



Dr.WEB

Agent for Windows

User Manual

Жасағаныңды қорға

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© **Doctor Web, 2021. All rights reserved**

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

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

Trademarks

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

Disclaimer

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

Dr.Web Agent
Version 11.0
User Manual
2/3/2021

Doctor Web Head Office

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

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

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

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

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

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

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

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

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



Table of Contents

1. Introduction	6
1.1 About This Manual	7
1.2 Document Conventions	7
1.3 Detection Methods	8
2. System Requirements	10
3. Installing, Removing, or Changing the Program	12
3.1 Installing via Full Installer	12
3.2 Installing via Personal Installation Package	13
3.3 Reinstalling or Removing the Program	18
4. Getting Started	21
4.1 Testing the Anti-virus	22
5. Tools	24
5.1 Quarantine Manager	24
5.2 Support	25
5.2.1 Report Wizard	25
6. Dr.Web Scanner	27
6.1 Scanning Your System	27
6.2 Actions upon Detection	29
6.3 Command-Line Scanning Mode	30
6.4 Console Scanner	31
6.5 Automatic Launch of Scanning	32
7. Settings	33
8. Main Settings	34
8.1 Notifications	34
8.2 Self-Protection	37
8.3 Devices	38
8.4 Advanced	39
8.5 Mode	42
9. Office Control	45
9.1 Configuring Office Control	45
10. Exclusions	49
10.1 Websites	49



10.2 Files and Folders	50
10.3 Programs and Processes	52
10.4 Anti-spam	55
11. Protection Components	58
11.1 SplDer Guard	58
11.1.1 Configuring SplDer Guard	58
11.2 SplDer Gate	63
11.2.1 Configuring SplDer Gate	63
11.3 SplDer Mail	65
11.3.1 Configuring SplDer Mail	66
11.3.2 Anti-spam	69
11.4 Scanner	71
11.5 Dr.Web Firewall	74
11.5.1 Training Dr. Web Firewall	74
11.5.2 Configuring Firewall	75
11.6 Dr.Web for Microsoft Outlook	85
11.6.1 Configuring Dr.Web for Microsoft Outlook	85
11.6.2 Threat Detection	86
11.6.3 Spam Check	87
11.6.4 Event Logging	90
11.6.5 Statistics	91
11.7 Preventive Protection	92
12. Statistics	97
Appendices	99
Appendix A. Command-Line Parameters	99
Scanner and Console Scanner Parameters	99
Installation Packages Parameters	103
Return Codes	106
Appendix B. Computer Threats and Neutralization Methods	107
Classification of Computer Threats	107
Actions Applied to Threats	112
Appendix C. Naming of Viruses	113



1. Introduction

Dr.Web Agent provides multilevel protection of RAM, hard disks, and removable media against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

The module architecture of Dr.Web is its significant feature. The anti-virus engine and virus databases are common for all components and different operating environments. At present, in addition to Dr.Web products for Windows, there are versions of anti-virus software for Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian®, BlackBerry®, and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

Dr.Web uses a convenient and efficient procedure for updating virus databases and program components via the Internet.

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

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

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

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

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

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

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

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

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



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

Dr.Web Agent—a utility that lets you set up and manage Dr.Web components.

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

1.1 About This Manual

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

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

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

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



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

1.2 Document Conventions

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

Convention	Comment
	Warning about potential errors or any other important comment.
<i>Signature</i>	A new term or an accent on a term in its description.
<key_file>	Fields whose function names can be replaced with actual values.
Next	Names of buttons, windows, menu items, and other interface elements.
C:\Windows\	Names of files and catalogs, code examples.
Appendix A	Cross references to topics and hyperlinks to external resources.



1.3 Detection Methods

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

Detection Methods

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".

While performing any of the abovementioned checks, Dr.Web anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web anti-virus laboratory discover new threats, the update for virus signatures, behavior characteristics, and attributes is issued. In some cases, updates can be issued several times per hour. Therefore, even if a brand new virus passes through Dr.Web resident guards and penetrates the system, after an update it is detected on the list of processes and neutralized.



2. System Requirements



Before installing Dr.Web:

- Remove any anti-virus software from your computer to prevent possible incompatibility of resident Dr.Web components.
- in case of installation of Dr.Web Firewall, uninstall all other firewalls from your computer.
- In Windows Server 2016, disable Windows Defender manually, using group policies.
- Install all critical updates recommended by the operating system developer. If the operating system is no longer supported, then upgrade to a newer operating system.

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

Component	Requirement
CPU	An i686-compatible processor.
Operating system	<p>For 32-bit platforms:</p> <ul style="list-style-type: none">• Windows XP with Service Pack 2 or higher• Windows Vista with Service Pack 2 or higher• Windows 7• Windows 8• Windows 8.1• Windows 10• Windows Server 2003 with Service Pack 1• Windows Server 2008 with Service Pack 2 or higher <p>For 64-bit platforms:</p> <ul style="list-style-type: none">• Windows Vista with Service Pack 2 or higher• Windows 7• Windows 8• Windows 8.1• Windows 10• Windows Server 2008 with Service Pack 2 or higher• Windows Server 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016
Free RAM	Minimum 512 MB.



Component	Requirement
Hard disk space	1 GB for Dr.Web components. Files created during installation will require additional space.
Resolution	Minimum recommended screen resolution is 800x600.
Other	To update Dr.Web virus databases and Dr.Web components, connection to the central protection server or to the Internet in the Mobile mode is required. For the Dr.Web for Microsoft Outlook extension, one of the following Microsoft Outlook clients from the Microsoft Office package is required: <ul style="list-style-type: none">• Outlook 2000• Outlook 2002• Outlook 2003• Outlook 2007• Outlook 2010 with Service Pack 2• Outlook 2013• Outlook 2016



Dr.Web Agent is not compatible with Dr.Web for Microsoft Exchange Server, Dr.Web for IBM Lotus Domino, Dr.Web for Kerio WinRoute, Dr.Web for Kerio MailServer, Dr.Web for Microsoft ISA Server and Forefront TMG, Dr.Web for Qbik WinGate version 6.0 and earlier.

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

Purpose	Direction	Port numbers
To connect to Dr.Web Cloud	outgoing	2075 (including UDP)

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



3. Installing, Removing, or Changing the Program

Before installing Dr.Web, note the [system requirements](#) and do the following:

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



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

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

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

3.1 Installing via Full Installer



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

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

- The background mode
- The graphical mode

Installation in the background mode

To start the installation of Dr.Web in the background mode, enter the executable file name and specify necessary parameters. For example, background installation of Dr.Web starts upon the execution of the following command:

```
drweb-esuite-agent-full-11.00.0-xxxxxxxx-windows.exe /silent yes
```

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

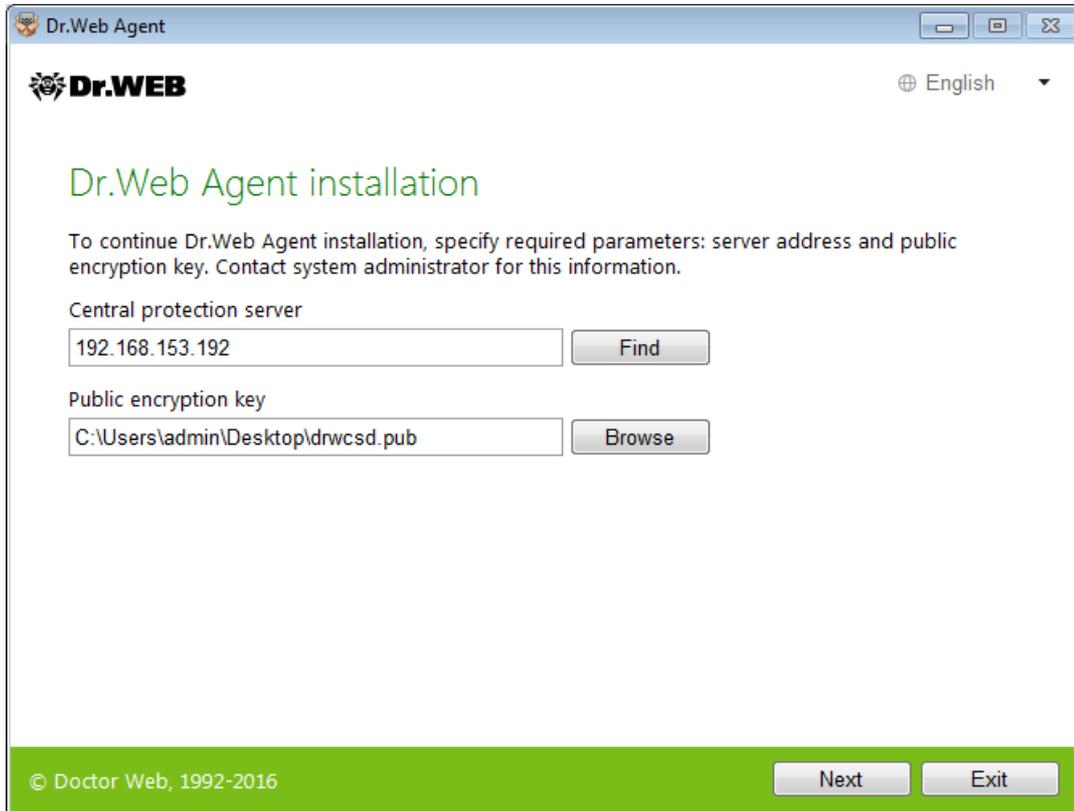
Installation in the graphical mode

1. Run the installation package received from the administrator.



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

The window of Dr.Web Installation Wizard opens.



2. In the **Central protection server** field, specify the network address of the server, from which Dr.Web is to be installed, and in the **Public encryption key** field specify the full path to the key (drwcsd.pub) residing on your computer.

Click **Next**. The Installation Wizard starts to establish the server connection.



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

- 3.

3.2 Installing via Personal Installation Package



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

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

- The background mode



- The graphical mode

Installation in the background mode

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

```
drweb-ess-installer.exe /silent yes
```

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

Installation in the graphical mode

1. Run the installation package received from the administrator.

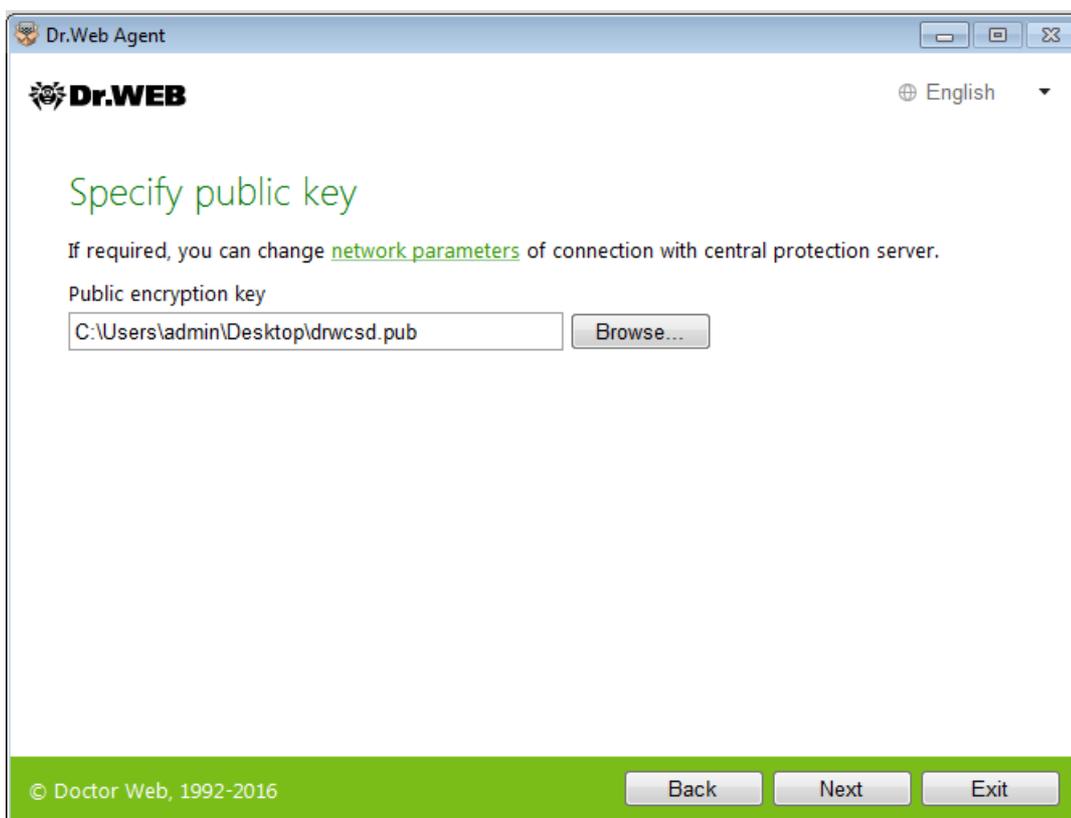


If there is any anti-virus software installed on the computer, the Installation Wizard will attempt to remove it before starting the installation. If the attempt fails, you need to remove the current anti-virus software manually.

The window of Dr.Web Installation Wizard opens.

Click **Next**.

2. In the next window, the full path to the public key (drwcsd.pub) residing on your computer is specified.



3. You can adjust parameters of connection to the central protection server. To do that, click the corresponding link and make required changes in the open **Connection parameters**.



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

Dr.Web Agent

English

Connection parameters

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

Central protection server
tcp/10.4.0.112:2193 Find

Manual authorization on server

Identifier
[Empty text box]

Password
[Empty text box]

Compression
Possible (by default)

© Doctor Web, 1992-2016 OK Cancel



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

In the **Central protection server** field, specify the network address of the server, from which Dr.Web is to be installed. This field is automatically filled in with parameters of the server selected for the installation.

To enable manual authorization on the server, select the corresponding check box. After that, specify the following authorization parameters: **Identifier** of the workstation and **Password** to access the server. In this case, the workstation does not require manual approval of the administrator to get access to the server.



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

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

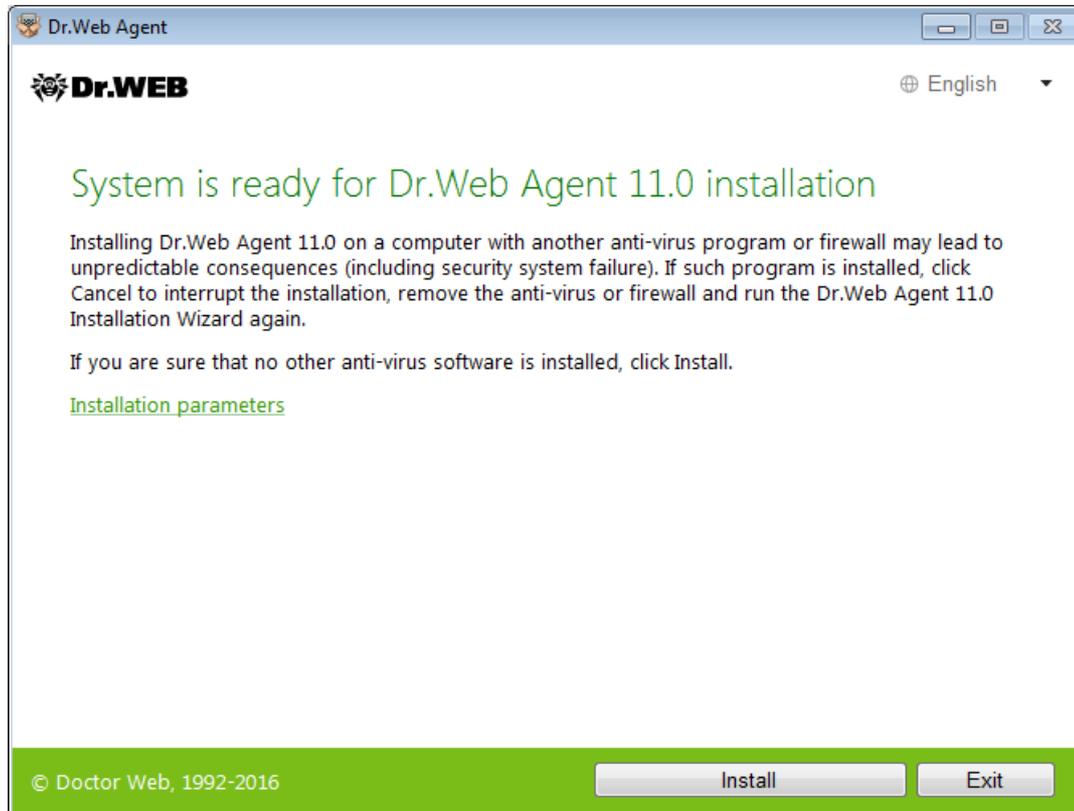
To save the changes, click **OK**. This will return you to the previous window.

Click **Next**. The Installation Wizard starts to establish the server connection.



