed faster on the cloud service than on the local computer.

In this section:

- Cloud service
- Software quality improvement program

To enable or disable Dr.Web Cloud

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 **Dr.Web Cloud** at the left of the window.
5. Enable or disable Dr.Web Cloud by using the switcher.

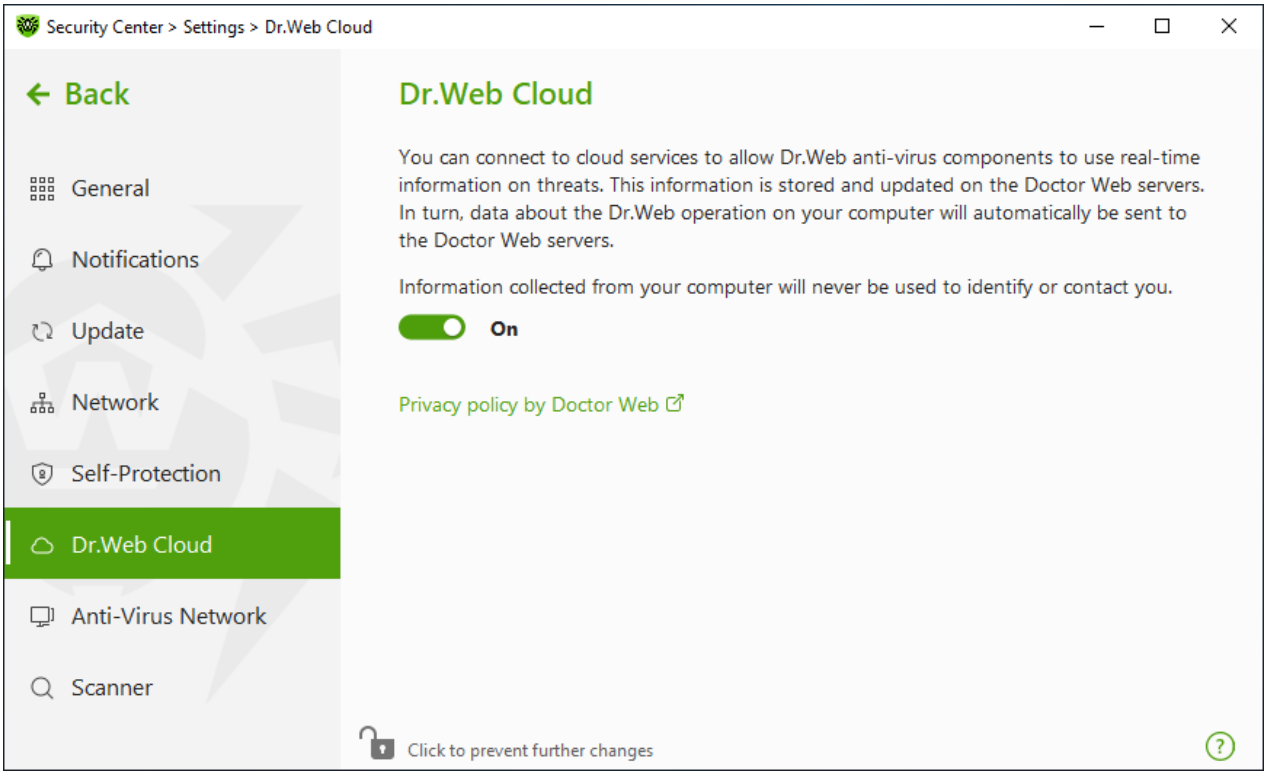

Figure 35. Connecting to Dr.Web Cloud

Cloud service

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

Depending on update settings, information on threats, that is used by your anti-virus protection components, could become obsolete. The use of cloud services allows you to protect users of your computer from infected files.

Software quality improvement program

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

Click the **Privacy policy by Doctor Web** link to look through a privacy policy on the Doctor Web official website.

9.7. Remote Access to Dr.Web

You can enable remote control of your anti-virus from other computers of the local network using the Anti-Virus Network component. Anti-virus network allows you to remotely control the security state (view statistics, enable or disable components, and change their settings) and

receive updates via local network. To use a computer as an update source for other anti-virus network computers with Dr.Web installed, configure Update mirror on it.

To enable or disable Dr.Web remote control

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 **Anti-Virus Network** at the left of the window.
5. Enable or disable remote control using the switcher.

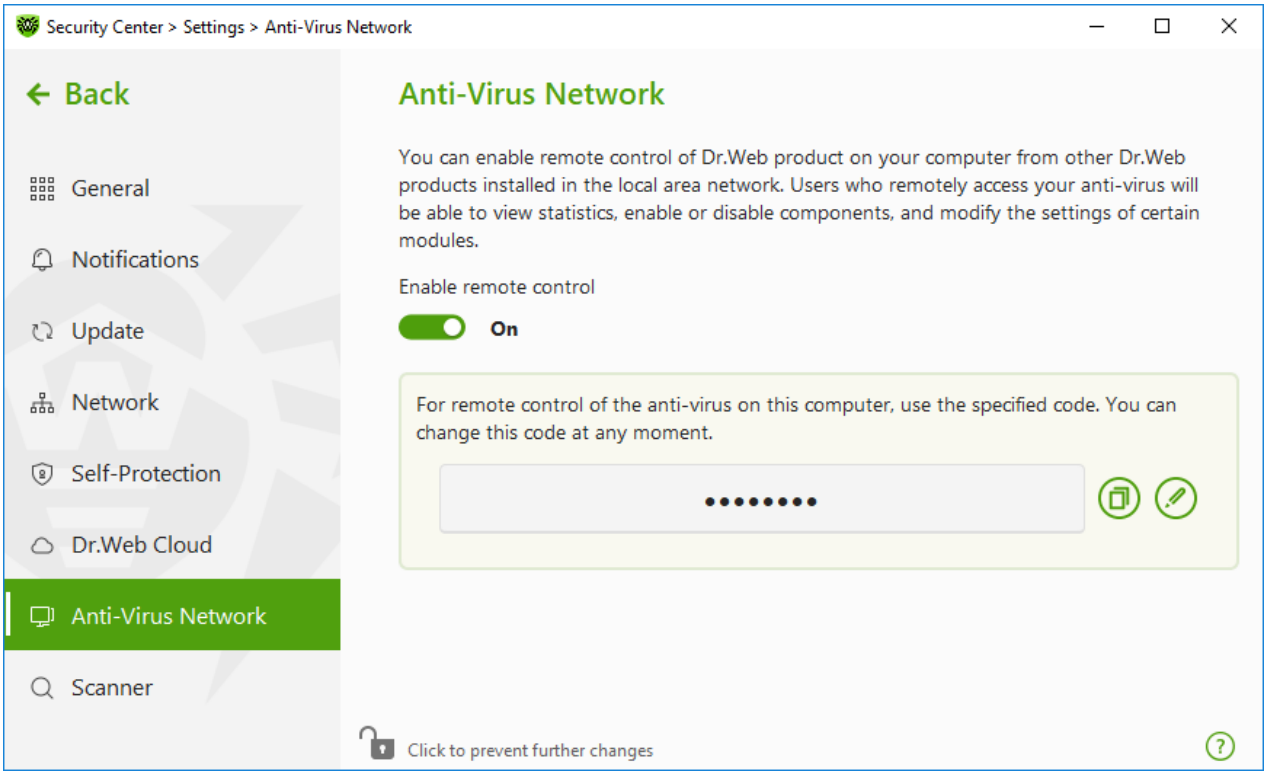

Figure 36. Switching on the anti-virus remote access

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

Remote control allows you to view statistics, enable or disable components, and change their settings. Quarantine, Scanner, Data Loss Prevention and Anti-Virus Network are not available.

9.8. 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.

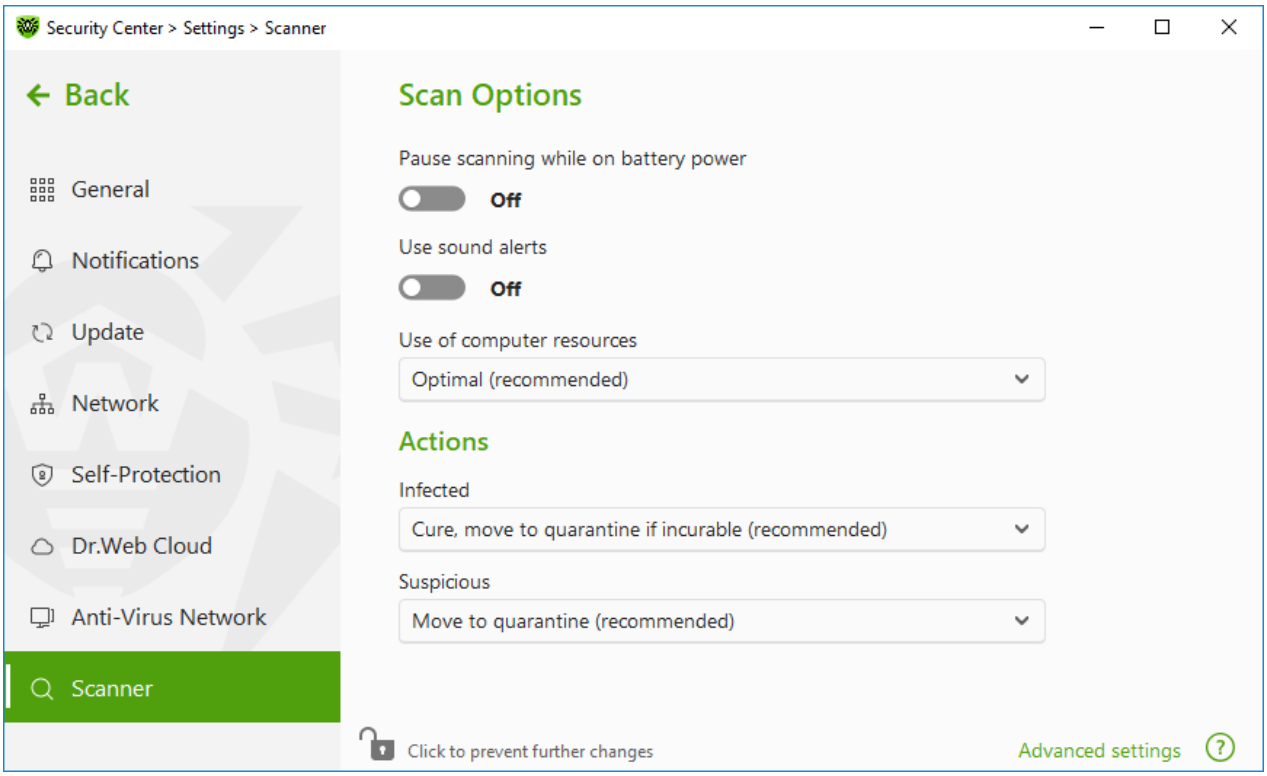

Figure 37. Scanner settings

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	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. 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.
Cure, delete if incurable	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. 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.
Delete	Instructs to delete the object. This action is not available for boot sectors.
Move to Quarantine	Instructs to move the object to a specific folder of Quarantine. This action is not available for boot sectors.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.

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.

10. 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.

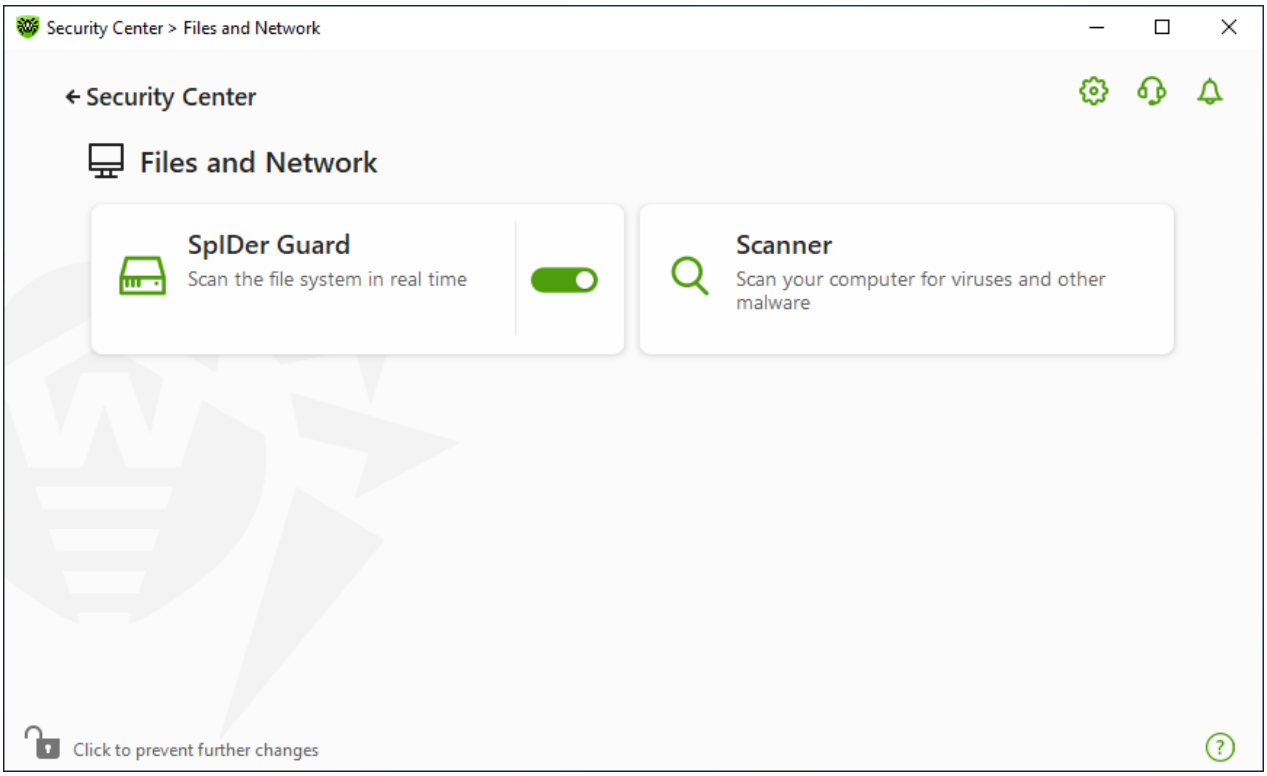

Figure 38. The Files and Network window

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.

- Scanner is a component that scans object on user demand or according to schedule.

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

10.1. 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.

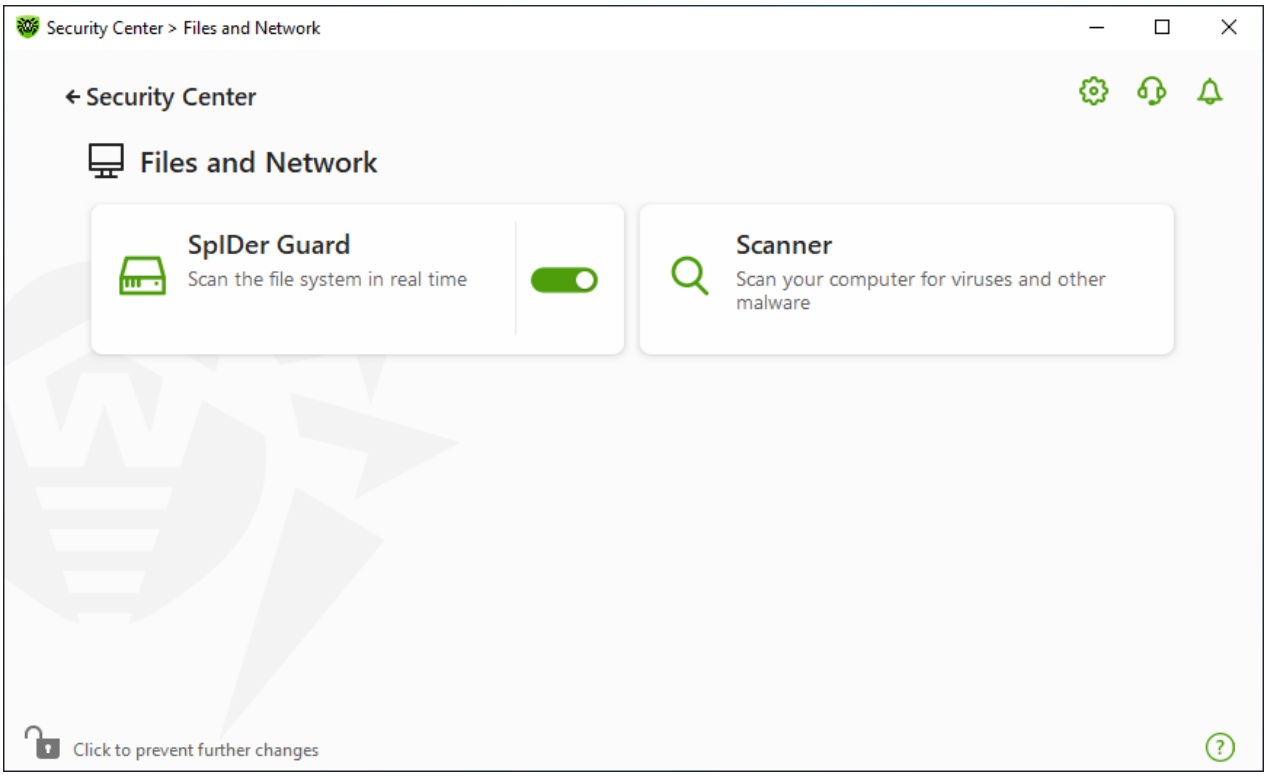

Figure 39. Enabling/Disabling SpIDer Guard

In this section:

- SpIDer Guard operation peculiarities
- Removable media scan
- Actions for detected threats

- Selecting the scan mode by SpIDer Guard
- Advanced settings

See also

- Excluding files and folders from scanning
- Excluding applications from scanning

SpIDer Guard operation peculiarities

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

> SpIDer 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, SpIDer 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 SpIDer Guard.

SpIDer Guard file system monitor parameters

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

To open SpIDer 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 **SpIDer Guard** tile. A component parameters window opens.

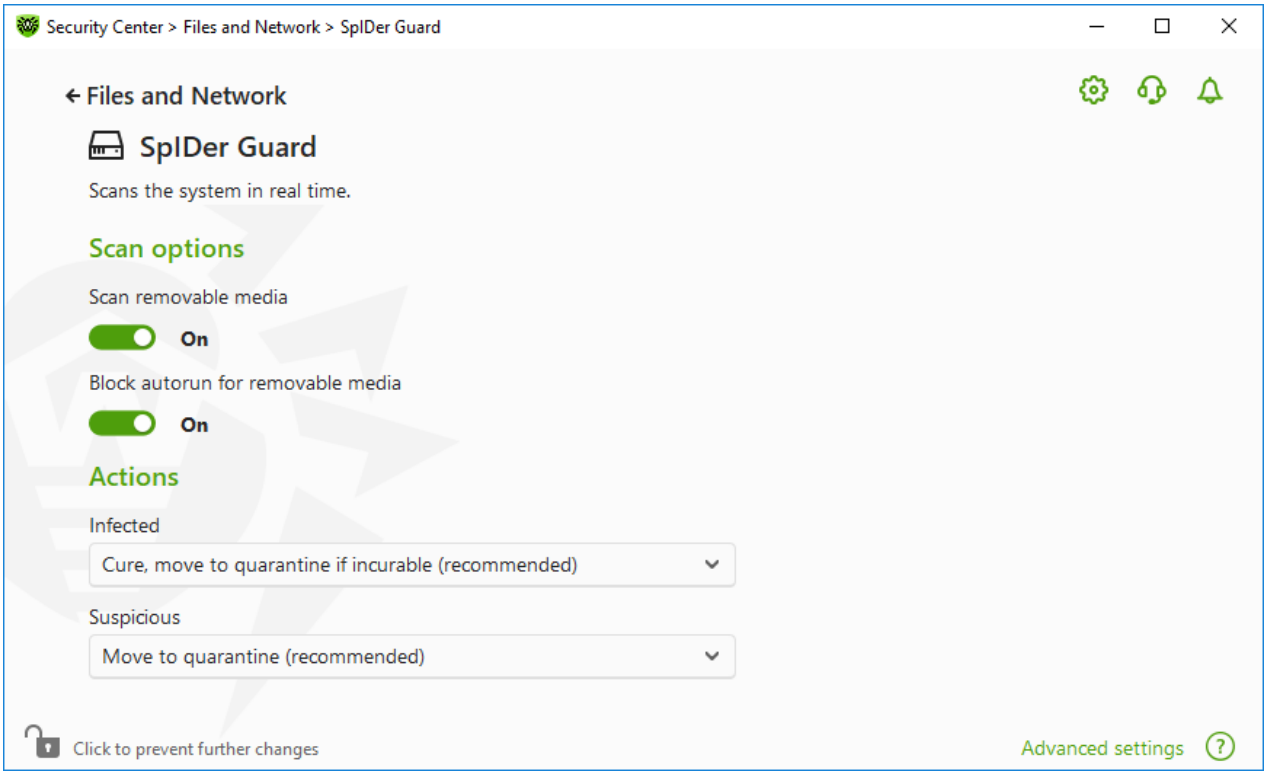

Figure 40. The file system monitor parameters

Removable media scan

By default, SpIDer 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 SpIDer 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, SpIDer 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 SpIDer Guard.

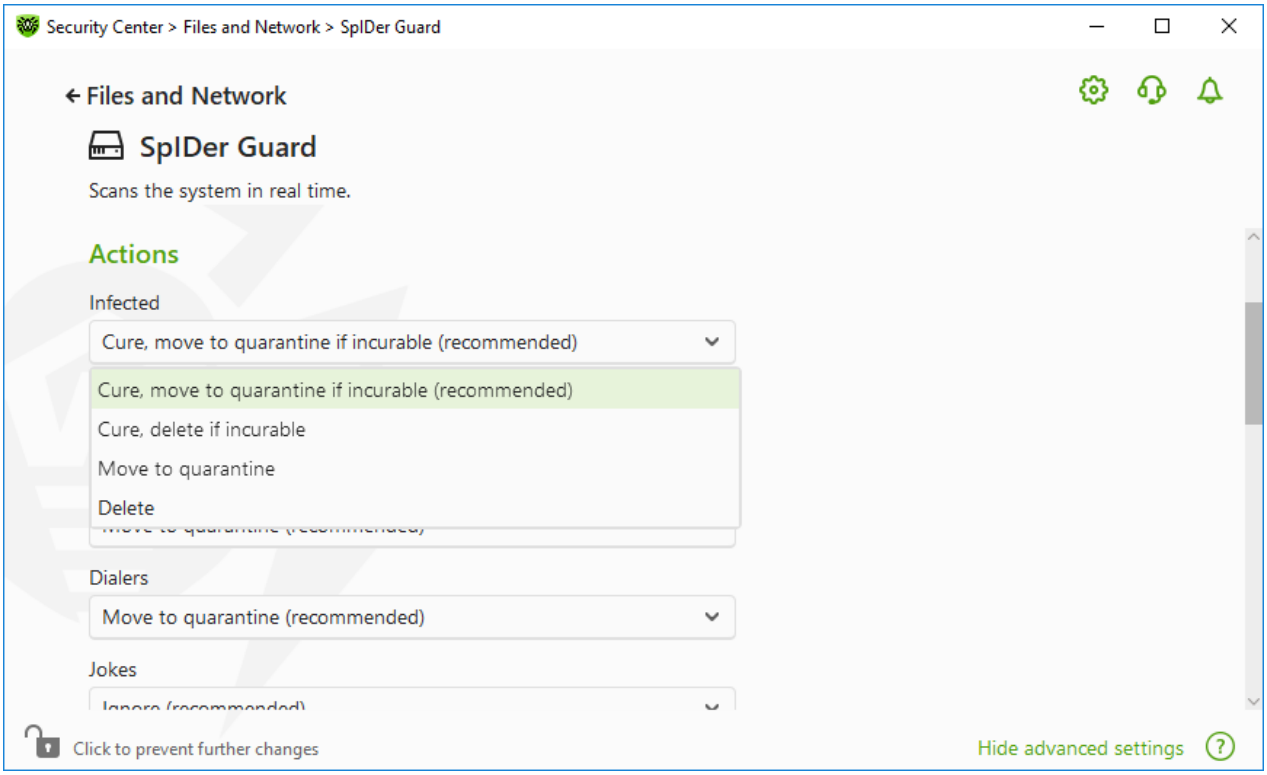

Figure 41. Configuring actions applied to threats

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	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. 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.
Cure, delete if incurable	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.

Action	Description
	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.
Delete	Instructs to delete the object. This action is not available for boot sectors.
Move to Quarantine	Instructs to move the object to a specific folder of Quarantine. This action is not available for boot sectors.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.

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: • For objects on hard drives, an attempt to execute a file, create a new file, or add a record to an existing file or boot sector. • For objects on removable media, an attempt to access file or boot sectors in any way (write, read, execute). It is recommended that you use this mode after a thorough scan of all hard drives by Dr.Web Scanner. With this mode activated, SpIDer 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.
Paranoid	In this mode, SpIDer Guard scans files and boot sectors on hard or network drives and removable media at any attempt to access them (create, write, read, execute). This mode ensures maximum protection but considerably reduces computer performance.

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 SpIDer 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 Server 2016 and later)

Heuristic analysis

By default, SpIDer Guard performs scan using heuristic analysis. If this option is disabled, SpIDer 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 SpIDer 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.

10.2. 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

10.2.1. Scan Start and Scan Modes

To start scan of the files

> When using Windows Server 2008 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.

