



User Manual

Defend what you create

© Doctor Web, 2015. All rights reserved.

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, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk 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 10.0
User Manual
25.02.2015

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site 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 antivirus 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 the program	12
3.1. Installing Via Installation Package	12
3.2. Installing Via Reduced Installation Package	17
3.3. Removing or changing the program	23
4. Getting Started	25
4.1. How to Test Anti-virus	27
5. Tools	28
5.1. Quarantine Manager	28
5.2. Support	30
5.2.1. Report	30
6. Dr.Web Scanner	32
6.1. Scanning Your System	32
6.2. Neutralizing Detected Threats	35
6.3. Scanner Settings	37
6.4. Scanning in Command Line Mode	43
6.5. Console Scanner	44
6.6. Automatic Launch of Scanning	44
7. Settings	45
8. Main Settings	46
8.1. Notifications	46
8.2. Self-protection	49
8.3. Devices	49
8.4. Advanced	51
8.5. Mode	54
9. Office Control	57



9.1. Office Control Settings	58
10. Exclusions	60
10.1. Websites	60
10.2. Files and Folders	60
10.3. Programs and Processes	61
10.4. Anti-spam	61
11. Protection components	63
11.1 SpIDer Guard	63
11.1.1. Configuring SpIDer Guard	63
11.2. SpIDer Gate	67
11.2.1. Configuring SpIDer Gate	67
11.3. SpIDer Mail	70
11.3.1. Configuring SpIDer Mail	71
11.4. Anti-spam	74
11.5. Dr.Web Firewall	76
11.5.1. Training Firewall	76
11.5.2. Configuring Firewall	77
11.6. Dr.Web for Outlook	85
11.6.1. Configuring Dr.Web for Outlook	85
11.6.2. Threat Detection	86
11.6.3. Spam Check	89
11.6.4. Logging	92
11.6.5. Statistics	93
11.7. Preventive Protection Page	94
Appendices	97
Appendix A. Command Line Parameters	97
Scanner and Console Scanner Parameters	97
Installation Packages Parameters	100
Return codes	103
Appendix B. Computer Threats and Neutralization Methods	104
Classification of Computer Threats	104
Actions Applied to Threats	107
Appendix C. Naming of Viruses	108



1. Introduction

Dr.Web Agent provides multilevel protection of RAM, hard disks, and removable devices 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 IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian®, 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 undesirable programs (adware, dialers, jokes, riskware, and hacktools) from your computer. To detect undesirable programs and perform actions with the files contained in the programs, anti-virus components of **Dr.Web** are used.

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

Dr.Web Scanner (Scanner) is an anti-virus scanner with graphical interface. The program runs on user demand and checks the computer for viruses.

Dr.Web Console Scanner – a command-line version of **Dr.Web Scanner**.

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

SpIDer Mail – the program intercepts calls sent from mail clients to mail servers through POP3/SMTP/IMAP4/NNTP protocols (IMAP4 stands for IMAPv4rev1), and detects and neutralizes mail viruses before a mail message is received by the mail client or before a mail message is sent to the mail server. **SpIDer Mail** also provides you with spam filtering by using **Dr.Web Anti-spam**.

Dr.Web for Outlook is a plug-in that checks Microsoft Outlook mail boxes for viruses and spam.

SpIDer Gate is an HTTP monitor. By default, the component automatically checks incoming HTTP traffic and blocks all malware objects. URL filtering of malicious and unreliable websites is also enabled by default.

Office Control is used to restrict access to websites, files and folders, and allows to set custom time limits on using your computer and the Internet.

Dr.Web Firewall is a components that protects your computer from unauthorized access and prevents vital data from leaking through networks.

SpIDer Agent is a utility that lets you set up and manage **Dr.Web** components.



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
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of Doctor Web products and components.
<u>Green and underlined</u>	Hyperlinks to topics and webpages.
Monospace	Code examples, input to the command line and application output.
<i>Italic</i>	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign (+)	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
Exclamation mark	A warning about potential errors or any other important comment.



1.3. Detection Methods

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

Detection Methods

Signature analysis

The scans begin with signature analysis which 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, the **Dr.Web** anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing™

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

Execution emulation

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

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm 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 by also 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 heuristics analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious".



While performing any of the abovementioned checks, the **Dr.Web** anti-virus solutions use the most recent information about known malicious software. As soon as experts of **Doctor Web 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 the **Dr.Web** resident guards and penetrates the system, then after an update the virus is detected in 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 components.
- If you install **Dr.Web Firewall**, uninstall all other firewalls from your computer
- Install all critical updates released for your operating system. 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 which 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• Microsoft® Windows® 7• Microsoft® Windows® 8• Microsoft® Windows® 8.1• Microsoft® Windows Server® 2003 with Service Pack 1• Microsoft® 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• Microsoft® Windows® 7• Microsoft® Windows® 8• Microsoft® Windows® 8.1• Microsoft® Windows Server® 2008 with Service Pack 2 or higher• Microsoft® Windows Server® 2008 R2• Microsoft® Windows Server® 2012• Microsoft® Windows Server® 2012 R2 <p>You may need to download and install certain system components from the Microsoft official website. If necessary, the program will notify you about the Dr.Web components required and provide download links.</p>
Free RAM	Minimum 512 MB.
Hard disk space	<p>1 GB for Dr.Web components.</p> <p>Files created during installation will require additional space.</p>
Resolution	Recommended minimum screen resolution is 800x600.
Other	<p>To update Dr.Web virus databases and Dr.Web components, connection to the central protection server or to the Internet in the Mobile mode is required.</p> <p>For the Dr.Web for Outlook extension, one of the following Microsoft Outlook clients from the Microsoft Office package is required:</p> <ul style="list-style-type: none">• Outlook 2000 (Outlook 9),• Outlook 2002 (Outlook 10 or Outlook XP),• Office Outlook 2003 (Outlook 11),• Office Outlook 2007,• Office Outlook 2010,• Office Outlook 2013.



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.



3. Installing 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's 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](#) or [reduced](#) installation package.

3.1. Installing Via Installation Package



To install **Dr.Web**, a user must have administrative privileges.

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

- The background mode
- The usual mode

Installation with command-line parameters

To start installation of **Dr.Web** from the command line, enter the executable file name (win-es-agent-setup.exe) and specify necessary parameters. For example, to start background installation of **Dr.Web** with reboot after the process completes, execute the following command:

```
drweb-esuite-agent-full-10.00.0-xxxxxxx-windows.exe /silent yes
```

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



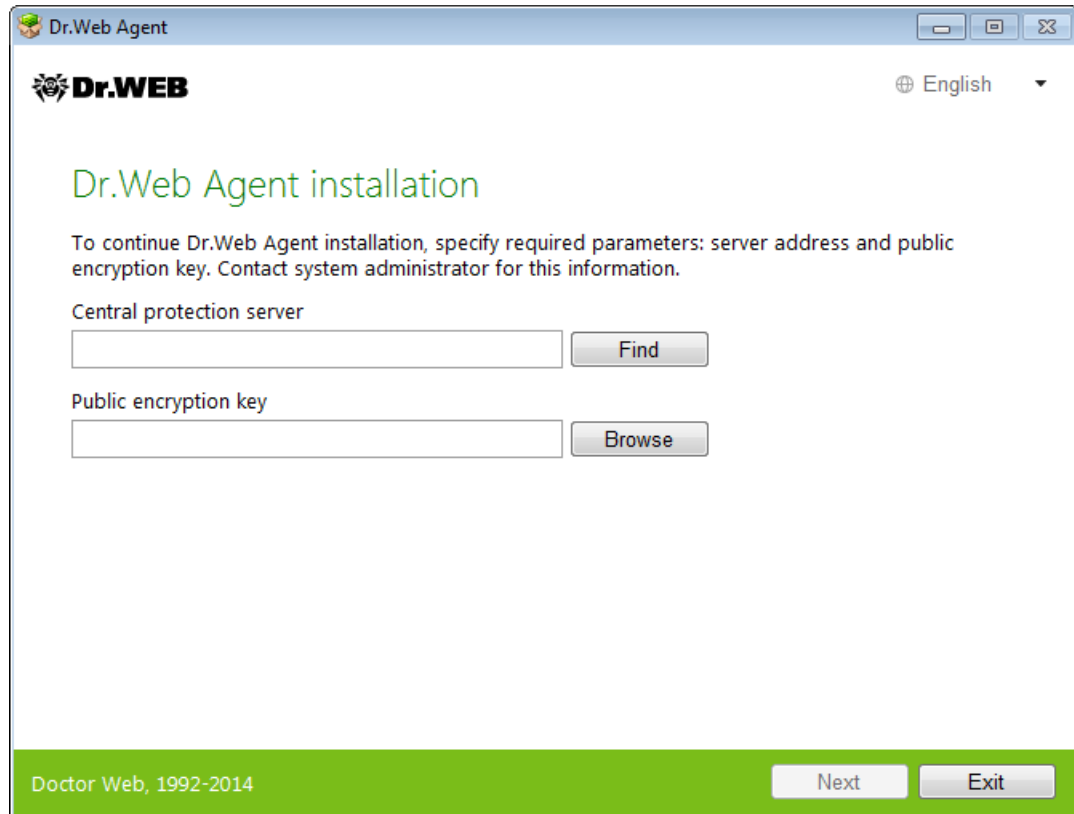
Usual Installation

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 used anti-virus software manually.

The window of **Dr.Web** Installation Wizard opens.



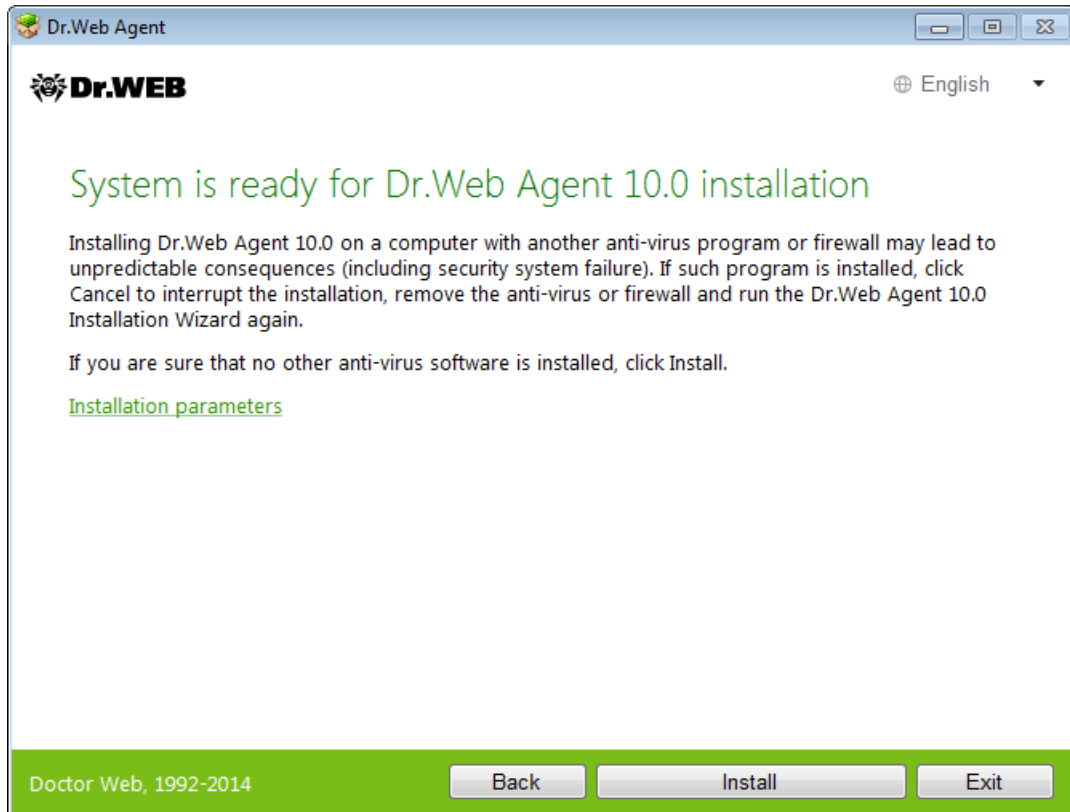
2. In the **Central protection server** field, specify the network address of the server, from which **Dr.Web** is to be installed and in the **Public encryption key** specify the full path to the key (drwcsd.pub) residing on your computer.

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



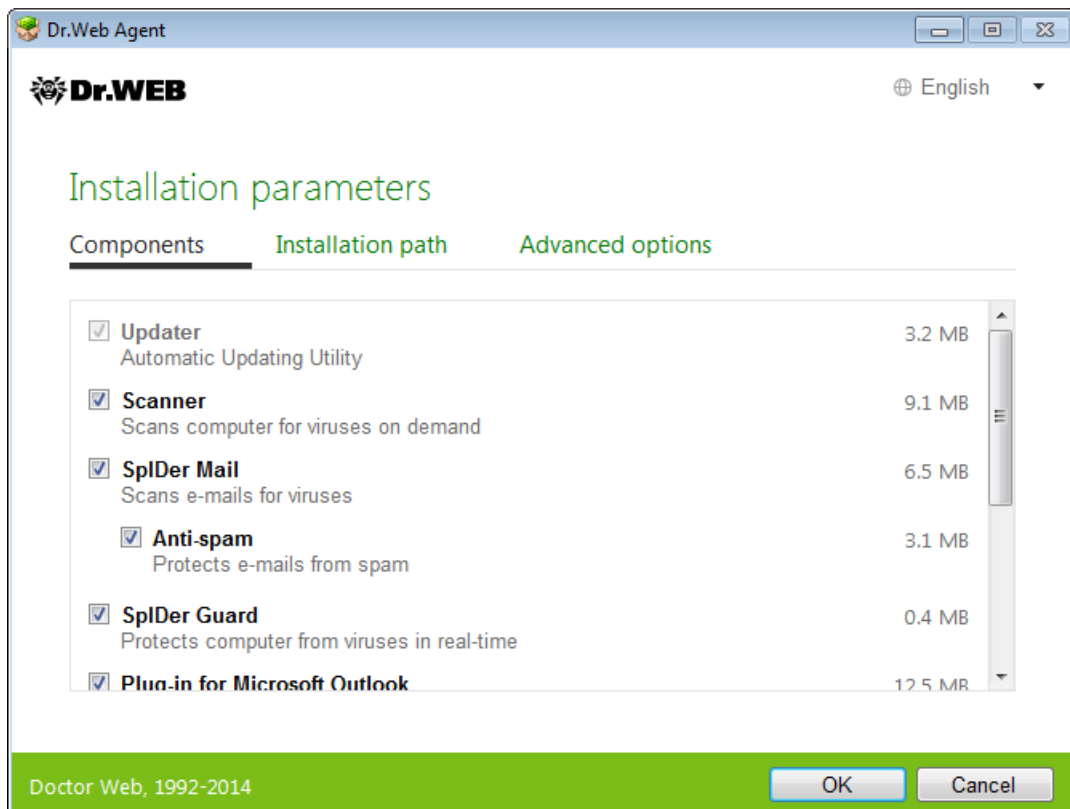
If the attempt to establish connection fails, follow the link to check network parameters and/or try to connect to the server again by clicking the corresponding button.