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

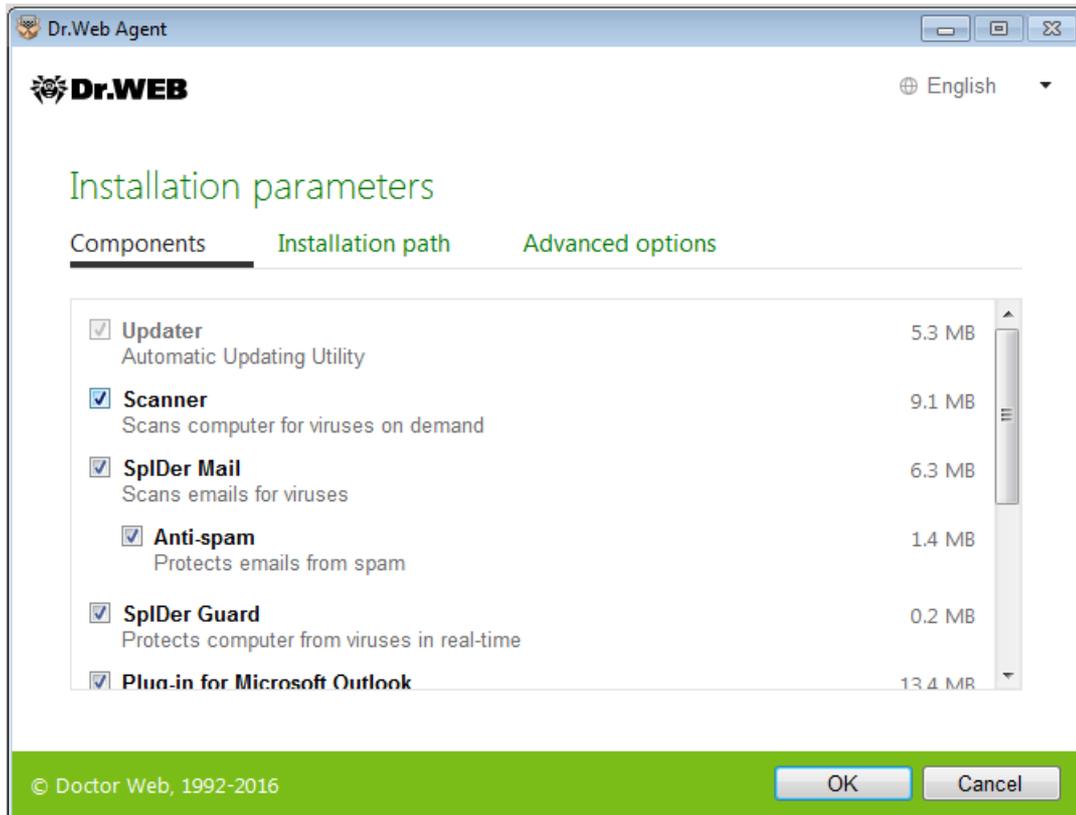
4. After the connection is established, the window opens notifying you that the product is ready to be installed. To start installation with the default parameters, click **Install**.



To select components you want to install, specify the installation path, and configure other settings, click **Installation parameters**. The option is meant for experienced users.

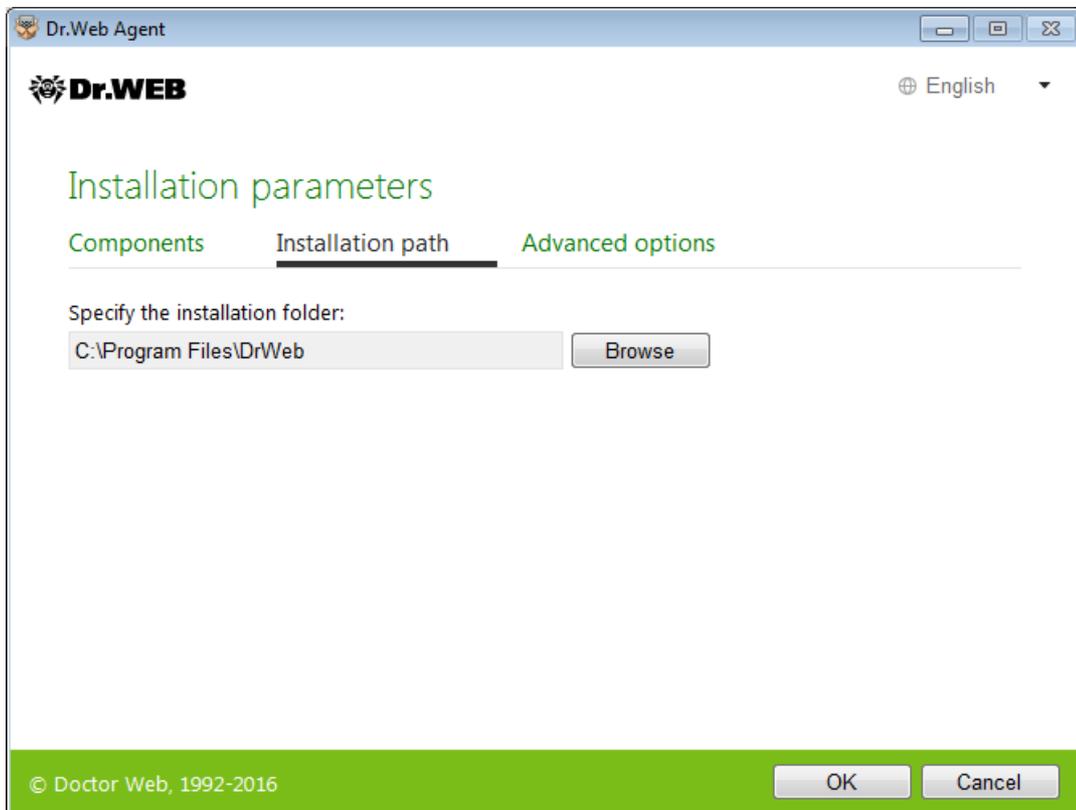
5. If you selected **Install** at the previous step, go to the description of step 8. Otherwise, the **Installation parameters** window opens.

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



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

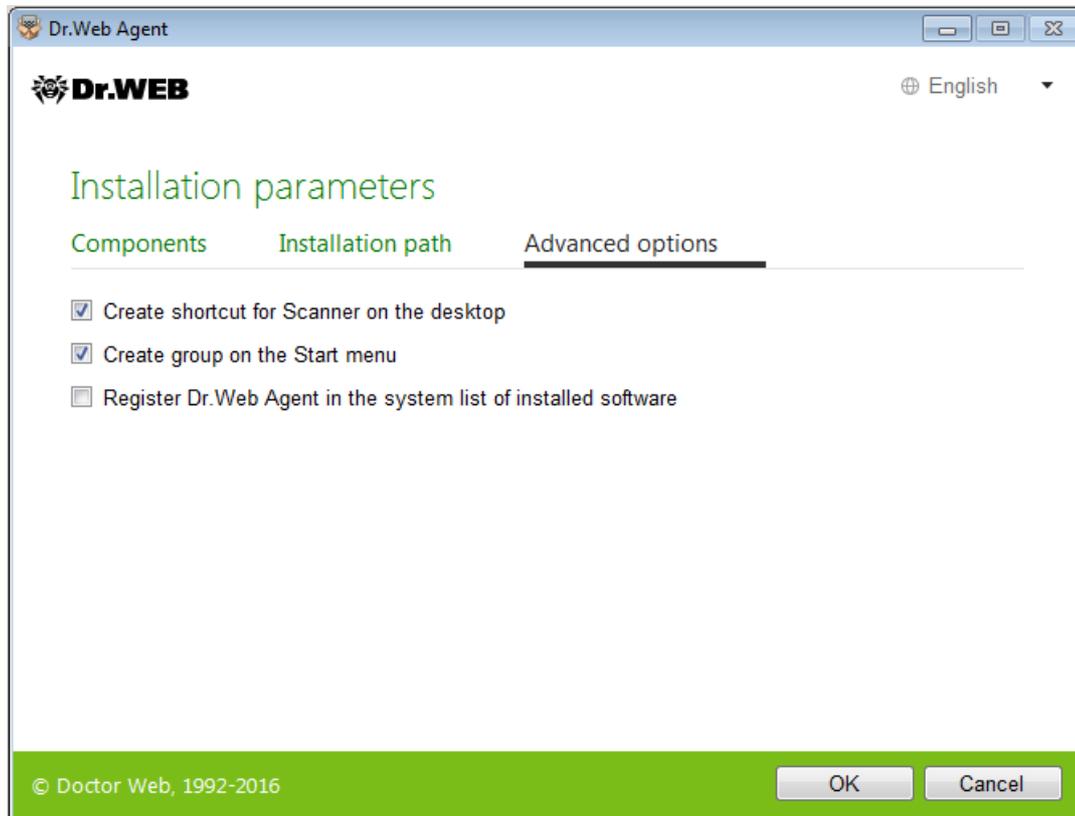
6. On the **Installation Path** page, specify the folder for Dr.Web to be installed into.





By default, it is installed into the Dr.Web folder in the Program files folder on the system disk. To change the installation path, click **Browse** and specify the necessary folder.

7. On the **Advanced options** page, you are prompted to create shortcuts that start Dr.Web.



If required, enable the **Register Dr.Web Agent in the list of installed programs** option. This option also allows to [remove](#) Dr.Web by the means of standard Windows tools.

To save the changes, click **OK**. This will return you to the previous window.

Click **Install**.

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

3.3 Reinstalling or Removing the Program



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

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



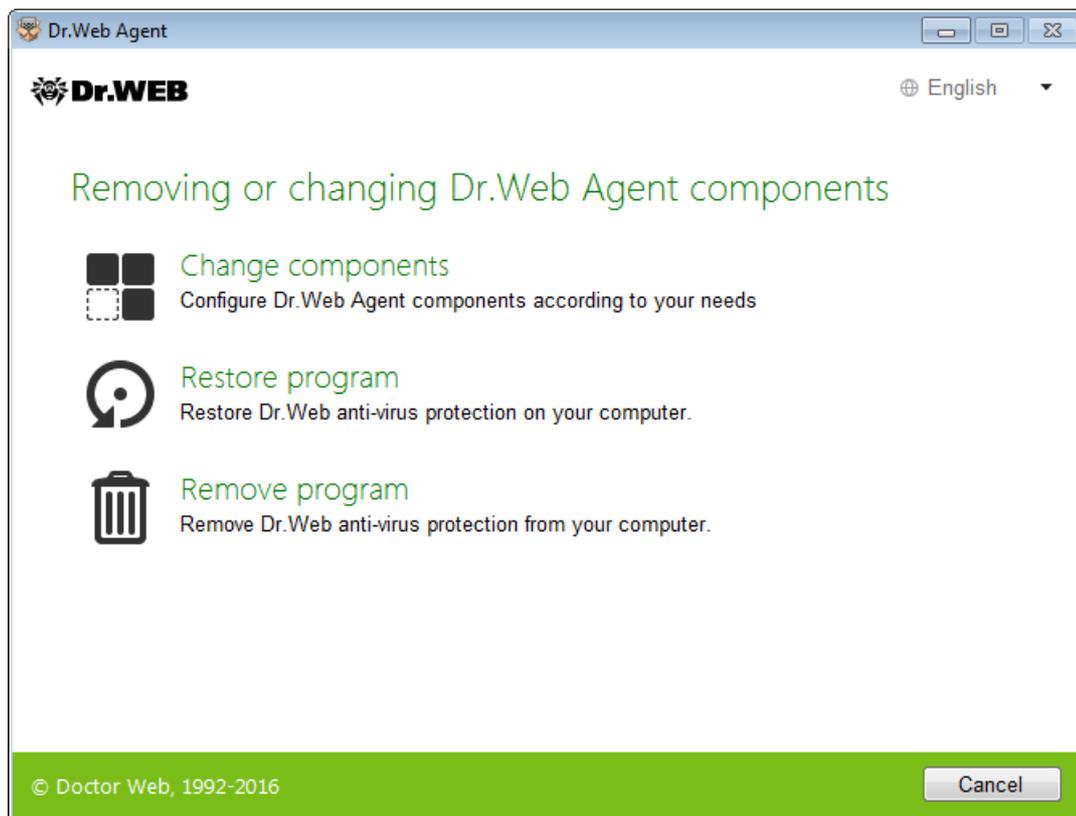
Uninstalling or changing Dr.Web with standard Windows tools



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

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

1. To uninstall Dr.Web or change its configuration by adding or removing individual components, run the standard Windows uninstall tool.
2. In the open window, select the program. To delete the program completely, click **Remove** and go to step 6. To change the configuration of Dr.Web by adding or removing certain components, click **Edit**. The window of the Installation Wizard opens.



3. To restore anti-virus protection on your computer, select **Restore program**.
4. To change the Dr.Web configuration, click **Change components**. In the open window, select check boxes of the components you want to add and clear check boxes of the components you want to remove. When you finish adjusting the component set, click **Apply**.
5. To delete all installed components, select **Remove program**.



6. In the **Parameters to save** window, select check boxes of those components that you do not want to remove from your system. Saved objects and settings can be used by the program if it is installed again. By default, all options—**Quarantine**, **Dr.Web Settings Agent** and **Protected file copies**—are selected. Click **Install**.
7. In the next window for the confirmation of deletion of Dr.Web click **Remove**.
8. Once you reboot your computer, the changes are applied. You can snooze the reboot by clicking **Later**. Click **Restart now** to immediately complete the procedure of Dr.Web components deletion or modification.

Uninstalling with command-line parameters

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



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

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

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



4. Getting Started

When Dr.Web is installed, the SpIDer Agent icon  displays in the notification area.



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

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

The SpIDer Agent icon indicates the status of Dr.Web:

- —all necessary components are running and protect your computer; connection to the central protection server is established.
- —Dr.Web self-protection or an important component is disabled, which compromises security of the anti-virus and your computer, or connection to the server is expected. Probably the server refused the connection or denied access to its resources. Enable self-protection or the disabled component, wait until the connection to the server is established or contact your anti-virus network administrator if the connection is not established.
- —components are expected to start after the operating system startup process is complete, thus wait until the components start; or an error occurred while starting one of the main Dr.Web components, and your computer is at risk of virus infection. If the icon does not change, contact your anti-virus network administrator.

Various notifications may appear over the SpIDer Agent icon  if [configured](#).

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



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

The SpIDer Agent menu  allows to access the main management and setting functions of Dr.Web.

Tools. Opens a submenu providing access to:

- [Quarantine Manager](#)
- Go to [Support](#).

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

Scanner. Quick access to launching different kinds of scanning.



Operation mode . Allows to switch between user mode and administrator mode. By default, Dr.Web starts in restricted user mode, which does not provide access to [Settings](#) and settings of [Protection components](#). To switch to another mode, click the lock. If UAC is enabled, operating system will prompt a request for administrative privileges. Besides, you also need to enter the password to change the mode, if you set **Protect Dr.Web settings with a password** option on the [Settings](#) window.

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

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



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

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

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

Help . Opens the help file.

4.1 Testing the Anti-virus

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

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

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

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

```
X5O!P%@AP[4\ZX54(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.



5. Tools

5.1 Quarantine Manager

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

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

To open this window, click the SpIDer Agent icon  in the notification area, select **Tools**, and then select **Quarantine Manager**.

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.

In the objects context menu, the following buttons are available:

- **Restore**—move the file to the selected folder and specify a new file name.



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

- **Scan**—scan the file in quarantine again.
- **Remove**—delete the file from the Quarantine and from the system.

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

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



5.2 Support

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

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

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

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

If you have not found a solution for the problem, you can request direct assistance from Doctor Web technical support by filling in the web form at <http://support.drweb.com/>.

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

5.2.1 Report Wizard

When contacting your anti-virus network administrator technical support, you can generate a report on your operating system and Dr.Web operation.

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

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

1. Technical information about the operating system:

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



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

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

Report generation from command line

To generate a report, use the following command:

```
/auto
```

For example: `Exampledwsysinfo.exe /auto`

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

You can also use the command:

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

where

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

For example: `Exampledwsysinfo.exe /auto /report:C:\report.zip`



6. Dr.Web Scanner

Dr.Web Scanner for Windows allows you to run anti-virus scans of disk boot sectors, random access memory (RAM), and both separate files and objects enclosed within complex structures (archives, containers, or email attachments). The program uses all [detection methods](#) to detect viruses and other malicious software. By default, Dr.Web Scanner checks all files for viruses using both the virus database and the heuristic analyzer (a method based on the general algorithms of virus developing allowing to detect the viruses unknown to the program with a high probability). Executable files compressed with special packers are unpacked when scanned. Files in archives of all commonly used types (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, etc.), in containers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM, etc.), and in mailboxes of mail programs (the format of mail messages should conform to RFC822) are also checked.

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

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

6.1 Scanning Your System

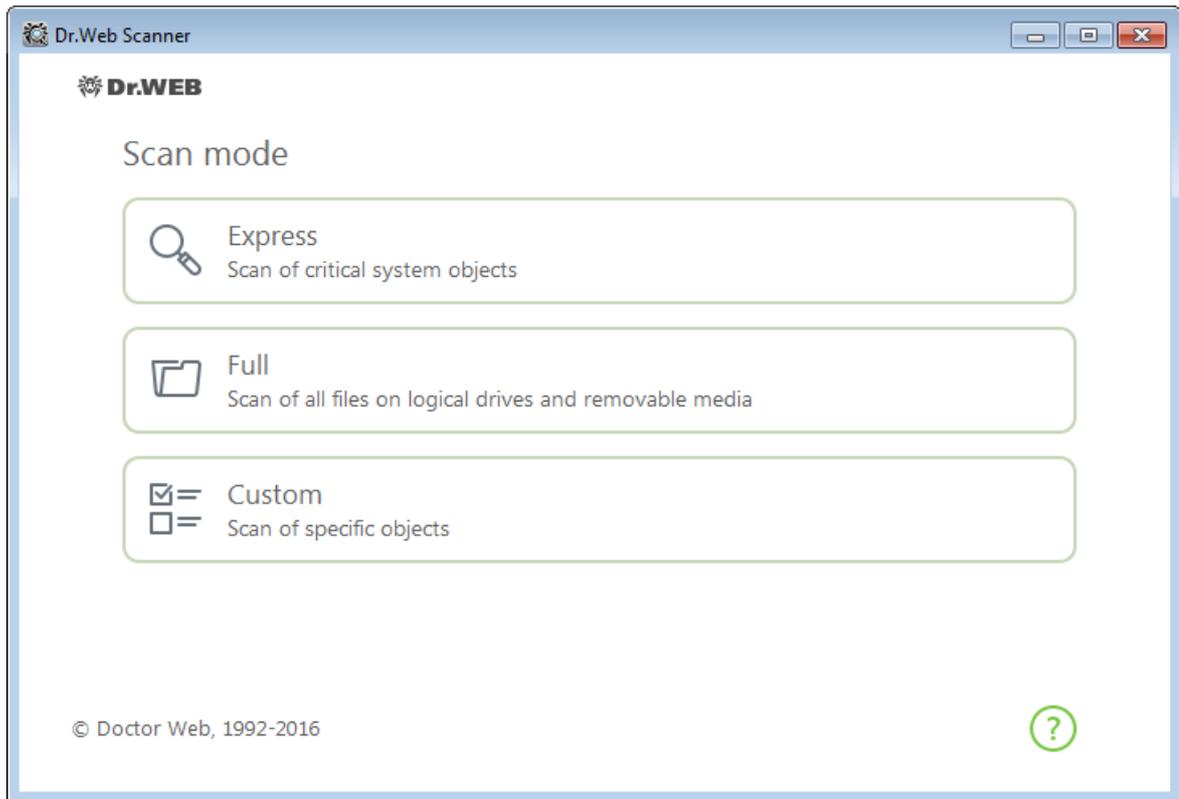
To select the scan mode



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

1. Click the SpIDer Agent [menu](#)  and select **Scanner**. The menu of quick access to different scan modes opens.
2. Click the **Custom** item to scan only selected objects. The Dr.Web Scanner window opens.
3. Click the **Express** or **Full** item to run the corresponding scan mode.

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



Configuring Dr.Web Scanner

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

Scan modes

Express scan

In this mode, Scanner checks the following:

- Boot sectors of all disks
- Random access memory
- Boot disk root folder
- Windows system folder
- User documents folder ("My Documents")
- Temporary files
- System restore points
- Presence of rootkits (if the process is run with administrative privileges)



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



Full scan

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

Custom scan

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

Scan process

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

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



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

6.2 Actions upon Detection

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



By clicking **Neutralize**, you apply actions to the objects selected in the table. Dr.Web Scanner selects all objects by default once scanning completes. If necessary, you can select objects or groups of objects manually to set an action applied by clicking **Neutralize**. To do this, use check boxes next to object names or the drop-down menu in the table header.

To select an action

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

There are the following limitations:

- For suspicious objects, curing is impossible.



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

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

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



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

6.3 Command-Line Scanning Mode

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

To run scanning from command line

For that purpose, use the following command:

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

where

- `<objects>` is a placeholder for the list of objects to be scanned.
- `<switches>` are command-line parameters that specify settings of Scanner. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them).



The list of objects for scanning can be empty or contain several elements separated by spaces. The most common scan modes are as follows:

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

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

6.4 Console Scanner

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



Console Scanner moves suspicious files to Quarantine.

To run Console Scanner

The command syntax to launch Console Scanner is as follows:

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

where

- <objects> is a placeholder for the list of objects to be scanned.
- <switches> is a placeholder for command-line parameters that configure Console Scanner operation.

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](#).

After the operation is complete, Console Scanner returns one of the following 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.

6.5 Automatic Launch of Scanning

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

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

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

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

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



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



7. Settings

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

Password protection

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



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



8. Main Settings

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



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

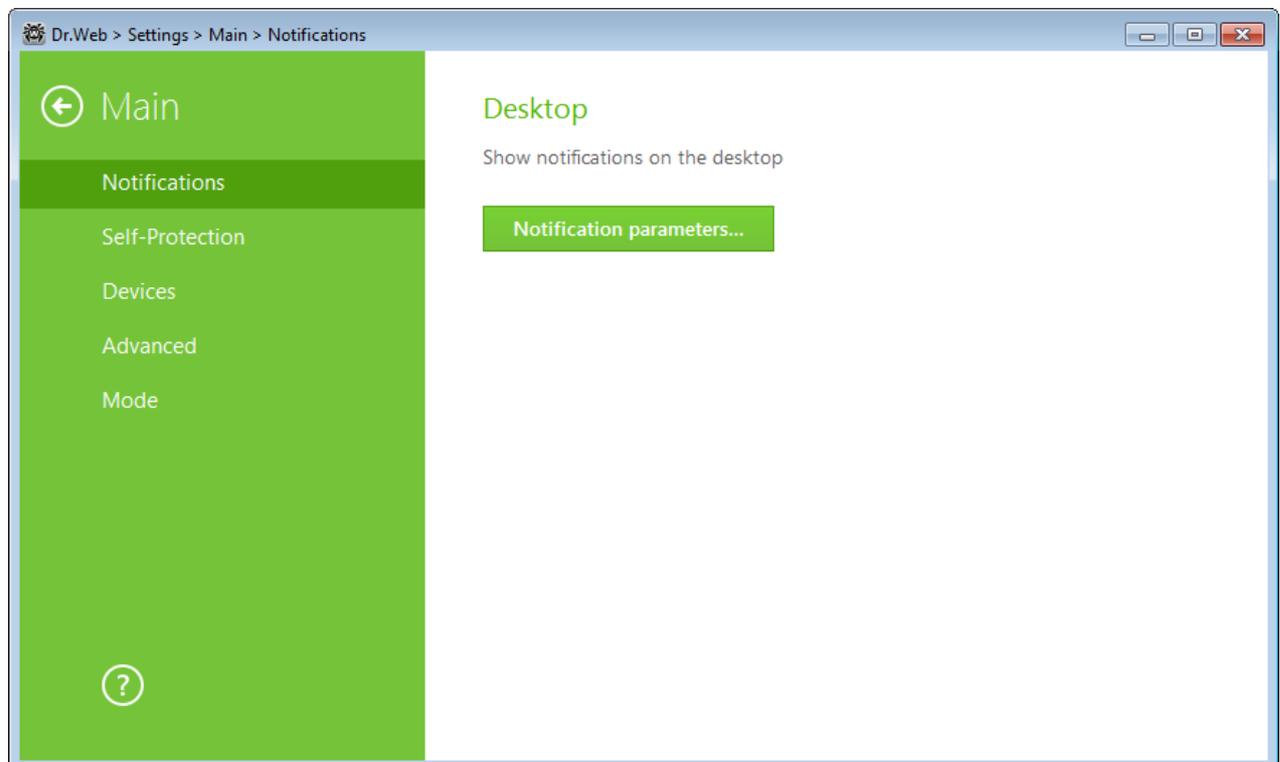
To access the main Dr.Web settings, you are prompted to enter the password if you enabled the **Protect Dr.Web settings with a password** option in the [Settings](#) window.

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

8.1 Notifications

Pop-up notifications

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





Notification parameters

1. Click **Notifications parameters**.
2. Select types of notifications that you want to receive and select the corresponding check boxes.

Notification type	Description
Threat notifications	Select to be notified on threats detected by SpliDer Guard and SpliDer Gate. Clear if you do not want to be notified. By default, these notifications are enabled.
Critical notifications	Select to be notified on the following critical issues: <ul style="list-style-type: none">• Connections waiting for Firewall to reply are detected• Your login and password are already used for connection to central protection server. Clear if you do not want to be notified on the issues listed above. By default, these notifications are enabled.
Major notifications	Select to be notified on the following major issues: <ul style="list-style-type: none">• Expiration of the time limit set for working on the computer.• Device is blocked.• An attempt to access a protected object is blocked by Preventive Protection.• Attempt to change system date and time is blocked.• Virus databases are out of date (when operating in Mobile mode). Clear if you do not want to be notified on the issues listed above. By default, these notifications are enabled.
Minor notifications	Select to be notified on the following minor issues: <ul style="list-style-type: none">• Successful update.• Update failures.• Expiration of the time limit set for Internet use.• URL is blocked by Office Control.• URL is blocked by SpliDer Gate.• An attempt to access a protected object is blocked by Office Control• Scan of your computer is run by administrator of your anti-virus network.• Scan of your computer is run according to schedule.• Scan of your computer is finished. Clear if you do not want to be notified on the issues listed above. By default, these notifications are disabled.



3. If necessary, configure additional parameters:

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



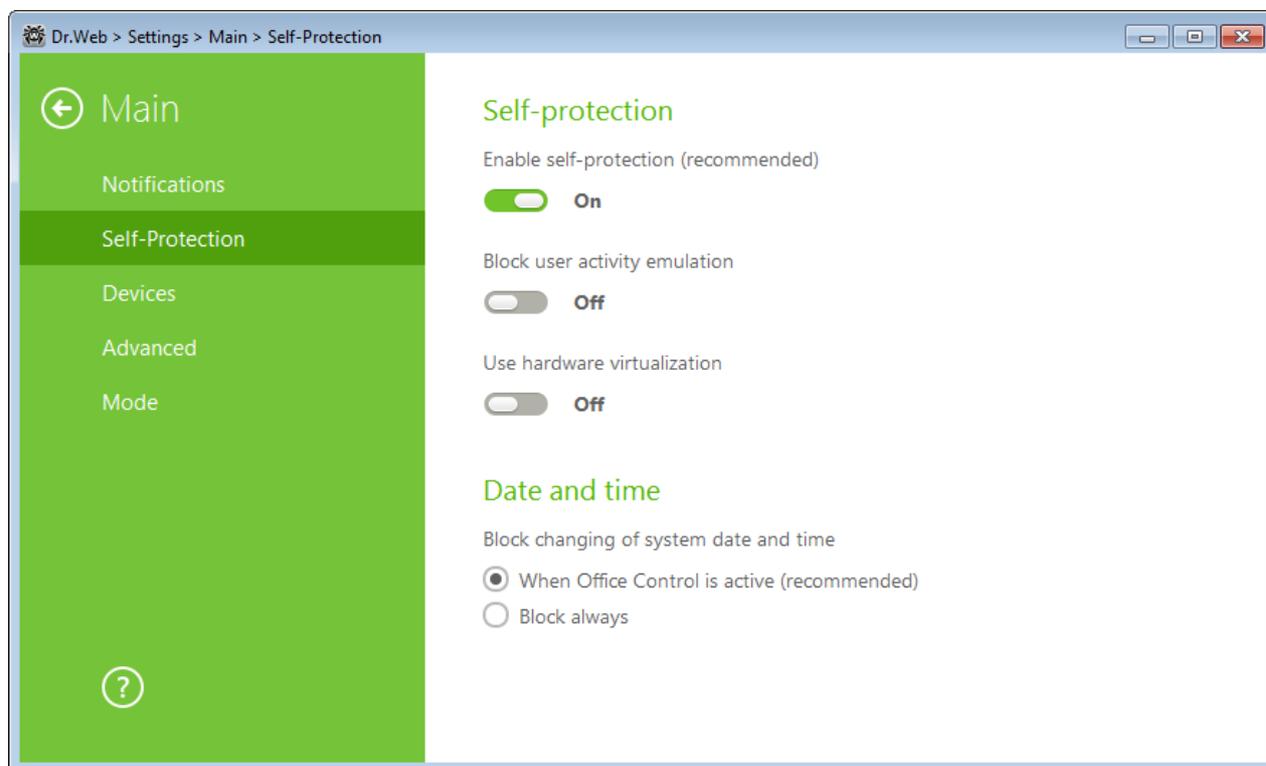
Notifications on the following issues are not included in any of the specified groups and are always displayed to the user:

- Priority updates installed and restart is required.
- To finish neutralizing threats, restart the computer.
- To enable or disable the hypervisor, restart the computer.
- Request for allowing a process to modify an object
- Messages sent by central protection server administrator.



8.2 Self-Protection

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



Self-protection

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



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

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

The **Block user activity emulation** option allows to prevent any automatic changes in Dr.Web settings, including execution of scripts that emulate user interaction with Dr.Web and are launched by the user (for example, scripts to make changes in Dr.Web settings, license removal and other actions aimed at changing Dr.Web operation).

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



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

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

If problems occur, disable this option.

32-bit platforms do not support hardware virtualization

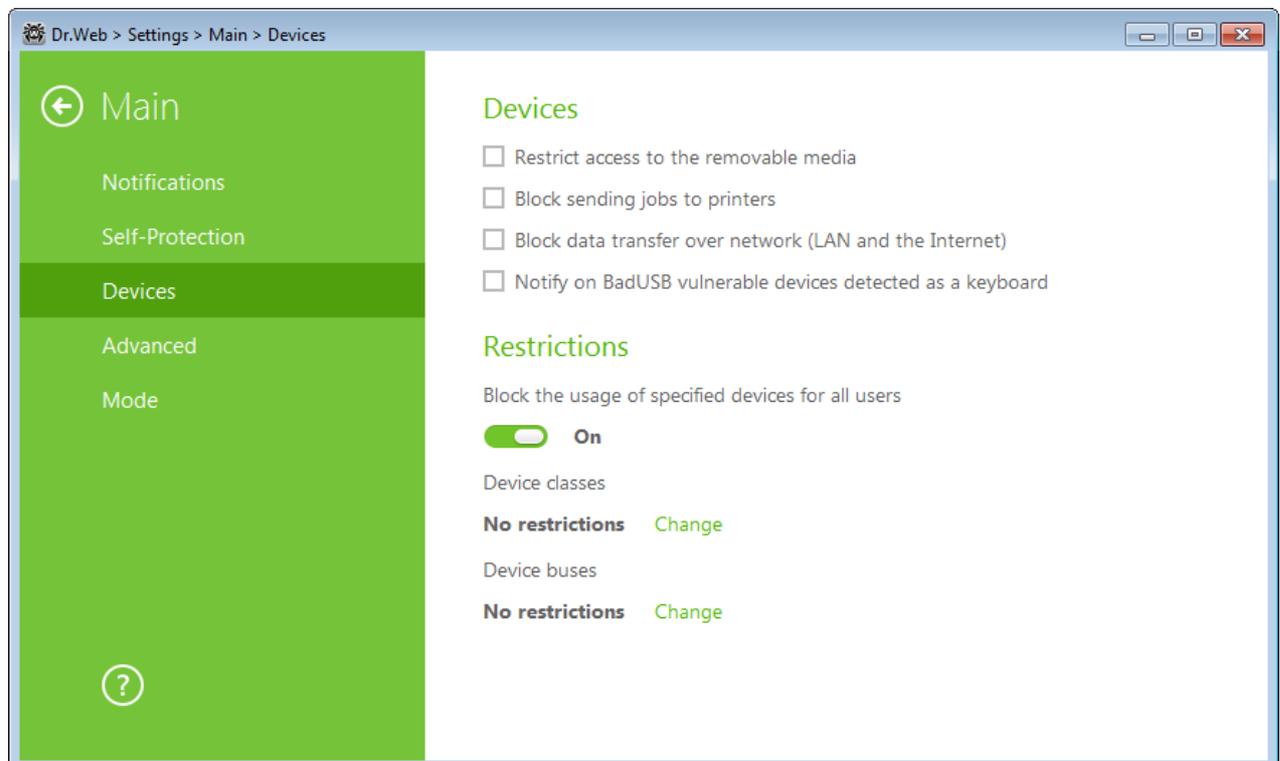
Date and time

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

8.3 Devices



Access control configurations are applied to all Windows accounts.





Devices

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

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

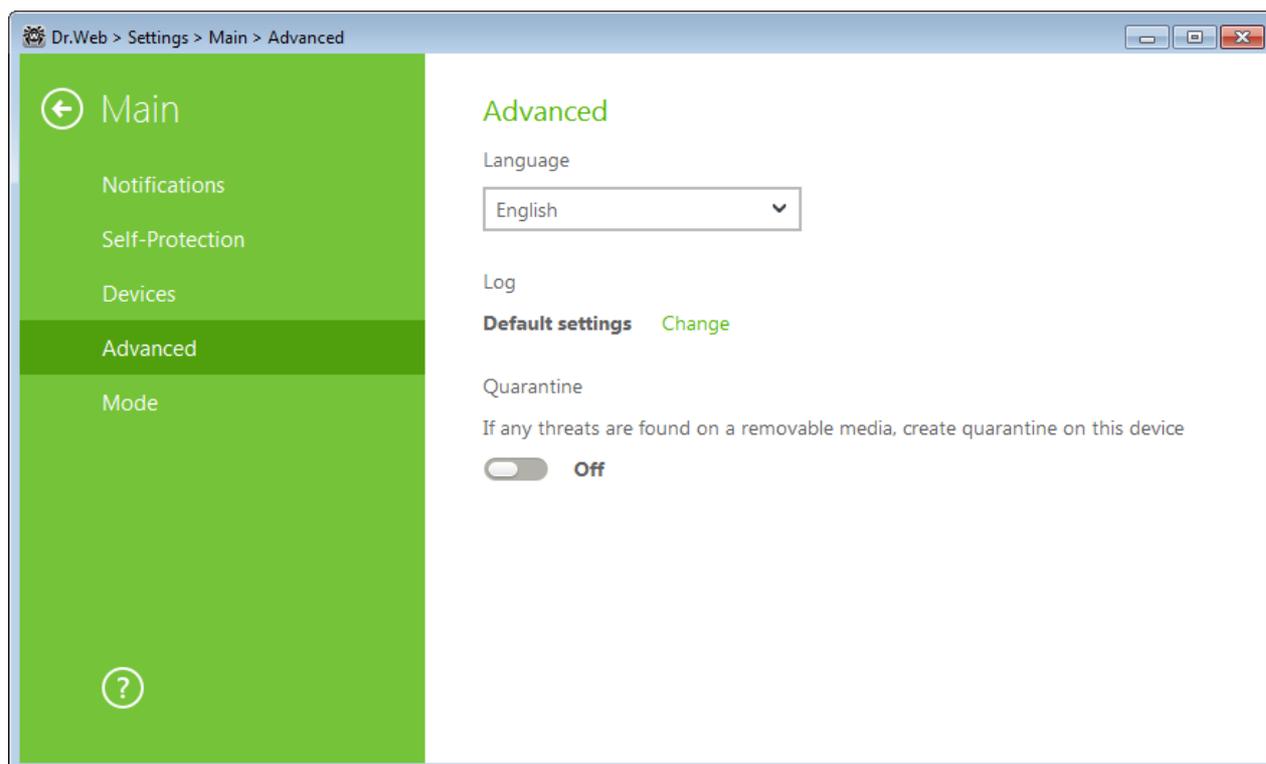
Device and bus classes

To block access to specified device or bus classes, enable the appropriate option. Click the **Edit** button to make a list of such objects. In the open window, select device or bus classes that you want to restrict access to. Click **OK** to save the changes. To close the window without saving the changes, click **Undo**.

8.4 Advanced

On this page, you can select a language for the settings, configure logging options and Quarantine settings.

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



Log settings

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



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

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

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

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

Component	Information
SpIDer Guard	<p>Time of updates and SpIDer Guard starts and stops, virus events, names of scanned files, names of packers, and contents of scanned complex objects (archives, email attachments, file containers).</p> <p>It is recommended to use this mode to determine the most frequent objects scanned by SpIDer Guard. If necessary, you can add these objects to the list of exclusions in order to increase computer performance.</p>



Component	Information
SplDer Mail	Time of updates and SplDer Mail starts and stops, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives. It is recommended to use this mode when testing mail interception settings.
SplDer Gate	Time of updates, starts and stops of SplDer Gate, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives. It is recommended to use this mode for reception of more detailed information on the checked objects and work of the HTTP watchman.
Scanner	In this mode, main events are logged, such as time of updates, time of Dr.Web Scanner starts and stops, information on detected threats, names of packers, and content of scanned archives.
Firewall	Firewall does not log its operation in the standard mode. When you enable detailed logging, the component collects data on network packets (pcap logs).
Update Dr.Web	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 Services	Information on Dr.Web components, changes in their settings, component starts and stops, preventive protection events, connections to central protection server.

Memory dump creation

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

Enabling detailed logging



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

1. To enable detailed logging for a Dr.Web component, select the corresponding check box.
2. Save the changes.

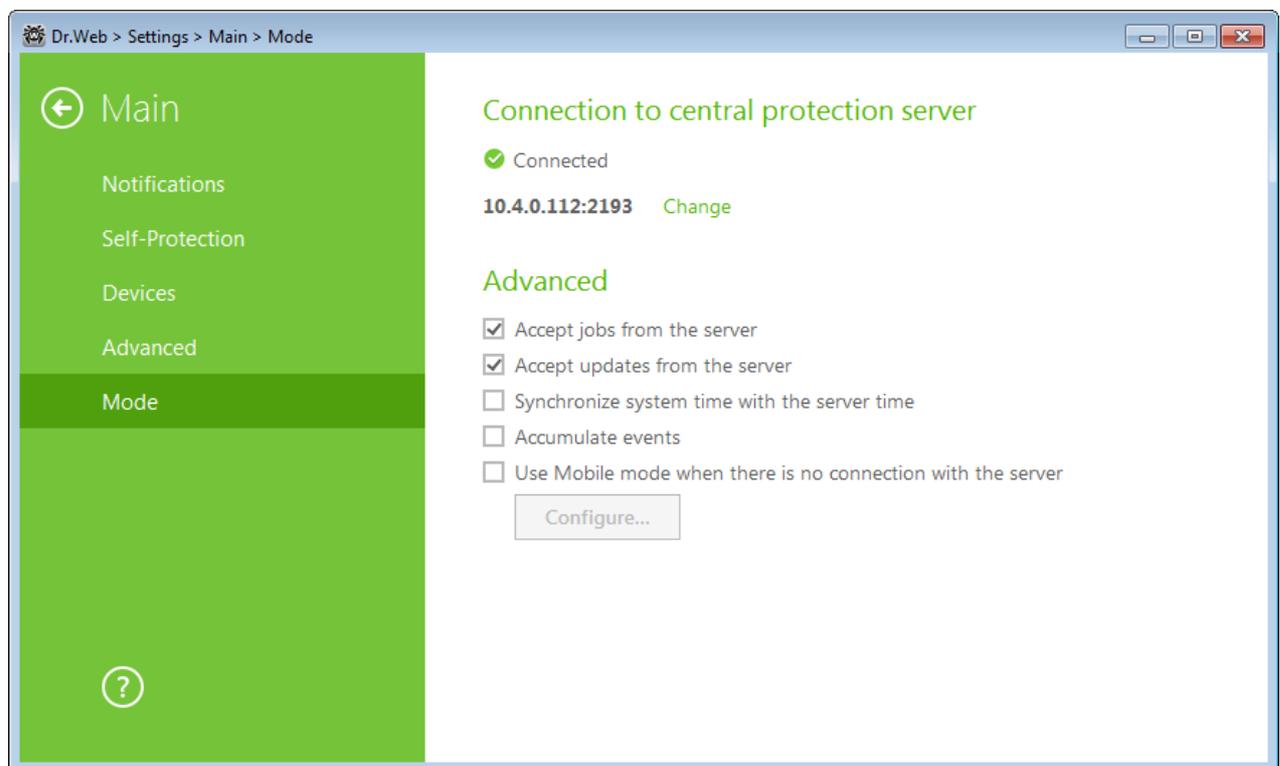


Quarantine settings

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

8.5 Mode

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



In the **Connection to central protection server** settings group, you can check Connection status and, if you have the corresponding permissions, view and adjust the server connection settings.



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

To configure connection to the current server or to a new one, click **Edit**. The [Settings](#) window opens.



If required, change the following parameters:

- **Address:** and **Port:**—specify address and port of the central protection server.
- **Public key**—specify a full path to the public key (drwcsd.pub).



By default, connection to the server cannot be established if no public key is specified, but you can adjust settings for the workstation and allow connection without the public key.

If you are going to use an invalid public key, select the corresponding check box.

After you click **Advanced**, the additional parameters become available:

- **Station ID**—specify the Dr.Web identifier assigned to your computer for registration on the server.
- **Password**—specify the Dr.Web password used for server connection.