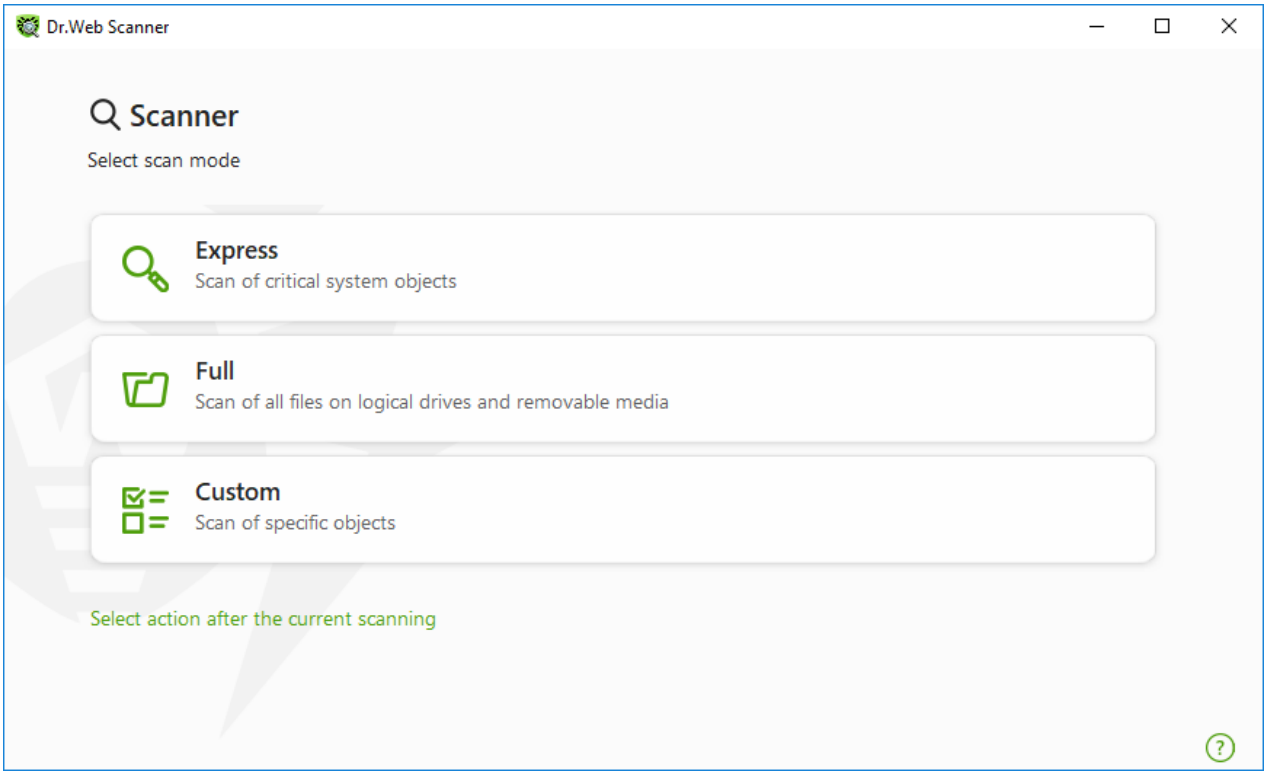

Figure 42. Selecting the scanning mode

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
Express	In this mode, Scanner checks the following: • Boot sectors of all disks

Scan mode	Description
	• Random access memory • Boot disk root folder • Windows system folder • User documents folder (“My Documents”) • Temporary files • System restore points • Presence of rootkits (if the process is run with administrative privileges) Scanner does not check archives and email files in this mode.
Full	In this mode, random access memory and all hard drives (including boot sectors of all disks) are scanned. Moreover, Scanner runs a check for rootkits.
Custom	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 ⊕.

10.2.2. 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.

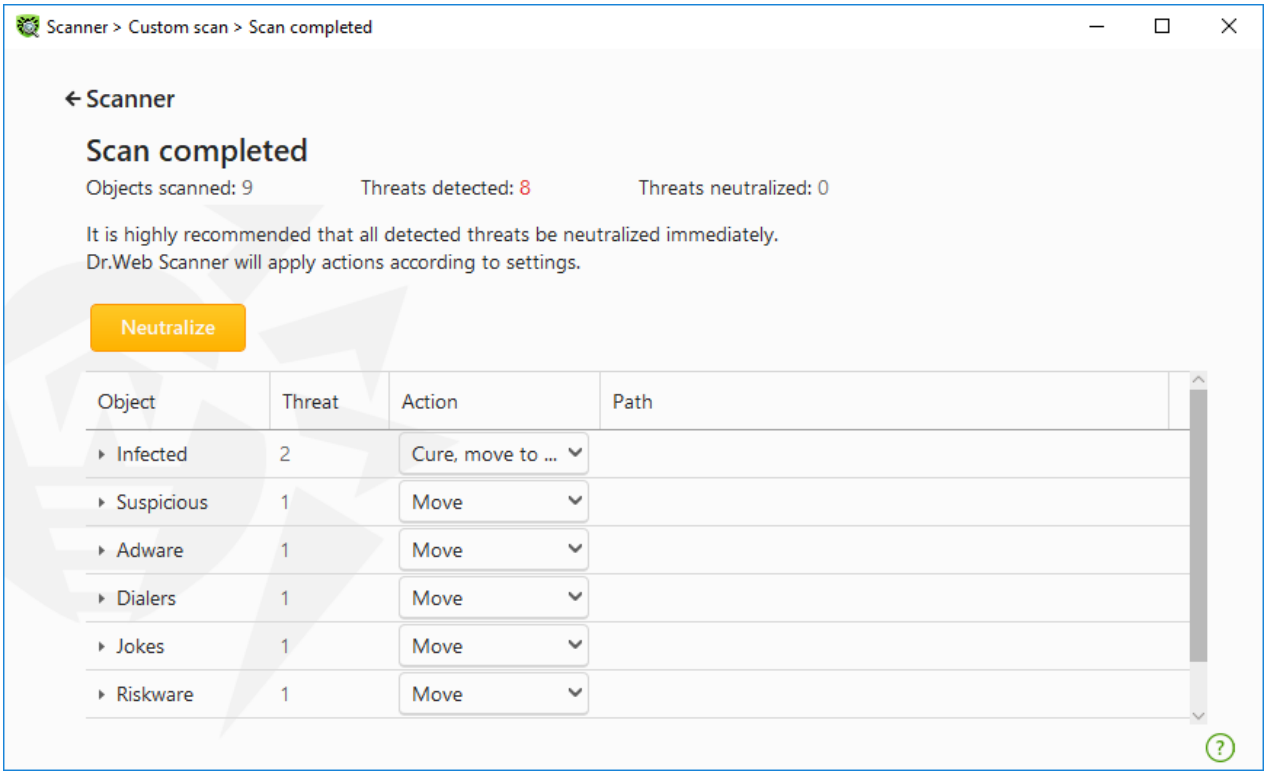

Figure 43. Selecting an action after a scan

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 **Boot sector** if a boot sector is infected, or **Master Boot Record** if an MBR of the hard drive is infected).
Threat	The names of viruses or virus modifications as per the internal classification of Doctor Web. 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 Scanner settings. 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.

10.2.3. Additional Options

This section contains information about the additional Scanner options:

- Command-Line Scanning Mode
- Console Scanner
- Automatic Launch of Scanning

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. Automatic Scanner launch is performed in this mode according to schedule.

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;

11—key file is not found or does not support Console Scanner;

12—Scanning Engine did not start;

255—scanning was aborted by user request.

Scanning Your System via the Task Scheduler

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

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

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

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

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

11. 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.

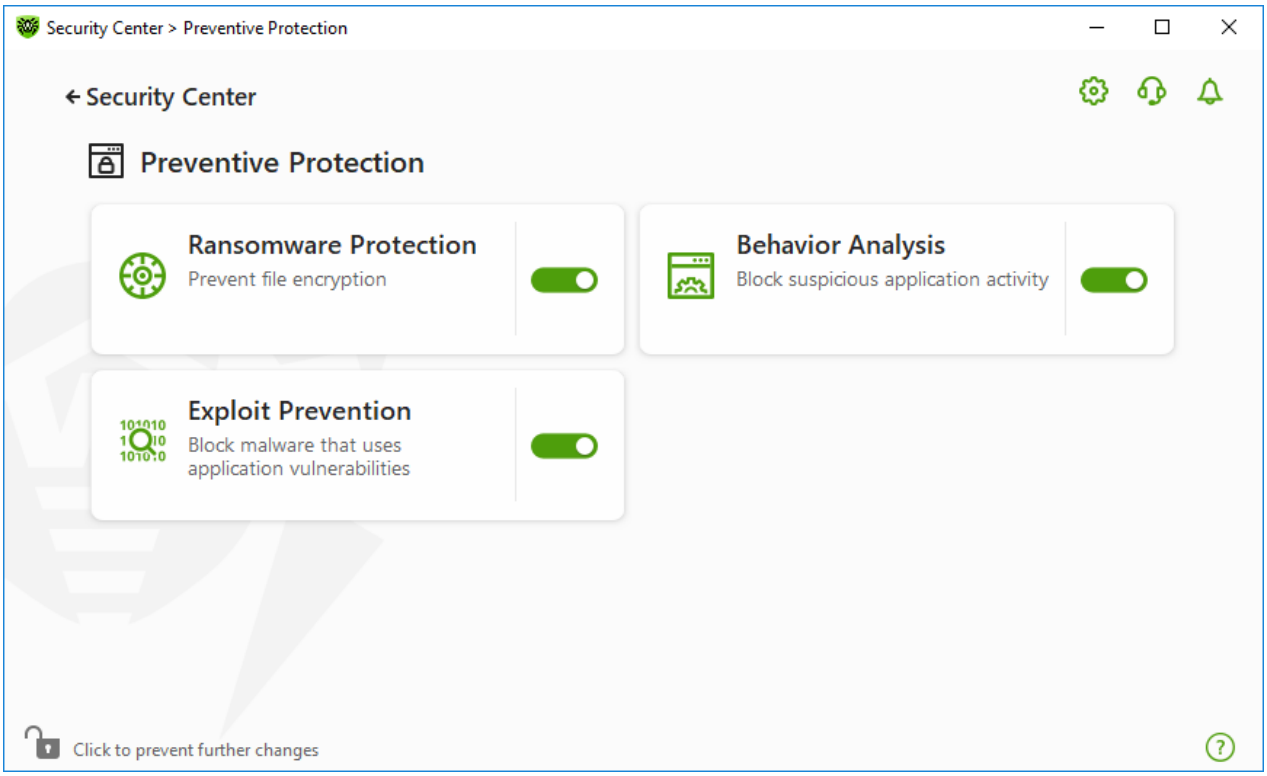

Figure 44. Preventive Protection window

Enable and disable protection components

Enable or disable the required 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:

- Ransomware Protection—prevent user files encryption.
- Behavior Analysis—configure application access to the system objects.

- Exploit Prevention—block the usage of application vulnerabilities.

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

11.1. Ransomware Protection

Ransomware Protection allows detection of processes that attempt to encrypt user 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 enable or disable Ransomware Protection

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.
3. Enable or disable Ransomware Protection by using the switcher.

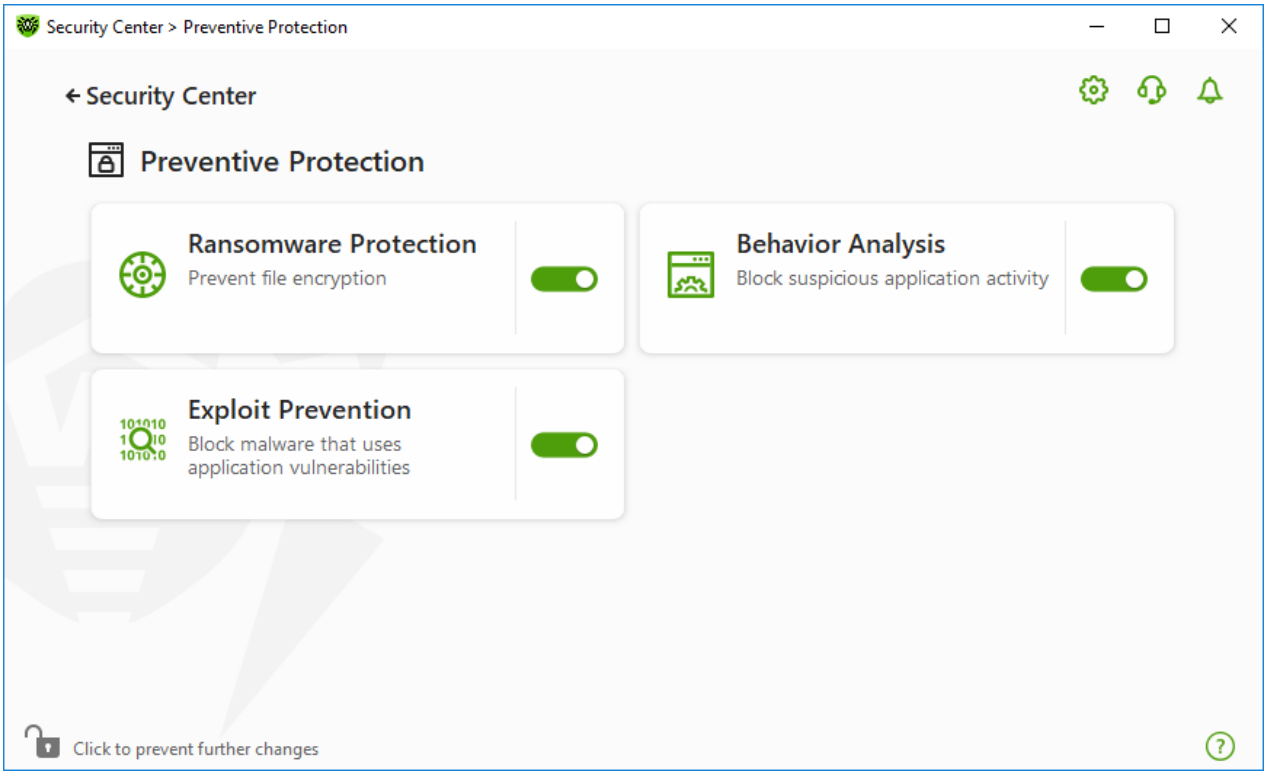

Figure 45. Enabling/Disabling Ransomware Protection

In this section:

- Configuring reaction to application attempts to encrypt files
- Scan exclusions

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.

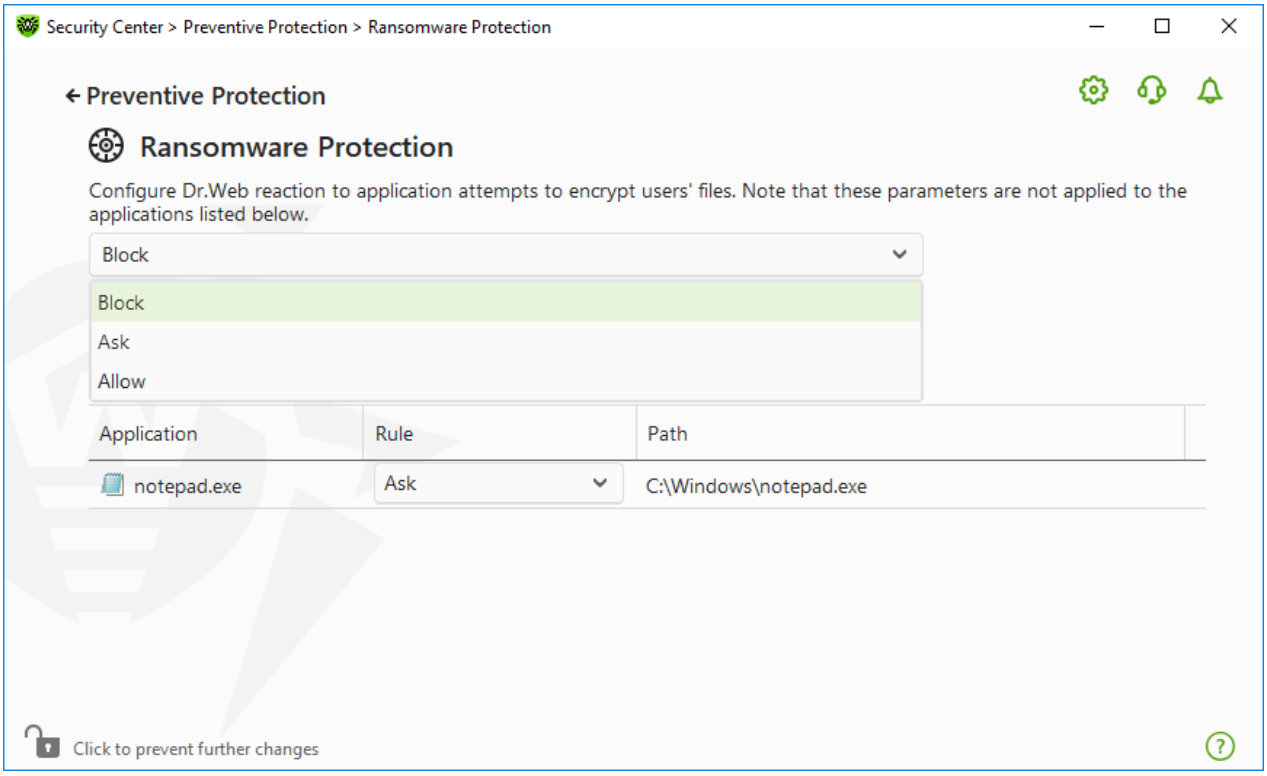

Figure 46. Selecting Dr.Web reaction

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

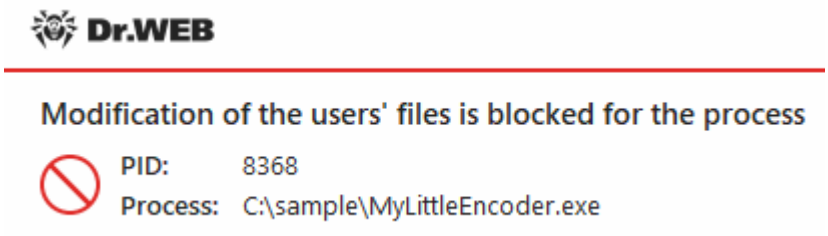

Figure 47. Notification example with a blocked application attempt to modify user files

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

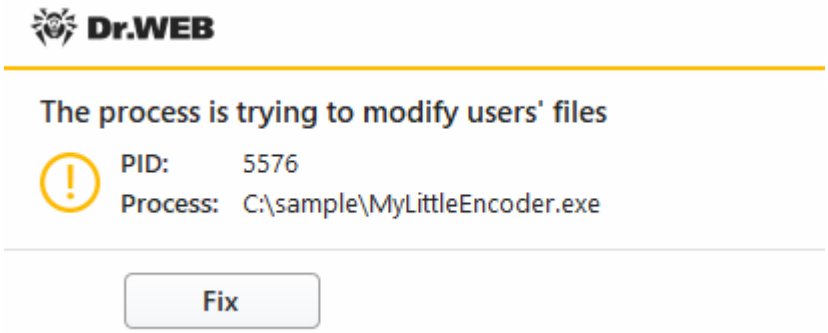

Figure 48. Notification example with an application attempt to modify user's files

- 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 and email notifications on Ransomware Protection actions.

See also:

- Notifications

List of applications, excluded from the scanning

You can create a list of applications, excluded from Ransomware Protection scanning. The following management elements are available to work with objects in the list:

- The button—add the application to the exclusion list.
- The button—delete the application from the exclusion list.

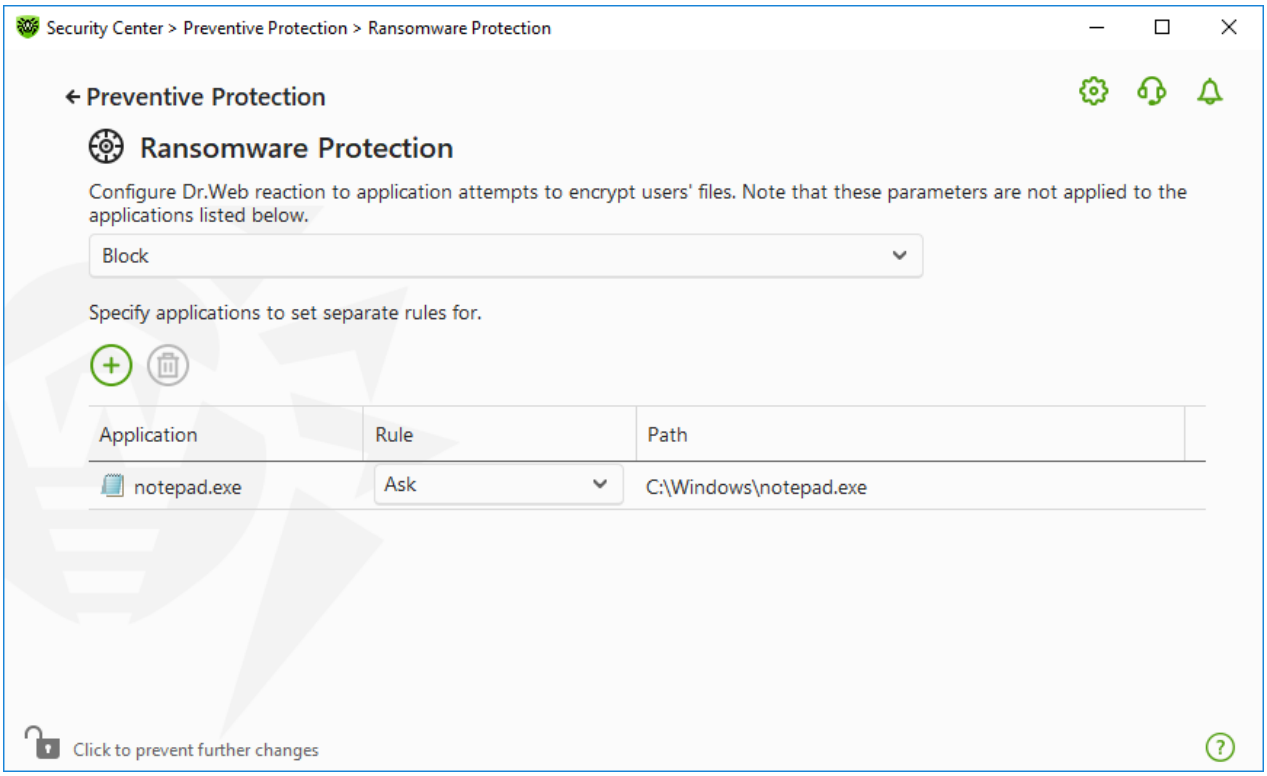

Figure 49. Excluding from Ransomware protection scanning

To add an application to the list

1. Click ⊕ and select a necessary application in the open window.
2. Click **OK**.

To protect your data from unauthorized changes, you can also add files to the list of protected files.

11.2. 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 determine whether an application is malicious, the component uses the real-time data from Dr.Web cloud service.

To enable or disable Behavior Analysis

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.
3. Enable or disable the Behavior Analysis component by using the switcher.

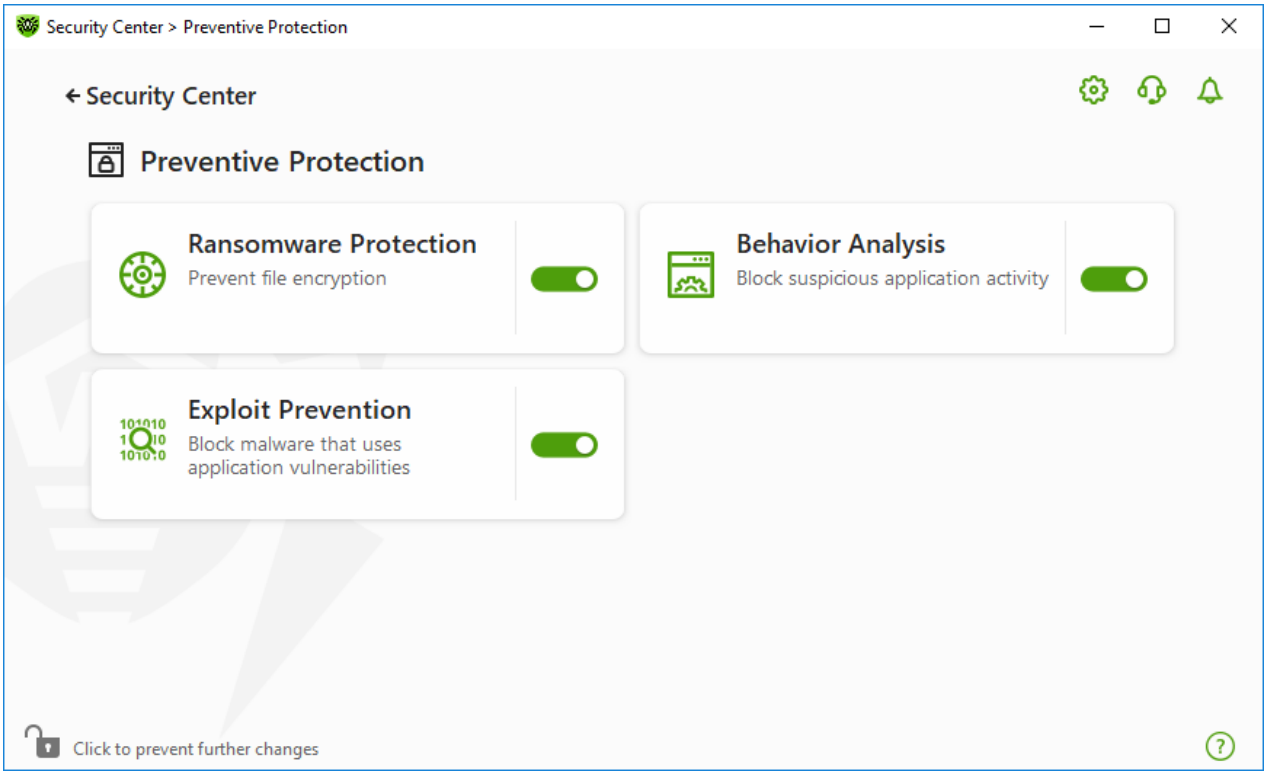

Figure 50. Enabling/Disabling the Behavior Analysis component

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.