3. 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.

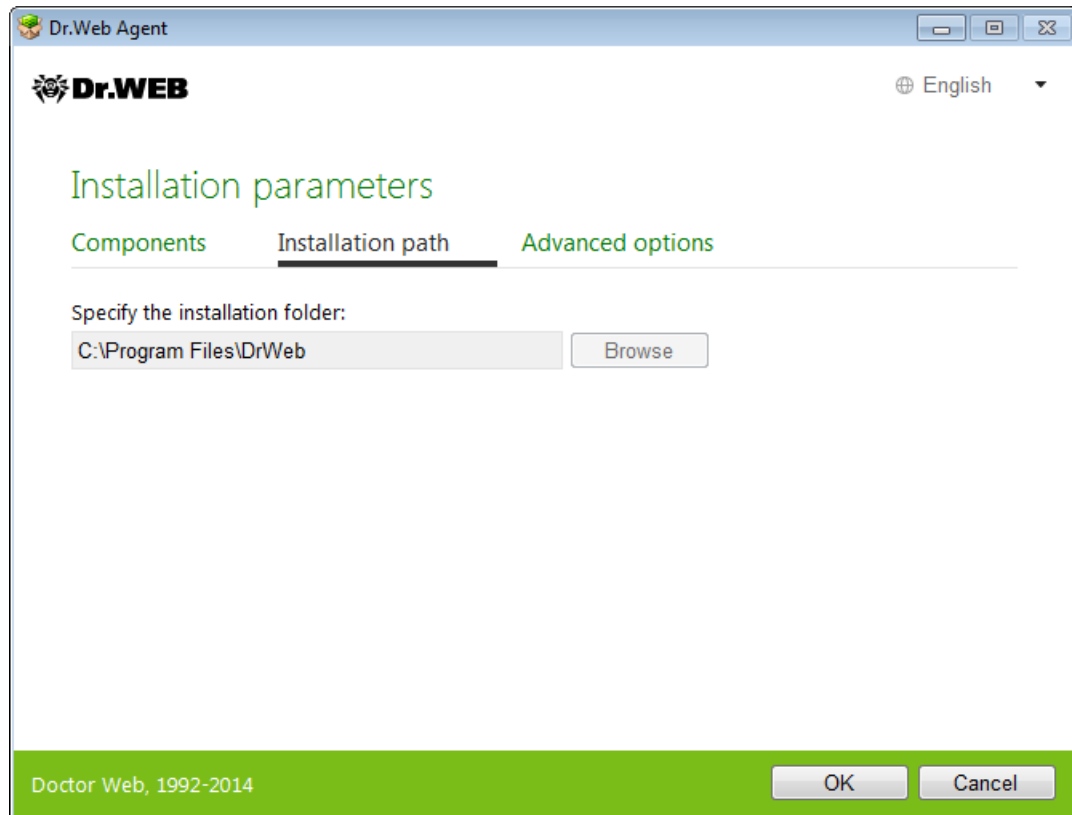
4. If you selected **Install** at the previous step, go to the description of step 7. Otherwise, the **Installation parameters** window opens. On the **Components** tab, **Dr.Web** components are listed.





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

5. On the **Installation path** tab, specify the folder for **Dr.Web** to be installed.



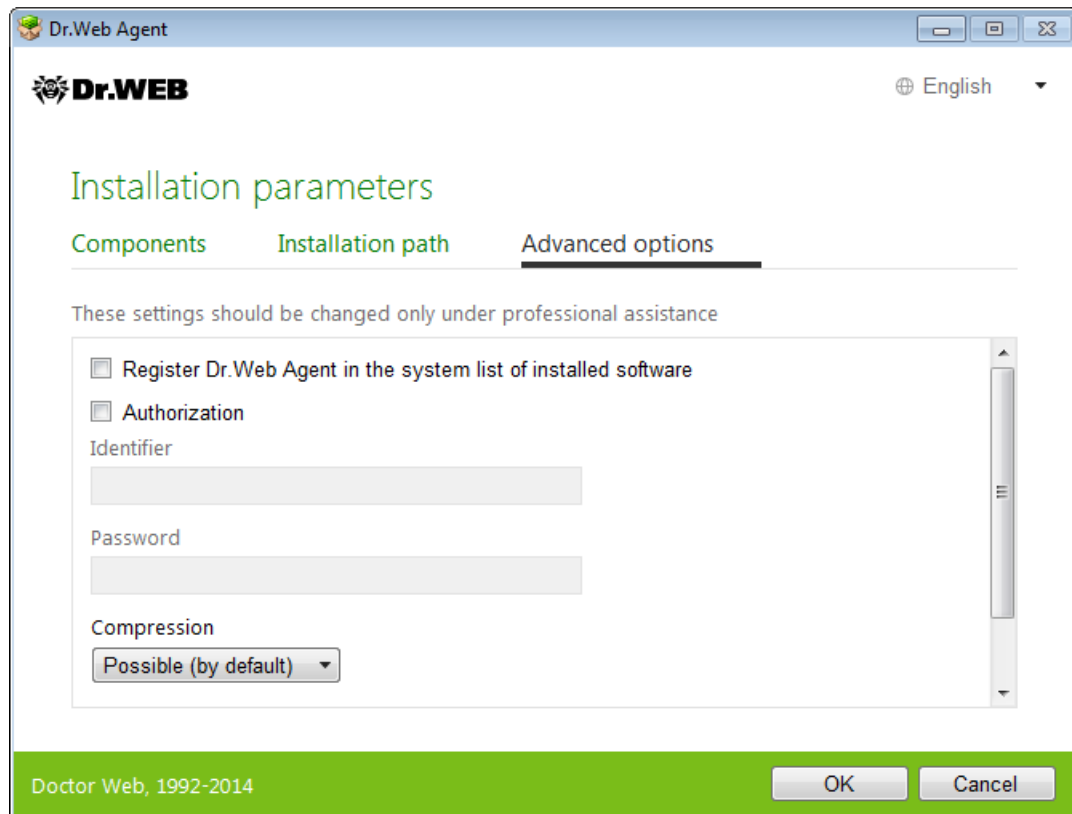
By default, it is installed to the DrWeb folder in the Program Files folder on the system disk. To change the installation path, click **Browse** and specify the necessary folder.

6. On the next tab, you are prompted to configure additional settings.

If required, select the **Register Dr.Web Agent in the system list of installed software** check box. This option also allows to [uninstall Dr.Web](#) by the means of standard Windows tools.

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.

In 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 **Install**.

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



3.2. Installing Via Reduced Installation Package



To install **Dr.Web**, a user must have administrative privileges.

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

- The background mode
- The usual mode

Installation with command-line parameters

To start installation of **Dr.Web** from the command line, enter the executable file name (win-es-agent-setup.exe) and specify necessary parameters. For example, to start background installation of **Dr.Web** with reboot after the process completes, execute the following command:

```
drweb-esuite-install.exe /silent yes
```

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

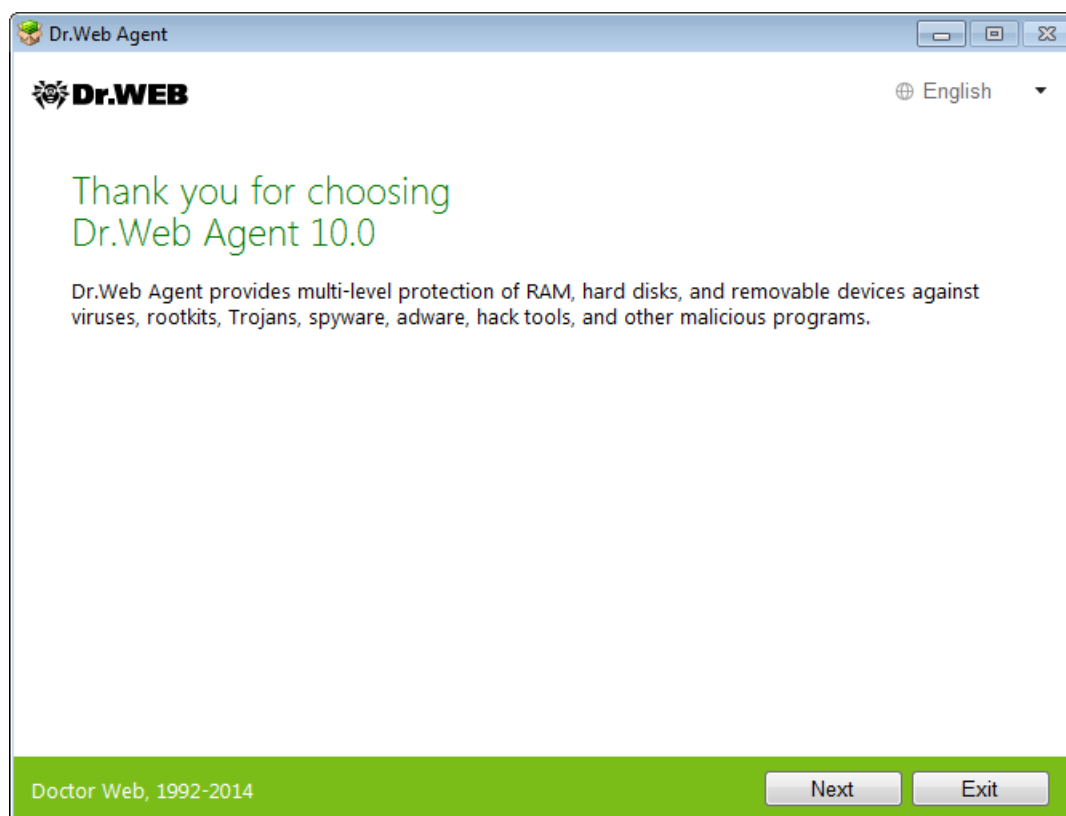
Usual Installation

1. Run the installation package received from the administrator.



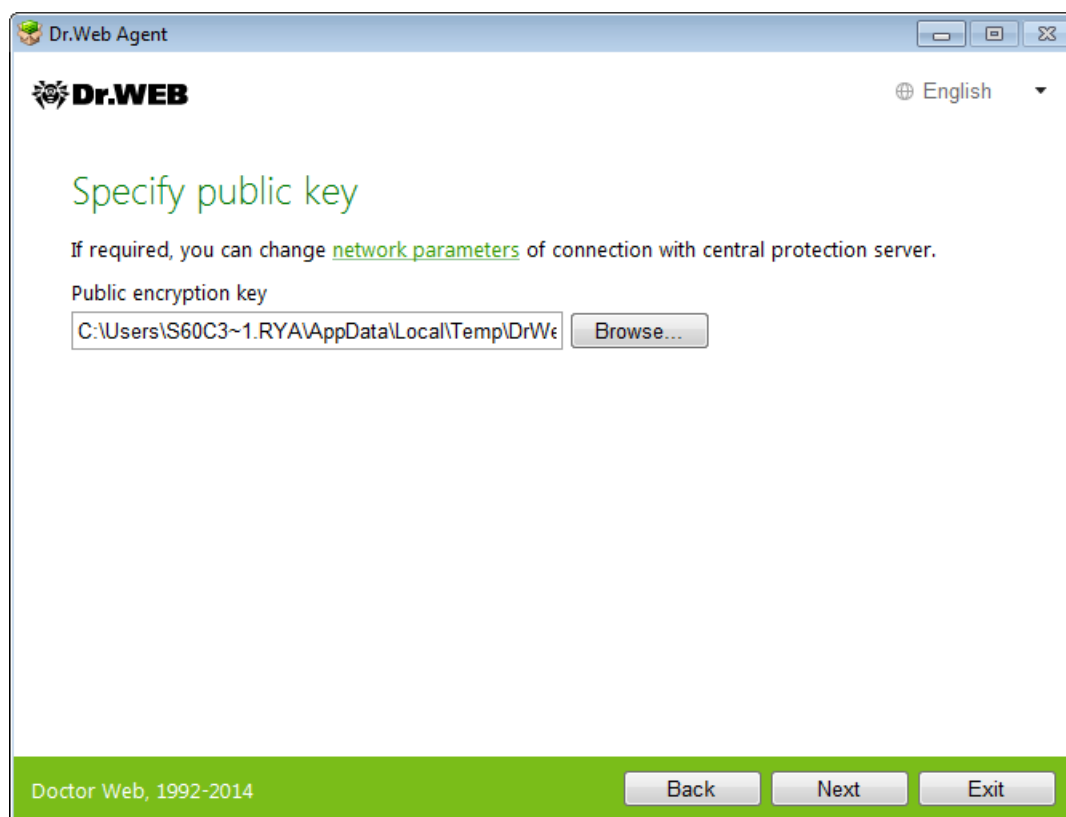
If there is any anti-virus software installed on the computer, the Installation Wizard will attempt to remove it before starting the installation. If the attempt fails, you need to remove the used anti-virus software manually.

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** window.



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



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.

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

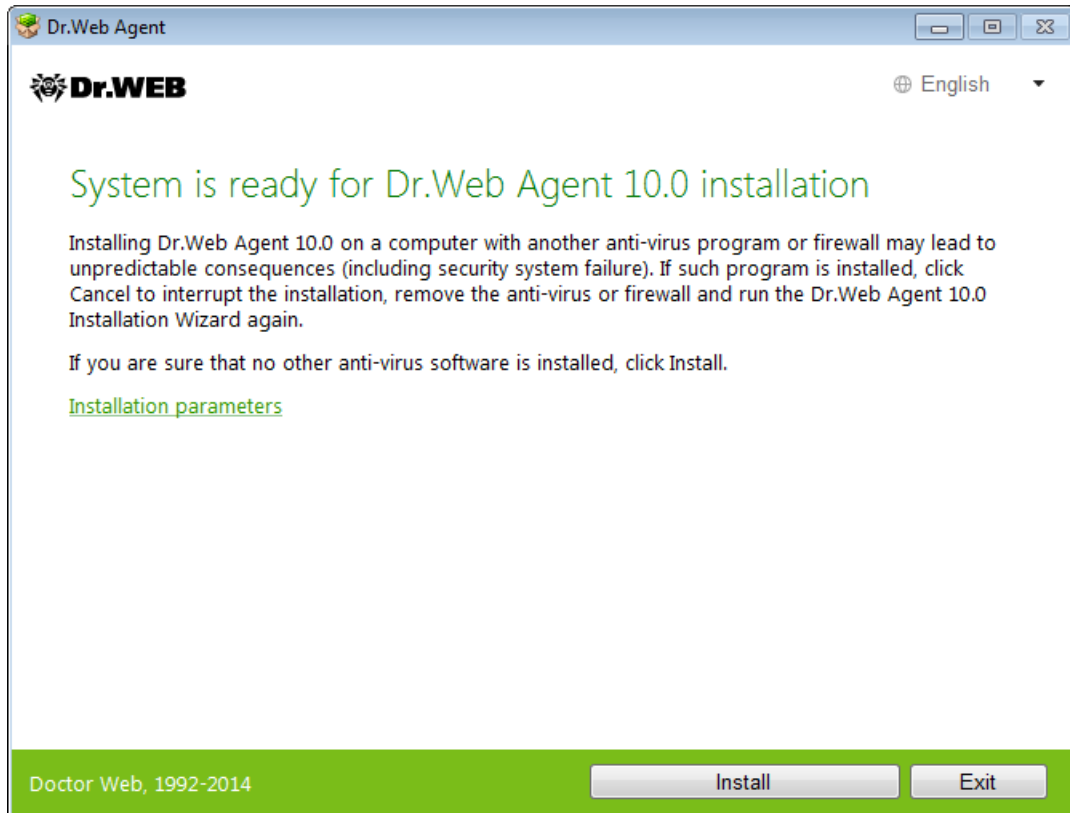
To save the changes, click **OK**. This will return you to the previous window.