When you enable the **Connect as a newbie** mode, you can send a request to register on the central protection server or establish connection to another server having adjusted the connection parameters (**Address:**, **Port:**, and **Public key**). After the registration is confirmed on the server, Dr.Web receives settings from .

After you finish adjusting the settings, close the Server **Settings** window by clicking **OK**. To close the window without saving the changes, click **Undo**.

In the **Advanced** settings group, you can select the following options:

- **Accept jobs from the server**—periodically receive tasks from the administrator.
- **Accept updates from the server**—receive updates for Dr.Web components and virus databases. Update settings are set on the server.
- **Synchronize system time with the server time**—synchronize system time on your computer with the time on the central protection server. In this mode, Dr.Web periodically sets the time on your computer in accordance with the server time.
- **Accumulate events**—save the event data for sending it to the central protection server. The event data will be sent as soon as connection to the server is established. If the check box is not selected and connection to the server is not established, important data (for example, information on detected threats and statistics) will be lost.
- **Use Mobile mode when there is no connection with the server**—keep virus databases up to date.

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



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



of the central protection server.

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

To configure Mobile mode settings, click **Configure**. The **Mobile mode** window opens.

From the **Update frequency** drop-down list, select the frequency of checking updates on the Doctor Web update servers.



If you select **Manually** from the **Update frequency** list, automatic updates are not performed. You can enable the update in the SplDer Agent menu.

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

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

After editing, click **OK** to save the changes or **Undo** to cancel them. To edit the proxy connection settings, click **Edit** again.



In the Mobile mode, only virus databases are updated.

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

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



9. Office Control

To configure Office Control, open the SpIDer Agent  in administrator mode, run **Settings**  and go to **Office Control**.

The Office Control component allows you to restrict access to websites, files, and folders. You can also set time limits on using the Internet and computer.

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

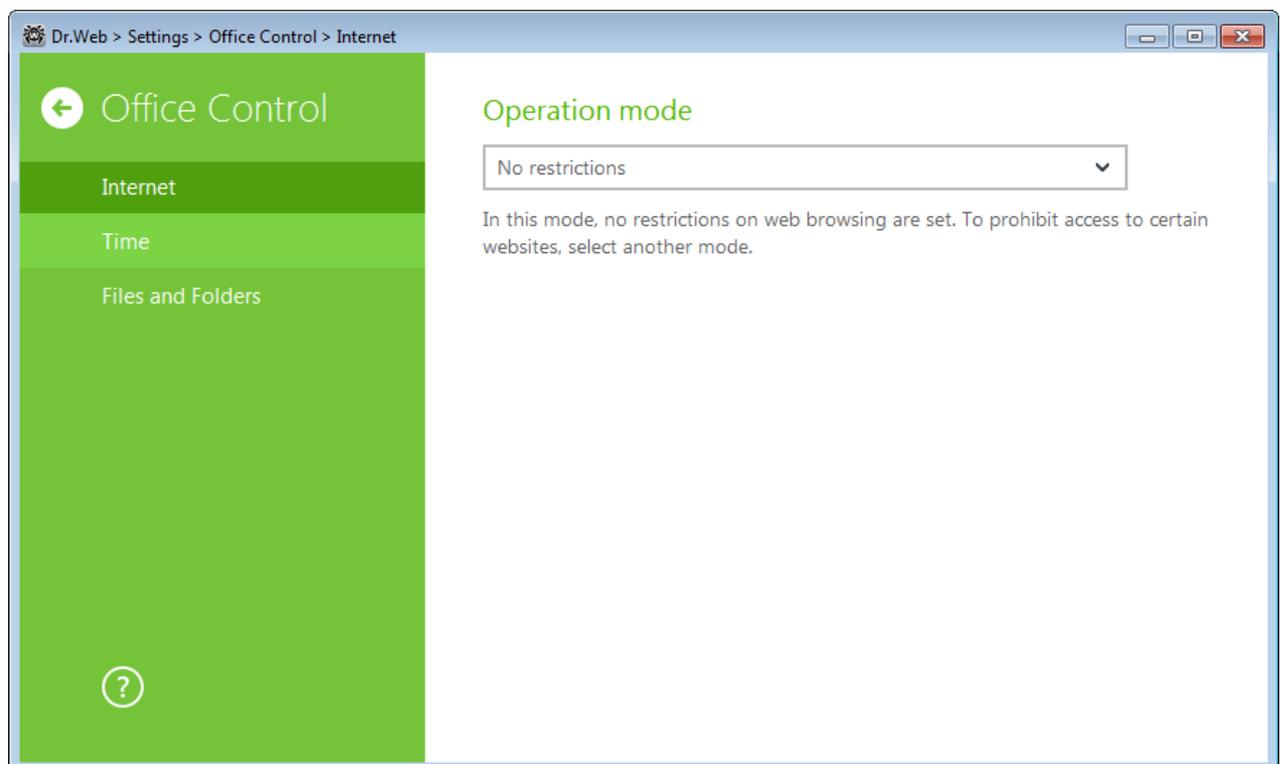
By controlling access to web resources, you can restrict a user from viewing undesirable websites (for example, pages on violence, gambling, adult content, etc.) or allow access only to certain websites that are specified in the Office Control settings.

9.1 Configuring Office Control



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

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





Configuring Office Control

The parameters of Office Control are applied to all users of the computer where Dr.Web Agent is installed. In the main part of the window, you can view the specified settings. By default, access to the Internet and to local resources is not restricted; no time limits are set.



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



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

Internet

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

Block by categories

In this mode, you can select categories of websites to block. You can also add websites to the manually populated black and while lists to block or allow access to the resources regardless of other restrictions.

Block all except websites from the white list

In this mode, you grant access to the websites from the white list only. Access to any other website is blocked.

Safe search

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

To create black and while lists

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

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

To configure black and white lists

1. Enter a domain name or a part of a domain name for the website in the **White list** or **Black list** field depending on whether you want to allow or block access to it. Details



- To add a certain website, enter its name (for example, `www.example.com`). This allows access to all webpages located on this website.
- To allow access to websites with similar names, enter the common part of their domain names. For example, if you enter `example`, then SpIDer Gate will allow access to `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru`, and other similar websites.
- To allow access to websites within a particular domain, enter the domain name with a period (.) character. This allows access to all webpages located on this website. If the domain name includes a forward slash (/), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter `example.com/test`, SpIDer Gate will allow access to such webpages as `example.com/test11`, `template.example.com/test22`, and so on.
- To allow access to certain websites, enter the mask of their names. Masks will be added in the `mask://... format`.
 - A mask denotes the common part of object names, at that:
 - The asterisk (*) character replaces any, possibly empty, sequence of characters.
 - The question mark (?) replaces any, including an empty, character (one).
 - Examples:
 - `mask://*.com`—enable access to all the domain .com websites;
 - `mask://mail`—enable access to all websites whose names contain the “mail” word;
 - `mask://???.com`—enable access to all the domain .com websites, whose names consist of three characters or less.

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

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

Time

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

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

To set time limits

1. Select days of the week and time when the user is restricted from accessing the Internet and then mark the corresponding timeslots blue.
 - To mark one timeslot, click it once.



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



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

Files and Folders

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

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

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

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

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

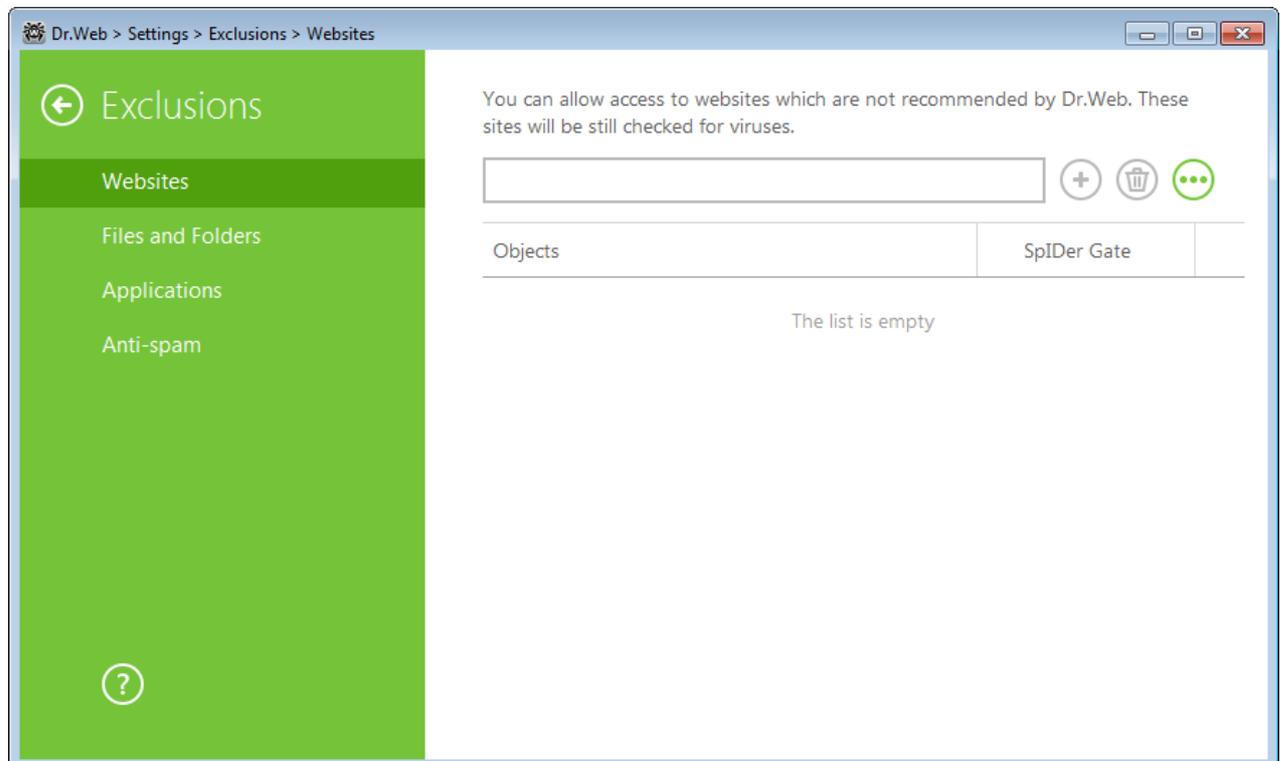


10. Exclusions

If you want to keep access to certain websites, files or folders, or to exclude certain processes from the anti-virus components analysis, add them to exclusions lists. Note that administrator of your anti-virus network can restrict you from modifying these settings.

10.1 Websites

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



To configure black and white lists

1. Enter a domain name or a part of a domain name for the website that you want to access regardless of other restrictions.
 - To add a certain website, enter its name (for example, `www.example.com`). This allows access to all webpages located on this website.
 - To allow access to websites with similar names, enter the common part of their domain names. For example, if you enter `example`, then SpIDer Gate will allow access to



example.com, example.test.com, test.com/example, test.example222.com, and other similar websites.

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

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

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

Examples:

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

Your input may be unified.

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

Managing listed objects

Click  to access the following options:

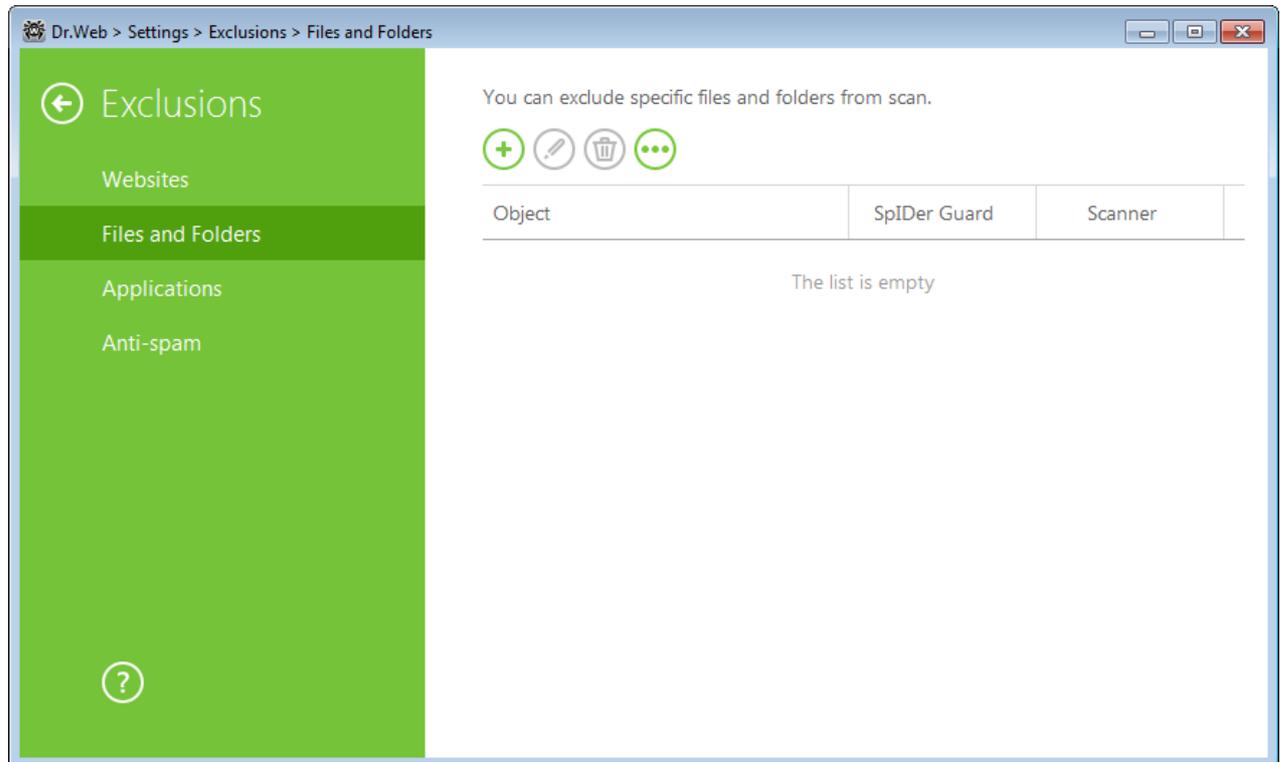
- **Export**—allows to save the created list of exclusions to be used on another computer where Dr.Web is installed.
- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.

10.2 Files and Folders

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



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



To configure list of exclusions

1. To add a file or folder to the exclusion list, do one of the following:
 - To add an existing file or folder, click . In the open window, click **Browse** and select the item in the standard dialog window. You can enter the full path to the file or folder or edit the path in the field before adding it to the list.
 - To exclude a file with a particular name, enter the name and the extension without the path;
 - To exclude a group of files or folders, enter the mask of their names.
2. In the configuration window, specify the components that must not scan this file.
3. Click **OK**. The file or folder will appear on the list.
4. To edit an existing exclusion, select the corresponding item from the list and click .
5. To list other files and folders, repeat steps 1 to 2. To remove a file or folder from the list, select the corresponding item and click .

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).



- Other mask characters do not replace anything and mean that in this place the name must contain this particular character.

Examples:

- file.txt—excludes all files with the name “file” and the .txt extension located in all folders.
- C:\folder\file.txt—excludes file.txt file stored in C:\folder.
- 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.
- file—excludes all files with the name “file” located in all folders without regard for the extension.
- C:\folder\ or C:\folder**—excludes all files located in C:\folder and its subfolders.
- 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.

Managing listed objects

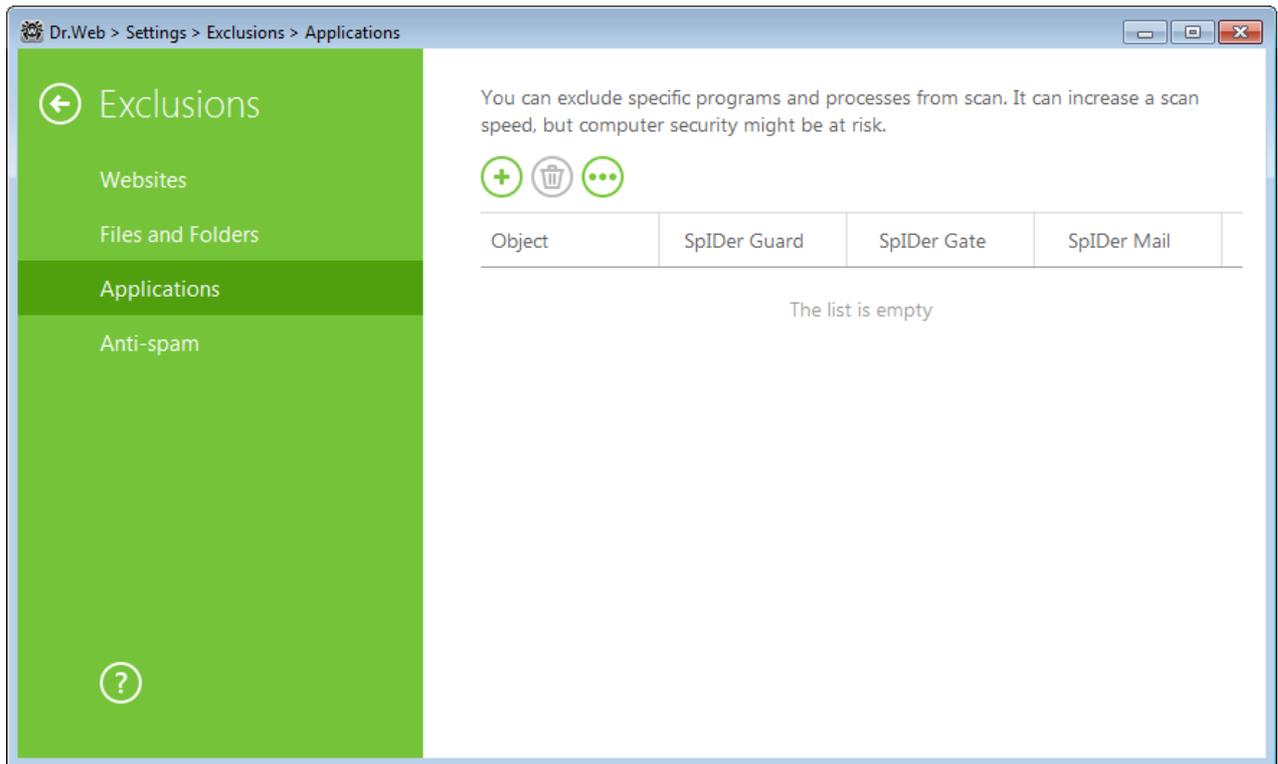
Click  to access the following options:

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

10.3 Programs and Processes

You can specify a list of programs and processes to be excluded from scanning by .

By default, the list is empty.



To configure list of exclusions

1. To add a program or a process to the exclusion list, click . Do one of the following:
 - In the open window, click **Browse** and select an application in the standard dialog window. You can enter the full path to the application in the field manually.
 - To exclude an application from scanning, enter its name in the field. The full path to the application is not required (for example, `example.exe`);
 - To exclude applications, enter the mask of their names;
 - You can exclude an application from scanning by the name of a variable if the name and a value of this variable are specified in the system variable settings.
2. In the configuration window, specify which components should not perform check of the selected application.
3. Click **OK**. The selected application will appear on the list.
4. If necessary, repeat the procedure to add other programs.
5. To edit an existing exclusion, select the corresponding item from the list and click .
6. To remove an application from the list, select the corresponding item and click .

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).



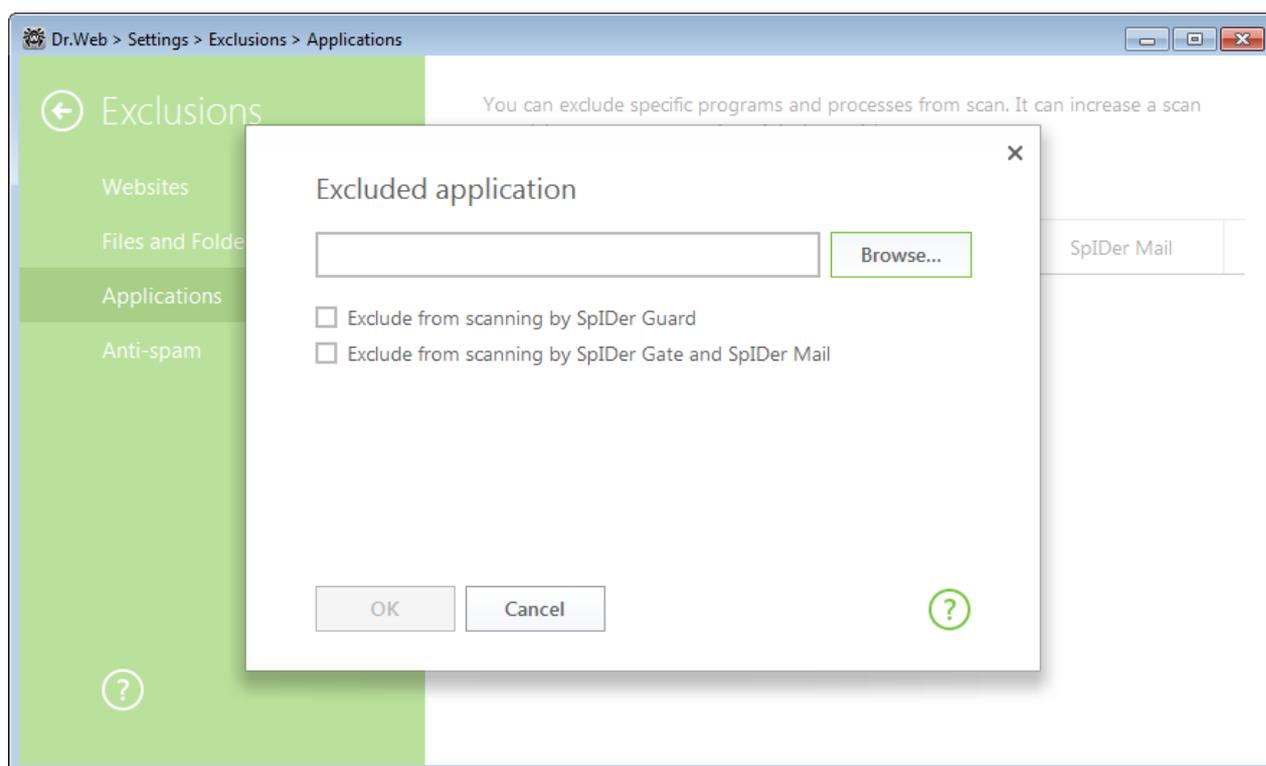
Examples:

- `C:\Program Files\folder\example.exe` – excludes the application `example.exe` in the folder `C:\Program Files\folder` from scanning.
- `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.
- `%EXAMPLE_PATH%\example.exe` – excludes an application by the name of a system variable. A name of a system variable and its value can be specified in the operating system settings.

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

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

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



Managing listed objects

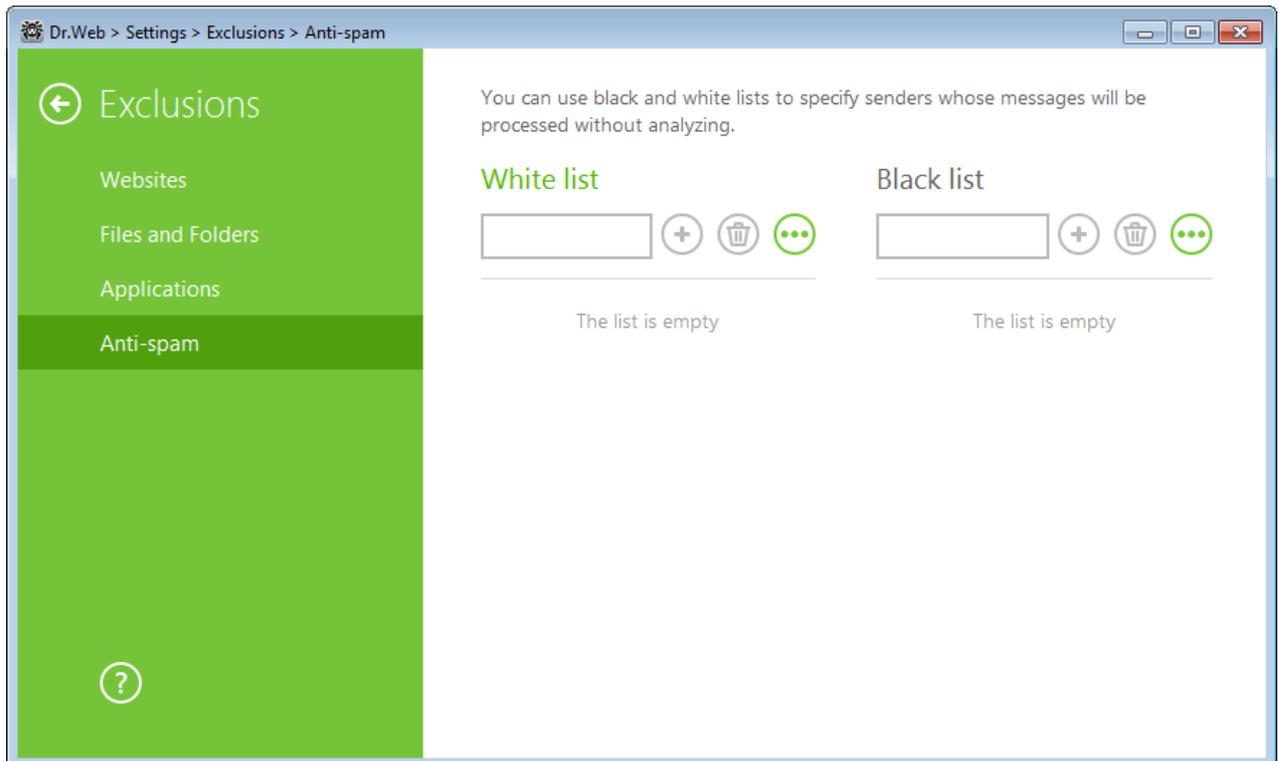
Click  to access the following options:

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

10.4 Anti-spam

In this window, you can configure lists of senders whose messages are delivered or blocked by SpIDer Mail automatically (that is, without analyzing their contents).

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



To configure anti-spam lists

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

Managing listed objects

Click  to access the following options:

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



- **Import**—allows to use the list of exclusions created on another computer.
- **Clear all**—allows to remove all objects from the list of exclusions.



11. Protection Components

11.1 SpIDer Guard

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

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

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

On detection of an infected object, SpIDer Guard applies actions to it according to the [specified settings](#). You can change settings to configure automatic reaction to different virus events.



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.

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