To open Behavior Analysis 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 **Behavior Analysis** tile. A component parameters window opens.

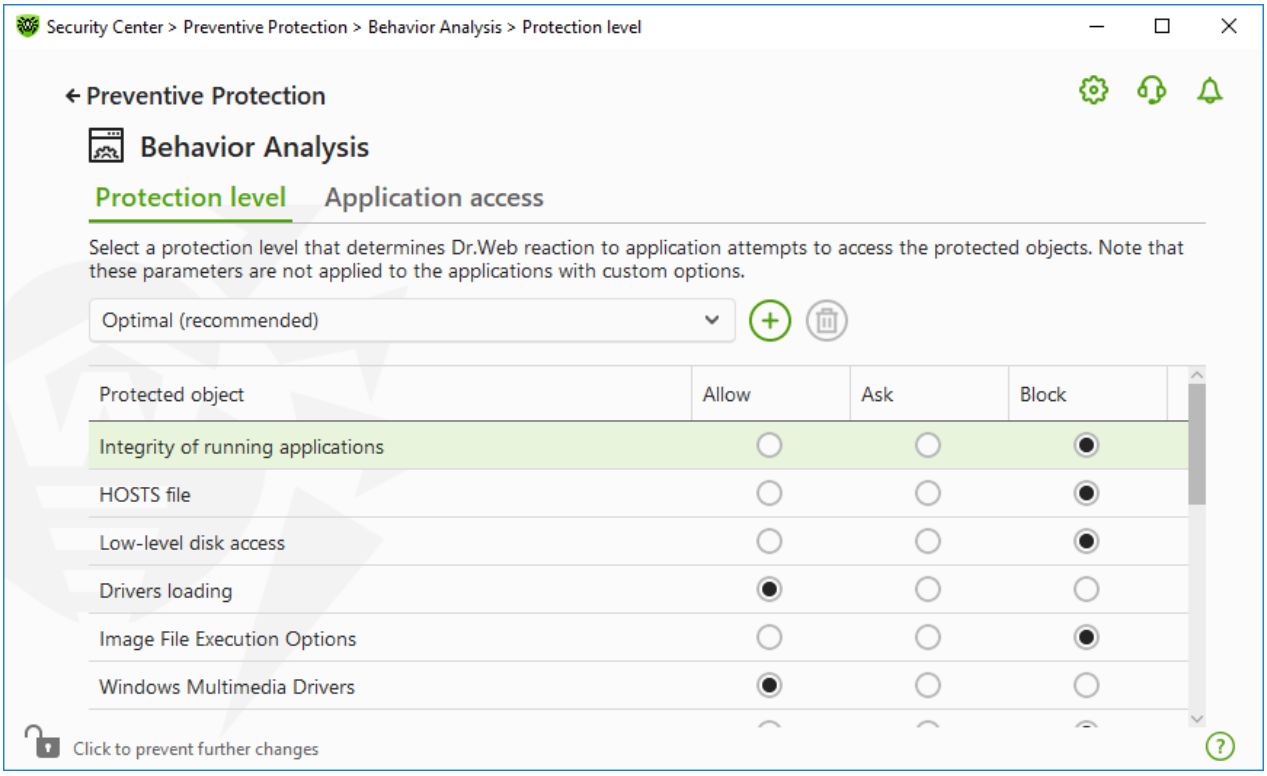

Figure 51. Behavior Analysis parameters

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
Optimal (recommended)	This mode is set by default. Dr.Web disables automatic changes of system objects, whose modification explicitly signifies a malicious attempt to harm the operating system. It also blocks low-level application access to disk and protects the HOSTS file from modification, if it explicitly signifies a malicious attempt to harm the operating system. Only actions by the applications that are not trusted, are blocked.
Medium	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. Using this mode may lead to compatibility problems with legitimate software that uses the protected registry

Protection level	Description
	branches.
Paranoid	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.
User-defined	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:

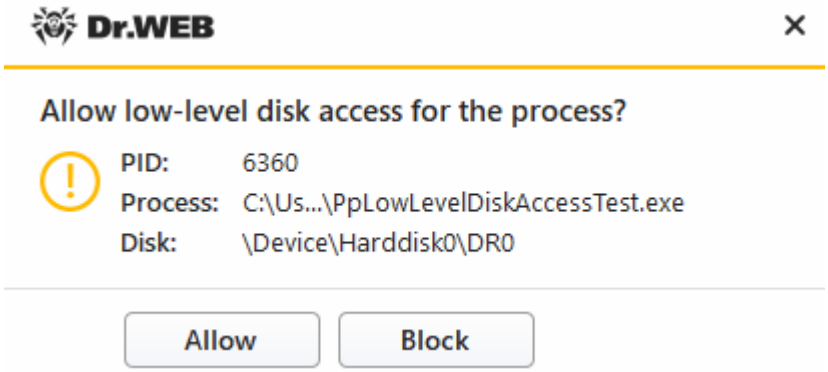

Figure 52. Notification example with an access to a protected object request

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

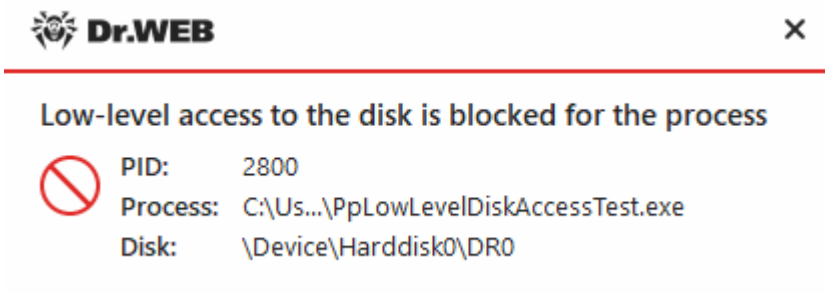

Figure 53. Notification example with a blocked access to a protected object

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 and email 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.

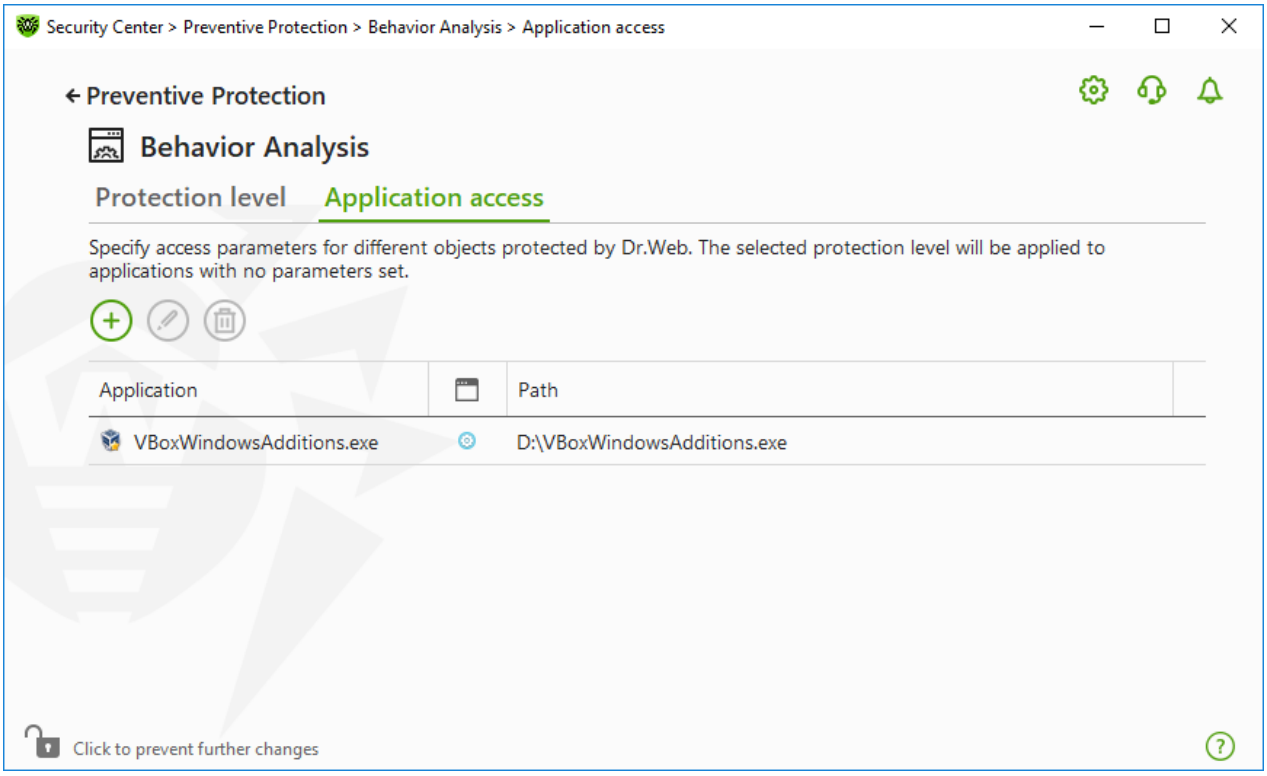

Figure 54. Application access parameters

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.

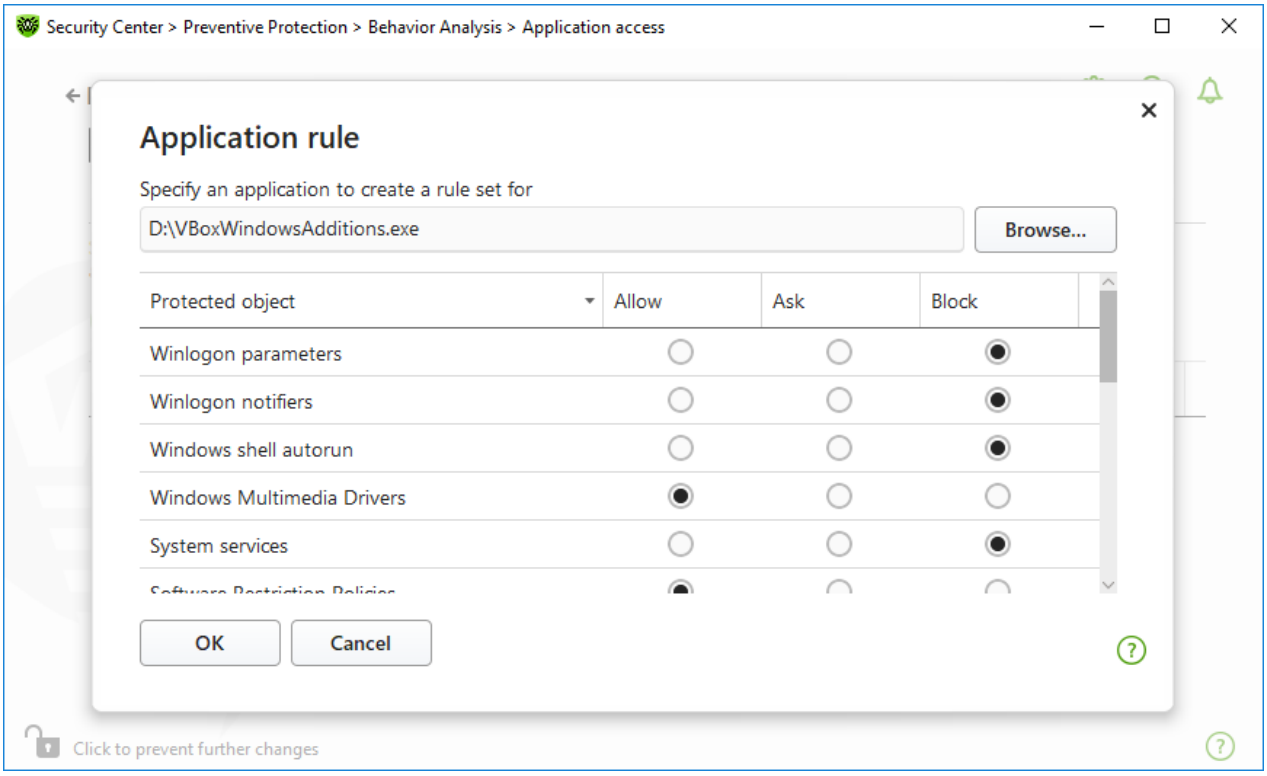

Figure 55. Adding a rule set for an application

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	Other options allow protection of the following registry branches from modification (in the system profile as well as in all the users' profiles). Image File Execution Options • `Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` Windows Multimedia Drivers:

Protected object	Description
	• `Software\Microsoft\Windows NT\CurrentVersion\Drivers32` • `Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers` Winlogon registry keys: • `Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL` Winlogon notifiers: • `Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify` Windows registry startup keys: • `Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib` Executable file associations: • `Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk` (keys) • `Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile` (keys) Software Restriction Policies (SRP): • `Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\*\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers` • `Software\Microsoft\Windows\CurrentVersion\Group Policy Objects\*\Software\Policies\Microsoft\Windows\SrpV2` • `Software\Policies\Microsoft\Windows\Safer` • `Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers` • `Software\Policies\Microsoft\Windows\SrpV2` Browser Helper Objects for Internet Explorer (BHO): • `Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects` Autorun of programs: • `Software\Microsoft\Windows\CurrentVersion\Run` • `Software\Microsoft\Windows\CurrentVersion\RunOnce` • `Software\Microsoft\Windows\CurrentVersion\RunOnceEx` • `Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup` • `Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup` • `Software\Microsoft\Windows\CurrentVersion\RunServices` • `Software\Microsoft\Windows\CurrentVersion\RunServicesOnce`

Protected object	Description
	Autorun of policies: • `Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run` Safe mode configuration: • `SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal` • `SYSTEM\ControlSetXXX\Control\SafeBoot\Network` Session Manager Parameters: • `System\ControlSetXXX\Control\Session Manager\SubSystems, Windows` System services: • `System\CurrentControlXXX\Services`

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

11.3. Exploit Prevention

The Exploit Prevention component allows you to block malicious programs that use vulnerabilities of well-known applications. To determine whether an object is malicious, the component uses also the data from Dr.Web cloud service.

To enable or disable Exploit Prevention

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Preventive Protection** tile.
3. Enable or disable the Exploit Prevention component by using the switcher.

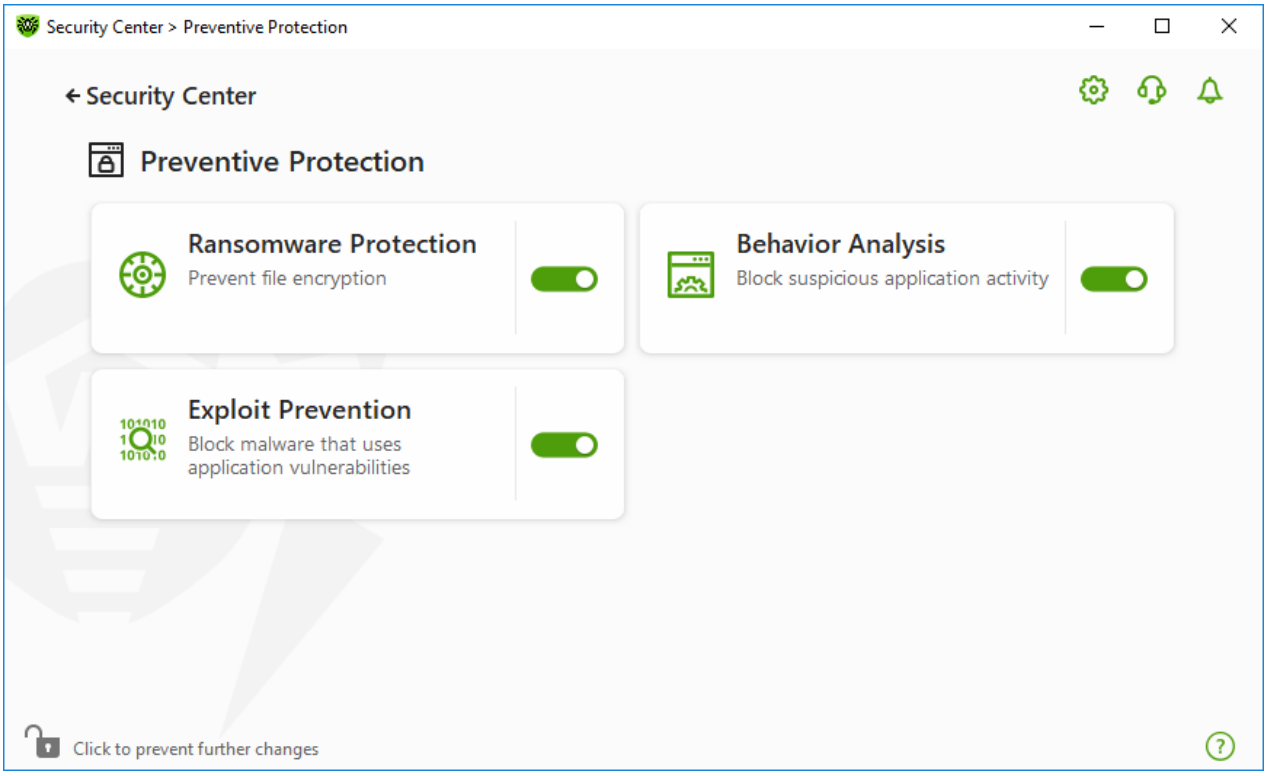

Figure 56. Enabling/Disabling the Exploit Prevention component

To open Exploit Prevention 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 **Exploit Prevention** tile. A component parameter window opens.

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

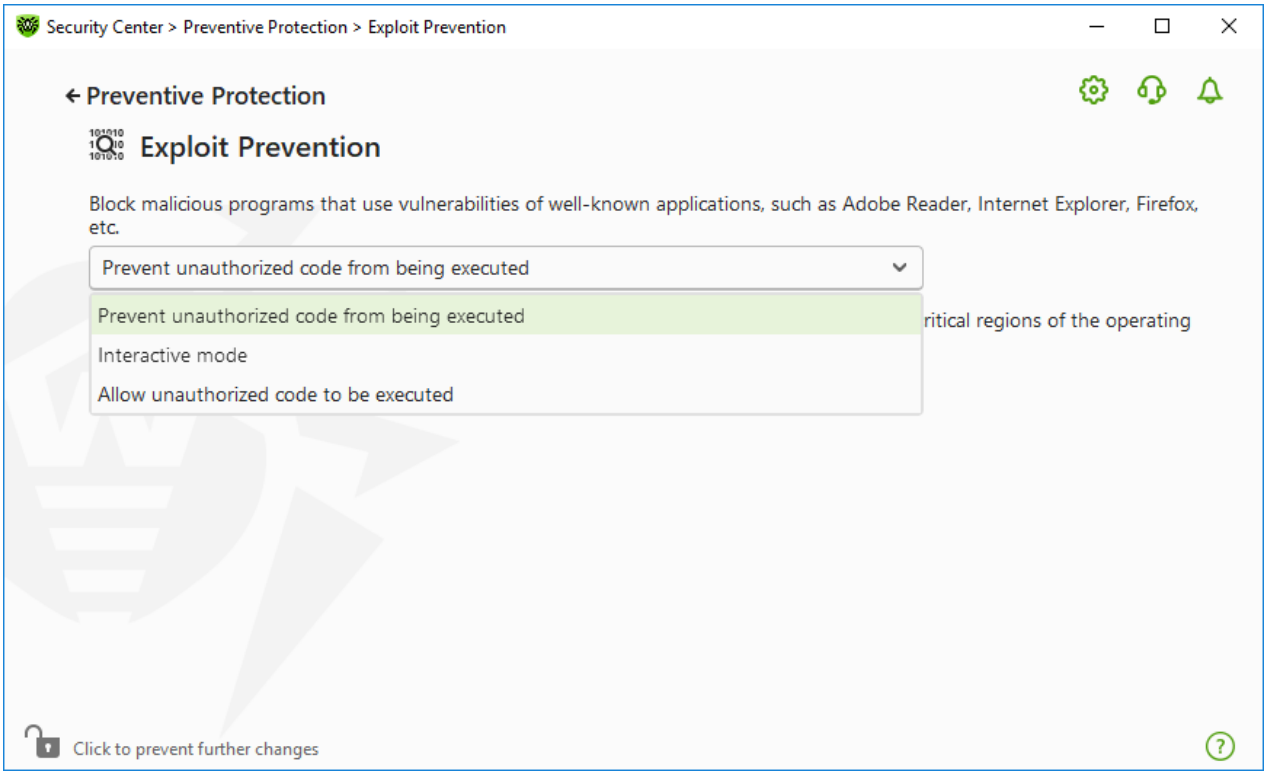

Figure 57. Selecting protection level

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 and email notifications on Exploit Prevention actions.

See also:

- Notifications

12. Devices and Personal Data

This group of settings allows you to protect important folders, and block access to certain buses and device classes.

To open the Devices and Personal Data group of settings

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Devices and Personal Data** tile.

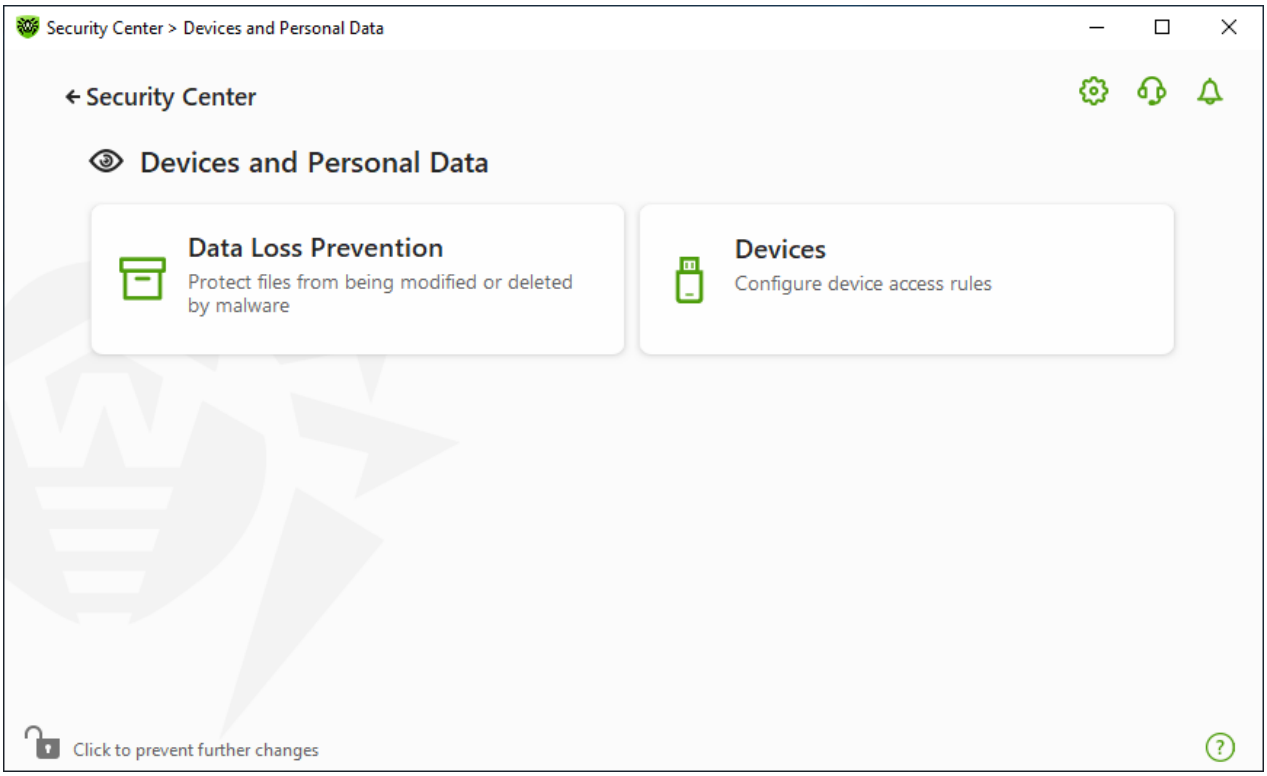

Figure 58. The Devices and Personal Data window

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 window:

- Data Loss Prevention—additional protection of important files and folders.
- Devices—control of device blocking.

12.1. Data Loss Prevention

To protect content of important folders from being changed by malicious software, use the *Data Loss Prevention* feature. With this feature enabled, you can view and add files to a protected folder, however, any modification or removal of files from this folder is blocked. To allow access to a folder for applications, add necessary applications to exclusions. You can also restore previously saved copies.

To open the Data Loss Prevention window

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Devices and Personal Data** 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 **Data Loss Prevention** tile.