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.

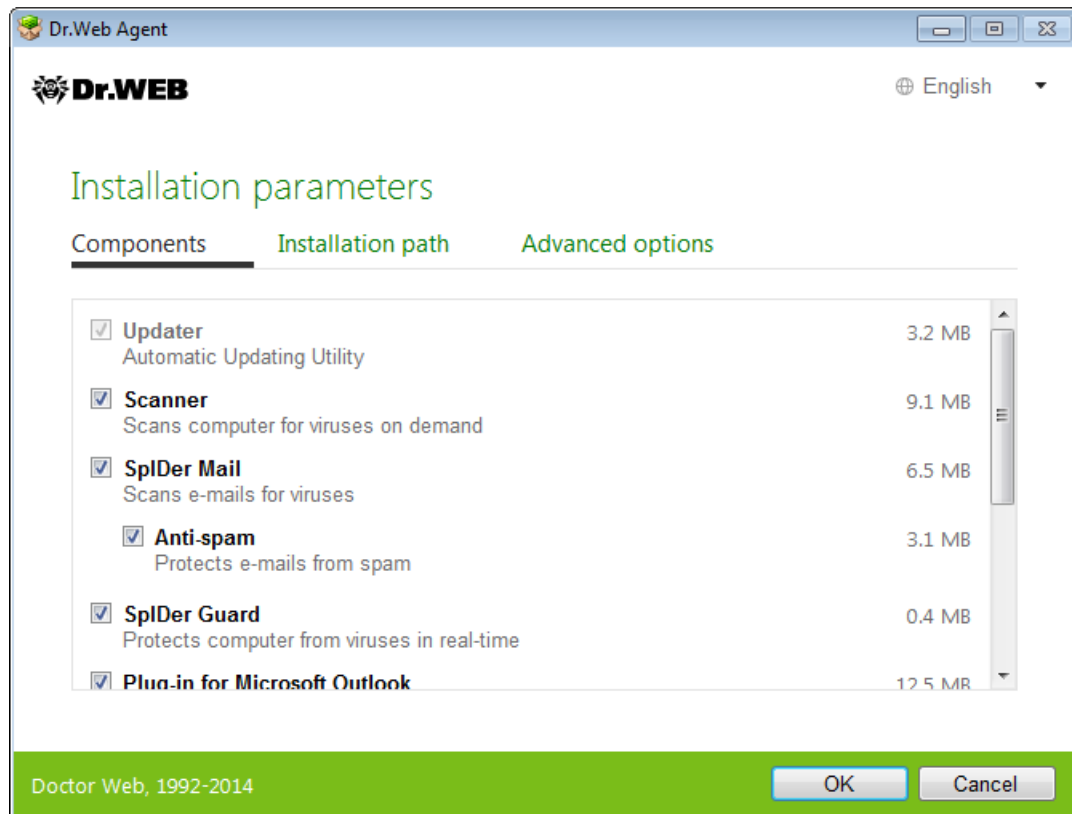
4. After the connection is established, the window opens notifying you that the product is ready to be installed. To start installation with the default parameters, click **Install**.



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.

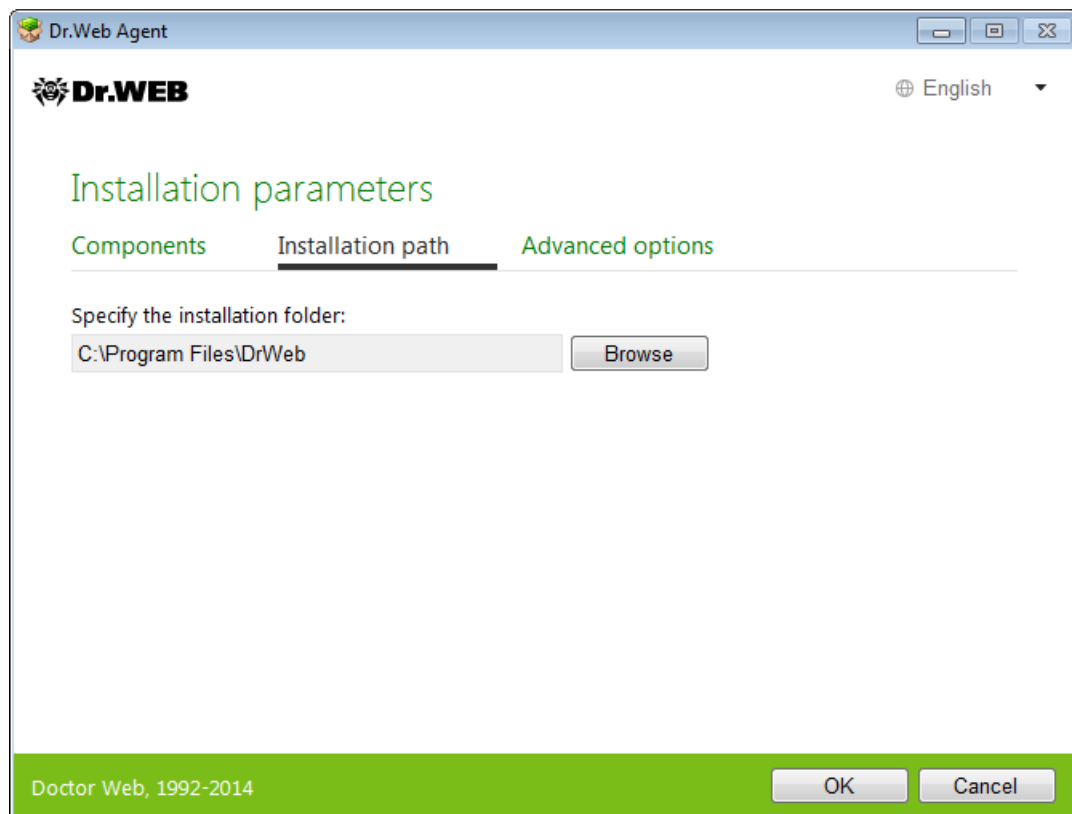
5. If you selected **Install** at the previous step, go to the description of step 8. Otherwise, the **Installation parameters** window opens.

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.

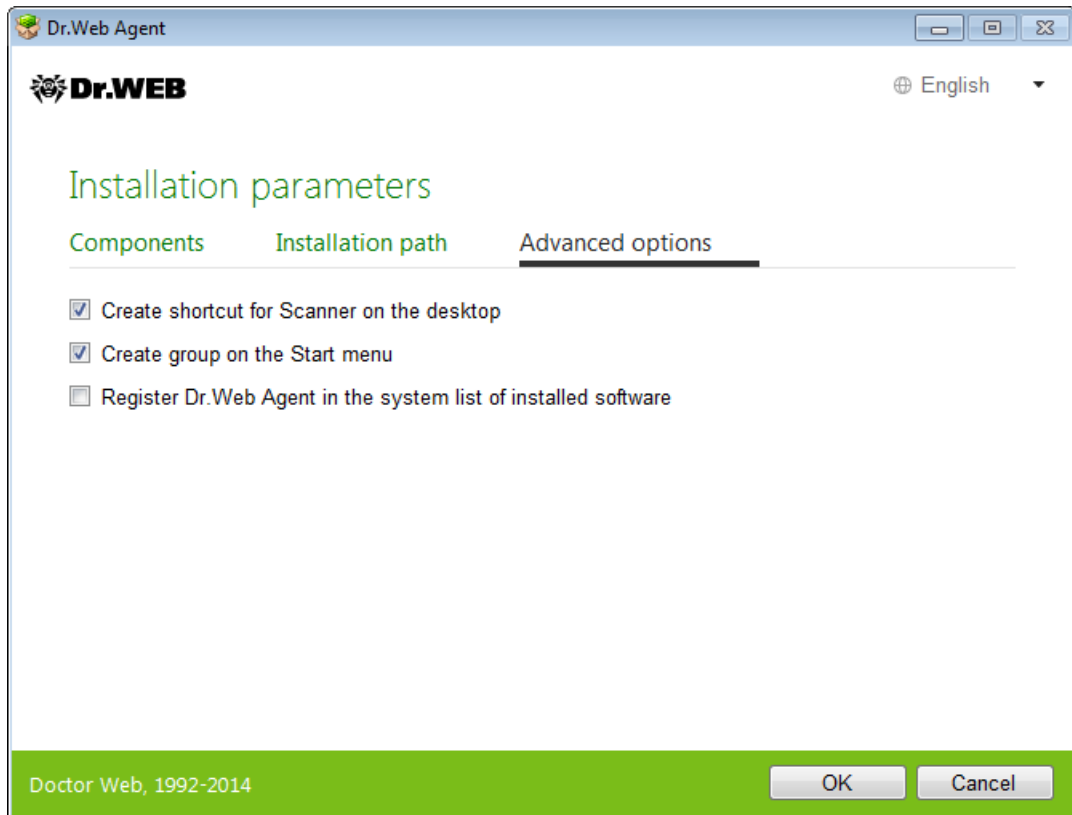
6. On the **Installation path** tab, specify the folder for **Dr.Web** to be installed.





By default, it is installed to the DrWeb 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** tab, you are prompted to create shortcuts that start **Dr.Web**.



If required, select the **Register Dr.Web Agent in the system list of installed software** check box. This option also allows to [uninstall 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. After installation completes, you are prompted to restart the computer. Click **Restart now**.



3.3. Removing or changing the program



To enable local uninstallation of **Dr.Web**, this option 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.

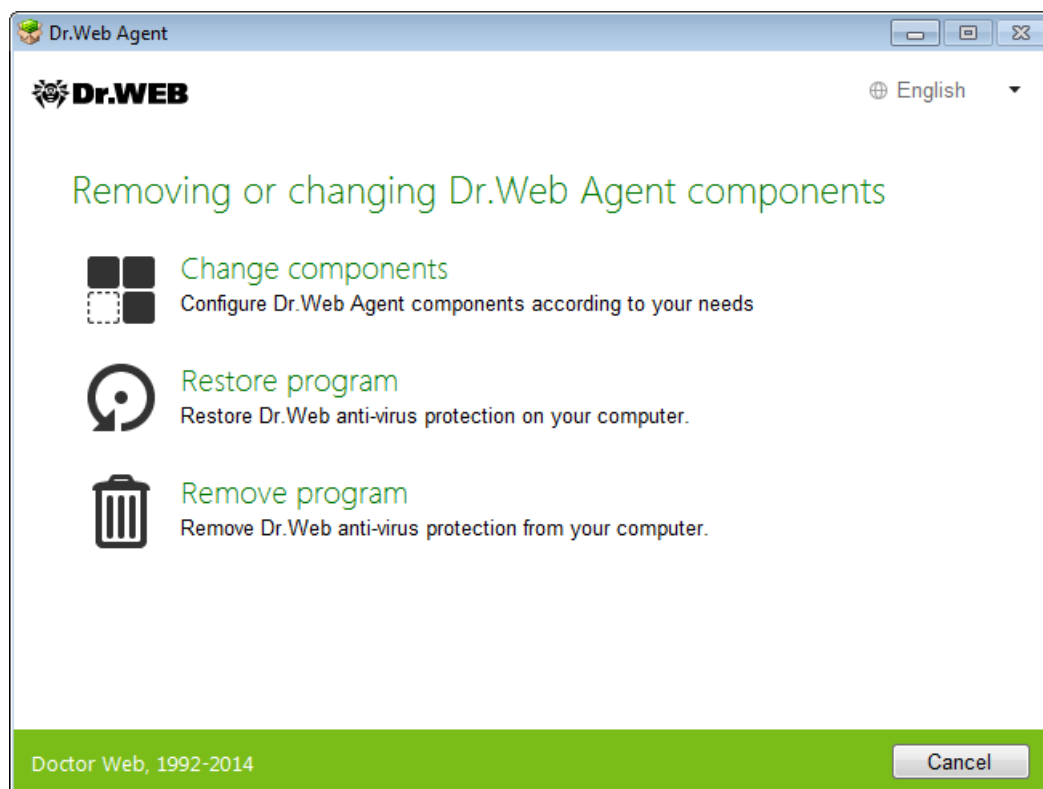
Uninstalling or Changing Dr.Web with Standard Windows Tools



This method is available only if you selected the **Register Agent in system list of installed software** check box 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 **Uninstall** and go to step 6. To **change** the configuration of **Dr.Web** by adding or removing certain components, click **Change**. 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 **Install**.



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

5. To delete all installed components, select **Remove program**.
6. In the **Parameters** 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 are selected, that is **Quarantine**, **Dr.Web Agent** settings and **Protected copies of files**. Click **Next**.
7. In the next window, confirm deletion of **Dr.Web** click **Remove**.
8. When prompted, restart the computer to complete the procedure.