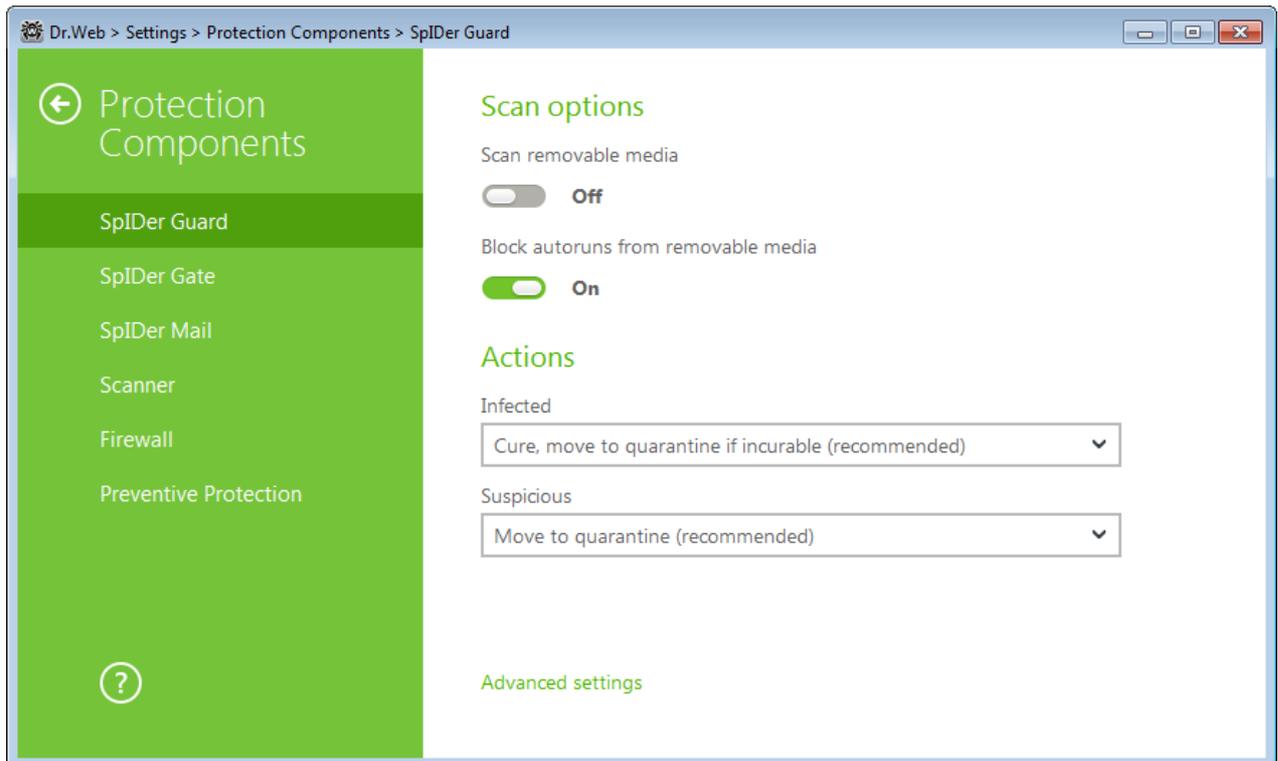
11.1.1 Configuring SpIDer Guard



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

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

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



Scan options

By default SpIDer Guard checks objects on removable media such as CD/DVD, flash memory, and so on. This option helps to protect your computer from viruses transmitted via removable media.



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

Actions

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

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

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

Reaction of SpIDer Guard to detection of various malicious software is also set separately. Set of actions available for the selection depends on the type of the virus event.



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

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

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



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

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



Scan mode

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

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



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

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

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

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



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

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



Advanced settings

The settings of this group allow to specify parameters for scanning objects on-the-fly and are always applied regardless of the selected 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).

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. This option is enabled by default.

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.



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



11.2 SpIDer Gate

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

By default, SpIDer Gate blocks all incoming malicious objects.

You can configure SpIDer Gate to completely disable monitoring of incoming or outgoing traffic, compose a list of applications whose HTTP traffic should always be checked or exclude certain applications from being monitored.

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

SpIDer Gate does not check data transmitted over cryptographic protocols.

SpIDer Gate resides in the main memory of the computer and automatically launches upon Windows startup.

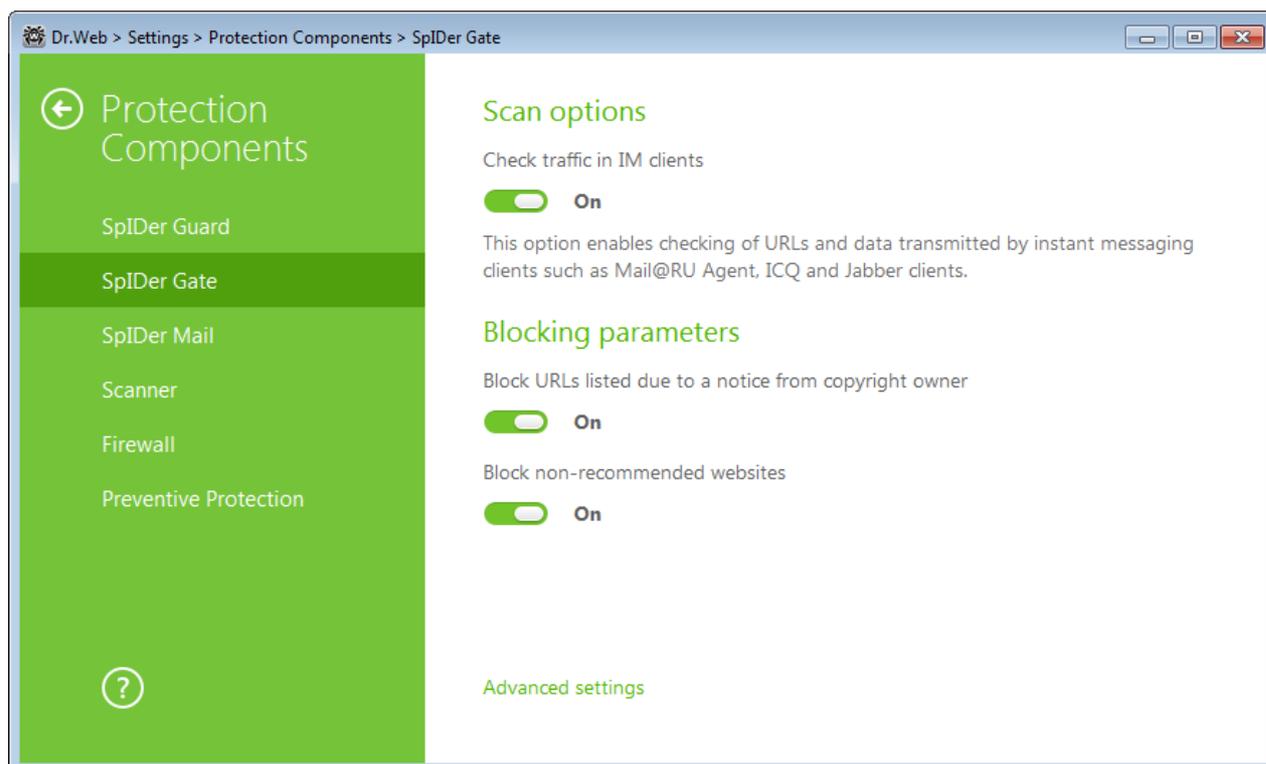
11.2.1 Configuring SpIDer Gate



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

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

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



Check traffic in IM clients

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

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

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

Blocking parameters

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



By default, SpIDer Gate blocks access to websites known as infection sources. At that, applications from the [exclusion list](#) are not blocked.



Programs to block

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

- Suspicious
- Riskware
- Dialers
- Hacktools
- Adware
- Jokes

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

Objects to block

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

Advanced settings

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

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

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

11.3 SpIDer Mail

SpIDer Mail is an anti-virus mail scanner that monitors data exchange between mail clients and mail servers made via POP3, SMTP, IMAP4, or NNTP (IMAP4 stands for IMAPv4rev1) protocols and detects and neutralizes threats before they are transmitted to or from your computer thus preventing spread of infection via email.

SpIDer Mail does not check encrypted email traffic.

The default program settings are optimal for beginners, provide maximum protection, and require minimum user interference. However, by default, SpIDer Mail may block some options of mail programs (for example, sending a message to multiple addresses might be considered as mass distribution, incoming mail is not scanned for spam); useful information from a safe text part of



infected messages becomes unavailable in case of automatic deletion. Advanced users can configure mail scanning settings and reaction of the program to various events.

Mail processing

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

By default, SpIDer Mail reacts to detection of infected incoming messages as well as messages that were not scanned (for example, due to a complicated structure) as follows (for details on how to modify the reaction, refer to [Settings SpIDer Mail](#)):

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

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

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

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

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

11.3.1 Configuring SpIDer Mail

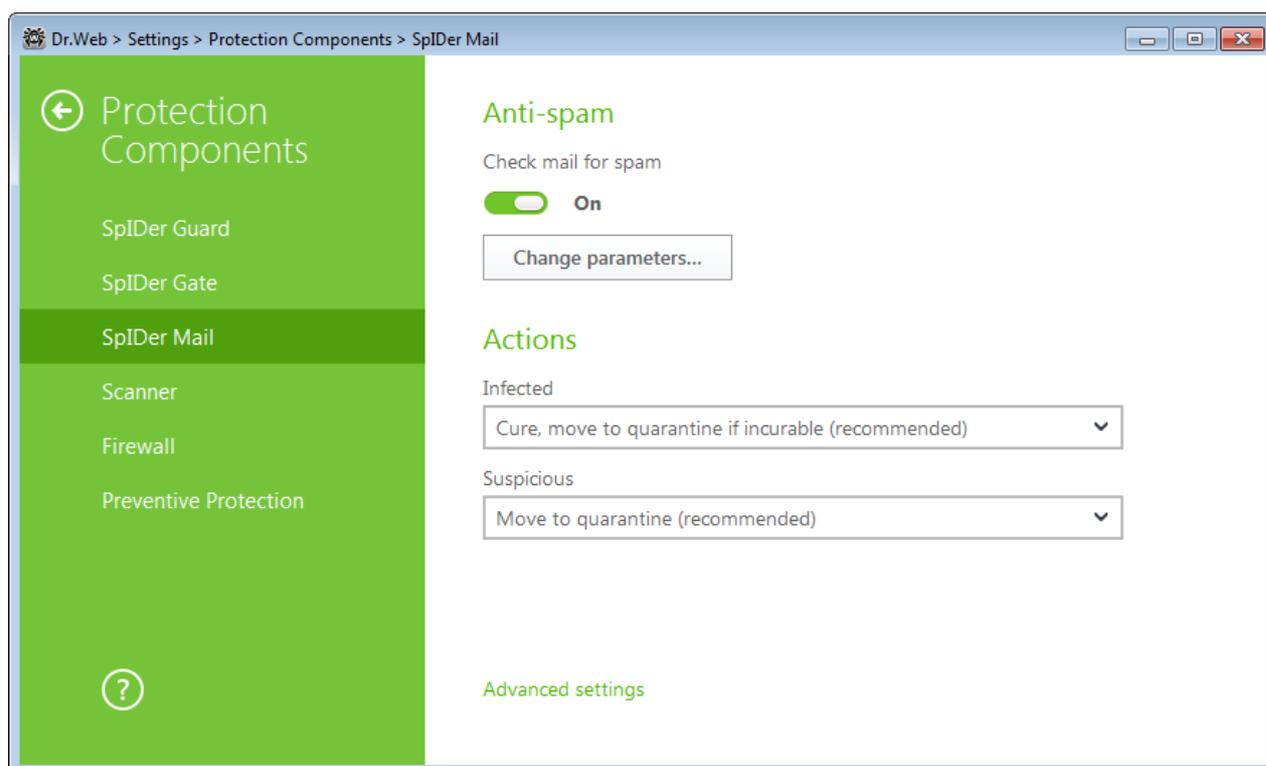


The component settings can be adjusted if the administrator of the central protection server, to which Dr.Web is connected, enabled this option.

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



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



Anti-spam

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

Actions

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

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

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

Action	Description
Cure, move to quarantine if not cured	Instructs to restore the original state of the message before infection. If the message is incurable, or the attempt of curing fails, the object is moved to quarantine.



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

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

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



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

Actions on messages

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

Option	Description
Insert 'X-AntiVirus' header into messages	This option is enabled by default. Instructs SpIDer Mail to add scan results and information on Dr.Web version to message headers after processing. You cannot edit data format.
Delete modified messages on server	Instructs to remove messages to which either Delete or Move to Quarantine action was applied by SpIDer Mail. The messages are removed from mail servers regardless of the mail client settings.



Scanning optimization options

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

Scanning archives

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

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

You can enable one or more options.



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

Additional tasks

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

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

11.3.2 Anti-spam

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

- Heuristic analysis—a highly intelligent technology that empirically analyzes all parts of a message: header, message body, and attachments, if any.
- Detection of evasion techniques—this advanced anti-spam technology allows detecting evasion techniques adopted by spammers to bypass anti-spam filters.
- HTML signature analysis—messages containing HTML code are compared with a list of known patterns from the anti-spam library. Such comparison, in combination with the data on sizes of



images typically used by spammers, helps to protect users against spam messages with HTML code linked to online content.

- Semantic analysis—the words and phrases of a message (both visible to the human eye and hidden) are compared with words and phrases typical of spam using a special dictionary.
- Anti-scamming—scam and pharming messages include so-called “Nigerian” scams, loan scams, lottery and casino scams and false messages from banks and credit organizations. A special module is used to filter scams.
- Technical spam—Bounces are delivery-failure messages sent by a mail server. Such messages are also sent by a mail worm. Therefore, bounces are as unwanted as spam.

You can configure the following Anti-spam options:

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

Processing mail by spam filter

SpIDer Mail adds the following header to the processed messages:

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

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



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

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



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

To report spam detection errors

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

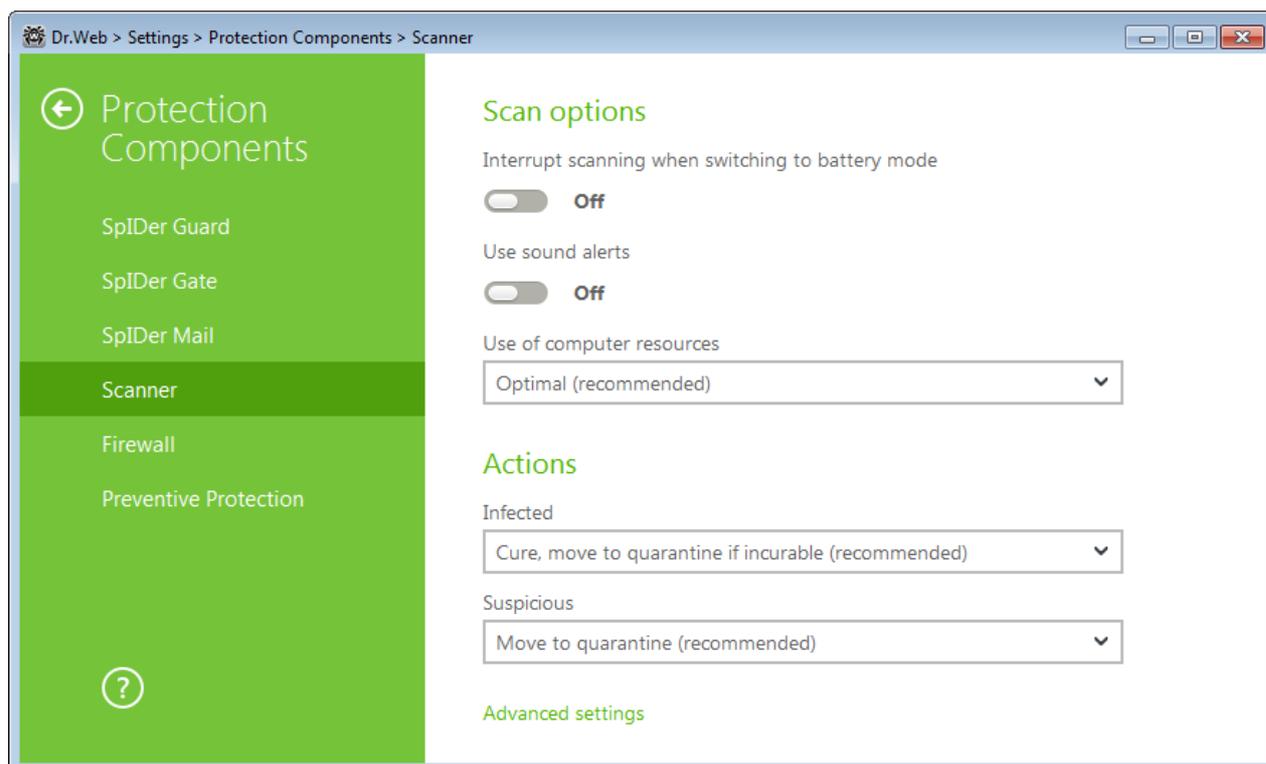
11.4 Scanner



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

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

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



Scan options

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

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

Actions

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

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

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

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



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

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

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



Threats within complex objects cannot be processed individually. For such threats, Dr.Web Scanner applies an action selected for this type of a complex object.

Additional tasks

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

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

1. **Do not apply action.** Scanner will display the list of detected threats.



2. **Neutralize detected threats.** Scanner will neutralize threats automatically.
3. **Neutralize detected threats and shut down computer.** Scanner will shut down the computer once threats are automatically neutralized.

11.5 Dr.Web Firewall

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

Firewall provides you with the following features:

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

11.5.1 Training Dr. Web Firewall

Once installation is complete, Firewall starts learning by intercepting all connection attempts from your operating system or user applications. If no filtering rules have been set for the program, Firewall prompts you to select the necessary action.



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

Application Rules

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

Information	Description
Application	The name of the application. Ensure that the path to the application executable, specified in the Application path entry field, corresponds to the file location.
Application path	The full path to the application executable file and its name.
Digital signature	Digital signature of the application.
Address	The used protocol and network address to which the application is trying to connect.



Information	Description
Port	The network port used for the connection attempt.
Direction	The direction of the connection.

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



You need administrative privileges to create a rule.

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

To set parent process rules

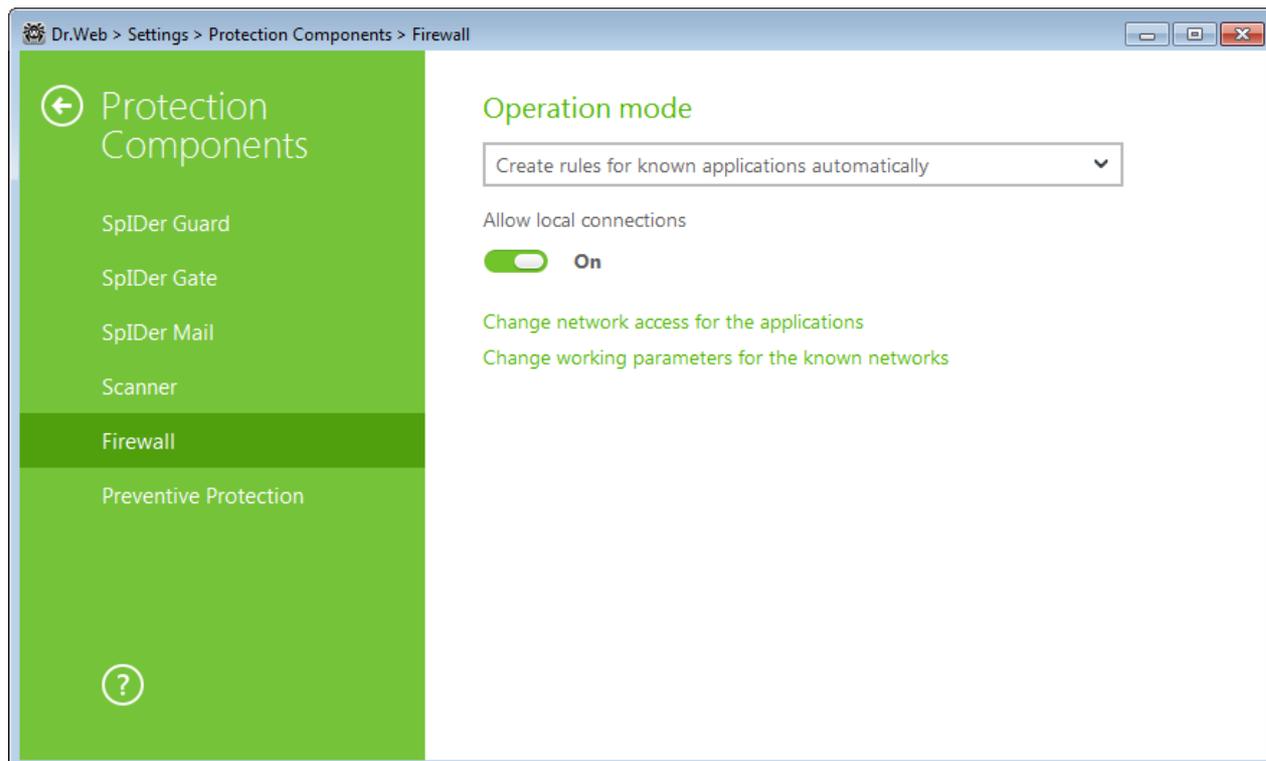
1. Consider information about the parent process in the notification displayed on a connection attempt.
2. Once you make a decision about what action to perform, select one of the following:
 - To block this connection once, select **Block**.
 - To allow this connection, click **Allow**.
 - To create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

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

11.5.2 Configuring Firewall



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



To start using Firewall, do the following:

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

By default, Firewall automatically creates rules for known applications. Regardless of the operation mode, events are logged.

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

The **Allow local connections** option allows all applications on your computer to interconnect (i.e., allow unlimited connections between applications installed on your computer). For this type of connection, no rules are applied. Disable this option to apply filtering rules to connections carried out both through the network and within your computer.

To set operation mode

Select one of the following operation modes:

- **Allow unknown connections**—free access mode, when all unknown applications are permitted to access networks.
- **Create rules for known applications automatically** – training mode, when rules for known applications are created automatically (set by default).
- **Interactive mode**—[learning mode](#), when the user is provided with full control over Firewall reaction.