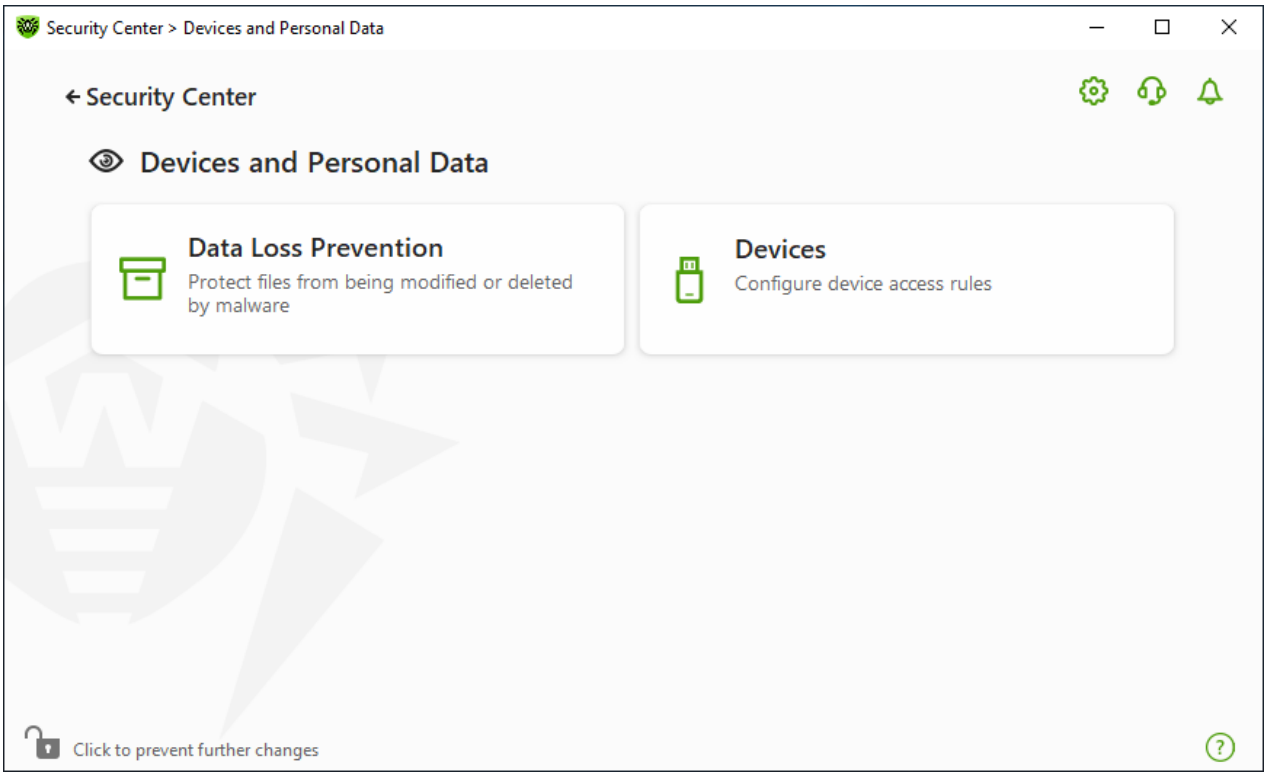

Figure 59. Access to the Data Loss Prevention window

In this section:

- Dr.Web operation with previously saved file copies
- Manage protected folders
- Exclusions
- Restore and delete saved copies

Dr.Web operation with previously saved file copies

Beginning from the version 12.0, you do not have an option to save file copies. As an alternative to the feature of saving copies, a new feature of protected folders is used from now on.

As the operation principle has been changed, you should configure protection of folders again. Folders that were protected in previous versions of program are added to the list of protected folders, regardless of whether copies of these folders have been saved or not. At the first program launch after updating to version 12.0, a notification appears informing you about switching the file backup feature to the protected folders feature:

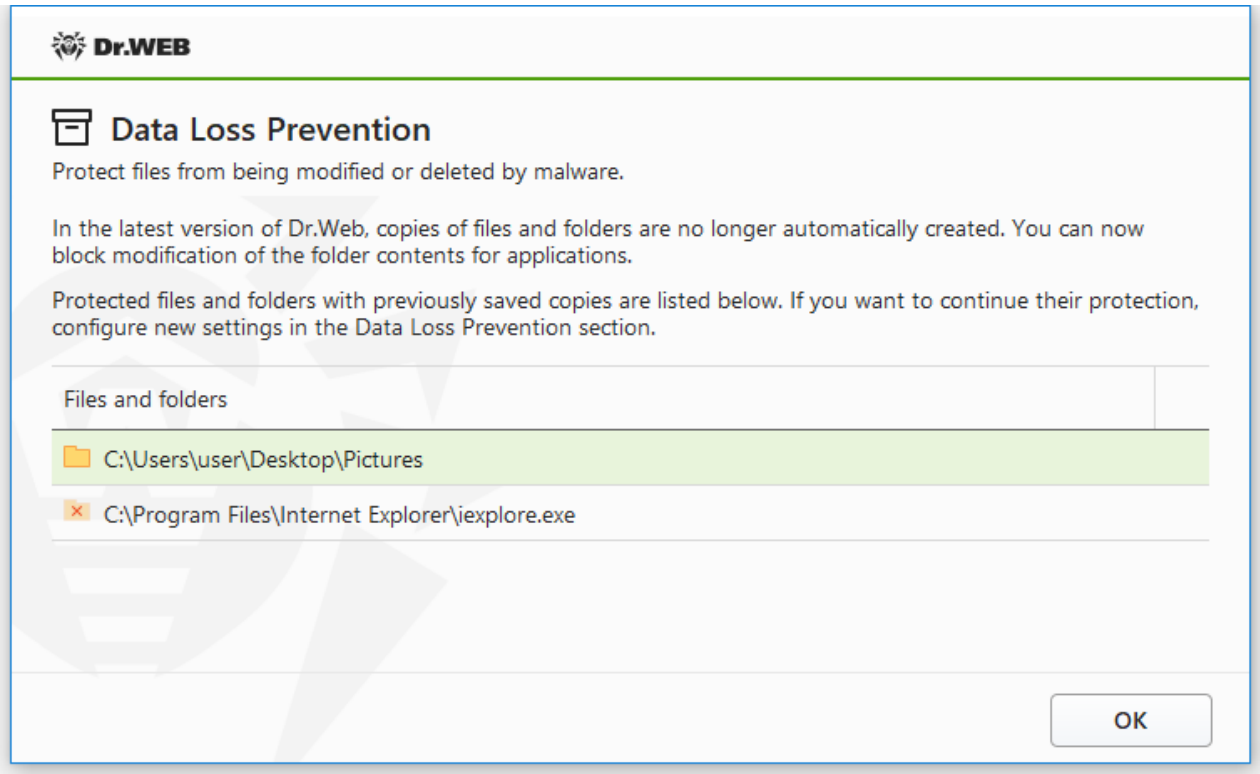

Figure 60. Notification on changing the component operation principle

In this notification, you can also see the list of all detected folders and files for which the protection has been enabled. If the folder cannot be added to the list of protected ones, it is marked with sign. System folders and separate files cannot be protected.

By default, the protection of the folders, that were transferred from previous product versions, is disabled. To protect such folders, go to the **Data Loss Prevention** window and check necessary folders in the **Enable protection** column.

You can also restore file copies saved in previous versions.

Notifications

After the program upgrade to the version 12.0, you are notified about the changes in Data Loss Prevention operation principals:

- Right after the computer restart, in the center of the screen, the notification on changing the component operation principle is shown. See the figure 60.
- In Notification Feed, the notification on changes in the method of folder protection. To access the new settings of folder protection, click **Configure protection** button. The notification is deleted after that.

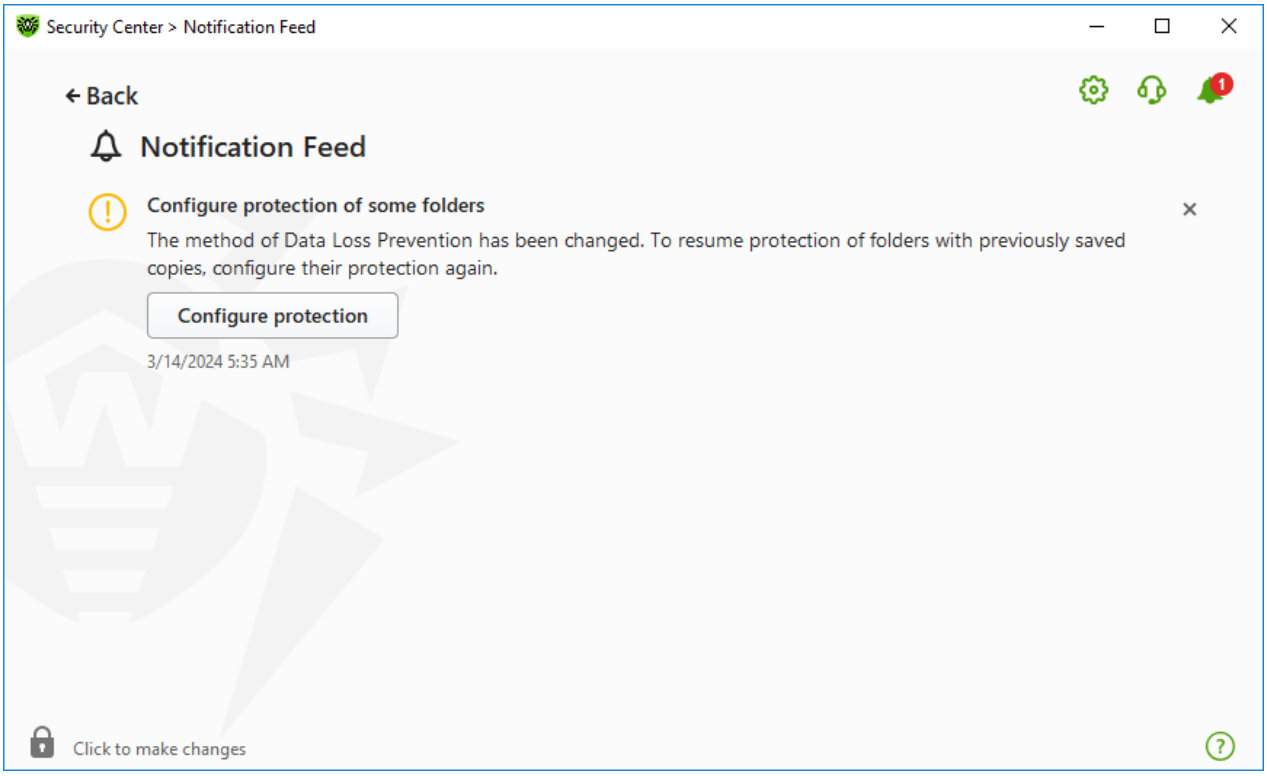

Figure 61. Notification in the feed

- When you open the **Data Loss Prevention** window for the first time after the program upgrade, a notification with the list of files and folders that cannot be protected is displayed.

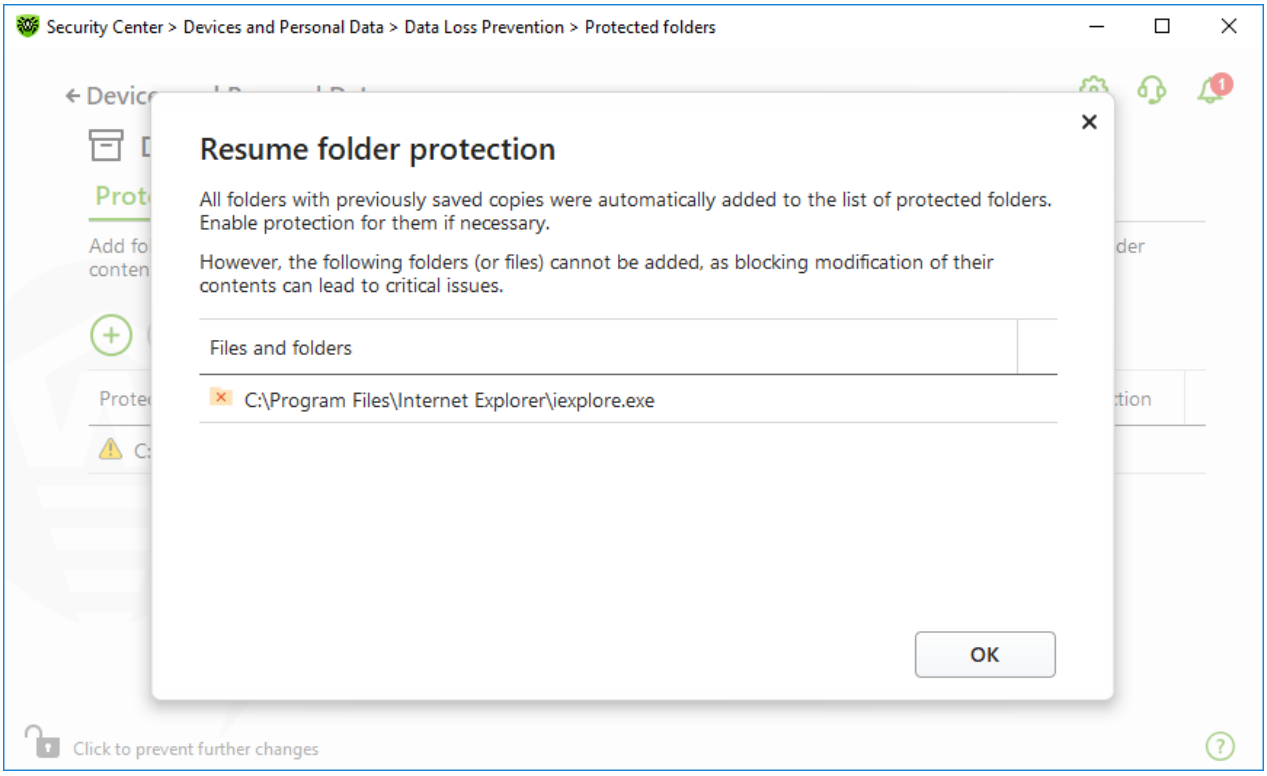

Figure 62. Notification on the first visit of the Data Loss Prevention window

Protected folders

For each folder, you can configure application access parameters. You can view and copy the protected folder. You can also create new elements in this folder. The processes that create the new elements can modify them until these processes are completed. When an application attempts to access the folder, a notification on access blocking will be displayed.

> If a threat is detected in files in protected folders, only Dr.Web can still remove and modify them.

If you add a folder to the list of protected folders, a default rule is applied to it. Thus, any modification and removal of the folder content is restricted for all applications, except those from the list of trusted applications. To view this list, visit the website https://products.drweb.com/services/data_protection/. The list contains the most popular applications, for example, some Microsoft and Adobe applications. System processes, such as `explorer.exe`, are not included into the list of trusted applications as they can be used by malicious objects to attack the system.

> It is restricted to add system folders to the list of protected ones. This may lead to critical system operation errors.
>
> Data Loss Prevention applies only to local files and folders (physically located on your device) within the same operating system on which the protection is configured. If you have

several operating systems on the same computer, you should configure Data Loss Prevention separately on each system. Protection of network files and folders is not possible.

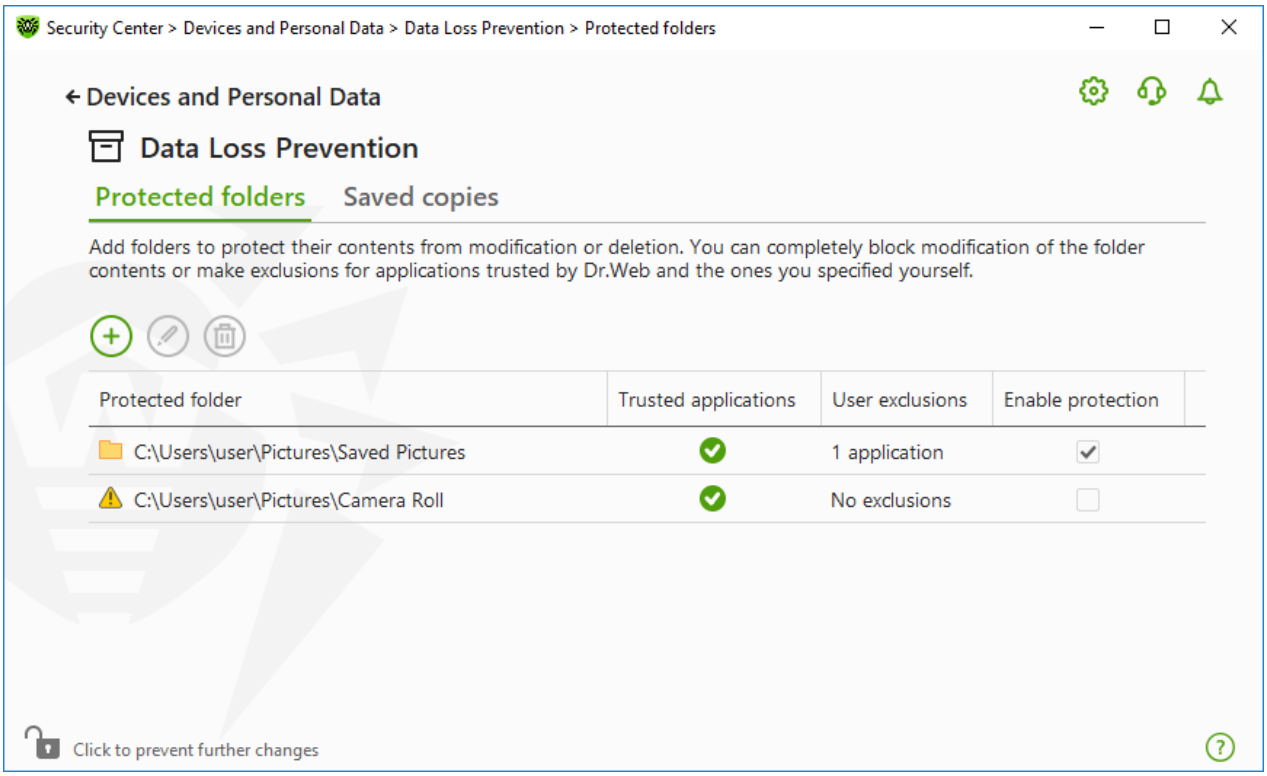

Figure 63. Protected folders

In the table, you can see information on:

- protected object,
- number of exclusions from a general rule, and
- protection status.

To activate protection, select the **Enable protection** check box for the necessary object. If this check box is cleared, the folder is not protected any more. It is displayed with the ⚠ icon.

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

- The ⊕ button—adding an object to the list of protected objects.
- The button—editing elements in the table.
- The button—removing an object from the list of protected objects.

To add a folder to the list of protected folders

1. Click the ⊕ button. In the open window, select the necessary object by clicking the **Browse** button.

2. If necessary, enable or disable access to the folder for trusted applications. This option is enabled by default.
3. You can also specify applications that will have full access to an object regardless the general settings.

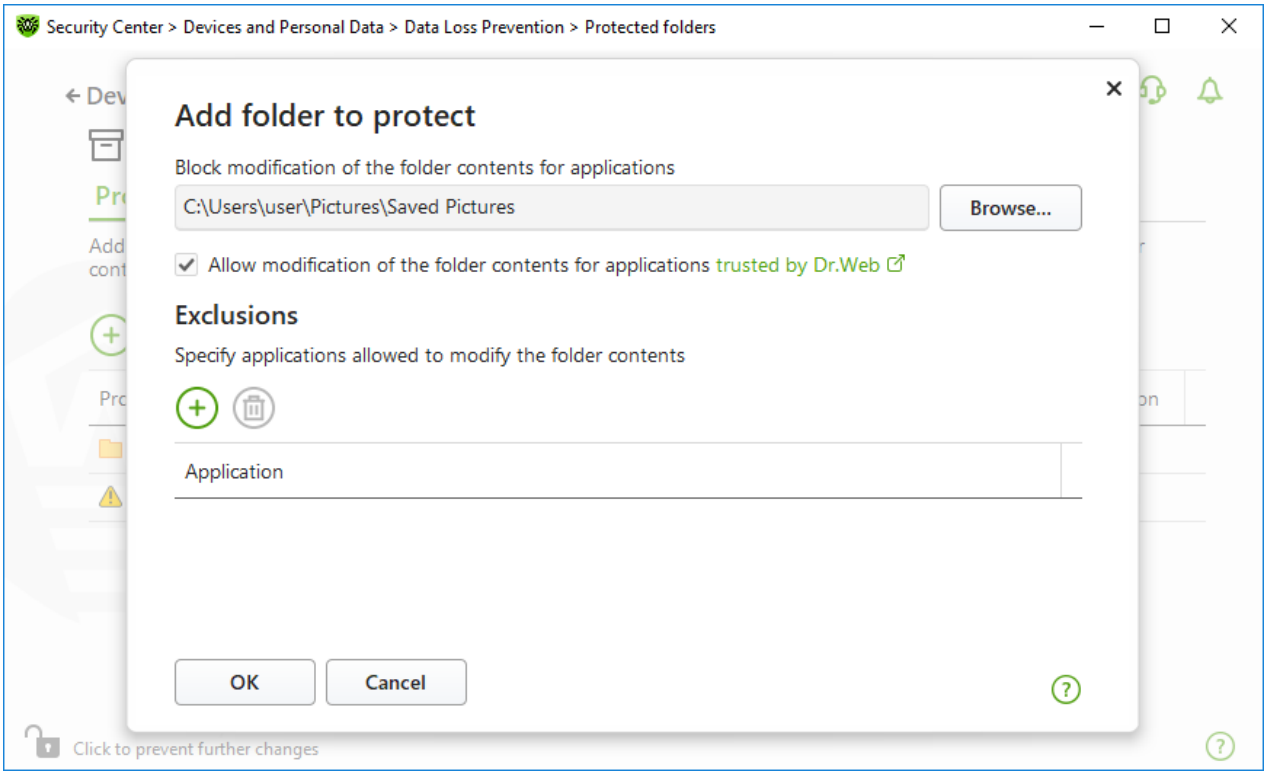

Figure 64. Adding a protected folder

Exclusions

The number of applications that have full access to the protected folder is displayed on the main window of Data Loss Prevention in the **User exclusions** column.

To add an application to the exclusions

1. In the Data Loss Prevention window, click ⊕ to add a new folder to the list of protected.
2. In the open window, click ⊕. Select an application that will have full access to the objects in the protected folder.
3. Click **OK**.

To edit the list of exclusions for protected folders

1. Select a folder from the list and click ✎.
2. At the bottom of the open window in the table, you can see all applications that have full access to the selected folder.
   - To add a new application, click ⊕.

- To delete an application from the list of exclusions, click .

3. Click **OK**.

Saved copies

The tab is available only if you have copies of files saved in the previous versions of the program. This function allows you to restore and remove saved copies. However, you cannot save new copies.

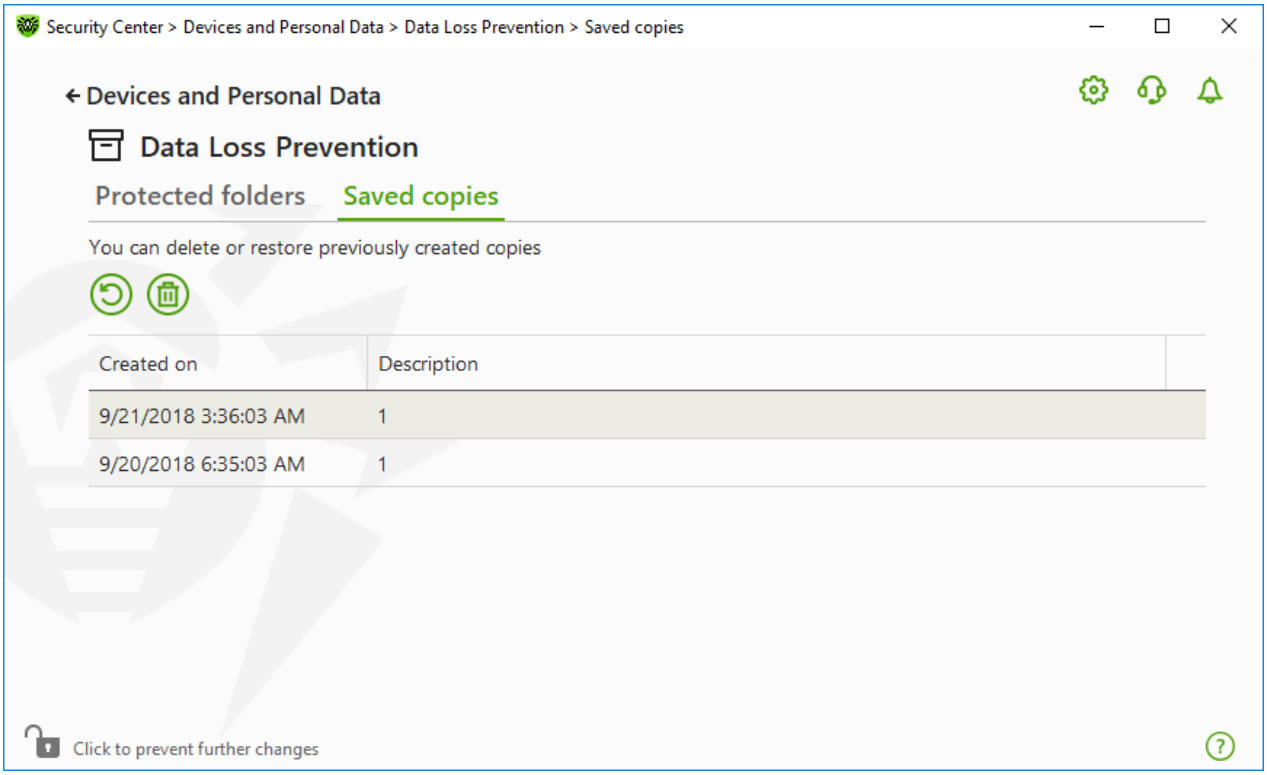

Figure 65. List of saved copies

Removal of created copies

You may also delete existing copies to free up some disk space (deleting the copies will not affect the original files). To do that, select the necessary copy and click the button.