Uninstalling with Command-Line Parameters

To start uninstallation of **Dr.Web** from the command line, enter the 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 /reboot yes
```




4. Getting Started




After **Dr.Web** is installed, the **SpIDer Agent**  icon is added to the notification area.




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**:

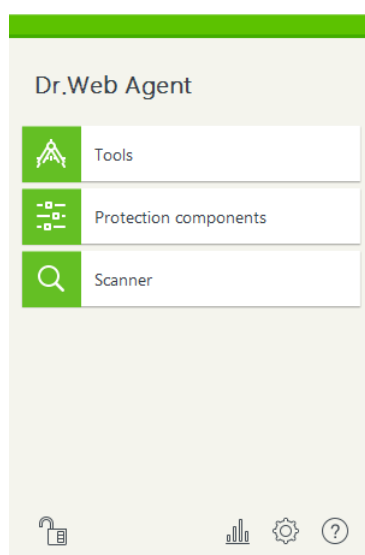
-  – All necessary components are running and protect your computer; connection to the central protection server is established.
-  – **Dr.Web** Self-protection or an important component such as **SpIDer Guard** or **Firewall** is disabled, which compromises security of **Dr.Web** and your computer; or connection to the server is expected. Probably the server refused the connection or denied access to its resources. Enable Self-protection or the component, wait until the connection to the server is established.
-  – **Dr.Web** components are expected to start after the operating system start up 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**  if [configured](#).

To open the **SpIDer Agent** 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 perform the main management and setting functions of **Dr.Web**.

Tools. Opens a submenu providing access to:


- [Quarantine Manager](#);





- [Support](#) section.

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.

Working 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 by password** option on the [Settings](#) window. Note that you will be returned to the user mode in 15 minutes after switching to the administrator mode. If you are still configuring the settings when this time expires, you will be returned to the user mode after closing the settings window.

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

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



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 **Protect Dr.Web settings by password** option on the [Settings](#) window.

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



4.1. How to Test 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 "virus", **Dr.Web** anti-virus solutions report the following: EICAR Test File (Not a Virus!) . Other anti-virus tools alert users in a similar way.

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

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

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

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



When you attempt to execute an EICAR file while **SpIDer Guard** is running in the optimal mode, the operation is not terminated 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.



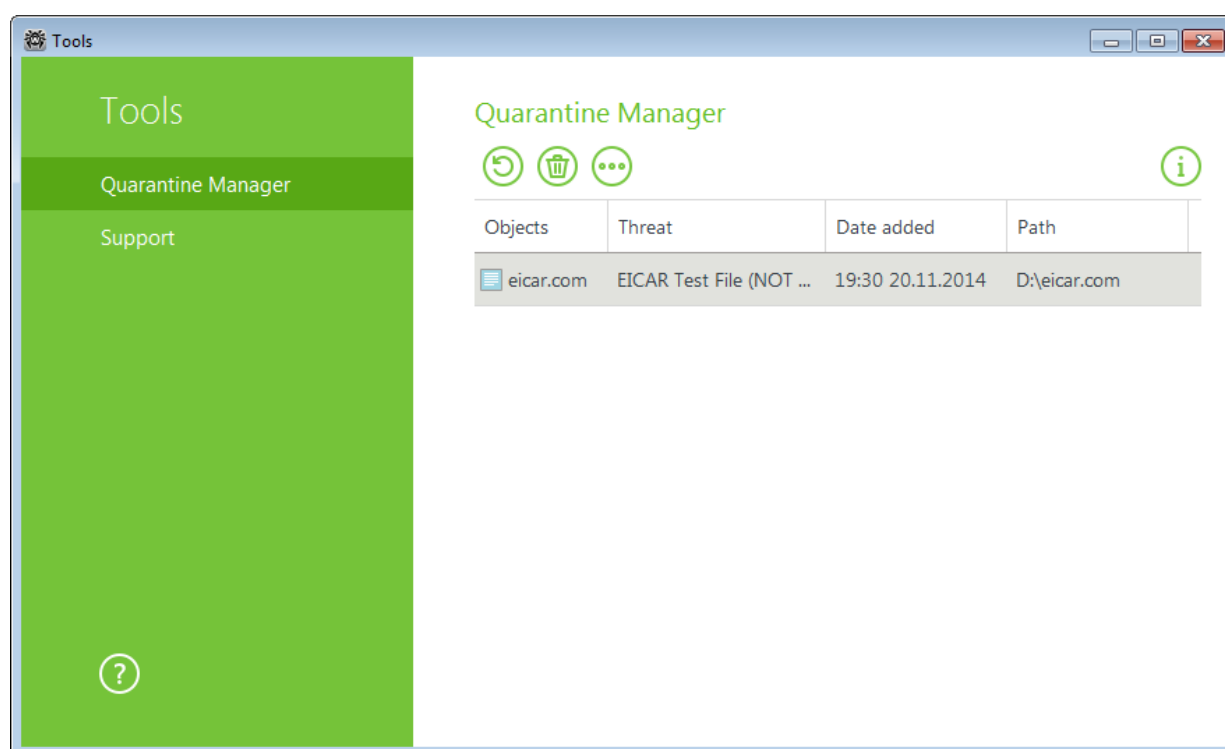
5. Tools

5.1. Quarantine Manager

Quarantine Manager provides the information about the **Quarantine** component which serves for isolation of files that are suspicious as malware. **Quarantine** also stores backup copies of files processed by **Dr.Web**.

Use the [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 that are available to you:

- **Object** – name of the quarantined object
- **Threat** – malware class of the object, which is assigned by **Dr.Web** when the object is moved to **Quarantine**
- **Date added** – the date and time when the object was moved to **Quarantine**
- **Path** – full path to the object before it was quarantined



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

In the **Quarantine Manager** window, the following buttons are available:

- **Restore** – move file to the selected folder and specify a new file name;



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

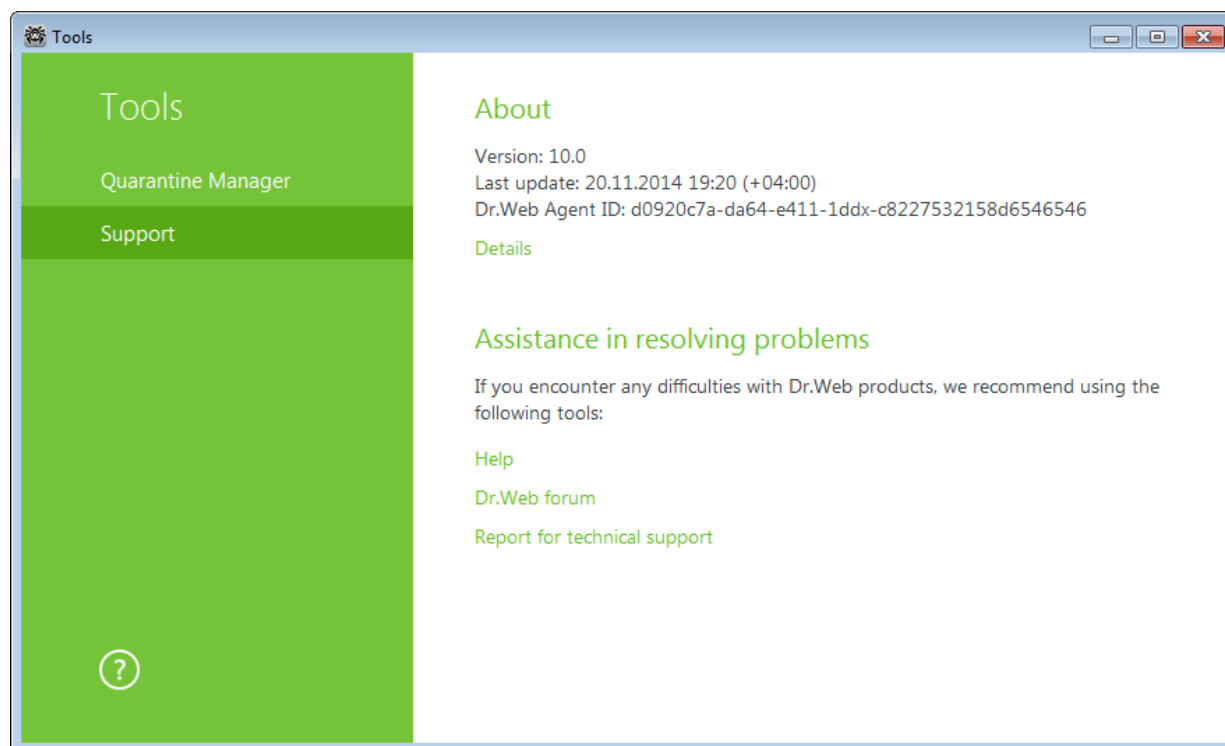
- **Scan** – rescan the file in the quarantine.
- **Delete** – delete file from the quarantine and from the system.

To delete all objects from quarantine, click  and select **Delete all** in the drop-down menu.



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**.



If you encounter any questions, take advantage of the following tools:

My Dr.Web. Opens your personal account of **Doctor Web** company site. There you can get your license information (license period, serial number), renew your license, ask a question to the support and more.

Help. Opens help file.

Dr.Web forum. Opens the **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 solution for the problem, you can request direct assistance from **Doctor Web** technical support by filling in the web form in the corresponding section of the support site 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

When contacting your anti-virus network administrator, 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**.



6. Dr.Web Scanner

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 them. 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 launch Scanner



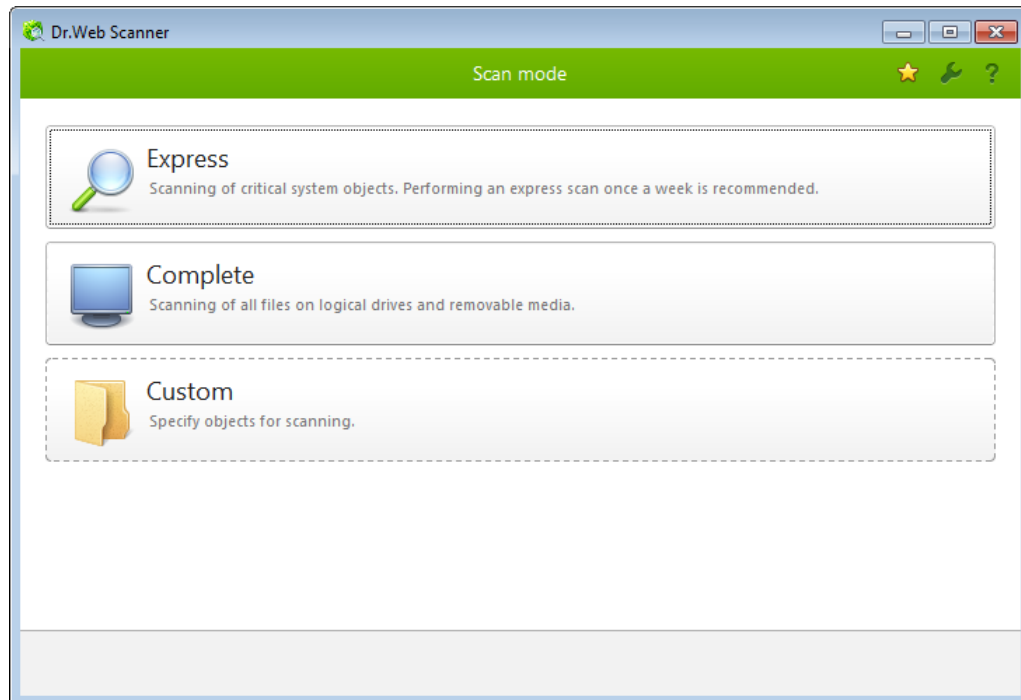
It is recommended to run **Scanner** under an account with administrative privileges. Otherwise, all folders and files (including system folders) that are not accessible to unprivileged user including system folder are not scanned.

1. To launch **Scanner**, do one of the following:
 - Click the **Scanner** icon on the desktop.
 - Click the **SpIDer Agent** icon  on the notification area and select **Scanner**.
 - Click **Start**, select the **Dr.Web** item and then select **Dr.Web Scanner**.
 - Enter the corresponding command in the Windows command line (for details, refer to [Scanning in Command-Line Mode](#)).

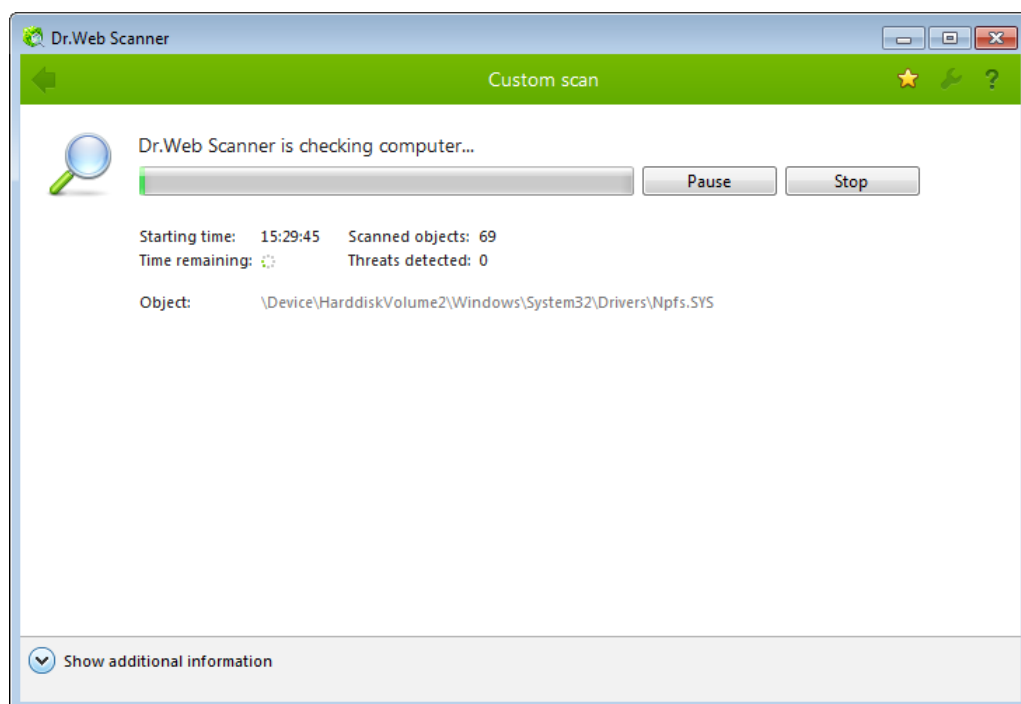
To launch **Scanner** with default settings to scan a certain file or folder, select **Check with Dr.Web**.



2. When **Scanner** launches, its main window opens.



If you instruct **Scanner** to check a file or folder, scanning is started immediately.



3. There are three scanning modes: **Express** scan, **Full** scan and **Custom** scan.

In *Express* scan 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")



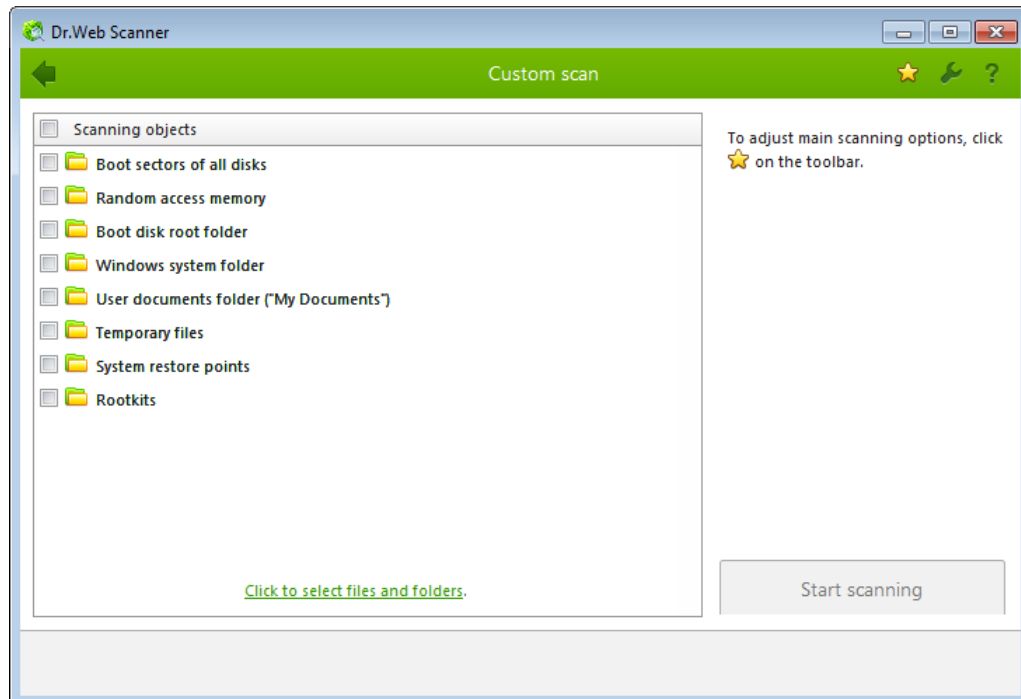
- Temporary files
- System restore points
- Presence of rootkits (if the process is run with administrative privileges)



Scanner does not check archives and email files in *Express scan* mode.

If *full scan mode* is selected, random access memory and all hard drives (including boot sectors of all disks) are scanned. **Scanner** also runs a check on rootkits.

Custom scan mode allows you to select any files and folders for scanning.



4. If you launch a custom scan, you can select objects from the list to be scanned: any files and folders, and such objects as random access memory, boot sectors, and so on. To start scanning selected objects, click **Start scanning**. In full scan or express scan modes, objects cannot be selected manually.
5. 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**.

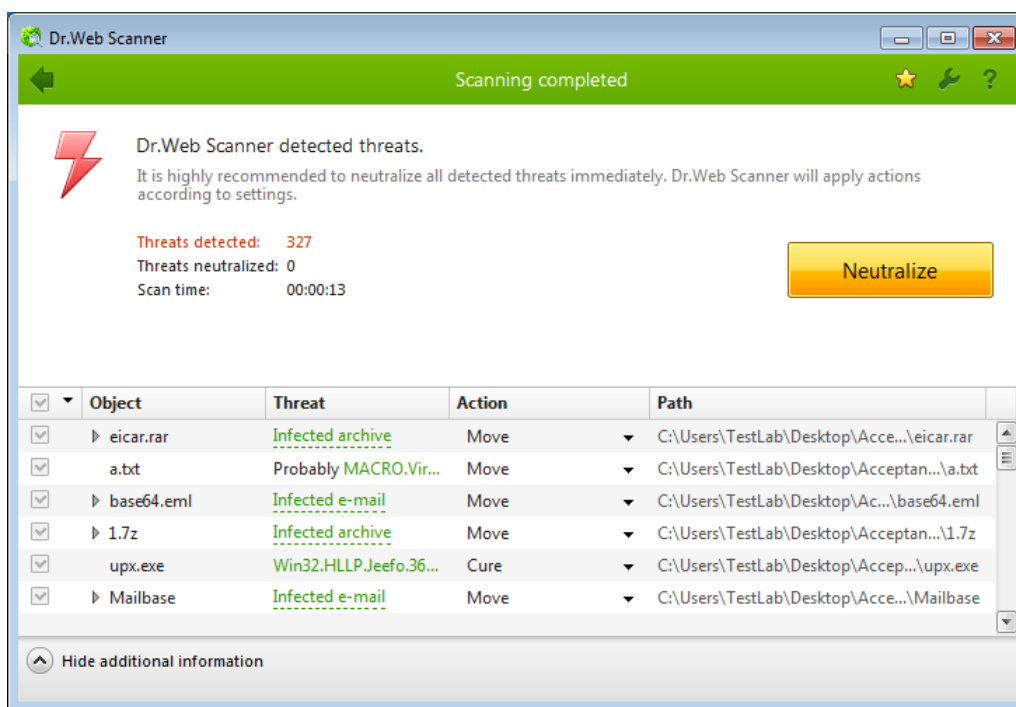


The **Pause** button is not available while processes and RAM are scanned.



6.2. Neutralizing Detected Threats

By default, if known viruses or computer threats of other types are detected during scanning, **Dr.Web Scanner** informs you about 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** selects all objects by default once scanning completes. When necessary, you can customize selection of objects to be neutralized by using check boxes next to object names or threat categories from 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 (it is 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).



Column name	Description
Threat	In this column, names of viruses or virus modifications are listed as per the internal classification of the Doctor Web package (a modification of a known virus is a code resulting from such alteration of a known virus which can still be detected, but cannot be treated with the curing algorithms applied to the initial virus). For suspicious objects, an indication that the object "is possibly infected" and the type of a possible virus according to the classification of the heuristic analyzer is displayed.
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 selected **Automatically apply actions to threats** check box on the **Main** [page](#), **Dr.Web Scanner** will neutralize threats automatically.





6.3. Scanner Settings



When using Windows , Windows Server 2003 or later operating systems, it is recommended to run **Dr.Web Scanner** under an account with administrative privileges.

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


To configure Scanner settings

1. Click the **SpIDer Agent icon**  and select **Scanner**. The menu of quick access to different modes of scan opens.
2. Click the **Custom** item. The **Dr.Web Scanner** window opens. **Express** and **Full** items run corresponding modes of scan (in this modes settings are not available till the scan is stopped or completed).