- **Block unknown connections**—restricted access mode, when all unknown connections are blocked. For known connections, Firewall applies the appropriate rules.

Allow unknown connections

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

Create rules for known applications automatically

This mode is used by default.

In this mode, rules for known applications are created automatically. For unknown applications, Firewall gives you the opportunity to manually allow or block connections or create new rules.

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

Interactive mode

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

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

Block unknown connections

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

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



Settings for Applications



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

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



If the file of an application for which the rule had been created was changed (for example, an update was installed), Firewall prompts to confirm that the application is still allowed to access network resources.

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



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

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

Application Rules

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

To open this window, in the Firewall [settings](#) window, select **Change network access for the applications** and click  or select an application and click .

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

Launching other applications

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

- **Allow**—if you want to enable the application to run other processes.
- **Block**—if you want to disable the application to run other processes.



- **Not specified**—if you want to use the settings specified for the selected [operation mode](#) of Firewall.

Access to network resources

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

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

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

Rule Settings

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

To create a rule



Configure the following parameters:

Parameter	Description
General	
Rule name	The name of the created/edited rule.
Description	The rule description.
Action	The action for Dr.Web Firewall to perform when an attempt to connect to the Internet is detected: <ul style="list-style-type: none">• Block packets—block the connection.• Allow packets—allow the connection.
State	Rule status: <ul style="list-style-type: none">• Enabled—the rule is applied for all matching connections.• Disabled—the rule is temporary not applied.
Connection type	The direction of the connection: <ul style="list-style-type: none">• Incoming—the rule is applied when someone from the network attempts to connect to an application on your computer.• Outgoing—the rule is applied when an application on your computer attempts to connect to the network.• Any—the rule is applied regardless of packet transfer direction.
Logging	Logging mode: <ul style="list-style-type: none">• Enabled—register events.• Disabled—do no log rule information.
Rule Settings	
Protocol	The network and transport level protocols used for the connection attempt. The following protocols of the network level are supported: <ul style="list-style-type: none">• IPv4• IPv6• IP all—any version of the IP protocol The following protocols of the transport level are supported: <ul style="list-style-type: none">• TCP• UDP• TCP & UDP—TCP or UDP protocol



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

Settings for Networks

To set rule sets for network interfaces

1. To create a set of rules for filtering packets transmitted through a certain interface, select **Change working parameters for the known networks** in the Firewall settings window.
2. For the required interface, select the appropriate rule set. If the appropriate rule set does not exist, you can [create](#) a new set of packet filtering rules.

To list all available interfaces, click  and select **Show all**. This opens a window where you can select interfaces that are to be permanently listed in the table. Active interfaces are listed in the table automatically.

Packet Filter

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

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

Firewall uses the following predefined rule sets:

- **Default Rule**—this rule set is used by default for new [network interfaces](#).
- **Allow All**—this rule set configures the component to pass through all packets.
- **Block All**—this rule set configures the component to block all packets.

For fast switching between filtering modes, you can create custom sets of filtering rules.



To set rule sets for network interfaces

In the Firewall settings window, click **Change working parameters for the known networks**, choose a network interface and click . On this page you can:

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

To configure rule sets

Do one of the following:

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

To configure additional settings

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

Option	Description
Use TCP stateful packet filtering	Select this check box to filter packets according to the state of existing TCP connections. Firewall will block packets that do not match the TCP protocol specification. This option helps to protect your computer from DoS attacks (denial of service), resource scanning, data injection, and other malicious operations. It is also recommended to enable stateful packet filtering when using complex data transfer protocols (FTP, SIP, etc.). Clear this check box to filter packets without regard to the TCP session state.
Management of fragmented IP packets	Select this check box to ensure correct processing of large amounts of data. The maximum transmission unit (MTU) may vary for different networks, therefore large IP packets may be fragmented. When this option is enabled, the rule selected for the first fragment of a large IP packet is applied to all other fragments. Clear this check box to process fragmented packets independently.



Set of rules for filtering packets

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

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

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

Edit rule set

1. If you selected to create or edit an existing rule set on the **Packet filter settings** page, specify the name for the rule set in the opened window.
2. Use the following options to create filtering rules:
 - To add a new rule, click . The new rule is added to the beginning of the list.
 - To modify a rule, select it and click ;
 - To add a copy of the selected rule, click . The copy is added before the selected rule.
 - To remove the selected rule, click .



3. If you selected to create or edit a rule, [configure the rule settings](#) in the open window.
4. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.
5. When you finish the list adjustments, click **OK** to save changes or **Undo** to cancel them.



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

Packet Filter Rule Sets

To add or edit a rule

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

Parameter	Description
Rule name	The name of the created/edited rule.
Description	The rule description.
Action	The action for Firewall to perform when a packet is intercepted: <ul style="list-style-type: none">• Block packets—block a packet;• Allow packets—allow a packet.
Direction	The direction of the connection: <ul style="list-style-type: none">• Incoming—the rule is applied when a packet is received from the network.• Outgoing—the rule is applied when a packet is sent into the network from your computer.• Any—the rule is applied regardless of packet transfer direction.
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log: <ul style="list-style-type: none">• Entire packet—log the whole packet.• Headers only—log packet headers only.• Disabled—do no log packet information.
Criterion	Filtering criterion. For example, transport or network protocol. To add a filtering criterion, select it from the list and click  . You can add any number of filtering criteria. For certain headers, there are additional criteria available.



3. When you finish the adjustments, click **OK** to save changes or **Undo** to cancel them.



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

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

11.6 Dr.Web for Microsoft Outlook

Main functions

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

- Anti-virus check of incoming email attachments;
- Spam check;
- Detection and neutralization of malware;
- Heuristic analysis for additional protection against unknown viruses.

11.6.1 Configuring Dr.Web for Microsoft Outlook

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



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

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

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



11.6.2 Threat Detection

Dr.Web for Microsoft Outlook uses different [detection methods](#). [Infected objects](#) are processed according to the actions defined by the user—that is, they can be cured, removed or moved to [Quarantine](#) to be isolated from the rest of the system.

Malicious Objects

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

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

Actions

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

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



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

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

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

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

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

- The **Infected** drop-down list sets the reaction to the detection of a file infected with a known and (presumably) curable virus.
- The **Not cured** drop-down list sets the reaction to the detection of a file infected with a known incurable virus (and in case an attempt to cure a file failed).
- The **Suspicious** drop-down list sets the reaction to the detection of a file presumably infected with a virus (upon reaction of the heuristic analyzer).
- In the **Malware** section, set a reaction to detection of unsolicited software of the following types:
 - Adware
 - Dialers
 - Jokes
 - Hacktools
 - Riskware
- The **If check failed** drop-down list allows to configure actions if the attachment cannot be checked, that is, if the attached file is corrupted or password protected.
- The **Check archives (recommended)** check box allows to enable or disable check of attached archived files. Select this check box to enable checking; clear this check box to disable.

For different types of objects, actions are specified separately.

The following actions for detected virus threats are available:

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

11.6.3 Spam Check

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

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



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

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

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

Spam Filter Settings

Spam Filter Settings

To configure spam filtering settings, do any of the following actions:

- To run spam checks, select the **Check for spam** check box.
- You can enable addition of special text to the spam message header by selecting the **Add prefix to message header** check box. Text of the added prefix is specified to the right of the check box. The default prefix is *****SPAM*****.
- If you want checked messages to be marked as read in message options, enable the **Mark as read** option. This option is enabled by default.
- You can also configure [white and black lists](#) for message filtering.



If spam filter processes certain messages incorrectly, you are advised to forward such messages to your anti-virus network administrator. Forward messages as attachments, that is, do not include them in the message body.

Black and White Lists

Black and white lists are used for message filtration.

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

To add addresses

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

To change addresses

1. Select the address you want to change and click **Edit**.
2. Make necessary changes to the information.



3. Click **OK** in the **Edit list** window.

To delete addresses

1. Select the address you want to delete from the list.
2. Click **Remove**.

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

White list

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

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

For example, the following variations are possible:

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



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

The 'at' sign (@) is mandatory.

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



Black list

If the sender's address is on the black list, the message will be automatically regarded as spam. List filling methods are as follows:

- To add a specific sender, enter the full email address (for example, `spam@spam.com`). All messages, received from these addresses, will be automatically regarded as spam.