Restoring files

If any threat has caused corruption of your files, you can restore copies of these files created on a specific date. To do that:

1. Select the necessary copy (the date when the copy was created is displayed in the left column) and click the button.
2. In the open window, specify the path to the folder to which the files will be restored.

12.2. Device Blocking

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. In the open window, click **Devices and Personal Data** 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 **Devices** tile.

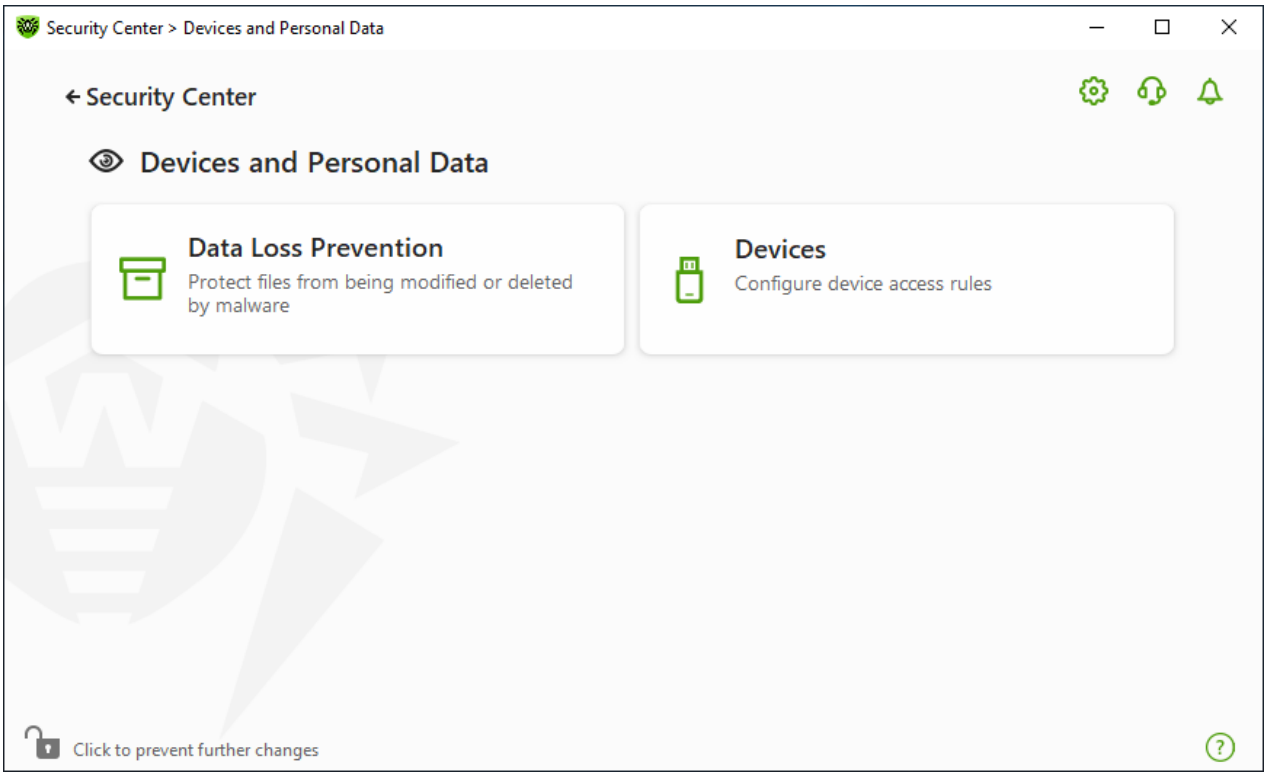

Figure 66. Access to the Devices window

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.

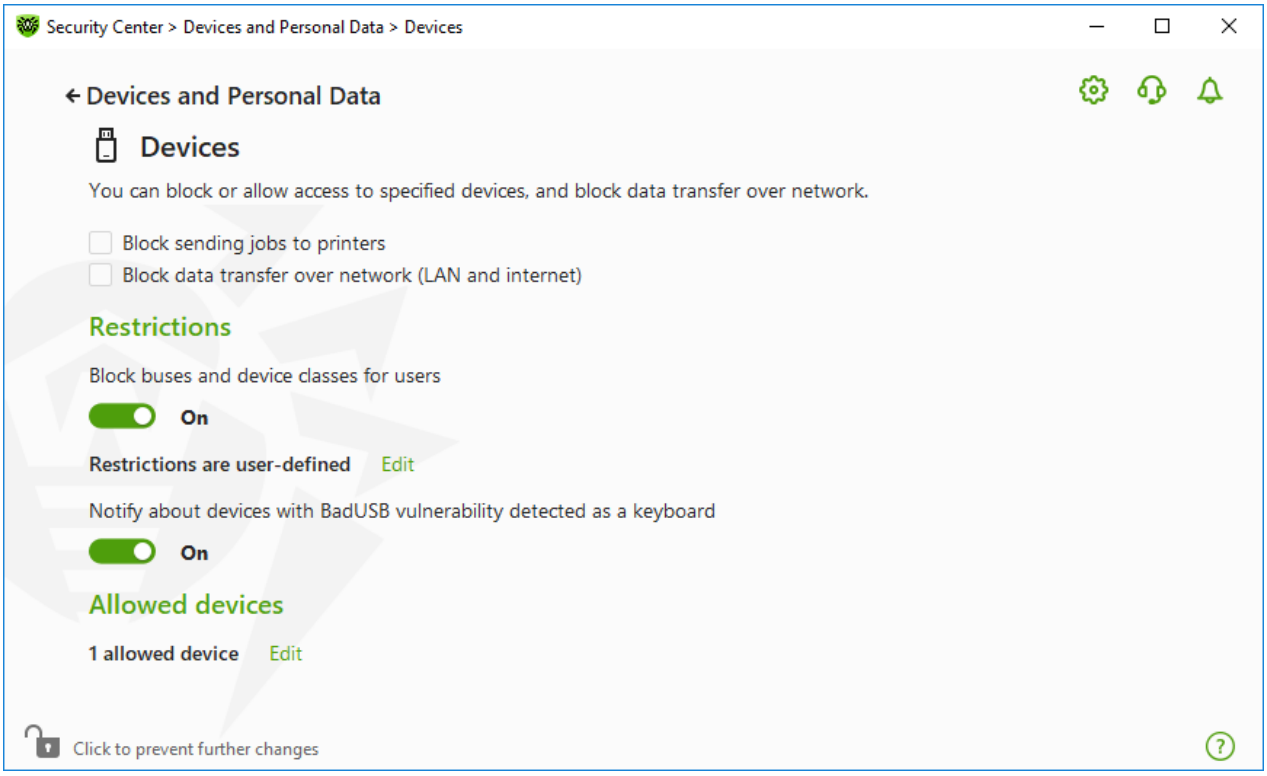

Figure 67. Device blocking parameters

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.

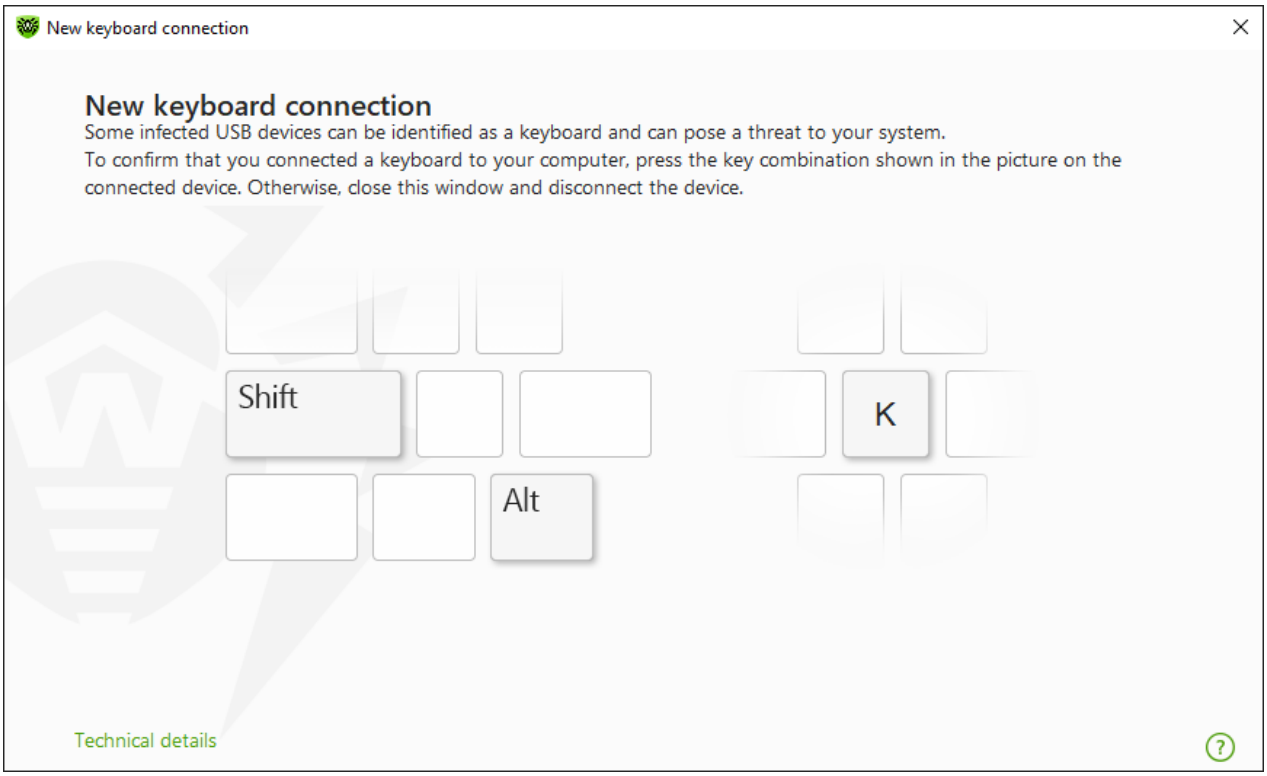

Figure 68. Keyboard unblock window

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 devices to the list of allowed devices, in the **Allowed devices** option click **Edit** (the link is active if restrictions are set). In the open window, you can generate a list of devices to which the access restrictions are not applied.

12.2.1. 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 and Personal Data** tile.
3. In the open window, click **Devices** tile.
4. In **Restrictions** setting group, enable the **Block device classes and buses for users** option by using the switcher.
5. Click **Edit**.
6. 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.

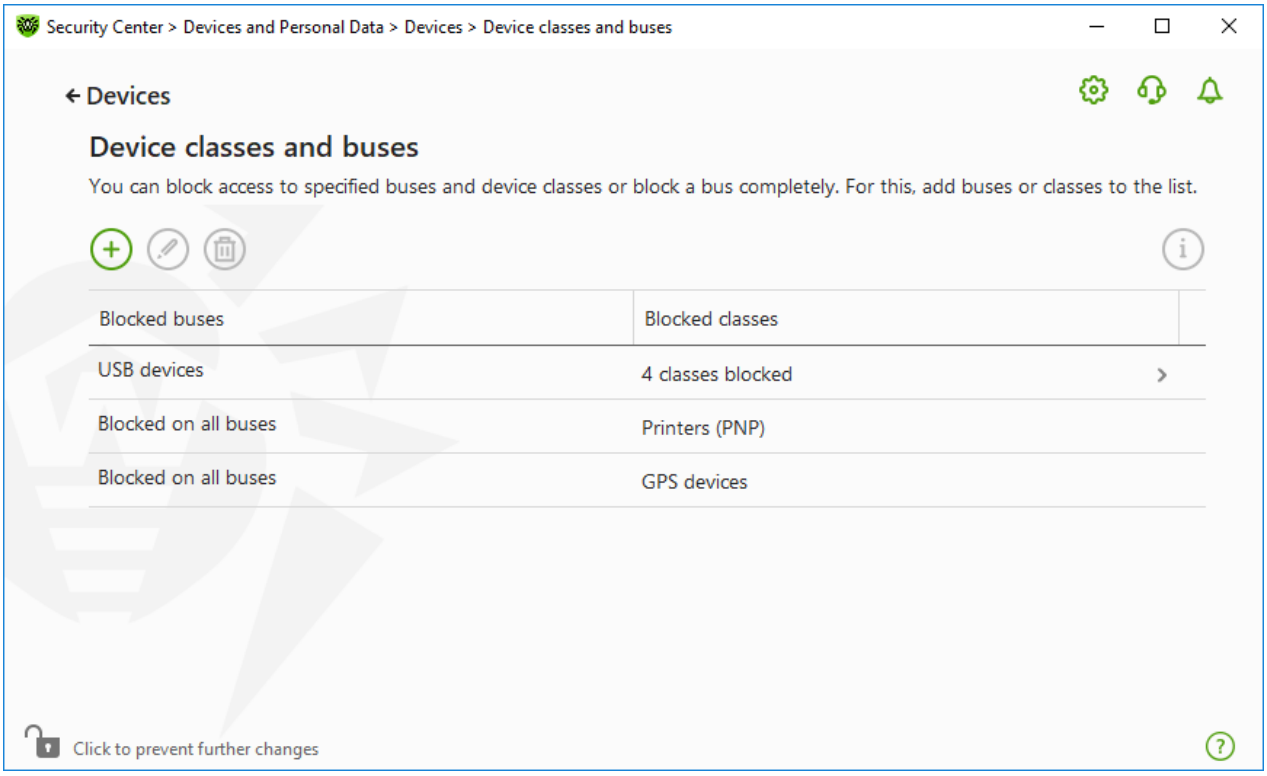

Figure 69. Blocked buses and classes

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**.

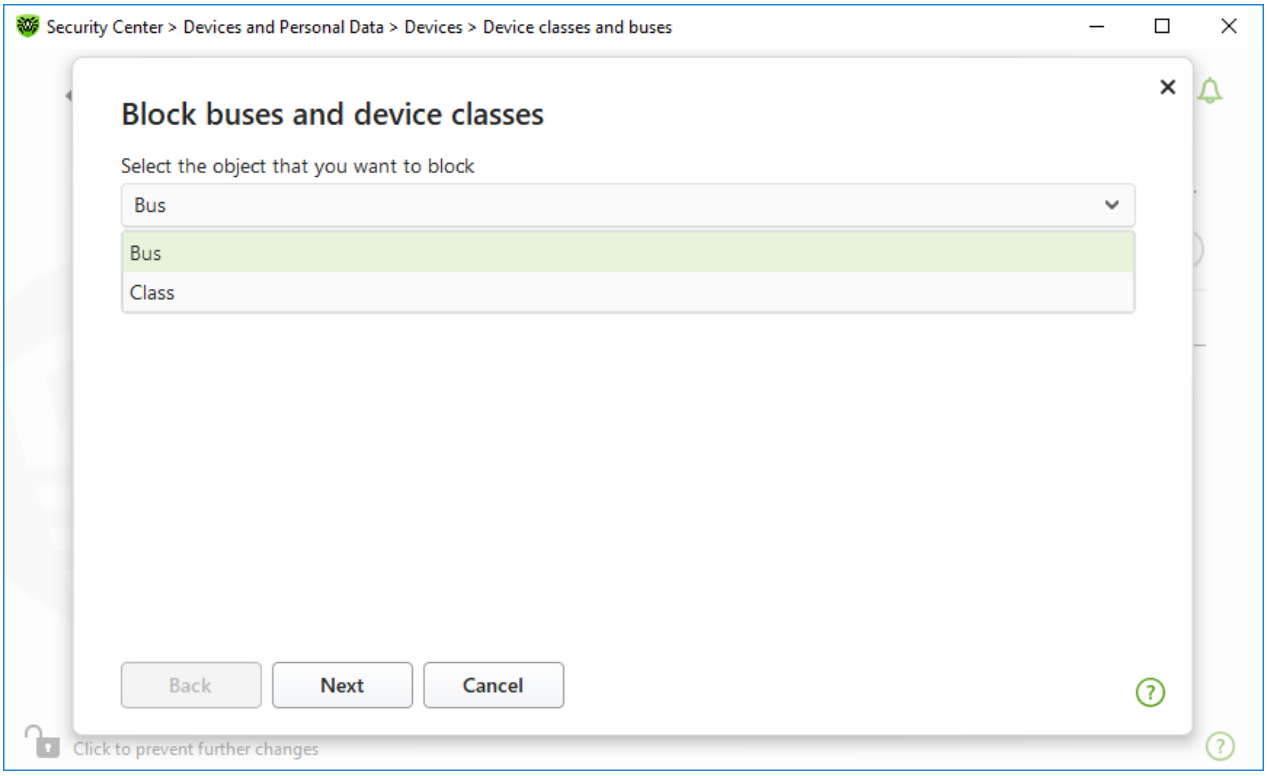

Figure 70. Selecting an object to be blocked

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

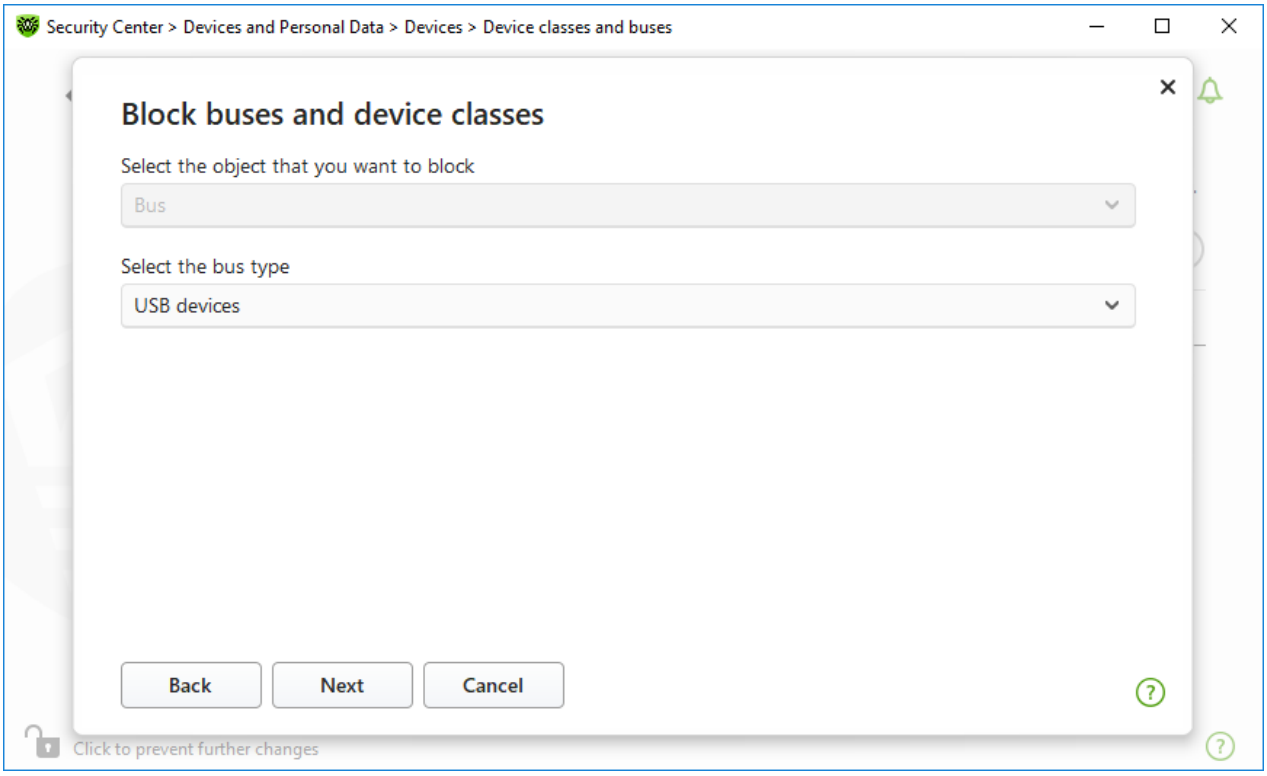

Figure 71. Selecting the bus type

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.

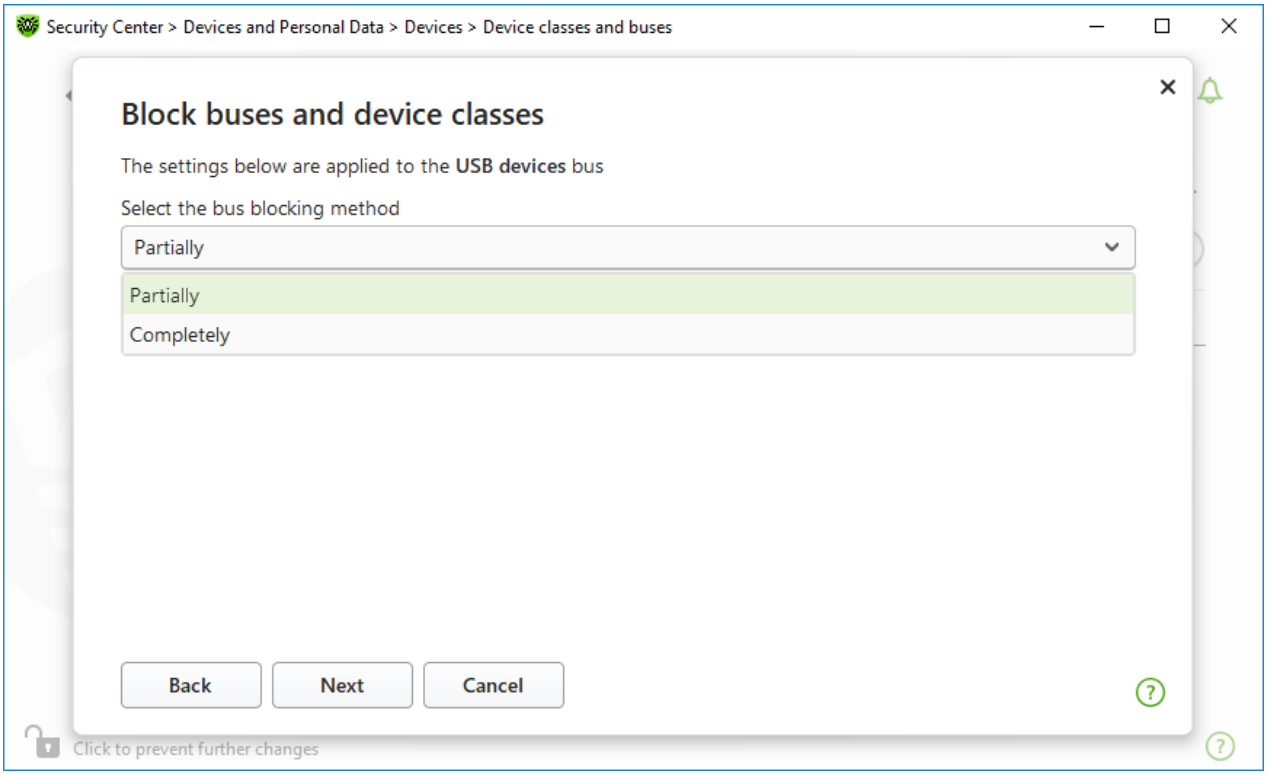

Figure 72. Selecting a bus blocking method

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

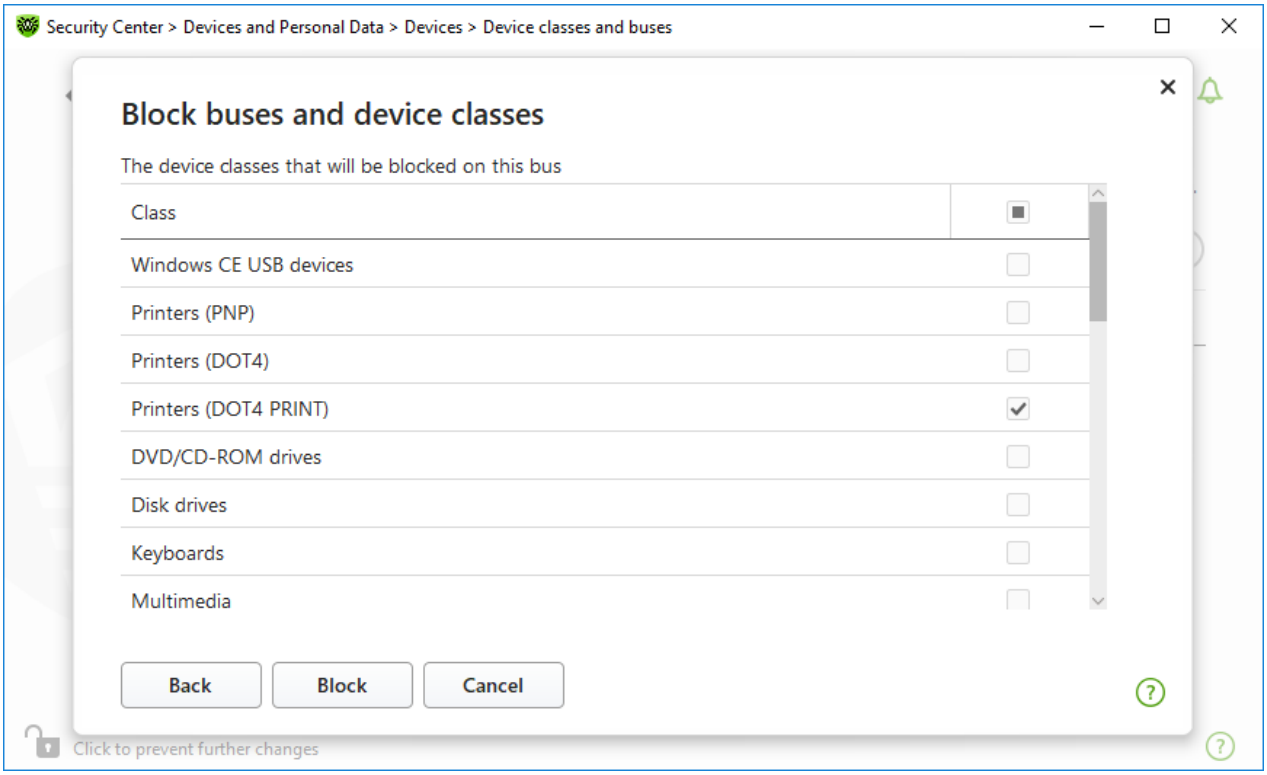

Figure 73. Selecting device classes on a bus

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**.