3. Click the **Settings icon**  on the toolbar.



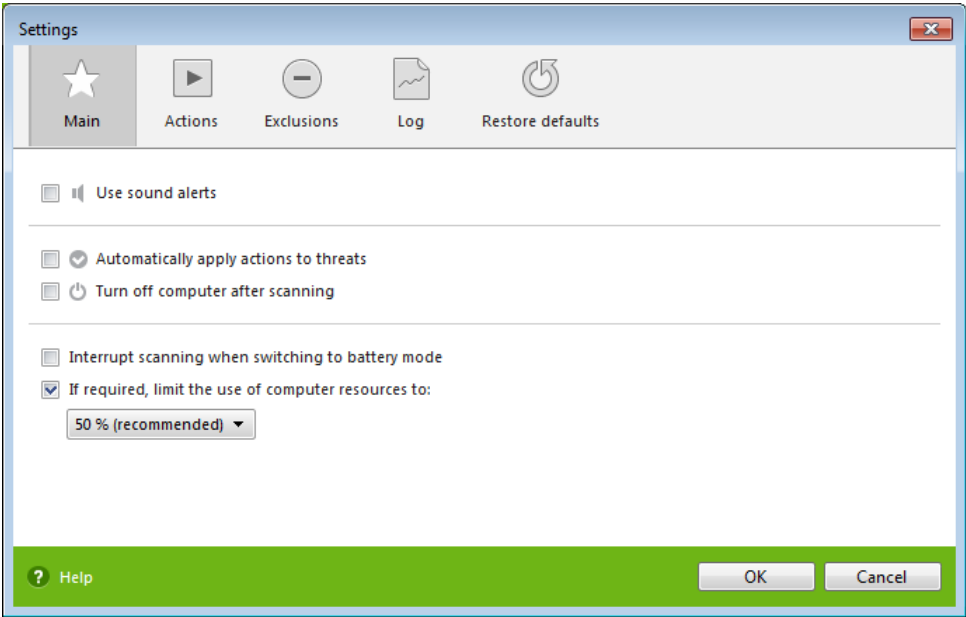
The main settings can be adjusted if the administrator of the central protection server, to which **Dr.Web** is connected, enabled this option.

This opens the window which contains several pages:



- The **Main** page, where you can configure general parameters of **Dr.Web Scanner** operation
 - The **Actions** page, where you can configure reaction of the **Dr.Web Scanner** on detection of infected or suspicious files and archives or other malicious objects
 - The **Exclusions** page, where you can specify files and folders to be excluded from scanning
 - The **Log** page, where you can set logging options for **Dr.Web Scanner**.
 - The **Restore defaults** page, where you can restore the **Dr.Web Scanner** settings to their default values
2. Configure options as necessary.
 3. For details on settings specified on each page, use the **Help**  button.
 4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

Main Page

On this page, you can set general parameters of **Dr.Web Scanner** operation.



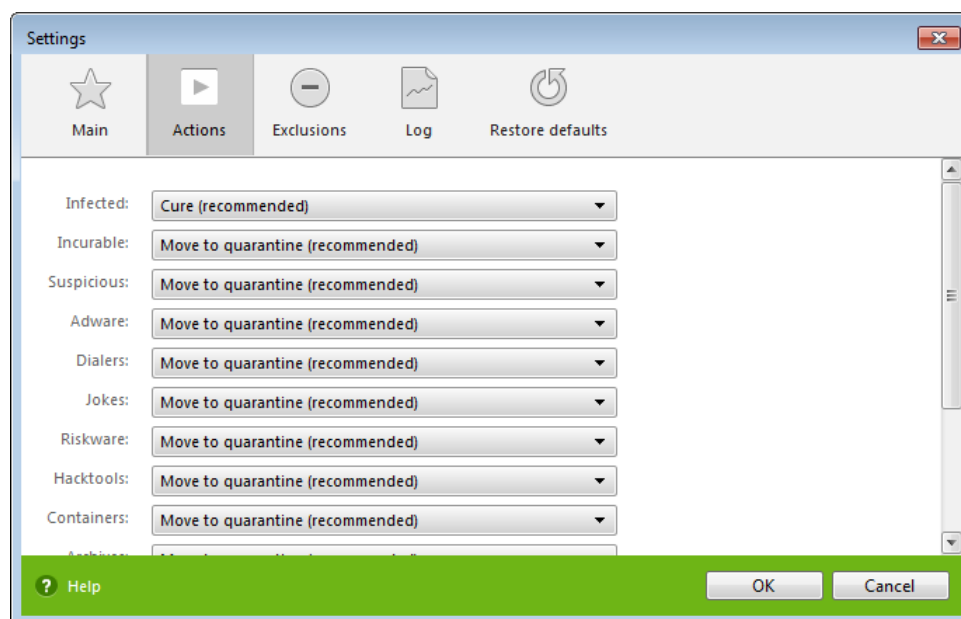
Option	Description
Use sound alerts	Enable Dr.Web Scanner to use sound alerts for every event.
Automatically apply actions to threats	Select to enable Dr.Web Scanner to apply actions to detected threats automatically.
Turn off computer after scanning	Select to turn off the computer after scanning. If Automatically apply actions to threats is selected, Dr.Web Scanner will apply the specified actions to detected threats.
Interrupt scanning when switching to battery mode	Select to interrupt scanning when switching to battery mode.
Limits on use of computer resources	This option limits the use of computer resources by Dr.Web Scanner . The default value is 50%.

 **Use sound alerts, Automatically apply actions to threats** and **Turn off computer after scanning** parameters can be also set in the **Dr.Web Scanner** Main window or Custom Scan Settings window. To set the parameters, click  icon on the toolbar.

Actions Page

To set reaction to threat detection

1. Select the **Actions** page in the settings window.



2. In the **Infected** drop-down list, select an action to take upon detection of an infected object.



The **Cure** action is the best in most cases.

3. In the **Incurable** drop-down list, select an action to take upon detection of an incurable object. The range of actions is the same as for infected objects, but the **Cure** action is not available.



The **Move to quarantine** action is the best in most cases.

4. In the **Suspicious** drop-down list select an action to take upon detection of a suspicious object (fully similar to the previous paragraph).
5. Similar actions should be specified for detection of objects containing Adware, Dialers, Jokes, Riskware and Hacktools.
6. The same way the automatic actions of the program upon detection of viruses or suspicious codes in file archives, installation packages and mailboxes, applied to these objects as a whole, are set up.
7. To cure some infected files it is necessary to reboot Windows. You can select one of the following:
 - **Prompt restart**
 - **Restart computer automatically.** It can lead to loss of unsaved data.

The best action for curable threats (e.g., files infected with known viruses) is curing, since it allows to restore the infected file completely. It is recommended to move other threats to quarantine in order to prevent loss of potentially valuable data. You can select one of the following actions:

Action	Description
Cure	<p>Instructs to restore the original state of an object before infection. If the object is incurable, or an attempt of curing fails, the action set for incurable viruses is applied.</p> <p>This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects (archives, email attachments, file containers). Trojan programs are deleted on detection.</p> <p>This is the only action available for boot sectors.</p>



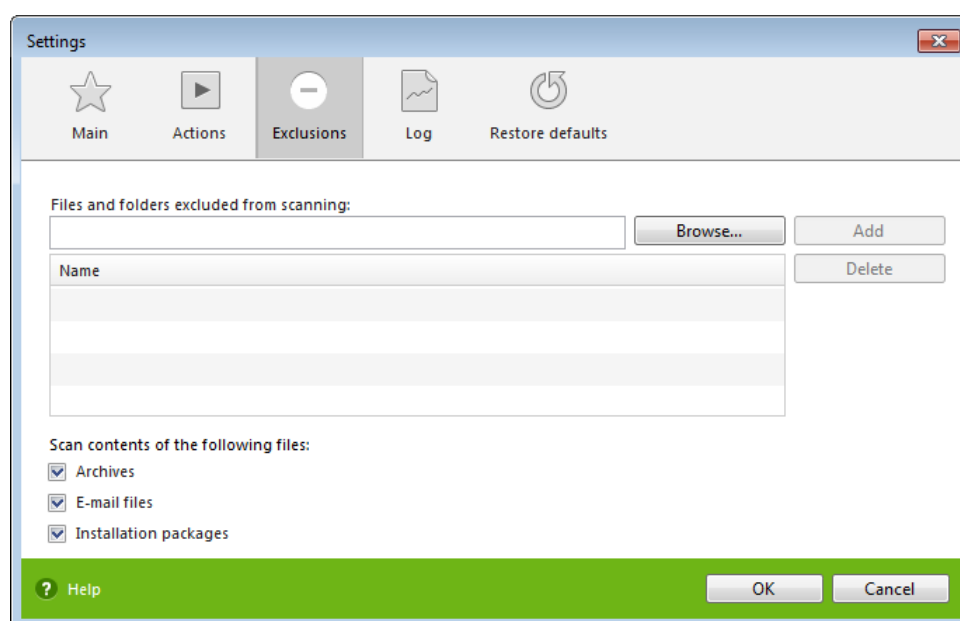
Action	Description
Move to Quarantine	Instructs to move the object to a specific folder for isolation. This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector.
Delete	Instructs to delete the object. This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.



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

Exclusions Page

On this page, you can specify files and folders to be excluded from scanning.



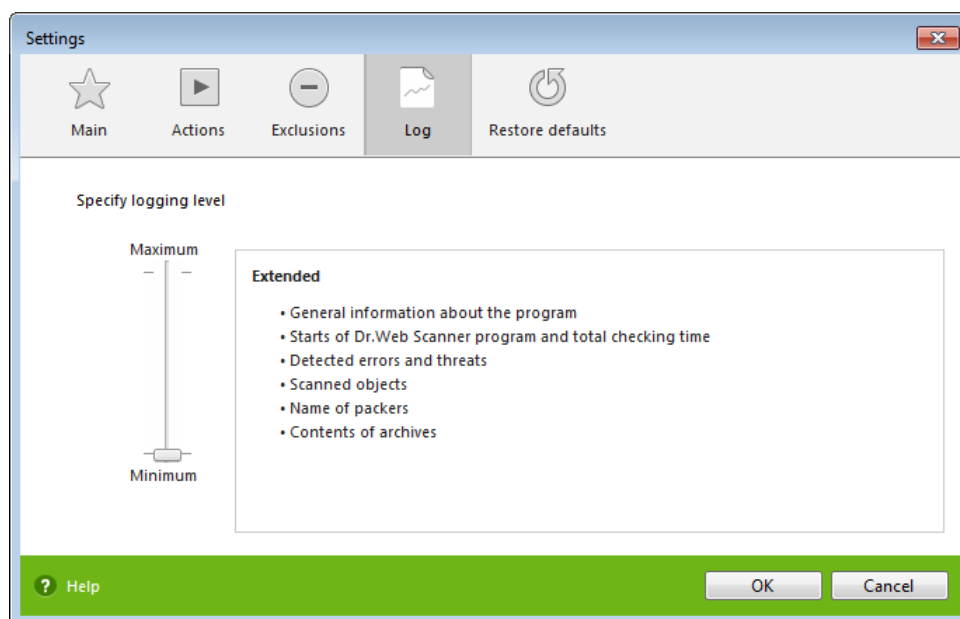
Here you can list names or masks for the files to be excluded from scanning. All files with the names which match the name or mask specified will be excluded from scanning (this option is appropriate for temporary files, swap files, etc.).

You can also add archives, email files, and installation packages to scanning.

Log Page

On this page, you can specify the logging mode.

Dr.Web Scanner operation is logged to the dwscanner.log file located in the %USERPROFILE%\Doctor Web folder. It is recommended to periodically analyze the log file.



Most parameters set by default should be left unchanged. However, you can change the details of logging (by default, information on infected or suspicious objects is always logged; information on scanned packed files and archives and on successful scanning of other files is omitted).

You can specify one of the following verbosity levels for logging:

- **Standard** – in this mode, main events are logged, such as time of updates, time of **Dr.Web Scanner** starts and stops, information on detected threats, and also names of packers and content of scanned archives is logged. If required, you can add such objects to the list of [exclusions](#), which can reduce system load. This logging mode is optimal for most uses.
- **Debug** – in this mode, all details on **Dr.Web Scanner** operation are logged, which may result in considerable log growth. It is recommended to use this mode only when errors occur in **Dr.Web Scanner** operation or by request of your anti-virus network administrator.

Size of the log file in the **Standard** mode is restricted to 10 MB. In the **Debug** mode, the log file size is not limited.

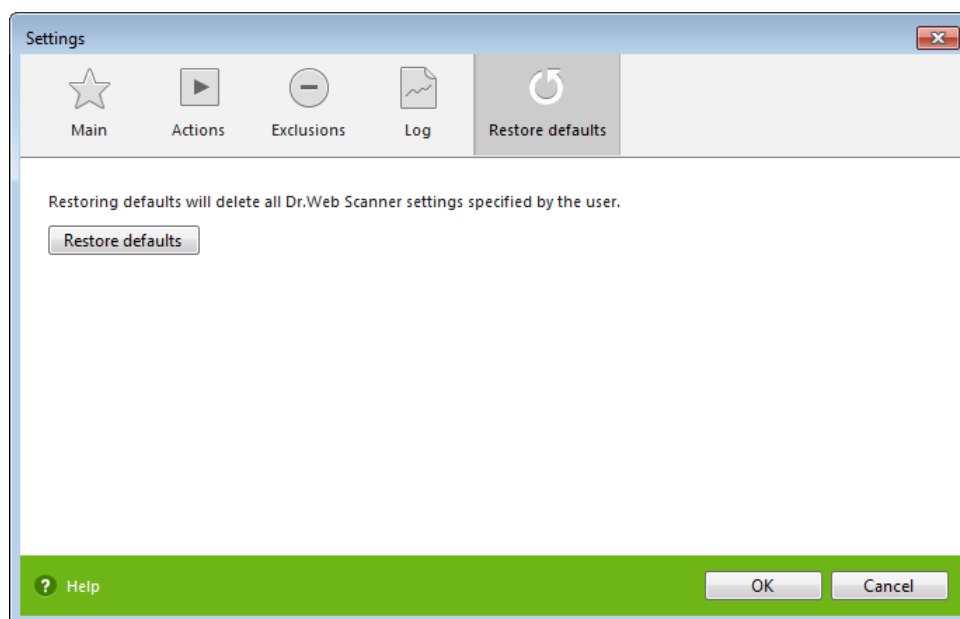
After scanning, if the log file size exceeds the limit, the content is reduced to:

- Specified size, if the current session information does not exceed the limit.
- Size of the current session, if the session information exceeds the limit (thus, the information is stored until the next scan).

When scanning starts, the log file is reduced to the size specified in the settings.

Restore Defaults Page

On the **Restore defaults** page, you can restore **Scanner** settings to their default values recommended by **Doctor Web**. For that purpose, click **Restore defaults**.





6.4. Scanning in Command Line Mode

You can run **Scanner** in the command line mode, then you can specify settings of the current scanning session and list 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>` is a placeholder for command-line parameters that configure **Scanner** operation. 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 commonly used examples of specifying the objects for scanning are given below:

- `/FAST` – perform an [express scan](#) of the system.
- `/FULL` – perform a full scan of all hard drives and removable data carriers (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.



6.5. Console Scanner

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



Console Scanner moves suspicious files to **Quarantine**.

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.

The list of objects for scanning can be empty or contain several elements separated by spaces. All switches start with the forward slash (/) and are separated by spaces. All **Console Scanner** parameters 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

6.6. Automatic Launch of Scanning

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

To view the parameters of the task, open **Control Panel** → **Administrative Tools** → **Task Scheduler**.

In 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, select the **History** tab.

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



7. Settings



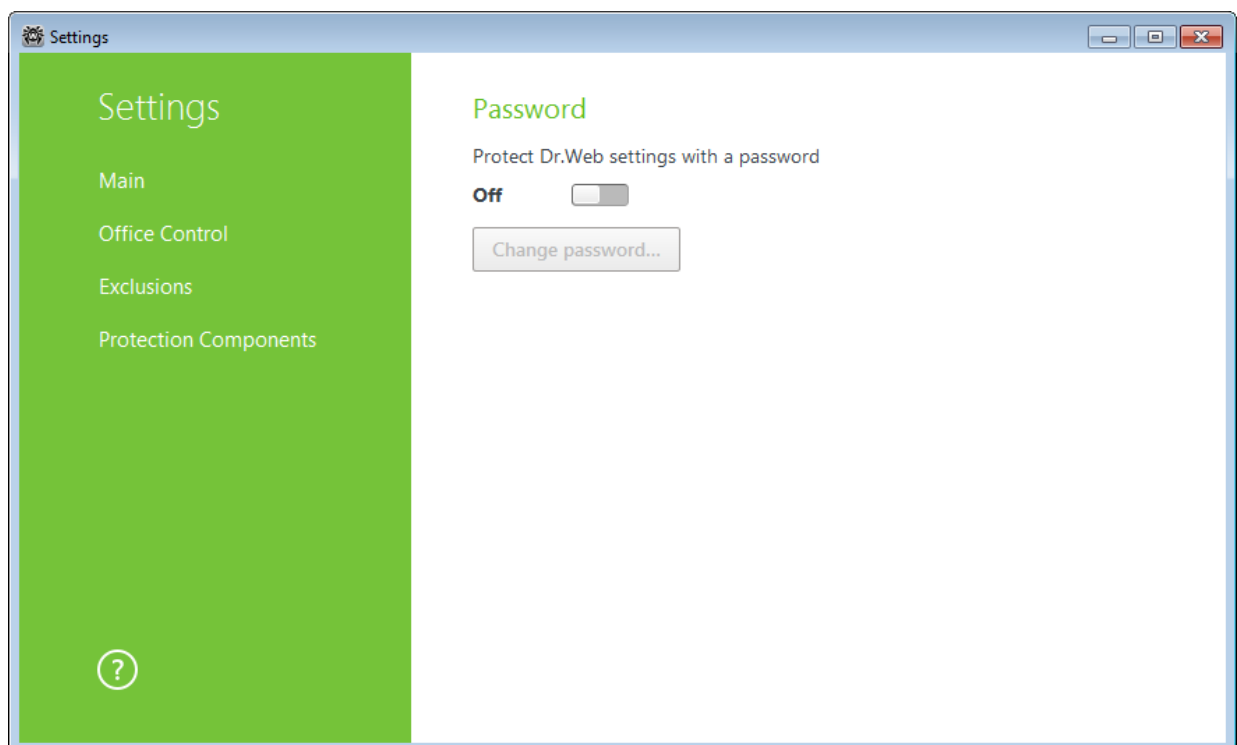
Managing settings is available only when having administrative privileges.

Password protection

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



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





8. Main Settings




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

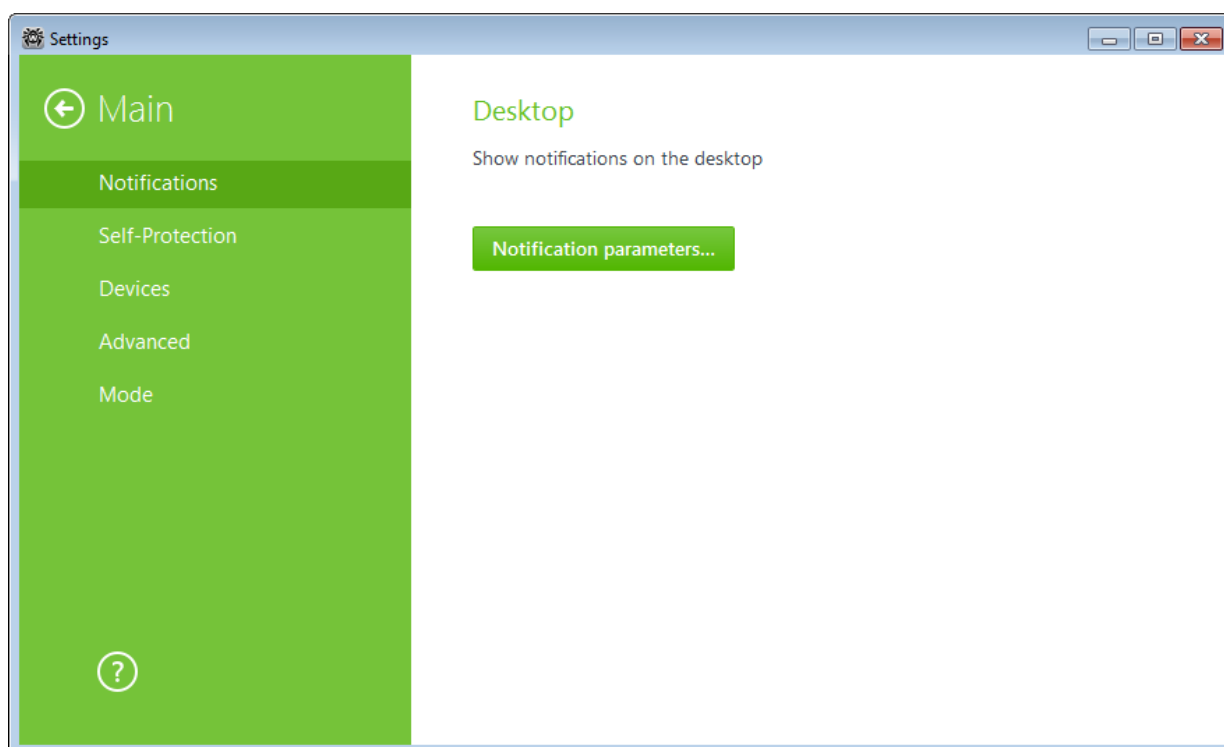
To access the main **Dr.Web** settings, you are prompted to enter the password if you enabled **Protect Dr.Web settings by password** option on the [Settings](#) window.