- Each list item can contain only one address or address mask.
- To add a group of sender addresses, enter the mask that determines their names. The mask defines a template for an object definition. It may contain regular characters from email addresses and a special asterisk character (*), which replaces any (including an empty one) sequence of characters.
- To regard messages sent from any email address within a domain as spam, use an asterisk character (*) instead of the username in the address. For example, if you enter `*@spam.com`, all messages from addresses within the `spam.com` domain will be regarded as spam automatically.
- To regard messages sent from an email address with a certain user name from any domain as spam, enter an asterisk character (*) instead of the domain name in the address. For example, if you enter `name@*`, all messages from all senders with the "someone" mailbox name will be regarded as spam automatically.
- Addresses from the recipient domain are not processed. For example, if the recipient mailbox (your mailbox) is in the `mail.com` domain, then messages from `mail.com` domain will not be processed with the anti-spam filter.

11.6.4 Event Logging

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

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

Event Log

The following information is registered in the Windows Event Log:

- Program starts and stops;
- Parameters of program modules: scanner, engine, virus databases (information is logged on program startup and module update);
- Information on threat detection;

To view Windows Event Log

1. Open **Control Panel** of the operating system.
2. Select **Administrative Tools** → **Event Viewer**.



3. In the tree view, select **Application**. The list of events, registered in the log file by user applications, opens. The source of **Dr.Web for Microsoft Outlook** messages is the **Dr.Web for Microsoft Outlook** application.

Debug Text Log

The following information is registered in the debug log:

- Information on threat detection;
- Read/write errors or errors occurred while scanning archives or password-protected files;
- Parameters of program modules: scanner, engine, virus databases;
- Core failures;

Configure logging

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



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

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



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

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

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

To view program log

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

11.6.5 Statistics

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



These scanned objects are classified as follows:

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

Then the number of processed objects is specified:

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

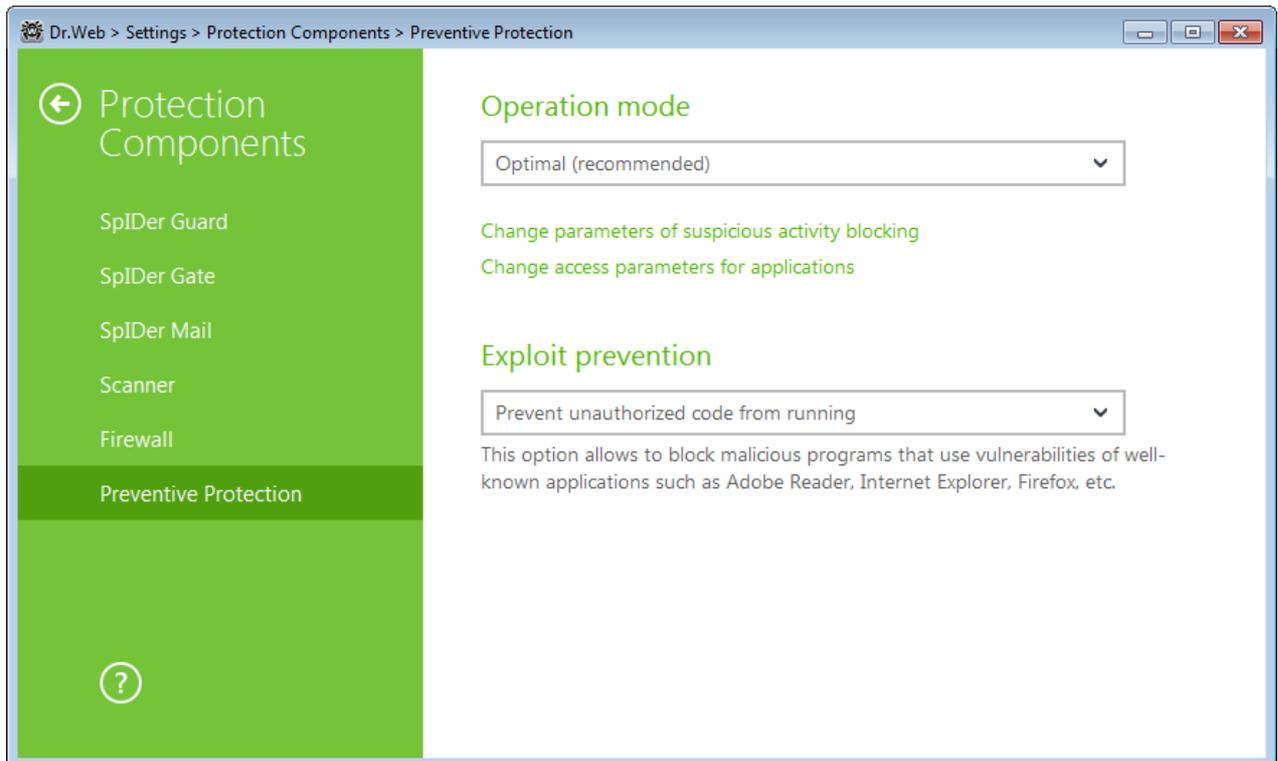
By default, statistics is saved to the drwebforoutlook.stat file located in the %USERPROFILE%\Doctor Web folder.



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

11.7 Preventive Protection

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



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

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

To create a new profile

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

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

To add a rule

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

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



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

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

Preventive protection level

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

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



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

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

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

Protected object	Description
Integrity of running applications	This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored.
Integrity of user files	This option allows detection of processes that modify user files with the known algorithm, which indicates that the process may compromise computer security. Processes that are added to the Exclusions are not monitored.
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 user profiles). Image File Execution Options:



Protected object	Description
	<ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>User Drivers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Winlogon registry keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Winlogon notifiers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Windows registry startup keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib <p>Executable file associations:</p> <ul style="list-style-type: none">• Software\Classes\exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) <p>Software Restriction Policies (SRP):</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer <p>Browser Helper Objects for Internet Explorer (BHO):</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>Autorun of programs:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup• Software\Microsoft\Windows\CurrentVersion\RunServices• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce <p>Autorun of policies:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run <p>Safe mode configuration:</p> <ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal



Protected object	Description
	<ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager parameters: <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows System services: <ul style="list-style-type: none">• System\CurrentControlXXX\Services



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

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

Exploit prevention

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

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



12. Statistics

To view statistics on the components operation, open the SpIDer Agent menu , go to **Statistics**  in [administrator mode](#). On the **Statistics** page, reports for the following groups are available:

- Threats
- Update
- Office Control

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

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

The following information is logged in the report:

- Frequency of visits;
- Action;
- URL.

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

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

Network activity

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

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

The report shows the following information for every active application:

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

The application log stores the following data:

- Application start time
- Application name
- Application processing rule name



- Direction
- Action
- Endpoint

Packet Filter Log shows the following information:

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

Click  to export or clear logs.

Detailed report

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

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

You can use filters to select a certain event.

Filters

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

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

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

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

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

All created filters can be edited or removed.



Appendices

Appendix A. Command-Line Parameters

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

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

The switches are listed alphabetically.

Scanner and Console Scanner Parameters

`/AA`—apply actions to detected threats automatically. (For Scanner only.)

`/AC`—scan installation packages. Option is enabled by default.

`/AFS`—use forward slash to separate paths in an archive. Option is disabled by default.

`/AR`—scan archives. Option is enabled by default.

`/ARC: <compression_ratio>`—maximum compression level. If the compression ratio of the archive exceeds the limit, Scanner neither unpacks nor scans the archive. By default: unlimited.

`/ARL: <nesting_level>`—maximum archive nesting level. By default: unlimited.

`/ARS: <size>`—maximum archive size (in KB). By default: unlimited.

`/ART: <size>`—minimum size of a file inside an archive beginning from which compression ratio check is performed (in KB). By default: unlimited.

`/ARX: <size>`—maximum size of a file inside an archive that is scanned (in KB). By default: unlimited.

`/BI`—show information on virus databases. Option is enabled by default.

`/CUSTOM`—perform a custom scan. If additional parameters are set (for example, objects to be scanned or `/TM` and `/TB` parameters), only the specified objects will be scanned. (For Scanner only.)

`/CL`—use Dr.Web cloud service. Option is enabled by default. (For Console Scanner only.)

`/DCT`—do not display estimated scan time. (For Console Scanner only.)

`/DR`—scan folders recursively (scan subfolders). Option is enabled by default.



`/E: <number_of_threads>`—perform scanning in specified number of threads.

`/FAST`—perform an [express scan](#) of the system. If additional parameters are set (for example, objects to be scanned or `/TM` and `/TB` parameters), the specified objects will also be scanned. (For Scanner only.)

`/FL: <file_name>`—scan paths listed in the specified file.

`/FM: <mask>`—scan files matching the specified mask. By default, all files are scanned.

`/FR: <regexpr>`—scan files matching the specified regular expression. By default, all files are scanned.

`/FULL`—perform a full scan of all hard drives and removable media (including boot sectors). If additional parameters are set (for example, objects to be scanned or `/TM` and `/TB` parameters), an express scan will be performed, and the specified objects will be scanned. (For Scanner only.)

`/FX: <mask>`—exclude from scan files that match the specified mask. (For Console Scanner only.)

`/GO`—Scanner operation mode that skips the questions that require answers from a user; decisions that require a selection are made automatically. This mode is useful for the automatic file scanning; for example, for the daily or weekly hard disc 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.

`/MA`—scan mail files.

`/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 priority of scanning process. By default: unlimited.



`/NOREBOOT`—cancel system reboot or shutdown after scanning. (For Scanner only.)

`/NT`—scan NTFS streams.

`/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 complete regardless of whether or not any actions have been applied to the detected threats. (For Scanner only.)

`/RA : <file_name>`—append the report on program operation to the specified file. By default, logging is disabled.

`/REP`—follow symbolic links while scanning. Option is disabled by default.

`/RK`—scan for rootkits. Option is disabled by default.

`/RP : <file_name>`—write the report on program operation to the specified file. By default, logging is disabled.

`/RPC : <sec>`—Scanning Engine connection timeout. Timeout is 30 seconds by default. (For Console Scanner only.)

`/RPCD`—use dynamic RPC identification. (For Console Scanner only.)



`/RPCE`—use dynamic RPC endpoint. (For Console Scanner only.)

`/RPCE : <target_address>`—use specified RPC endpoint. (For Console Scanner only.)

`/RPCH : <host_name>`—use specified host name for remote call. (For Console Scanner only.)

`/RPCP : <protocol>`—use specified RPC protocol. Possible protocols are as follows: `lpc`, `np`, `tcp`. (For Console Scanner only.)

`/SCC`—show content of complex objects. Option is disabled by default.

`/SCN`—show installation package name. Option is disabled by default.

`/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 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.

`/W : <sec>`—maximum time to scan (sec.). By default: unlimited.

`/WCL`—drwebwcl compatible output. (For Console Scanner only.)

`/X : S [:R]`—set one of the following states for the computer to enter once scanning is complete: Shutdown/Reboot/Suspend/Hibernate.

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

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



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

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

`/AC-` option is clearly disabled

`/AC, /AC+` option is clearly enabled.

These modifiers can be useful if the option was enabled or disabled by default or was set in the configuration file earlier. The following switches can have modifiers:

`/AC, /AFS, /AR, /BI, /DR, /HA, /LN, /LS, /MA, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SLS, /SPN, /SPS, /SST, /TB, /TM, /TR, /WCL.`

For `/FL` parameter '-' modifier directs to scan the paths listed in the specified file and then delete this file.

For `/ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL, /RPC, /W` parameters "0" value means that there is no limit.

The following example shows how to use command-line switches with Console Scanner:

```
[<path_to_program>]dwscancl /AR- /AIN:C /AIC:Q C:\
```

scan all files on disk 'C:', excluding those in archives; cure the infected files and move to quarantine those that cannot be cured. To run Scanner the same way, enter the `dwscancl` command name instead of `dwscanner`.

Installation Packages Parameters

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

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

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

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



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

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

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

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

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

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

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

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

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

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

`/installdir <folder>`—installation folder.



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

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

- `remove`—remove the installed product.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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.



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.

Classification of Computer Threats

Herein, the term "threat" defines any kind of software that can potentially or directly inflict damage on a computer or network or compromise the user's information or rights (in other words, malicious and other unwanted programs). However, generally speaking, the term "threat" may be used to indicate any potential danger to computer or network security (that is, vulnerabilities that can be exploited to launch attacks).

All program types described below have the ability to endanger the user's data or confidentiality. Programs that do not hide their presence from the user (for example, spam-sending software or traffic analyzers) usually are not considered to be computer threats, although they can become threats under certain circumstances.

In the documentation and products by Doctor Web, threats are divided into two categories in accordance with the severity of danger they pose.

- **Major threats** are classic computer threats that can perform destructive or illegal actions in the system on their own (erase or steal important data, crash networks, and so on). To this type of computer threats belong programs that are traditionally referred to as "malicious" (viruses, worms, and Trojans).
- **Minor threats** are less dangerous than major threats, but may be used by a third party to carry out malicious activities. Moreover, mere presence of minor threats in the system indicates its low protection level. Information security specialists sometimes refer to this type of threats as "grayware" or potentially unwanted programs. This category consists of adware, dialers, jokes, riskware, and hacktools.



Major threats

Computer viruses

This type of computer threats is characterized by their ability to inject malicious code into running processes of other programs. This action is called *infection*. In most cases, the infected file becomes a virus carrier itself, and the injected code does not necessarily match the original one. The majority of viruses are created with a purpose to damage or destroy data in the system.

Doctor Web divides viruses by the type of objects they infect into the following categories:

- **File viruses** infect operating system files (usually, executable files and dynamic-link libraries) and are activated when an infected file is run.
- **Micro viruses** infect documents used by Microsoft® Office or other programs supporting macro commands (usually, written in Visual Basic). Macro commands are a type of built-in programs (macros) that are written in a fully functional programming language and can be launched under specific circumstances (for example, in Microsoft® Word, macros can be activated upon opening, closing, or saving a document).
- **Script viruses** are created using script languages, and, mostly, they infect other scripts (such as OS service files). By exploiting vulnerable scripts in web applications, they can also infect other file types that support script execution.
- **Boot viruses** infect boot sectors of disks and partitions or master boot records of hard disks. They require little memory and can perform their tasks until the operating system is rolled out, restarted, or shut down.

Most viruses have special mechanisms that protect them against detection. These mechanisms are constantly improved, and ways to overcome them are constantly developed. According to the type of protection they use, all viruses can be divided into two following groups:

- **Encrypted viruses** self-encrypt their malicious code upon every infection to make its detection in a file, boot sector, or memory more difficult. Each sample of such viruses contains only a short common code fragment (decryption procedure) that can be used as a virus signature.
- **Polymorphic viruses** use a special decryption procedure in addition to code encryption. This procedure is different in every new virus copy. This means that such viruses do not have byte signatures.

Viruses can also be classified according to the language they are written in (most viruses are written in Assembly, high-level programming languages, script languages, and so on) and operating systems that can be infected by these viruses.

Computer worms

Recently, worms have become much more widespread than viruses and other malicious programs. Like viruses, these malicious programs can replicate themselves. A worm infiltrates a computer from



a network (usually, as an email attachment) and spreads its functional copies among other computers. Distribution can be triggered by some user action or automatically.

Worms do not necessarily consist of only one file (the worm's body). Many of them have a so-called infectious part (shellcode) that is loaded into the main memory. After that, it downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be easily removed by restarting the system (at that, RAM is reset). However, if the worm's body infiltrates the computer, only an anti-virus program can fight it.

Even if worms do not bear any payload (do not cause direct damage to a system), they can still cripple entire networks because of how intensely they spread.

Doctor Web classifies worms in accordance with their distribution methods as follows:

- **Network worms** spread via various network and file-sharing protocols.
- **Mail worms** spread via mail protocols (POP3, SMTP, and others).

Trojan programs (Trojans)

These programs cannot replicate themselves. However, they can perform malicious actions on their own (damage or delete data, forward confidential information, and others) or provide cybercriminals with authorized access to a computer to harm a third party.

Like viruses, these programs can perform various malicious activities, hide their presence from the user, and even be a virus component. However, usually, Trojans are distributed as separate executable files (through file-exchange servers, data carriers, or email attachments) that are run by users themselves or by some specific system process.

Here are some Trojan types divided by Doctor Web into separate categories as follows:

- **Backdoors** are Trojans that allow an intruder to get privileged access to the system bypassing any existing protection mechanisms. Backdoors do not infect files—they register themselves in the registry modifying registry keys.
- **Droppers** are file carriers that contain malicious programs in their bodies. Once launched, a dropper copies malicious files to a hard disk without user consent and runs them.
- **Keyloggers** can log data that users enter by means of a keyboard. These malicious programs can steal various confidential information (including network passwords, logins, bank card data, and so on).
- **Clickers** redirect users to specified Internet resources (may be malicious) in order to increase traffic to those websites or to perform DoS attacks.
- **Proxy Trojans** provide cybercriminals with anonymous Internet access via the victim's computer.
- **Rootkits** are used to intercept operating system functions in order to hide their presence. Moreover, a rootkit can conceal processes of other programs, registry keys, folders, and files. It can be distributed either as an independent program or as a component of another malicious application. Based on the operation mode, rootkits can be divided into two following categories: User Mode Rootkits (UMR) that operate in user mode (intercept functions of user-mode libraries)



and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions at the system kernel level, which makes these malicious programs hard to detect).

Trojans can also perform other malicious actions besides those listed above. For example, they can change the browser home page or delete certain files. However, such actions can also be performed by threats of other types (viruses or worms).

Minor threats

Hacktools

Hacktools are designed to assist intruders with hacking. The most common among these programs are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Such tools can be used not only by hackers but also by administrators to check security of their networks. Sometimes various programs that use social engineering techniques are designated as hacktools too.

Adware

Usually, this term refers to a program code incorporated into freeware programs that forcefully display advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements, for example, in web browsers. Many adware programs operate based on data collected by spyware.

Jokes

Like adware, this type of minor threats cannot be used to inflict any direct damage on the system. Joke programs usually just generate messages about allegedly detected errors and threaten to perform actions that may lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that, after asking for user's permission, employ Internet connection to access specific websites. Usually, these programs have a signed certificate and inform the user about all their actions.

Riskware

These programs are not intended to be computer threats. However, they can still cripple system security due to certain features and, therefore, are classified as minor threats. This type of threats includes not only programs that can accidentally damage or delete data but also programs that can be used by hackers or some malicious applications to harm the system. Among such programs are various remote chat and administrative tools, FTP-servers, and so on.



Suspicious objects

These are potential computer threats detected by the heuristic analyzer. Such objects can be any type of threat (even unknown to information security specialists) or turn out safe in case of a false detection. It is strongly recommended to move files containing suspicious objects to quarantine and send them for analysis to Doctor Web anti-virus laboratory.



Actions Applied to Threats

There are many methods of neutralizing computer threats. Products of Doctor Web combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and a comprehensive approach to security assurance. The main actions for neutralizing malicious programs are:

1. **Cure**—an action applied to viruses, worms and Trojans. It implies deletion of malicious code from infected files or deletion of a malicious program's functional copies as well as the recovery of affected objects (that is, return of the object's structure and operability to the state which was before the infection) if it is possible. Not all malicious programs can be cured. However, products of Doctor Web are based on most effective curing and file recovery algorithms.
2. **Move to quarantine**—an action when the malicious object is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to Doctor Web anti-virus laboratory.
3. **Delete**—the most effective action for neutralizing computer threats. It can be applied to any type of malicious objects. Note that deletion will sometimes be applied to certain files for which curing was selected. This will happen if the file contains only malicious code and no useful information. For example, curing of a computer worm implies deletion of all its functional copies.
4. **Block, rename**—these actions can also be used for neutralizing malicious programs. In the former case, all access attempts to or from the file are blocked. In the latter case, the extension of the file is renamed, which makes it inoperative.



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 <http://vms.drweb.com/classification/>.

In certain cases this classification is conventional as some viruses can possess several features at the same time. Besides, it should not be considered exhaustive as new types of viruses constantly appear, and the classification is made more precise.

The full name of a virus consists of several elements, separated by full stops. Some elements at the beginning of the full name (prefixes) and at the end of it (suffixes) are standard for the accepted classification.

Prefixes

Affected operating systems

The prefixes listed below are used for naming viruses infecting executable files of certain operating systems:

- Win—16-bit Windows 3.1 programs
- Win95—32-bit Windows 95/98/Me programs
- WinNT—32-bit Windows NT/2000/XP/Vista programs
- Win32—32-bit Windows 95/98/Me and NT/2000/XP/Vista programs
- Win32.NET—programs in Microsoft .NET Framework operating system
- OS2—OS/2 programs
- Unix—programs in various Unix-based systems
- Linux—Linux programs
- FreeBSD—FreeBSD programs
- SunOS—SunOS (Solaris) programs
- Symbian—Symbian OS (mobile OS) programs

Note that some viruses can infect programs of one system even if they are designed to operate in another system.



Macrovirus prefixes

The list of prefixes for viruses which infect MS Office objects (the language of the macros infected by such type of virus is specified):

- WM—Word Basic (MS Word 6.0-7.0)
- XM—VBA3 (MS Excel 5.0-7.0)
- W97M—VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- X97M—VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- A97M—databases of MS Access'97/2000
- PP97M—MS PowerPoint presentations
- O97M—VBA5 (MS Office'97), VBA6 (MS Office 2000); this virus infects files of more than one component of MS Office

Development languages

The HLL group is used to name viruses written in high-level programming languages, such as C, C++, Pascal, Basic, and others. To specify functioning algorithms, the following modifiers can be used:

- HLLW—worms
- HLLM—mail worms
- HLL0—viruses overwriting the code of the victim program
- HLLP—parasitic viruses
- HLLC—companion viruses

The following prefix also refers to development language:

- Java—viruses designed for the Java virtual machine

Trojan programs (Trojans)

Trojan—a general name for different Trojan programs (Trojans). In many cases the prefixes of this group are used with the Trojan prefix.

- PWS—password stealing Trojan
- Backdoor—Trojan with RAT-function (Remote Administration Tool—a utility for remote administration)
- IRC—Trojan which uses Internet Relay Chat channels
- DownLoader—Trojan which secretly downloads different malicious programs from the Internet
- MulDrop—Trojan which secretly downloads different viruses contained in its body
- Proxy—Trojan which allows a third-party user to work anonymously in the Internet via the infected computer



- `StartPage` (synonym: `Seeker`)—Trojan which makes unauthorized replacement of the browser home page address (start page)
- `Click`—Trojan which redirects a user's browser to a certain website (or websites)
- `KeyLogger`—a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- `AVKill`—terminates or deletes anti-virus programs, firewalls, etc.
- `KillFiles`, `KillDisk`, `DiskEraser`—deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- `DelWin`—deletes files vital for the operation of Windows OS
- `FormatC`—formats drive C (synonym: `FormatAll`—formats all drives)
- `KillMBR`—corrupts or deletes master boot records (MBR)
- `KillCMOS`—corrupts or deletes CMOS memory

Tool for attacking vulnerabilities

- `Exploit`—a tool exploiting known vulnerabilities of an OS or application to implant malicious code or perform unauthorized actions

Tools for network attacks

- `Nuke`—tools for network attacks on known vulnerabilities of operating systems leading to abnormal shutdowns of the attacked system
- `DDoS`—agent program for performing a DDoS attack (Distributed Denial Of Service)
- `FDoS` (synonym: `Flooder`)—Flooder Denial Of Service—programs for performing malicious actions in the Internet which use the idea of DDoS attacks; in contrast to DDoS, when several agents on different computers are used simultaneously to attack one victim system, an FDoS program operates as an independent "self-sufficient" program (Flooder Denial of Service).

Script viruses

Prefixes of viruses written in different scrip languages:

- `VBS`—Visual Basic Script
- `JS`—Java Script
- `Wscript`—Visual Basic Script and/or Java Script
- `Perl`—Perl
- `PHP`—PHP
- `BAT`—MS-DOS command interpreter



Malicious programs

Prefixes of malicious programs that are not viruses:

- **Adware**—an advertising program
- **Dialer**—a dialer program (redirecting modem calls to predefined paid numbers or paid resources)
- **Joke**—a joke program
- **Program**—a potentially dangerous program (riskware)
- **Tool**—a program used for hacking (hacktool)

Miscellaneous

Generic—this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.

Silly—this prefix was used with different modifiers to name simple featureless viruses in the past.

Suffixes

Suffixes are used to name some specific virus objects:

- **generator**—an object which is not a virus but a virus generator.
- **based**—a virus which is developed with the help of the specified generator or a modified virus. In both cases the names of this type are generic and can define hundreds and sometimes even thousands of viruses.
- **dropper**—an object which is not a virus but an installer of the given virus.