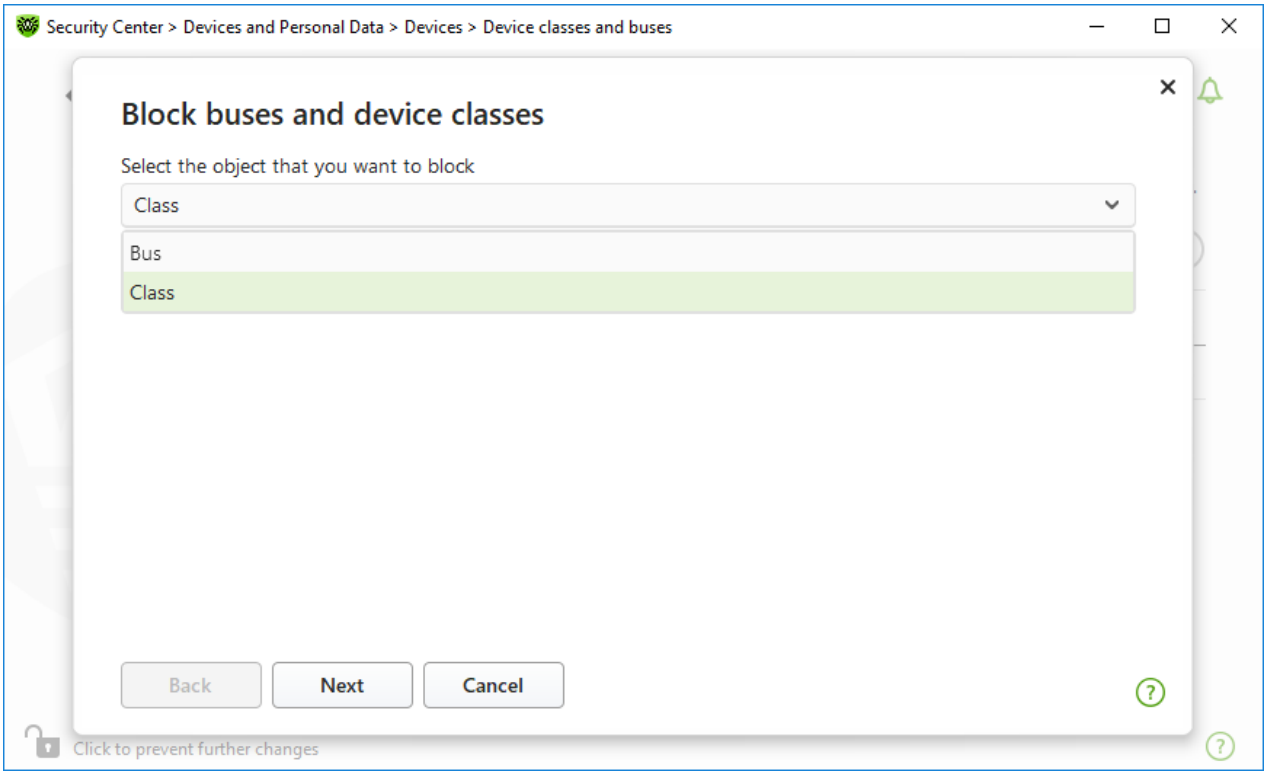

Figure 74. Selecting an object to be blocked

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

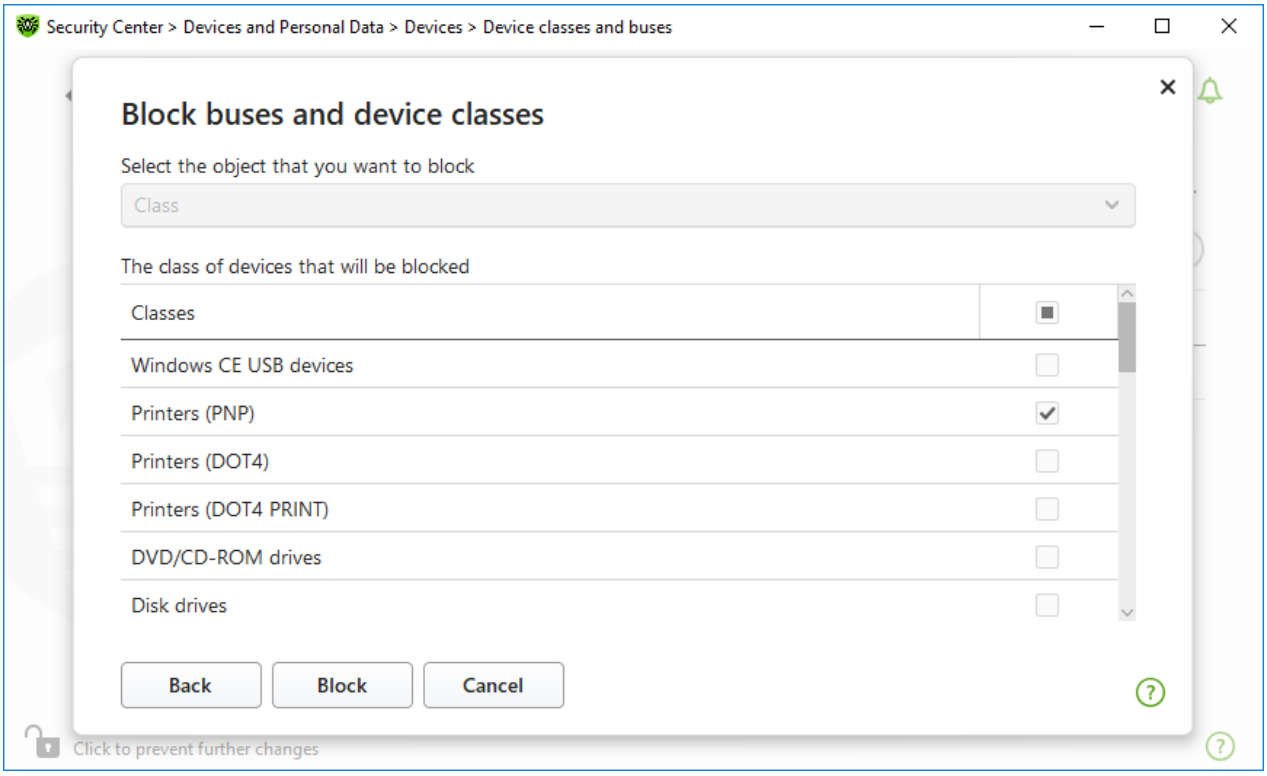

Figure 75. Selecting device classes

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.

Receiving notifications

You can configure displaying pop-ups and receiving notifications by email on blocking a device.

12.2.2. Allowed Devices

To open the Allowed devices window

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Devices and Personal Data** tile.
3. In the open window, click **Devices** tile.
4. 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:

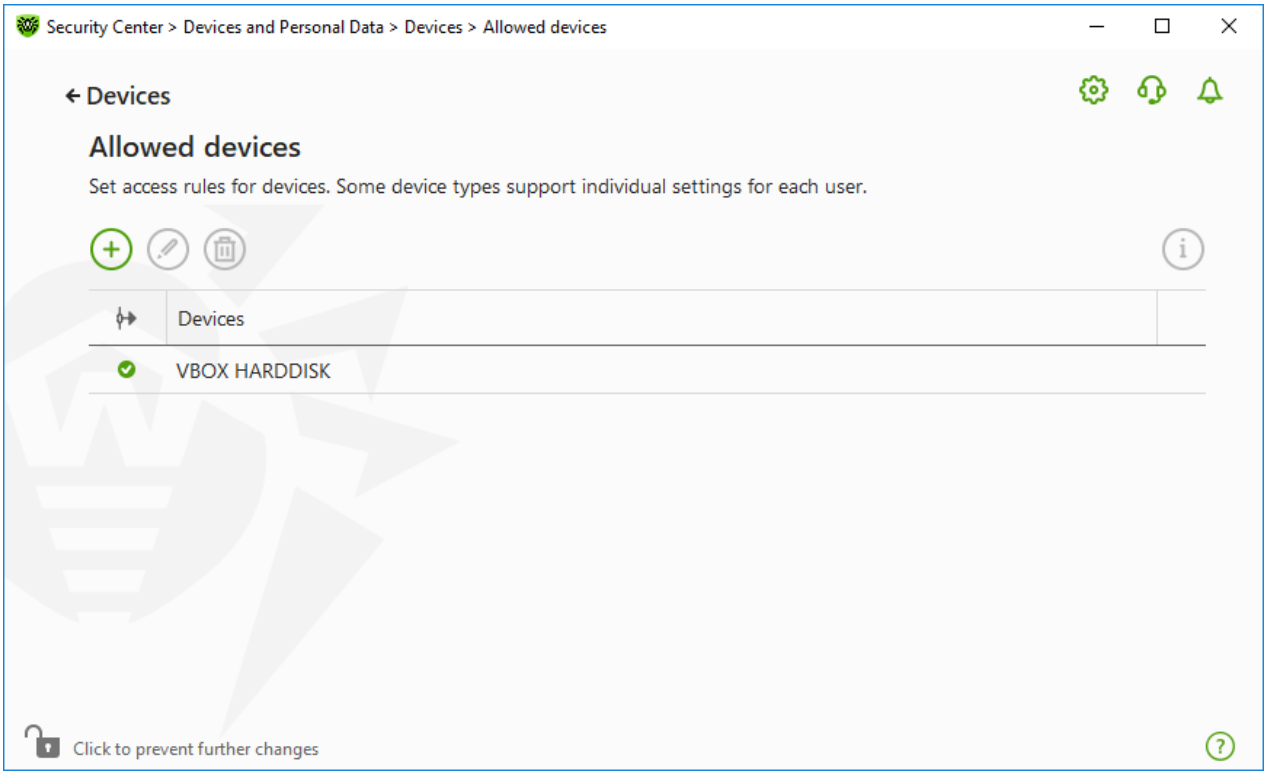

Figure 76. Allowed Devices

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**.

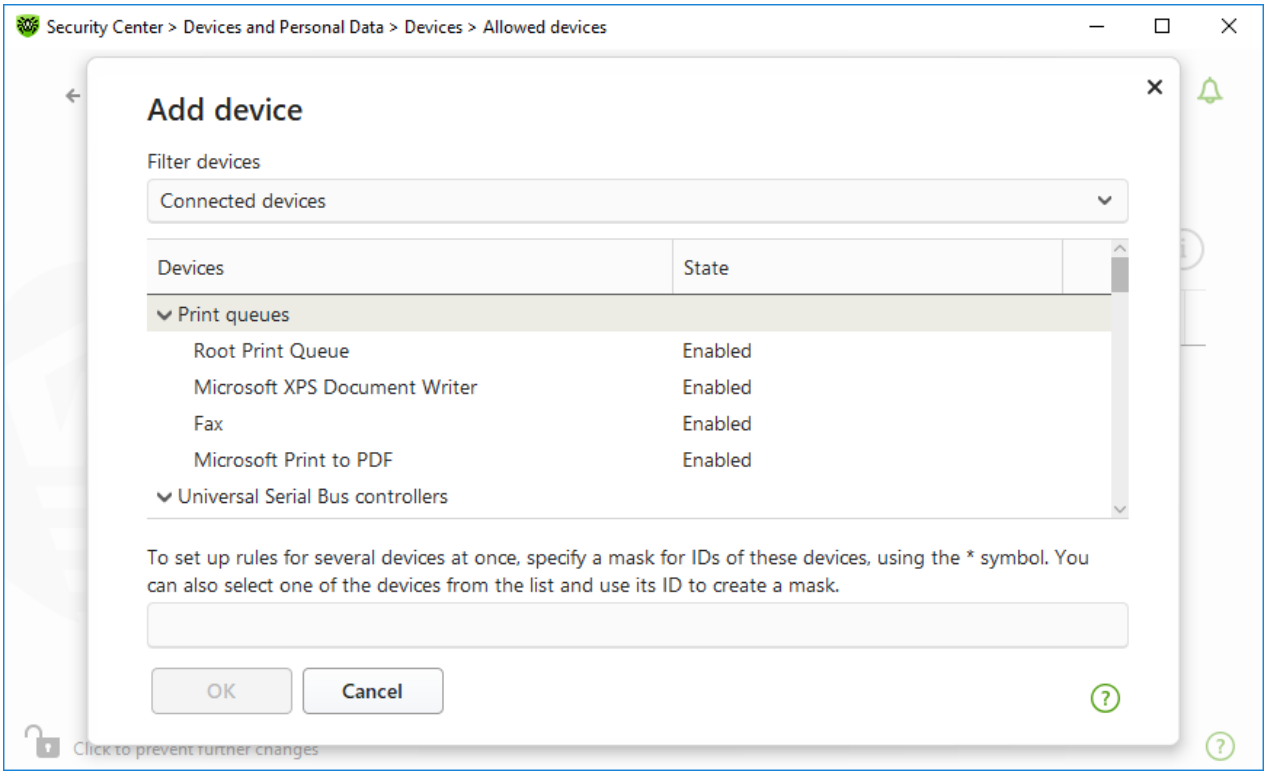

Figure 77. Adding a device to the list of allowed devices

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 🗑.

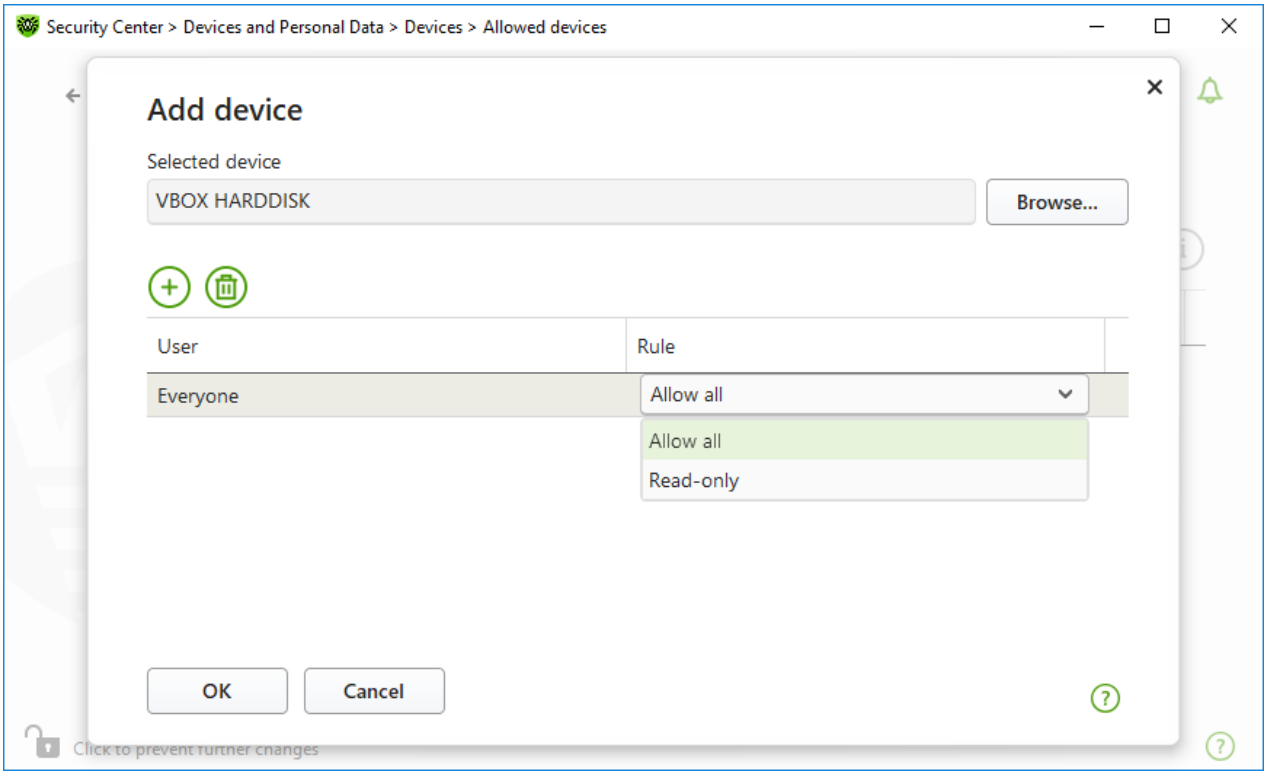

Figure 78. Selecting a rule for a certain user

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.

13. Tools

In this window, you can provide access to advanced tools to control Dr.Web product.

To open the Tools group of settings

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click **Tools** tile.

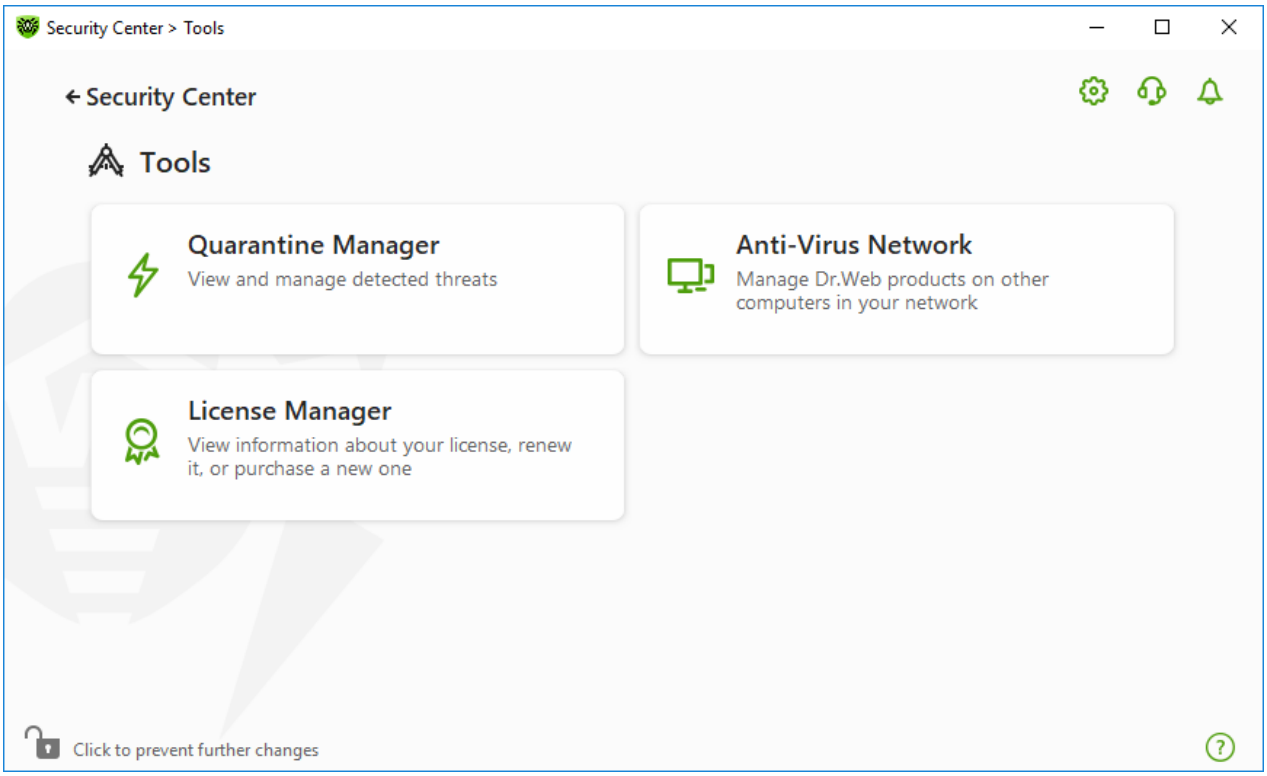

Figure 79. Tools

To open a necessary tool window, tap the corresponding tile.

In this section:

- Quarantine Manager—list of isolated files and a possibility to restore them.
- Anti-Virus Network—remote access to Dr.Web products, installed on other computers within your network.
- License Manager—license information, receiving new license.

13.1. 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. In the open window, click the **Tools** tile.
3. Click the **Quarantine Manager** tile.

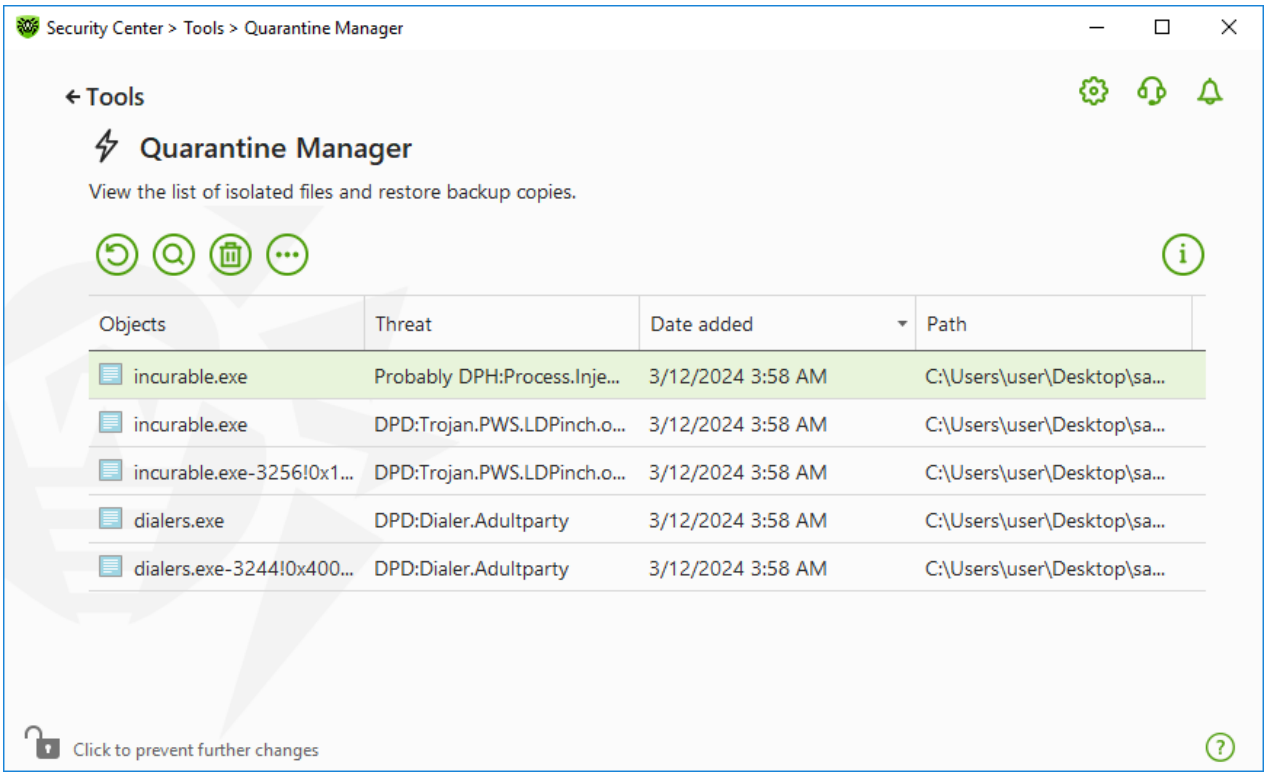

Figure 80. Objects in Quarantine

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.

13.2. Anti-Virus Network

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

To open the Anti-Virus Network window

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click the **Tools** tile.
3. Click the **Anti-Virus Network** tile.