Dr.Web settings are available when run with administrative privileges.

Centralized settings adjustment allows you to configure main **Dr.Web** settings and settings of all its components except **Scanner**.

8.1. Notifications

On this page, you can set the types of pop-ups that appear above the **SpIDer Agent** icon  in the notification area.



Pop-up notifications

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

**Notifications parameters**

Notifications parameters

Notification type Desktop

Threat detected	<input checked="" type="checkbox"/>
Critical	<input checked="" type="checkbox"/>
Major	<input type="checkbox"/>
Minor	<input type="checkbox"/>

☒ Do not show notifications in full-screen mode

☒ Display Firewall notifications on separate desktop in full-screen mode

OK Cancel ?

1. Click **Notification parameters**. The window listing available notifications opens.
2. Select types of notifications that you want to receive and select the corresponding check boxes.
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 to display notifications on the same desktop where an application is running in the full screen mode.

After editing, click **OK** to save the changes or **Cancel** to cancel them.

Option	Description
Threat notifications	Select to be notified on detected threats. Clear if you do not want to be notified. 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• Attempts to change system date• Outdated virus databases (when operating in the Mobile mode) Clear this check box if you do not want to be notified on the issues listed above. By default, these notifications are enabled.



Option	Description
Critical notifications	<p>Select to be notified on the following critical issues:</p> <ul style="list-style-type: none">• Detection of connections waiting for Firewall to reply• Your login and password are already used for connection to central protection server <p>Clear this check box if you do not want to be notified on the issues listed above. By default, these notifications are enabled.</p>
Minor notifications	<p>Select to be notified on the following minor issues:</p> <ul style="list-style-type: none">• Virus databases update• Failures to update• Changes in Self-protection state• Expiration of the time limit set for Internet use• Blocked URLs• Blocked attempt to access a protected object• 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 <p>Clear this check box if you do not want to be notified on the issues listed above. By default, these notifications are disabled.</p>



8.2. Self-protection

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

The **Enable Self-protection** option allows to protect **Dr.Web** files, registry keys, and processes from damage or deletion. 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** operation, including execution of scripts that emulate user interaction with **Dr.Web** and are launched by the user.

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](#) so that to be informed on attempt to change the system time.

To restrict access to **Dr.Web** settings on your computer, enable the **Protect Dr.Web settings with a password** option in the [Settings](#) section.

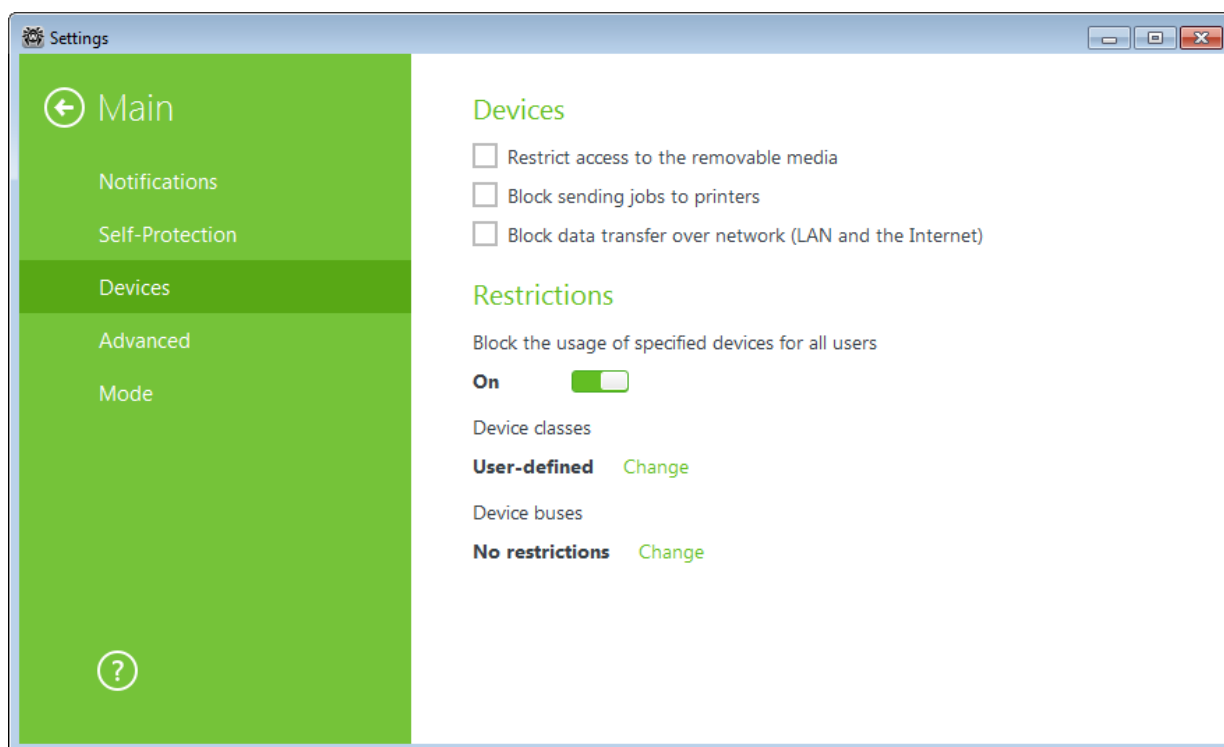
8.3. Devices



Access control configuration are applied to all Windows accounts.

Devices

To block access to data on the 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** flag. This option is disabled by default. You can also block data transfer over network (LAN and the Internet).



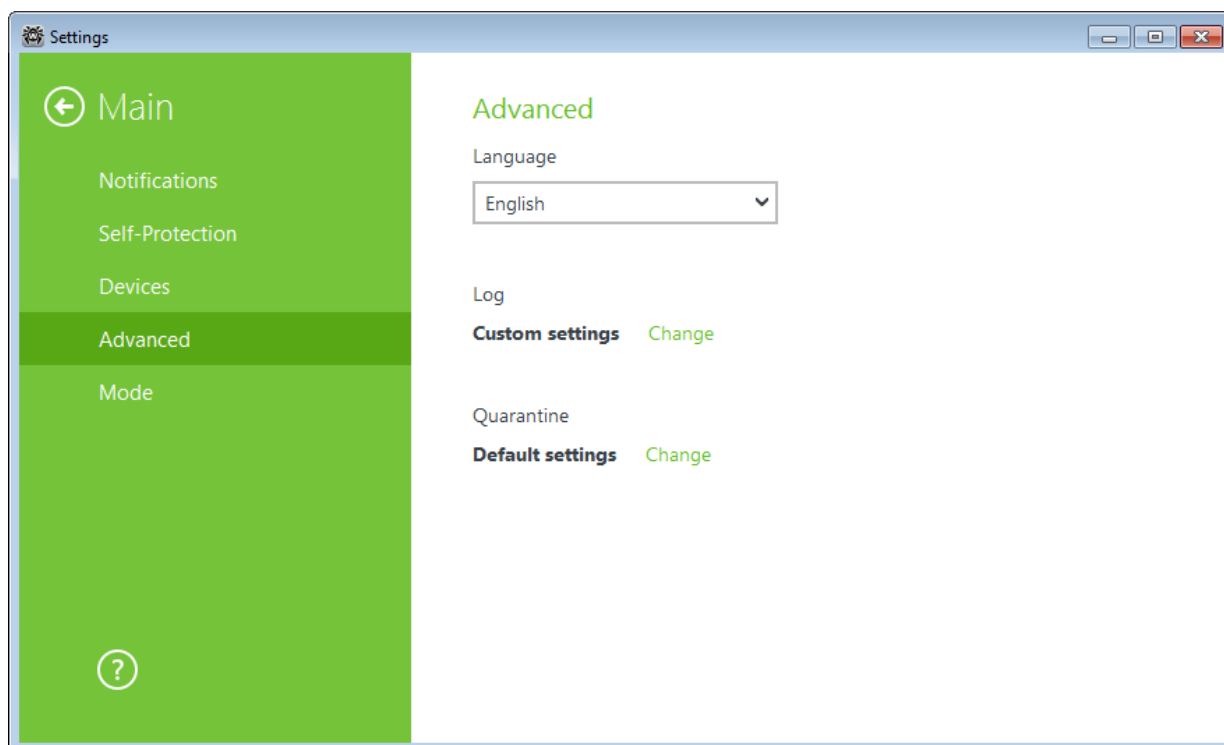
Device and bus classes

To block access to specified device or bus classes, enable the appropriate option. Click the **Change** button to make a list of such objects.



8.4. Advanced

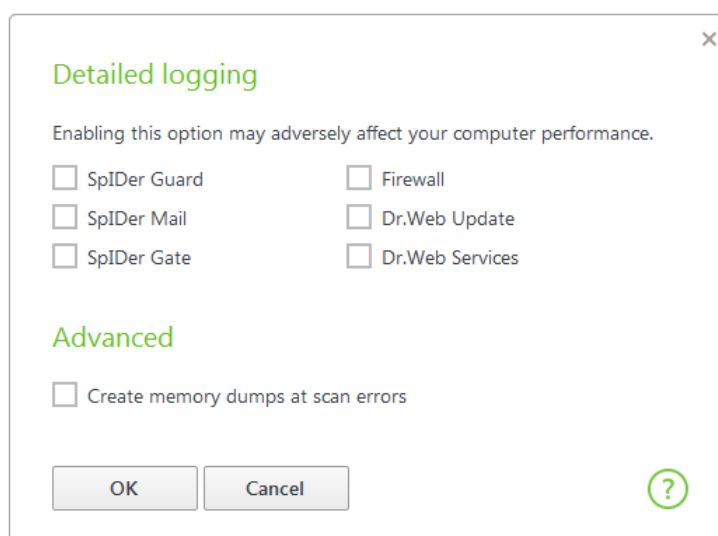
On this page, you can configure additional settings.



To set another program language, select it in 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 **Change** button.



By default, the standard logging mode is enabled and the following information is logged:



Component	Information
SpIDer Guard	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). 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.
SpIDer Mail	Time of updates and SpIDer 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.
SpIDer Gate	Time of updates, starts and stops of SpIDer 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 up objects and work of the HTTP watchman.
Dr.Web 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).
Dr.Web Update	List of updated Dr.Web files and their download status, date and time of updates, and details on auxiliary script execution and Dr.Web component restart.
Dr.Web 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 .dmp file located in the %PROGRAMFILES%\Common Files\Doctor Web\Scanning Engine\ folder.

Enabling detailed logging



Logging detailed data on **Dr.Web** operation may result in considerable log file growth and increase in process load. 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.



By default, size of a log file is restricted to 10 MB.

Quarantine settings

To configure **Quarantine** settings, click the corresponding **Change** button.

You can configure **Dr.Web Quarantine**, estimate its size, and delete isolated files from a specified logical drive.

Folders of **Quarantine** are created separately on each logical drive where suspicious files are found.



To empty Quarantine

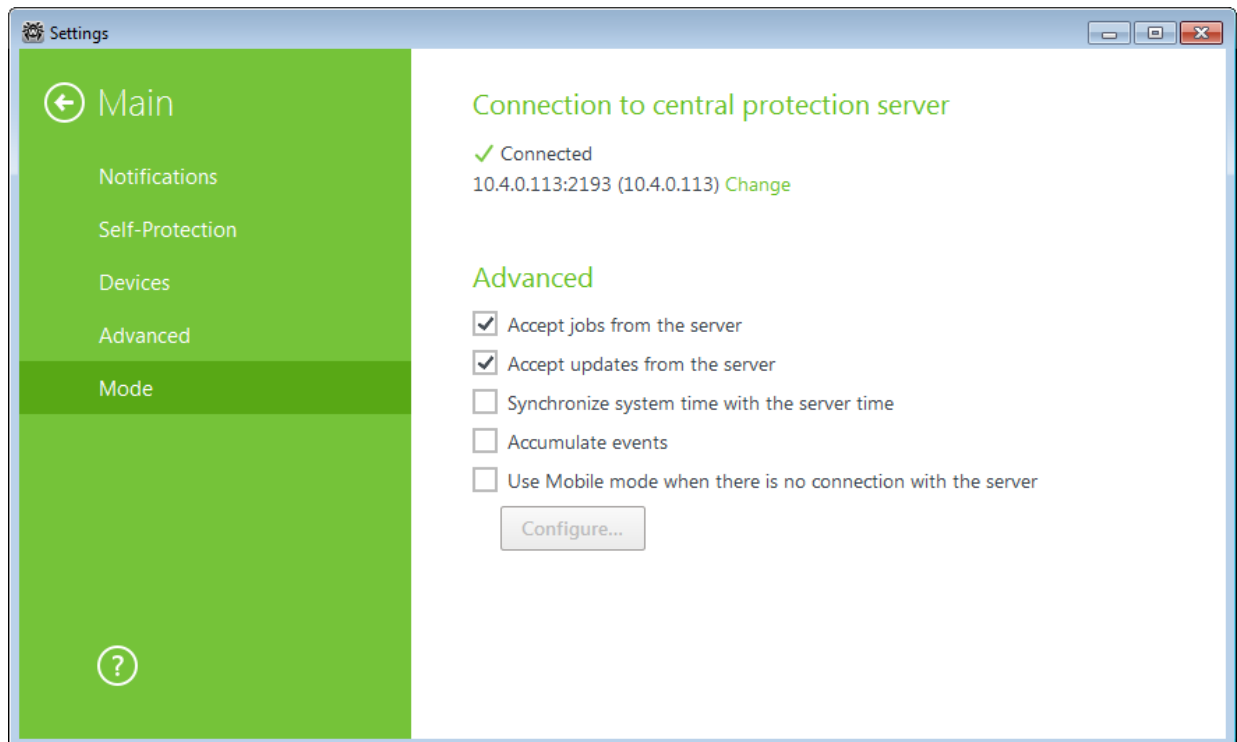
1. To remove all quarantined files on a particular drive, select the drive in the list.
2. Click **Clear** and confirm the deletion when prompted.

Use **Advanced** settings to select the isolation mode for infected objects detected on portable data carriers. By default, 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.



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 configure connection to a new one, click **Change**. The **Server 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 the administrator 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 following additional parameters become available:

- **Station ID** – specify the **Dr.Web** identifier assigned to your computer for registration on the server.



- **Password** – specify **Dr.Web** password used for server connection.

You can send a request to register on the central protection server as a new user. For that, click the **Connect as a newbie** button. You can also establish connection to another server having adjusted the connection parameters (**Address**, **Port** and **Public key**). After the registration is confirmed on the central protection server, **Dr.Web** will receive settings from the administrator.

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

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

- **Accept jobs from the server for checking your computer** – periodically receive tasks from the administrator.
- **Accept updates from the server** – receive updates for **Dr.Web** components and virus databases. Updating settings are set on the server.
- **Synchronize system time with server time** – synchronize system time on your computer with the time on the central protection server. In this mode, **Dr.Web** periodically sets the time on you computer in accordance with the server time.
- **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 **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** check box can be selected 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 HTTP update from **Doctor Web** update servers. Attempts to establish central protection server connection are performed with an interval of about one minute.

To configure Mobile mode settings, click **Configure**. The **Mobile mode** [window](#) opens.

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



If you select **Manually** in the **Update frequency** list, automatic updates are not performed.

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.
User	Specify the username to use when connecting to the proxy server.



Option	Description
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 **Cancel** to cancel them. To edit the proxy connection settings, click **Change** again.



In the Mobile mode, only virus databases are updated.

If you clear the **Use Mobile mode when there is no connection with the server** check box before the connection to the central protection server is established, updating of virus databases will be blocked but **Dr.Web** will continue searching the server.

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



9. Office Control

The **Office Control** component allows you to restrict access to devices on your computer and both local and web resources. You can also set time limits on using the Internet and computer for certain Windows accounts.

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. It is possible to restrict access to separate files or folders on local drives and external data carriers. You can also completely restrict copying data to any kinds of external data carriers. To prevent unauthorized access to data or its theft, you can restrict access to such devices as USB ports, hard drives, disk drives, and so on.


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 to certain websites only that are specified in the **Office Control** settings.



9.1. Office Control Settings

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

To configure Office Control settings

1. Click the **SpIDer Agent** icon  in the notification area, select **Office Control** and then select **Settings**.
2. Configure the settings as necessary.
3. To get information on options available on the page, click **Help**.



To manage **Office Control** module, the password is required if you set **Protect Dr.Web settings by password** check box on the [Settings](#) window.

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

Configuring Office Control module parameters for different users

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



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

Internet

By default, the **No restrictions** mode is set for all users. To change these settings, select another mode in 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 white 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 in 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 the search engines. This option allows to exclude unwanted webpages from search results.



Time

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

By default, users have unlimited access to use the computer and the Internet.

To set time limits

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



Setting time limits for using the computer or 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 for all users. To change these settings, enable the appropriate option and add the objects to which you want to block access.

Please note that access blocking is not guaranteed when loading the computer from external locations or connecting from other operating systems.



10. Exclusions

If you want to keep access to certain websites, files or folders, or to exclude certain processes from the antivirus components analyse, add them to the exclusions lists. Note that administrator of your antivirus 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 the **Doctor Web** company, 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 the **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 the **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 webpages such as **example.com/test11**, **template.example.com/test22**, and so on.

Your input may be unified.

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

10.2. Files and Folders



In this section, you can manage the list of files and folders that are excluded from **SpIDer Guard** scanning. 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.

Configuring 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 it 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 all files or folders with a particular name, enter the name without path.
 - To exclude a group of files or folders, enter the mask of their names.
2. Click **OK**. The file or folder will appear in the list.
 3. 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 .

Examples:




- `C:\folder` or `C:\folder**` – excludes from scanning all files stored in `C:\folder`. The files stored within the subfolders will be scanned.
- `C:\folder*` – excludes all files located in `C:\folder` and its subfolders.
- `C:\folder*.txt` – excludes all *.txt files stored in `C:\folder`. The *.txt files stored within the subfolders will be scanned.
- `C:\folder**.txt` – excludes all *.txt files stored in the first-level subfolders of `C:\folder`.
- `C:\folder***.txt` – excludes all *.txt files stored in subfolders of any level within `C:\folder`. The files stored in `C:\folder` itself, including *.txt files, will be still scanned.

10.3. Programs and Processes

You can specify a list of processes to be excluded from scanning by **SpIDer Guard**, **SpIDer Gate** and **SpIDer Mail**.

The default list is empty. Add particular files and folders to exclusions or use masks to disable scanning of a certain group of files.

To configure list of exclusions

1. To add a program or a process to exclusion list, click . In the open window, click **Browse** and select it in the standard dialog window.
2. In the configuration window, specify the components that must not scan this file.
3. Click **OK**. The process or program will appear in the list.
4. If necessary, repeat the procedure to add other processes.
5. To edit existing exclusion, click .
6. To remove a file from the list, select the corresponding item and click .

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 (i.e., 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 `pochta.ru` domain, enter `*@pochta.ru`.
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 .



11. Protection components

11.1 SpIDer Guard

SpIDer Guard is an on-access anti-virus scanner that constantly resides in memory while scanning files and RAM "on the fly" and instantly detects 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 checked. 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 archived files or download the attachment. To prevent spread of viruses and other malicious objects with email, [use SpIDer Mail](#).

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



Incompatibility between **Dr.Web** and MS 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 **Protect Dr.Web settings by password** option on the [Settings](#) window.

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

Background Rootkit Scanning

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

If this option is enabled, **Dr.Web Anti-rootkit** constantly resides in memory. In contrast to 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 the **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 that and neutralizes the malicious



activity.



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

To enable background scanning, set the **Scan computer for rootkits (recommended)** check box.



Disabling of **SpIDer Guard** does not affect background scanning. If the check box is set, background scanning is performed regardless of whether **SpIDer Guard** is enabled or disabled.

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:

- **Objects infected** with a known and (supposedly) curable virus
- **Supposedly infected** (suspicious) objects
- Objects that pose potential threat (riskware)

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

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

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

Action	Description
Cure, move to quarantine if not cured	Instructs to restore the original state of an object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Cure, delete if not cured	Instructs to restore the original state of an object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
Delete	Instructs to delete the object. This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector.
Move to Quarantine	Instructs to move the object to a specific folder of Quarantine . This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.
Report	Instructs to display the notification and skip the object without performing any action. The action is available only for suspicious objects and malware.



SpIDer Guard does not check complex objects. No action is performed on such objects or 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 devices, 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 portable data storages 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 for 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 devices 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 check boxes in the **Additional tasks** group are selected.



Operating system may register some removable devices as hard drives (e.g. 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 checked. 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.

Additional Tasks

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.

In this group, you can configure **SpIDer Guard** parameters to check the following objects:



- Executables of running processes regardless of their location (this option is enabled by default)
- Installation files
- Files on network drives
- Files and boot sectors on removable devices (this option is enabled by default)