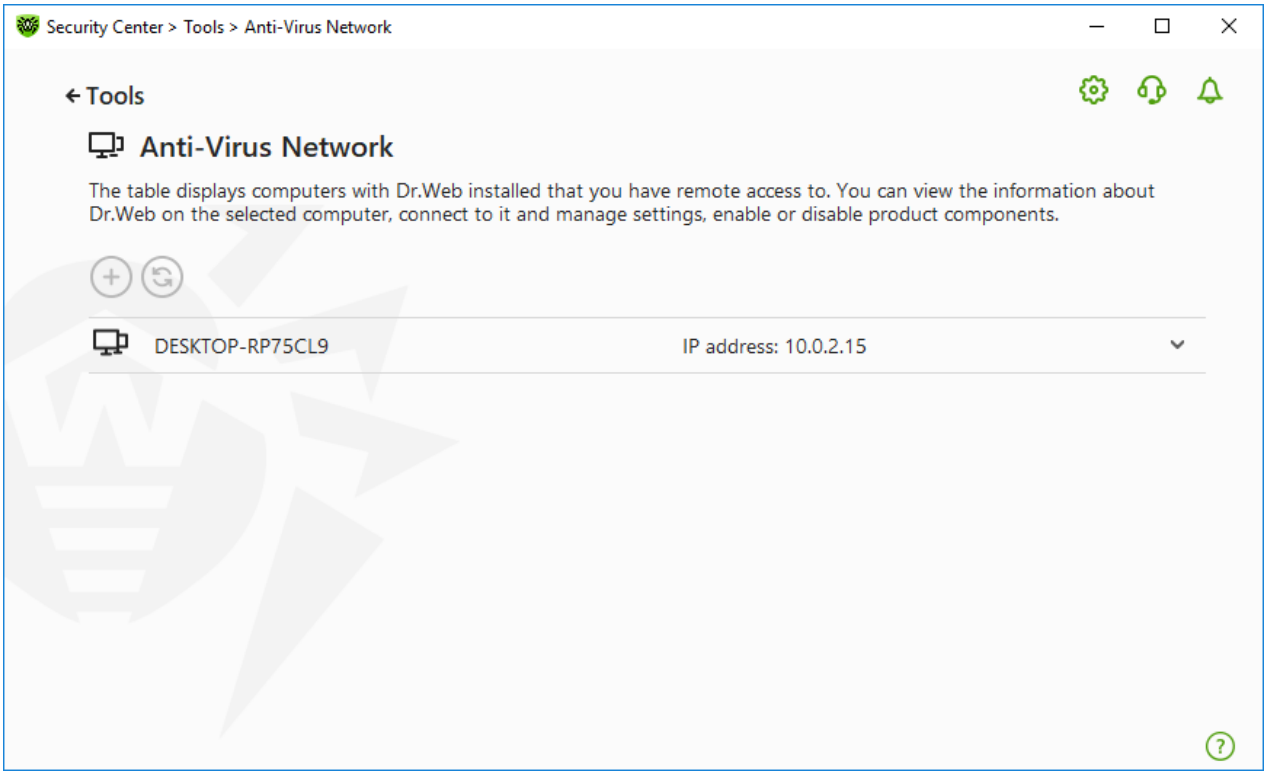

Figure 81. Anti-virus Network nodes

Computers are listed if Dr.Web products installed on these computers allow remote connection. You can allow connection to your Dr.Web on the Anti-virus network settings page.

If the required computer is not on the list, try to add it manually. For this, click ⊕ and enter an IP-address in a IPv4 or IPv6 format.

> ⚠ If a component is disabled on the station, an exclamation mark is displayed.

Parameters for Anti-Virus Network operation

During anti-virus network operation multicast and UDP requests with following parameters are used:

Parameters for multicast request:

- IP address: 239.194.75.48 or ff08::28 for IPv4 and IPv6 respectively
- Port: 55566
- Polling interval: 2000 ms

Parameters for UDP request:

- Port: 55566

- Polling interval: 2000 ms

To connect to remote Dr.Web

1. Select a necessary computer from the list. In the expanded line, a detailed information about status of components on the station and about the last update is displayed.
2. Click **Connect**.
3. Enter the code specified in the settings of the remote anti-virus. An icon for the remote SplDer Agent appears in the notification area, and the notification about successful connection will be displayed.

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

You can view statistics, enable or disable components, and change their parameters. Anti-Virus Network, Quarantine, Scanner and Data Loss Prevention are not available.

You have also an access to the **Disconnect** option. When choosing this option, the current connection to the remote anti-virus disables.

13.3. License Manager

This tool allows you to view all Dr.Web licenses for your computer. You can also modify the current license, renew it or purchase a new license and activate it.

To open the License Manager window from Security Center

1. Open Dr.Web menu, then select **Security Center**.
2. In the open window, click the **Tools** tile.
3. Click the **License Manager** tile.

To open the License Manager window from the program menu

1. Open Dr.Web menu.
2. Select **License** item.

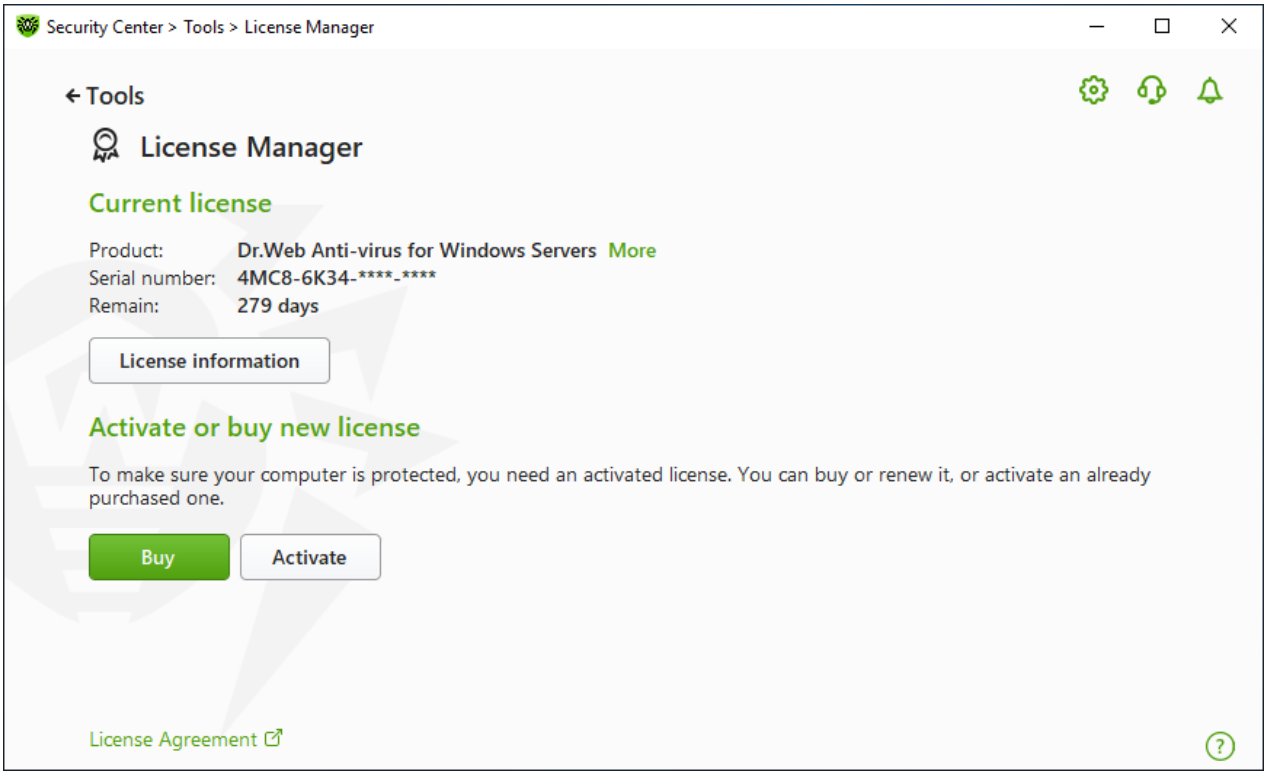

Figure 82. License Manager

To view detailed information on a current license, click **License information**.

To view information on a license that is not currently in use

1. Click **License information** to open the License Information window.
2. Select the relevant license from the drop-down list.

If the license covers multiple products, the list of all the products is available in the drop-down list by clicking the link **More**.

> If you have several licenses activated at the same time, each license will be expiring. To avoid this, specify the serial numbers of previously activated licenses when activating a new one. In this case, the periods of all the licenses will be combined.

To delete a license

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 **License information** to open the License Information window.
3. Select a license that you are going to delete from the drop-down list and click . Please note that the only valid license cannot be deleted.

To set a license as current

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 **License information** to open the License Information window.
3. Select a license that you are going to set as current from the drop-down list, and click .

Once you click the **Buy** button, the program opens the page on the Doctor Web website where you can purchase a new license or renew your current one.

- If you do not have an activated license, the program opens the page where you can purchase a new license. Follow the instructions on the website to purchase and activate a new license.
- If you already have an activated license, the program opens the renewal page where all parameters of the current license will be transmitted. Follow the instructions on the website to purchase and activate the renewal of your license. For the detailed information on license renewal, refer to the Renewing License section.

Once you click **Activate**, the window opens where you can activate a new license.

Advanced

The License Agreement link opens the license agreement on the Doctor Web official website.

14. Exclusions

In this group, you can configure exclusions from SpIDer Guard and Scanner.

To open the Exclusions group of settings

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

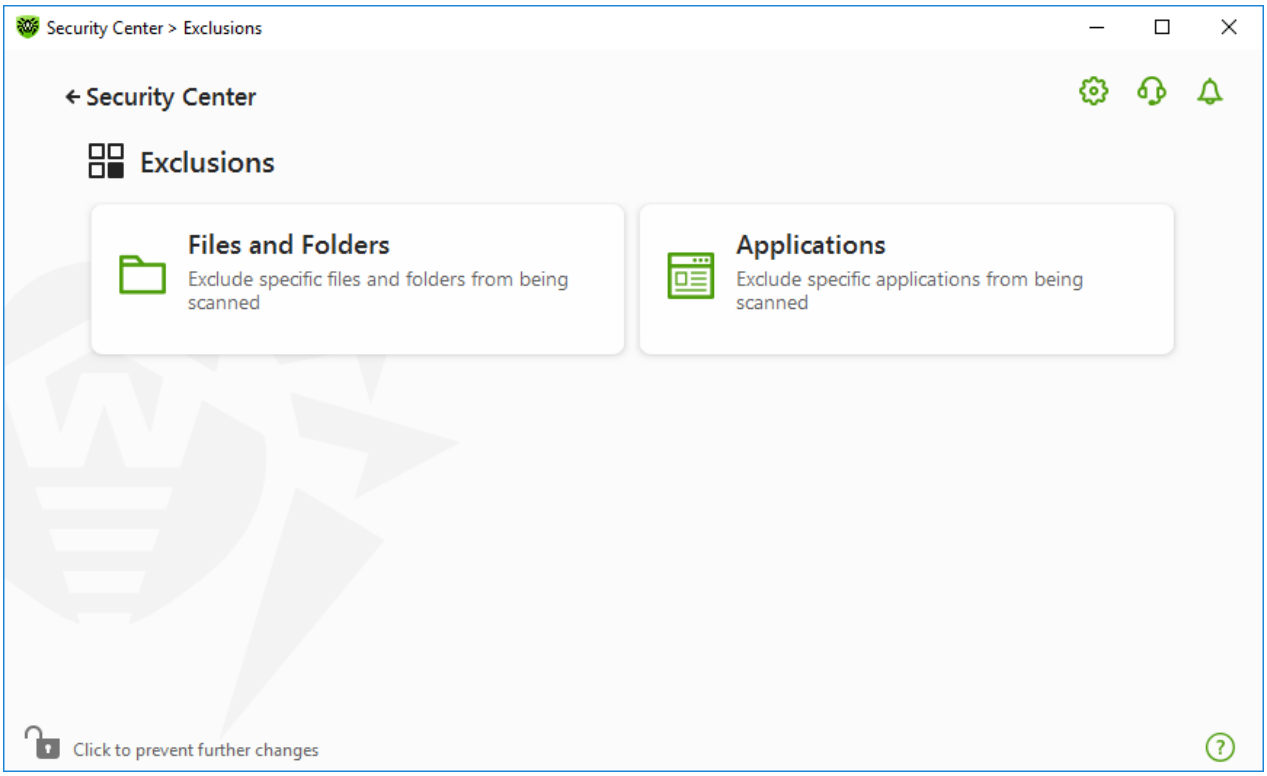

Figure 83. Exclusions

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.

In this section:

- Files and Folders—exclude certain files and folders from SpIDer Guard and Scanner scans.
- Applications—exclude specific processes from SpIDer Guard scans.

14.1. 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. Archived files can also be excluded from scanning.

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.

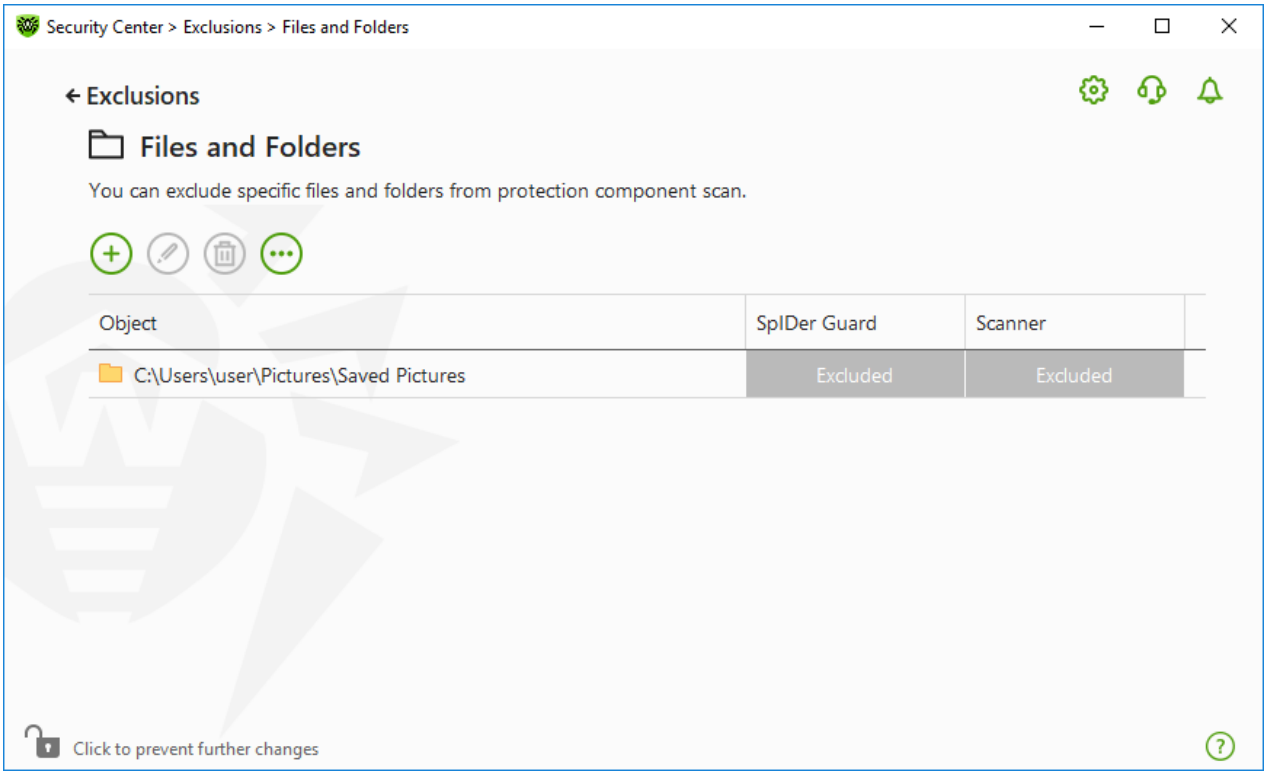

Figure 84. Files and folders exclusion list

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.

14.2. Applications

You can specify a list of programs and processes which activity will be excluded from scanning by the file monitor SpIDer Guard. 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.

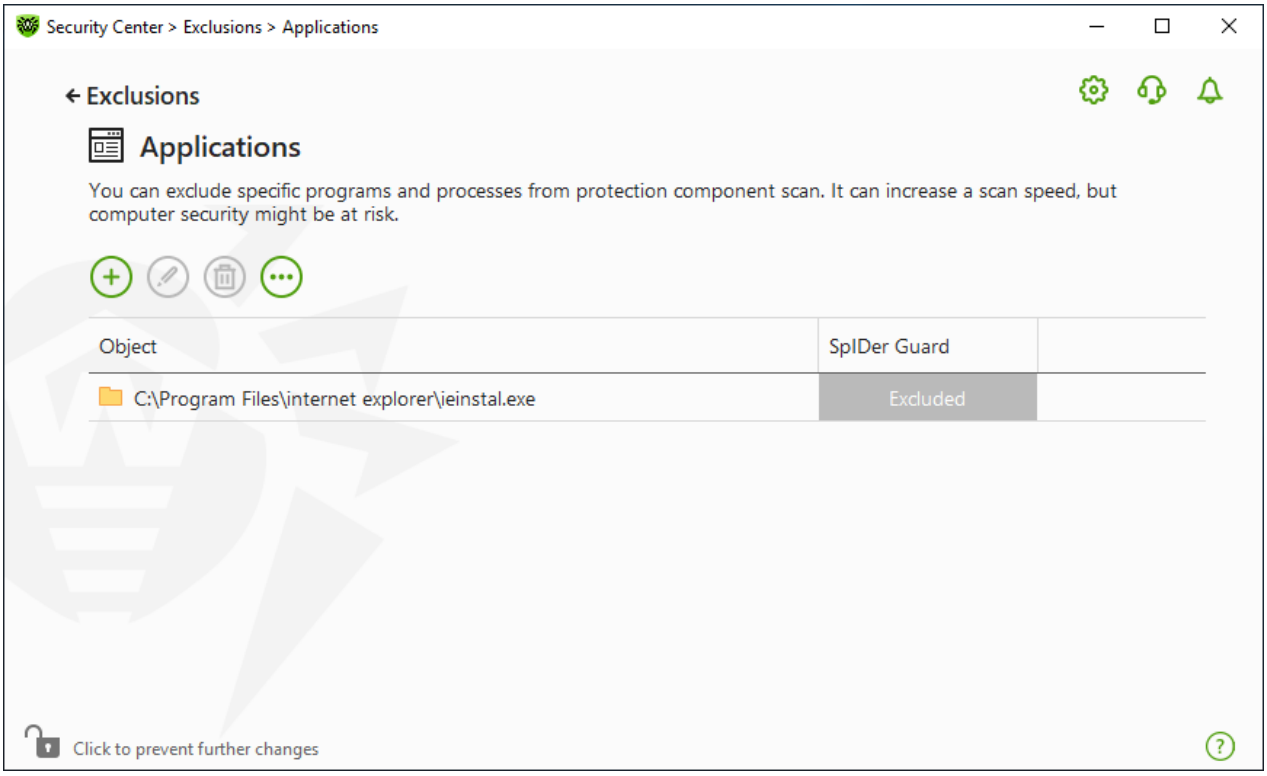

Figure 85. Excluded applications list

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 Server 2008 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 that SpIDer Guard should not scan the selected application.

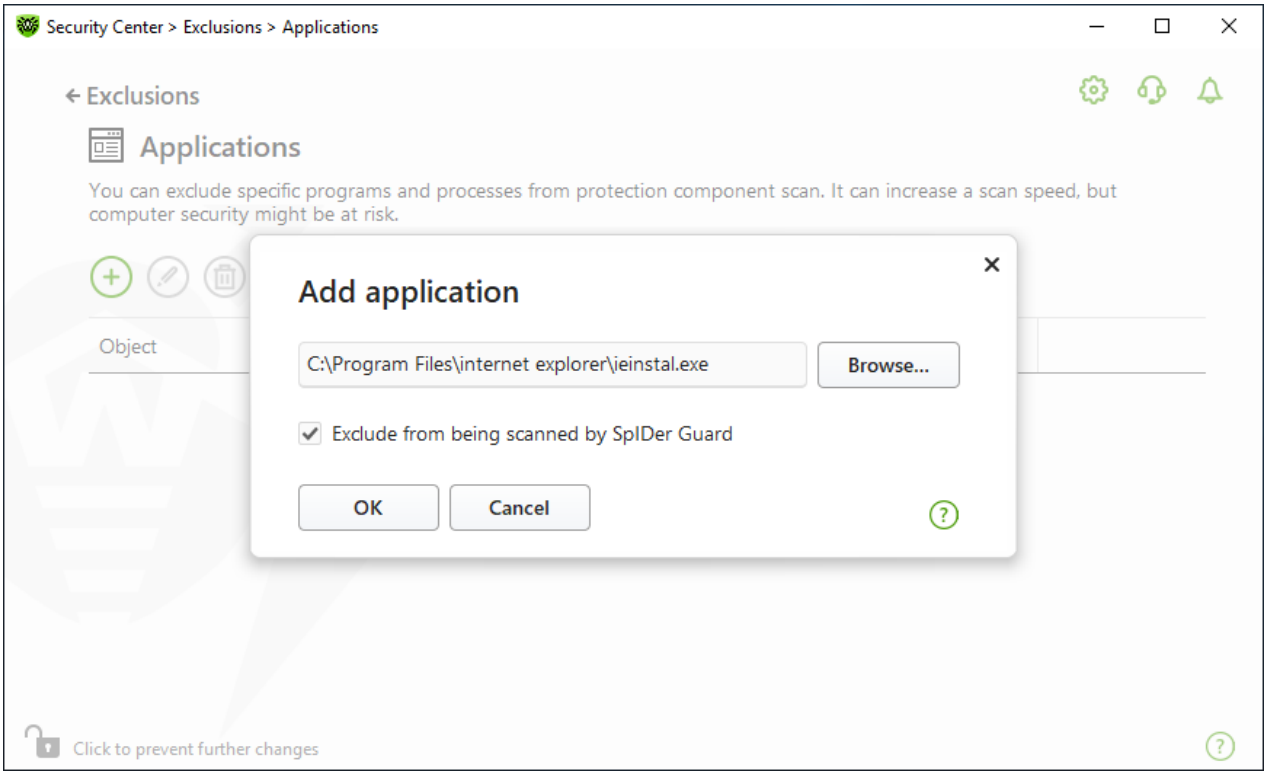

Figure 86. Adding applications to the exclusions

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

Managing listed objects

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.

15. 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
   - Threats

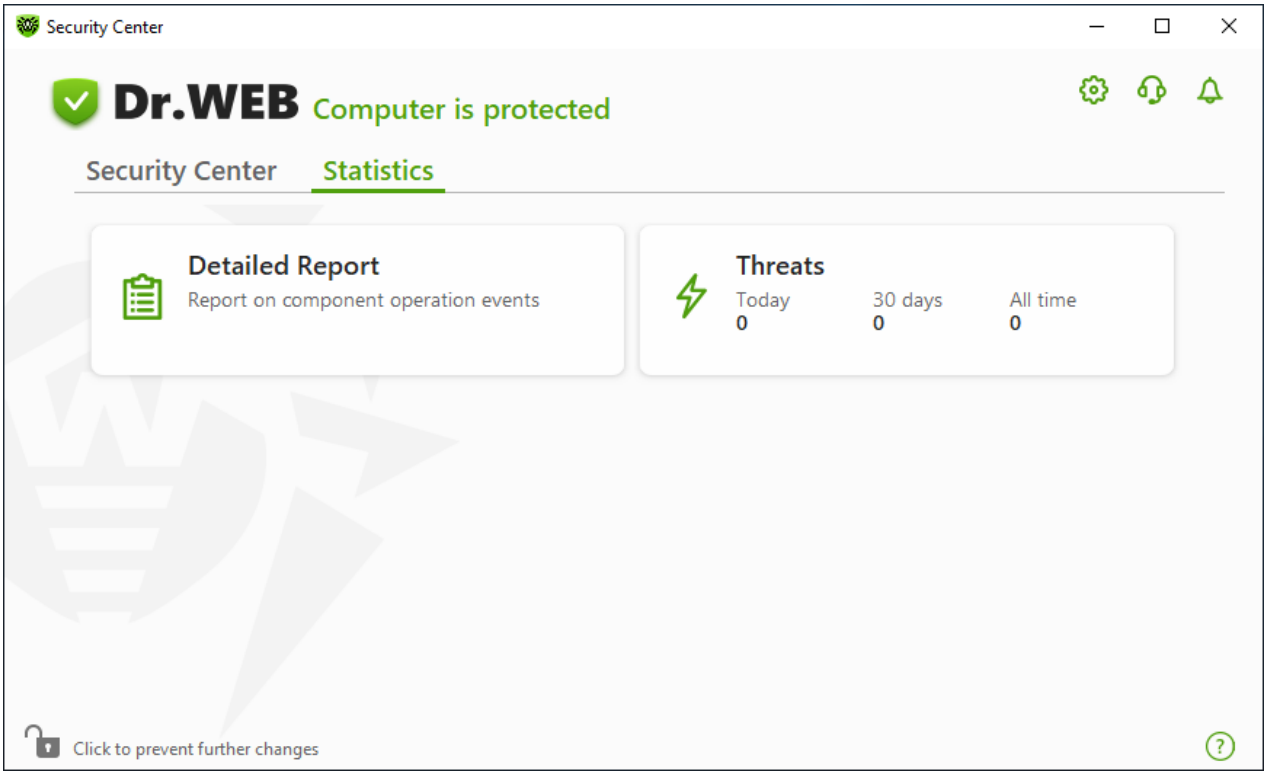

Figure 87. Statistics on component operation

4. Select a group to review the reports.

Detailed Report

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

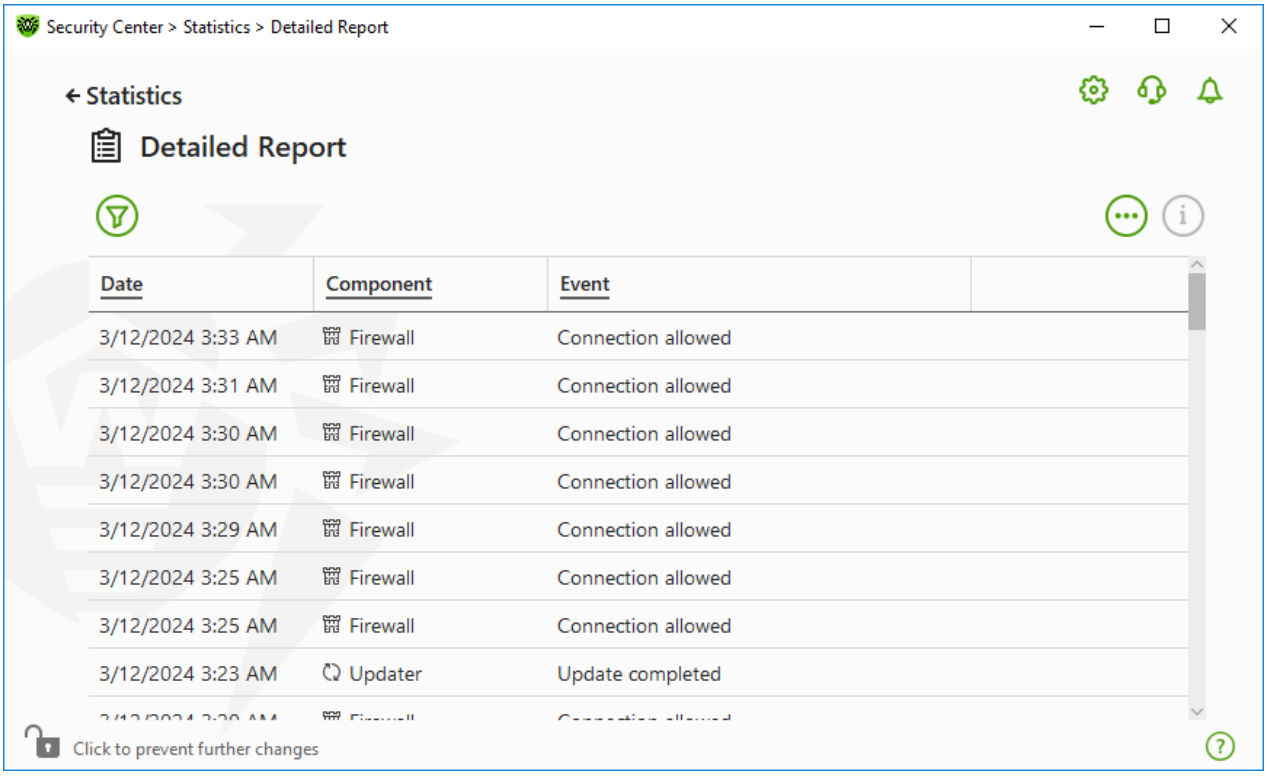

Figure 88. Detailed report window

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.

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.

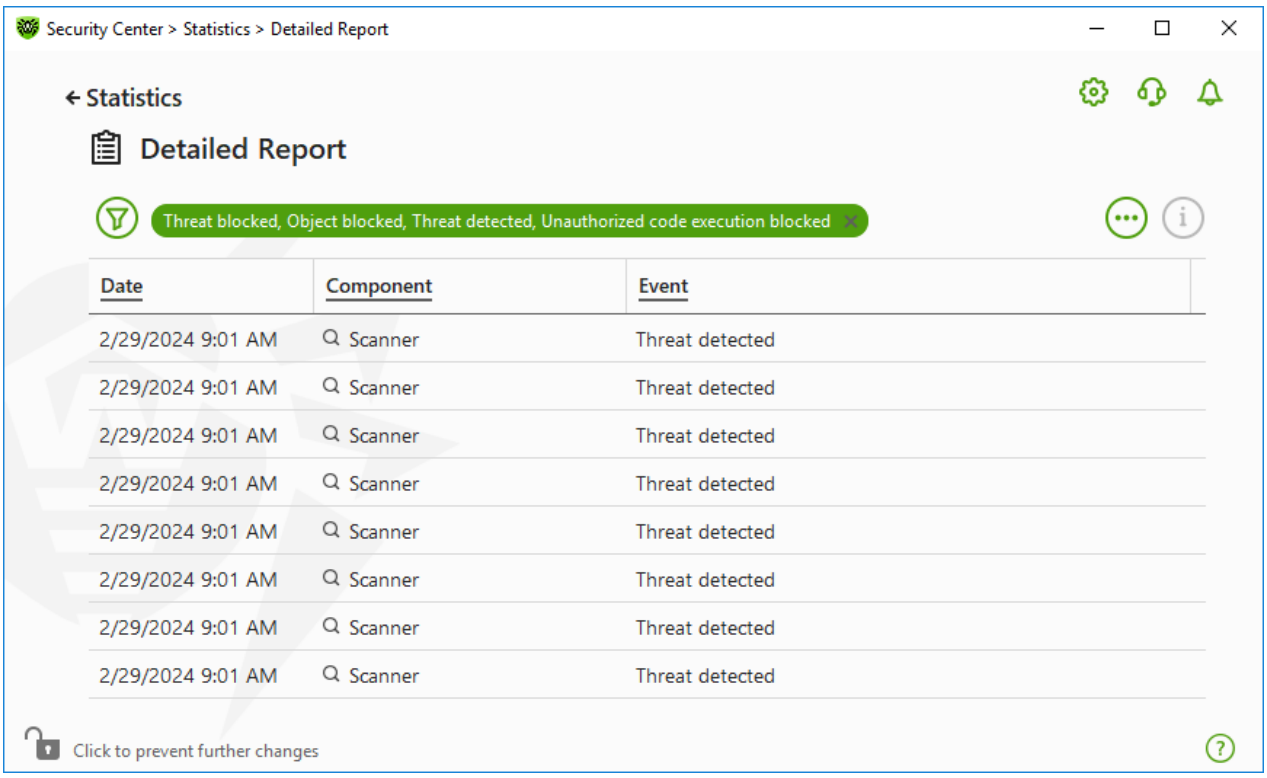

Figure 89. Statistics on threats window

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.

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.

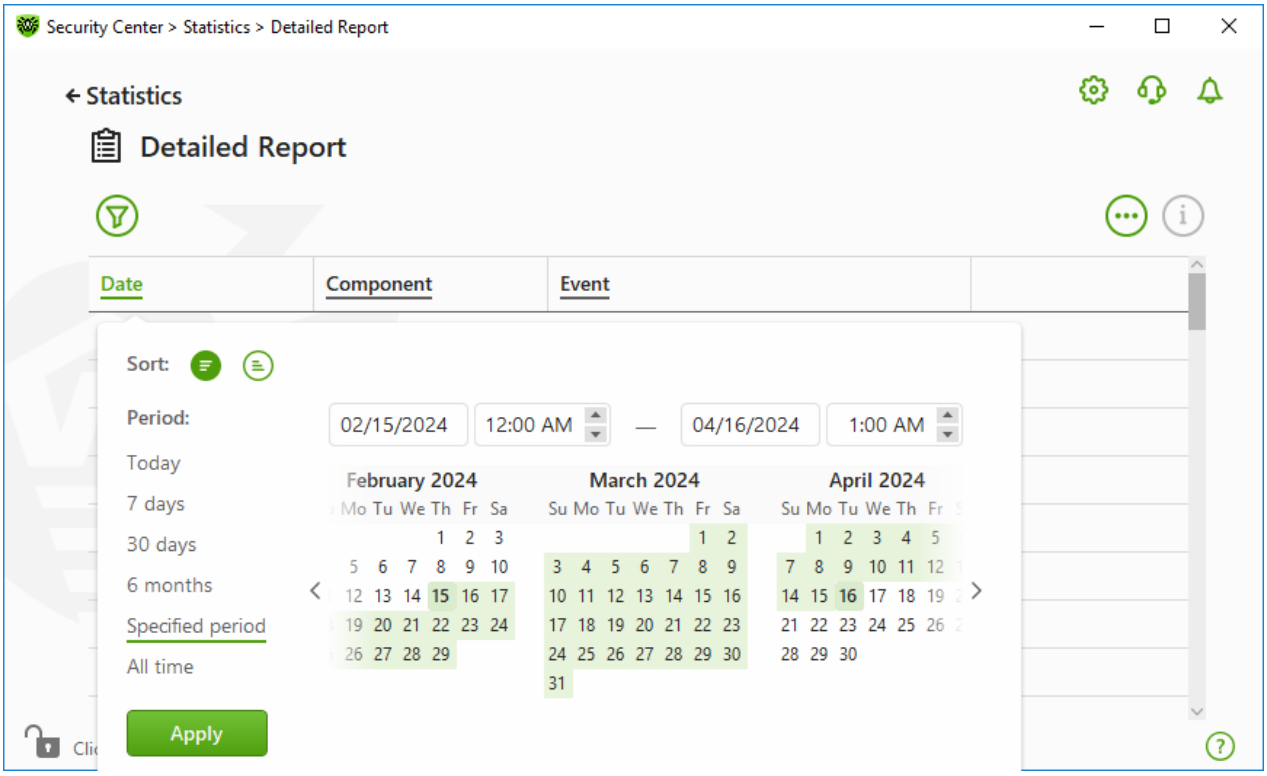

Figure 90. Data sorting

- 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.

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

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

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

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

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

16.1. Assistance in Resolving Problems

When contacting Doctor Web technical support, 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.

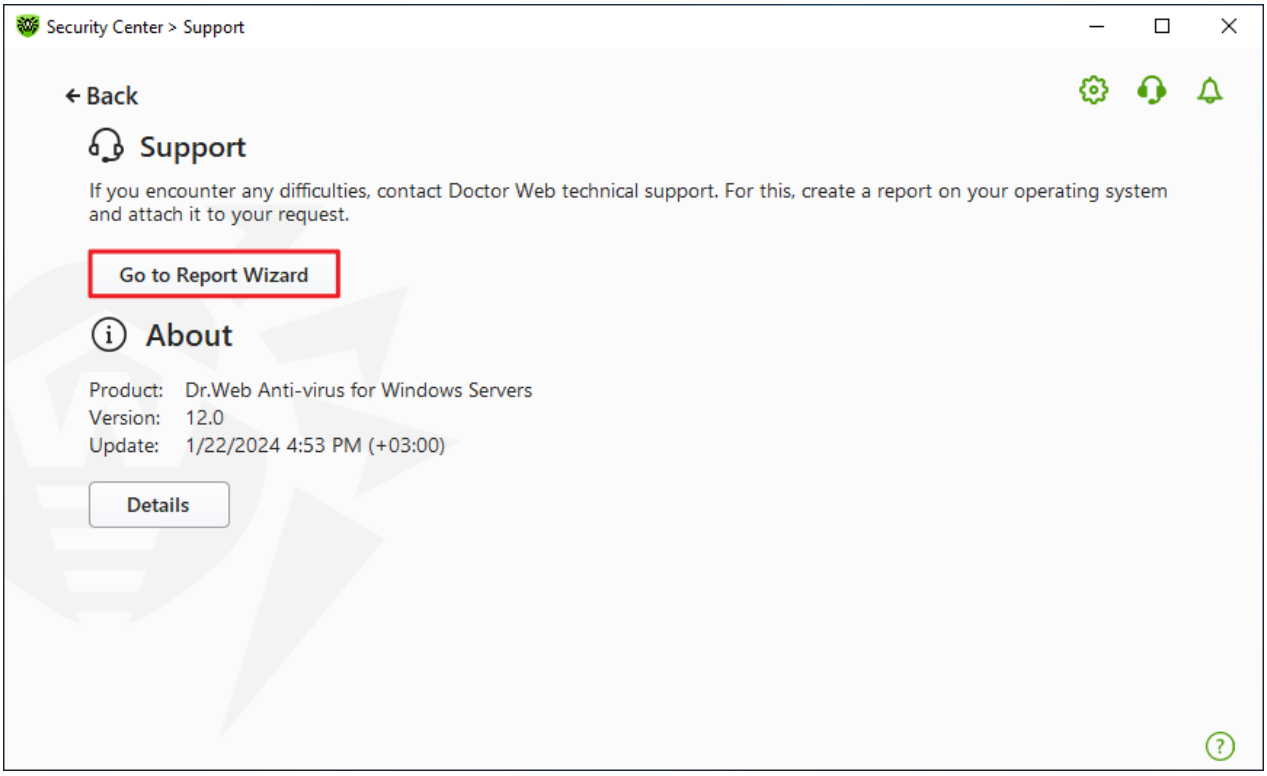

Figure 91. Support

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

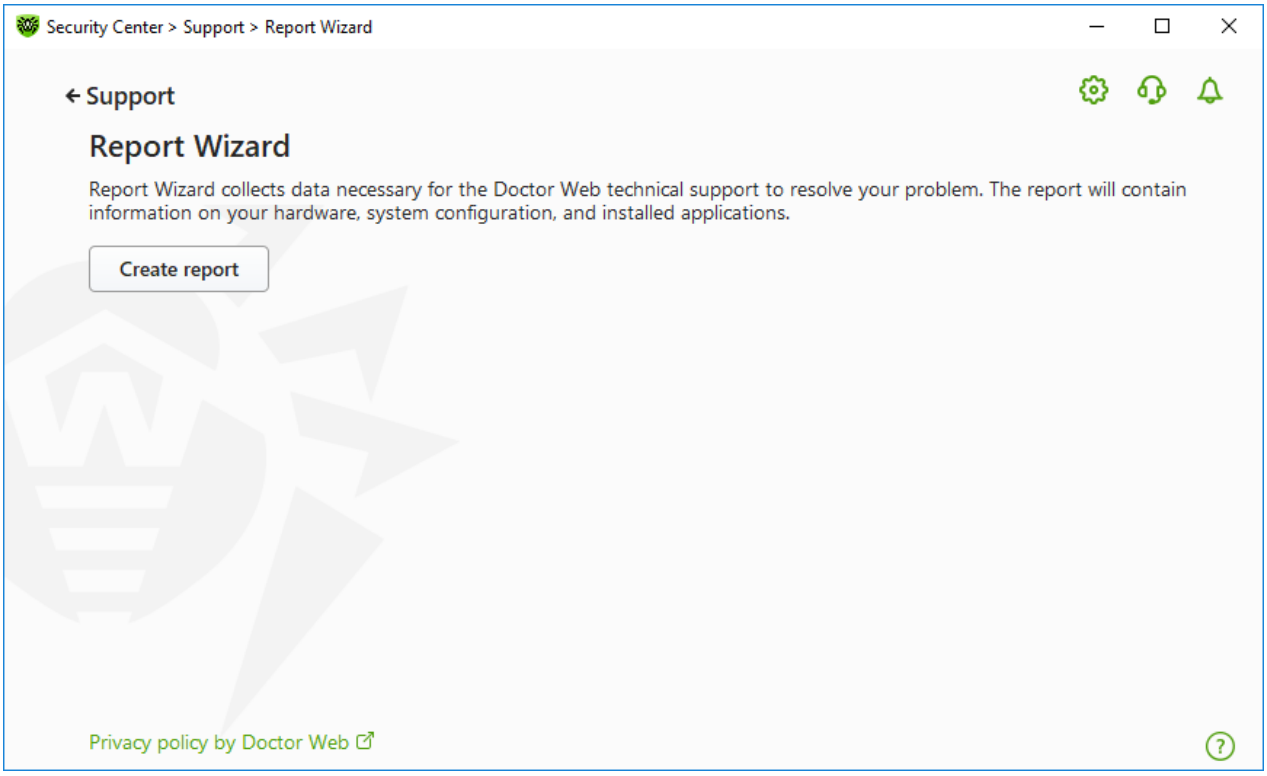

Figure 92. Generating a report for technical support

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

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 , 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.

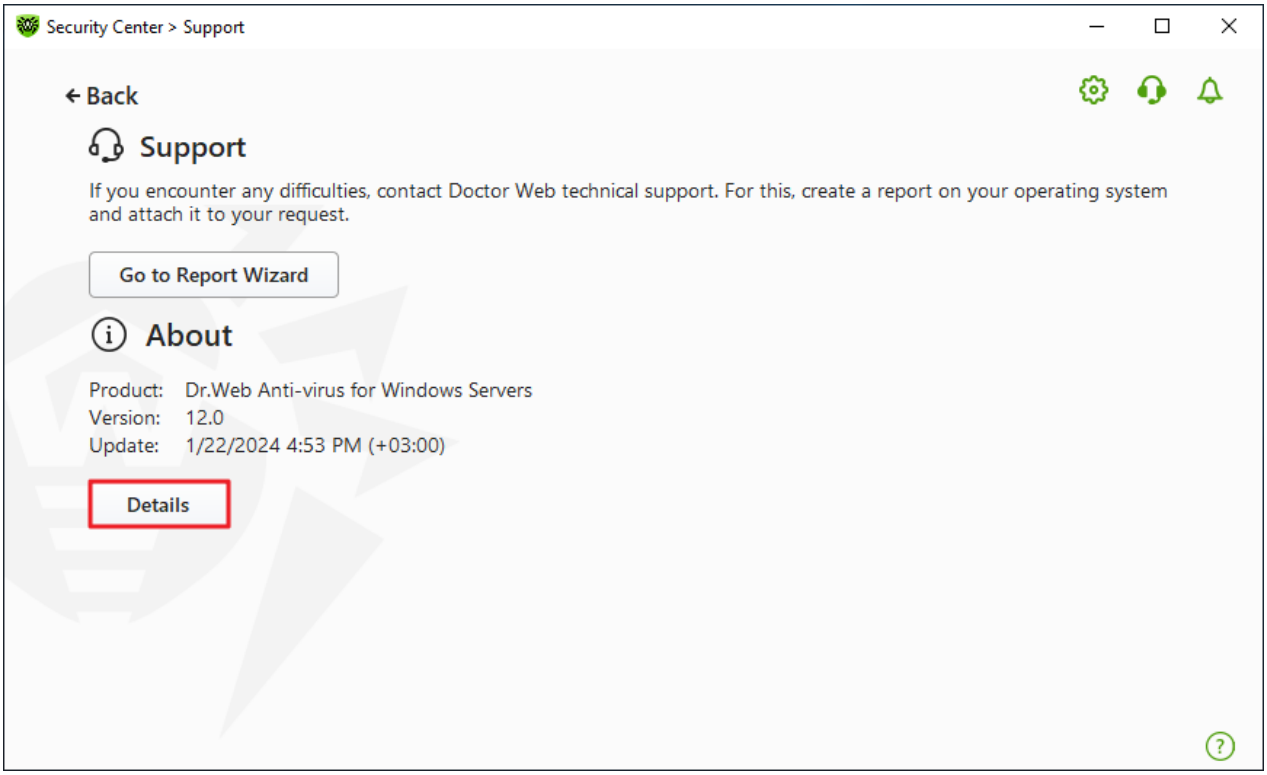

Figure 93. Access to the About Dr.Web window

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, Console Scanner and Dr.Web Updater.

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:<*commpression_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.)
/CL	Use cloud checking. Option is enabled by default. (For Console Scanner only.)
/DCT	Do not display estimated scan time. (For Console Scanner only.)
/DR	Scan folders recursively (scan subfolders). Option is enabled by default.

Switch	Description
/E:<*number_of_threads*>	Perform scanning in specified number of threads.
/FAST	Perform an express scan of the system. If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), the specified objects will also be scanned. (For Scanner only.)
/FL:<*file_name*>	Scan paths listed in the specified file.
/FM:<*mask*>	Scan files matching the specified mask. By default, all files are scanned.
/FR:<*regexpr*>	Scan files matching the specified regular expression. By default, all files are scanned.
/FULL	Perform a full scan of all hard drives and removable media (including boot sectors). If additional parameters are set (for example, objects to be scanned or /TM and /TB parameters), an express scan will be performed, and the specified objects will be scanned. (For Scanner only.)
/FX:<*mask*>	Exclude from scan files that match the specified mask. (For Console Scanner only.)
/GO	Scanner operation mode that skips the questions that require answers from a user; decisions that require a selection are made automatically. This mode is useful for the automatic file scan; for example, for the daily or weekly hard disk scanning. An object for scanning must be indicated in the command line. Along with the /GO parameter, it is also possible to use the following parameters: /LITE, /FAST, /FULL. In this mode, the scanning stops when switching to the battery power.
/H or /?	Show brief help. (For Console Scanner only.)
/HA	Use heuristic analysis to detect unknown threats. Option is enabled by default.
/KEY:<*key_file*>	Specify a path to the key file. It is necessary to use this parameter if your key file is stored outside of the installation folder where the scanner executables reside. By default, drweb32.key or another suitable file from the C:\Program Files\DrWeb\ folder is used.
/LITE	Perform a basic scan of random access memory and boot sectors of all disks as well as run a scan for rootkits. (For Scanner only.)
/LN	Resolve shell links. Option is disabled by default.
/LS	Scan using LocalSystem account rights. Option is disabled by default.

Switch	Description
/MA	Scan mail files. Option is enabled by default.
/MC:<*number_of_attempts*>	Set the maximum number of cure attempts. By default: unlimited.
/NB	Do not backup cured or deleted files. Option is disabled by default.
/NI[:X]	Limits usage of system resources at scanning (%). Defines the amount of memory required for scanning and the system priority of scanning process. By default: unlimited.
/NOREBOOT	Cancel system reboot or shutdown after scanning. (For Scanner only.)
/NT	Scan NTFS streams. Option is enabled by default.
/OK	Show the full list of scanned objects and mark clean files with Ok. Option is disabled by default.
/P:<*priority*>	Priority of the current scanning task. Can be as follows: 0—the lowest L—low N—normal (default priority) H—high M—maximal
/PAL:<*nesting_level*>	Maximum nesting level for executable packers. If a nesting level is greater than the specified value, scanning proceeds until this limit is reached. The nesting level is 1,000 by default.
/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	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

Switch	Description
	command-line mode).
/REP	Follow symbolic links while scanning. Option is disabled by default.
/RK	Scan for rootkits. Option is disabled by default.
/RP:<*file_name*>	Append the report on program operation to the specified file. By default, logging is disabled (when running Scanner in the command-line mode).
/RPC:<*sec*>	Scanning Engine connection time-out. Time-out 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	Display 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.

Switch	Description
/W:<*sec*>	Maximum time to scan (sec.). By default: unlimited.
/WCL	drwebwcl compatible output. (For Console Scanner only.)
/X:S[:R]	Set one of the following states for the computer to enter once scanning is 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. 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. Dr.Web Updater Command-Line Parameters

Common options

Parameter	Description
-h [--help]	Show a short help message on how to use the program.
-v [--verbosity] arg	Log level. Can be one of following: `error` (standard), `info` (extended), `debug`.
-d [--data-dir] arg	Folder where repository and settings are located.
--log-dir arg	Folder for storing the log file.
-r [--repo-dir] arg	Repository folder (<*data_dir*>`/repo` by default).
-t [--trace]	Enable tracing.
-c [--command] arg (=update)	Command to execute: `getversions`, `getcomponents`, `update`, `uninstall`, `exec`, `keyupdate`, and `download`.
-z [--zone] arg	Zones that are to be used instead of those specified in the configuration file.

update command parameters

Parameter	Description
-p [--product] arg	Product name. If specified, only this product will be updated. If neither a product nor certain components are specified, all products will be updated. If certain components are specified, only they will be updated.
-n [--component] arg	Components that are to be updated to the specified version. <*name*>, <*target revision*>.
-x [--selfrestart] arg (=yes)	Reboot after an update of Dr.Web Updater. Default value is `yes`. If the value is set to `no`, notification that reboot is required will appear.
--geo-update	Get the list of IP addresses from `update.drweb.com` before updating.
--type arg (=normal)	Can be one of the following: • `reset-all`—forced update of all components • `reset-failed`—reset revision for damaged components • `normal-failed`—try to update all components including damaged from the current revision to the newest or specified

Parameter	Description
	• `update-revision`—try to update all components of the current revision to the newest if exists • `normal`—update all components
-g [--proxy] arg	Proxy server for updating. *<address>:<port>*.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
--param arg	Pass additional parameters to the script. *<name>: <value>*.
-l [--progress-to-console]	Print information about downloading and script execution to the console.

getcomponents command parameters

Parameter	Description
-s [--version] arg	Version number.
-p [--product] arg	Specify the product to get the list of components that are included in this product. If the product is not specified, all components of this version will be listed.

getrevisions command parameters

Parameter	Description
-s [--version] arg	Version number.
-n [--component] arg	Component name.

uninstall command parameters

Parameter	Description
-n [--component] arg	Name of the component that is to be uninstalled.
-l [--progress-to-console]	Print information about command execution to the console.
--param arg	Pass additional parameters to the script. *<name>: <value>*.

Parameter	Description
-e [--add-to-exclude]	Components to be deleted. Update of this components will not be performed.

keyupdate command parameters

Parameter	Description
-m [--md5] arg	MD5 hash of the previous key file.
-o [--output] arg	Output file name to store new key.
-b [--backup]	Backup of an old key file if exists.
-g [--proxy] arg	Proxy server for updating. <*address*>:<*port*>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-l [--progress-to-console]	Print information about downloading of the key file to the console.

download command parameters

Parameter	Description
--zones arg	Zone description file.
--key-dir arg	Folder where the key file is located.
-l [--progress-to-console]	Print information about command execution to the console.
-g [--proxy] arg	Proxy server for updating. <*address*>:<*port*>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-s [--version] arg	Version name.
-p [--product] arg	Name of the product to download.

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 varies 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
- `HLLO`—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.

© Doctor Web, 2024