By default **SpIDer Guard** blocks autoplay option for portable data storages such as CD/DVD, flash memory, and so on. This option helps to protect you computer from viruses transmitted via removable media.



If any problem occur during installation with autorun option, it is recommended to clear **Block autoruns from removable media** check box.



11.2. SpIDer Gate

SpIDer Gate is an HTTP monitor. By default, the component automatically checks incoming HTTP traffic and blocks all malware 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 resides in the main memory of the computer and automatically launches upon Windows startup.

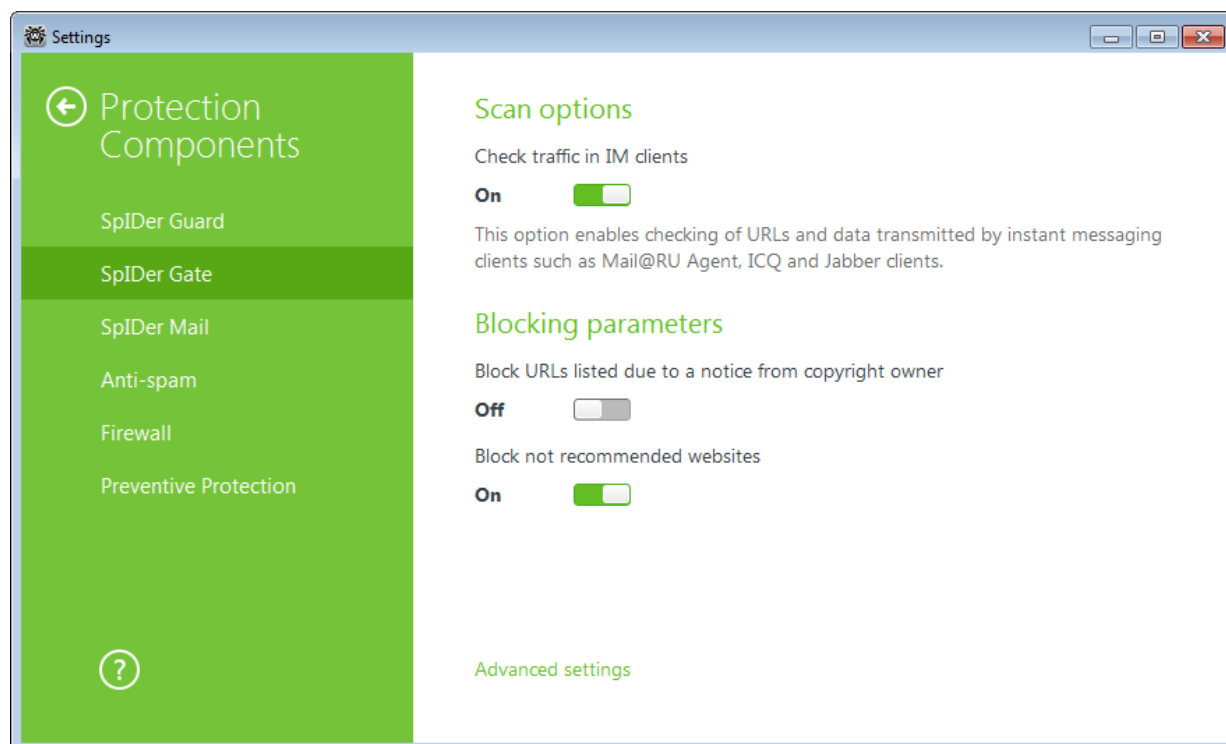
11.2.1. Configuring SpIDer Gate



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 **Protect Dr.Web settings by password** option on the [Settings](#) window.

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





IM Clients Check

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

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 URLs due to a notice from copyright owner are blocked only if the corresponding options are enabled on the [Actions](#) page. At that, [white list](#) and [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 setting 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 block of URLs due to a notice from the copyright owner (for that, select the corresponding check box) and block of unreliable websites (select **Block not recommended sites**). Click **White list** to [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

Objects to block

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

Advances 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, [white list](#) and [excluded applications](#) also have an effect.



11.3. SpIDer Mail

SpIDer Mail is an anti-virus mail scanner that installs by default and monitors data exchange between mail clients and mail servers made via POP3, SMTP, IMAP4, or NNTP (IMAP4 stands for IMAPv4rev1) protocols. **SpIDer Mail** uses [Dr.Web Anti-spam technologies](#), which allows to scan mail for spam messages.

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

Mail 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 immediately 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 complicated structure) as follows (for details on how to modify the reaction, refer to [Configuring 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 deleted or moved messages are also deleted from the POP3 or IMAP4 mail server.
- Messages that were not 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**, the infected messages are even not delivered to mailboxes.
- **Scanner** does not check the mailboxes at the moment of the mail receipt, but either on user demand.

Thus, when all anti-virus components are operating with their default settings, **SpIDer Mail** detects viruses and suspicious objects distributed via email first and prevents them from infiltrating into 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.

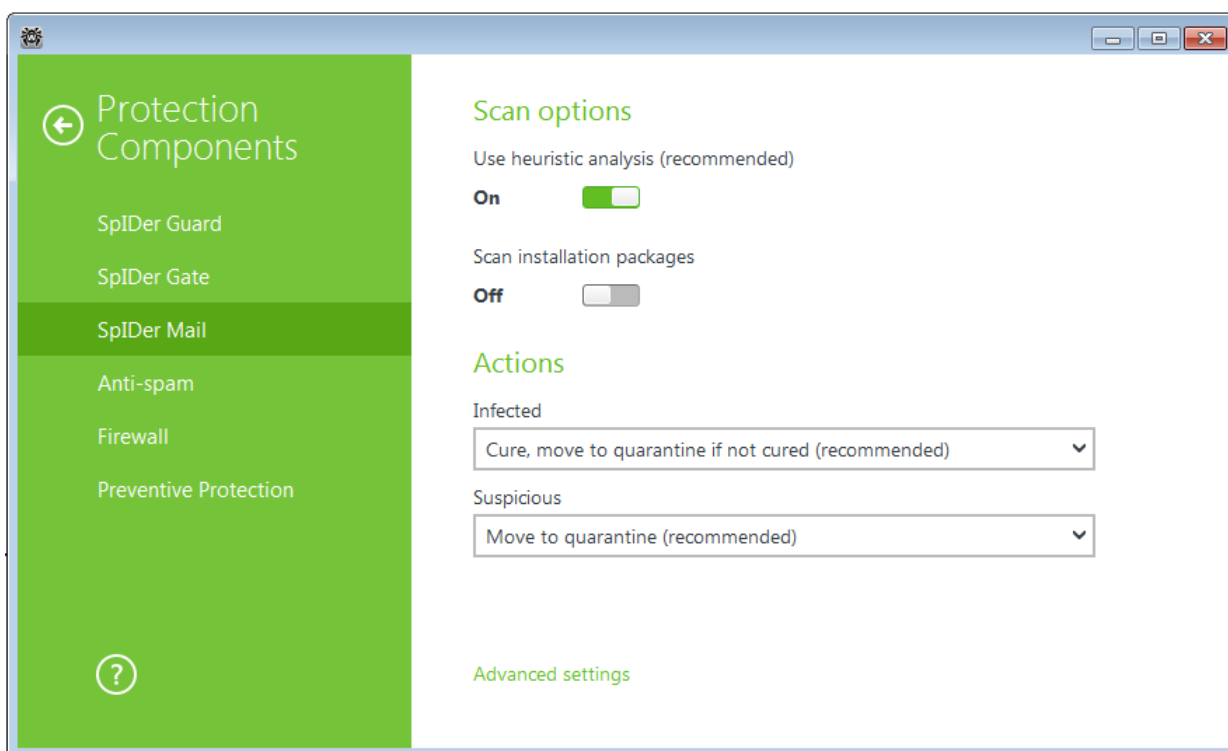
To access the **SpIDer Mail** settings, you are prompted to enter the password if you enabled **Protect Dr.Web settings by password** option on the [Settings](#) window.

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

Scan Options

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

- Heuristic analysis – in this mode, [special methods](#) are used to detect suspicious objects infected with unknown viruses with high probability. To disable the analyzer, clear the **Heuristic analysis (recommended)** check box.
- Check of installation packages. This option is disabled by default.



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 applied by **SpIDer Mail** to detected threats:



Action	Description
Cure	Instructs to try to restore the original state of the message before infection. If the message is incurable, or the attempt of curing fails, the action set for incurable message is applied. Available for Infected messages only except Trojan programs that are deleted on detection. This is action is not applicable to files within archives.
Delete	Instructs to delete the message. The message is not sent to 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, i.e. 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 **Unchecked messages**, and then scan the moved file with **Dr.Web Scanner**.



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

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

Actions on Messages

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

Option	Description
Insert 'X-Antivirus' heading 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 the server	Instructs to remove messages to which 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 too complicated 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, **SpIDer Mail** stops check of the message.

Scanning archives

Enable the **Scan archives** option if you want **SpIDer Mail** to scan the archived files, transferred via email. The following parameters will be available to configure:

- **Maximum file size to extract.** If an archive size exceeds the specified value, **SpIDer Mail** does not unpack and check the archive.



- **Maximum compression ratio** – the maximum compression ratio of an archive. If an archive compression ratio exceeds the specified value, **SpIDer Mail** does not unpack and check the archive.
- **Maximum archive nesting level** – the maximum nesting level for archived files. If a nesting level is greater than the specified value, **SpIDer Mail** proceeds unpacking and scanning the archive until this limit is exceeded.

To enable one or more options, select the corresponding check boxes.



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

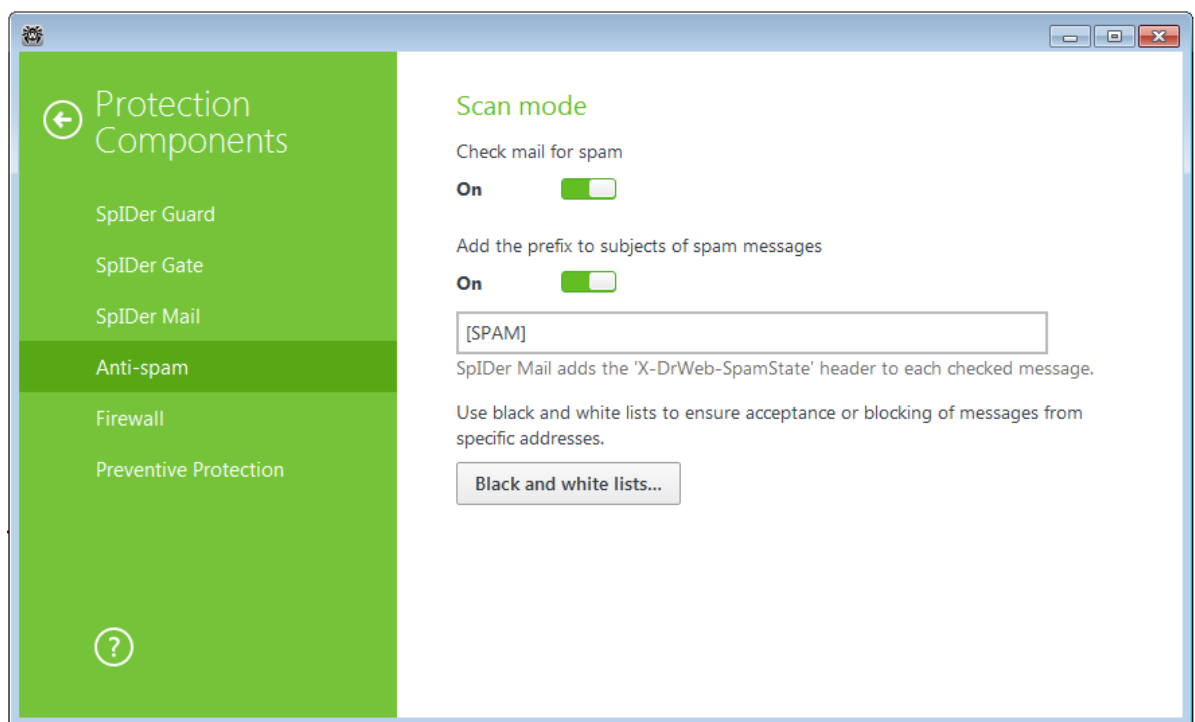


11.4. Anti-spam

Dr.Web 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 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 (as well as pharming messages) is the most dangerous type of spam including so-called “Nigerian” scams, loan scams, lottery and casino scams and false messages from banks and credit organizations. A special module of **Dr.Web Anti-spam** 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.



SpIDer Mail scans incoming messages for spam by default. To deliver messages without scanning, disable the corresponding option.

You can select messages that should not be regarded as spam automatically and configure the way to mark filtered email.



Option	Description
Add the following prefix to subjects of spam messages	<p>By default, this option is enabled and SpIDer Mail adds the [SPAM] prefix to the Subject field of all spam messages.</p> <p>Instructs SpIDer Mail to add a special prefix to the 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>
White and Black lists	Click to list senders whose messages you want to deliver or regard as spam automatically.

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 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 with 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.

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.



11.5. 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 Firewall

By default, once installation completes, **Firewall** starts learning usual behavior of your operating system by intercepting all new (unknown to the firewall) connection attempts and prompting you to select the necessary action. You can either select a temporary solution, or create a rule which will be applied each time **Firewall** detects this type of connection.



When running under limited user account (Guest) **Dr.Web Firewall** does not prompt requests for network access attempts. Notifications are then forwarded to the session with administrator privileges if such session is simultaneously active.

To set application rules

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

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

2. Once you make a decision, select an appropriate action:
 - To block this connection once, select **Block once**.
 - To allow this connection once, select **Allow once**.
 - To open a window where you can create a new application filter rule, select **Create rule**. In the open window, you can either choose one of the predefined rules or [create your rule](#) for 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 was initiated by a trusted application (an application with existing rules), but this application was run by an unknown parent process, the corresponding notification displays:

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 **Protect Dr.Web settings by password** option on 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** operates in [training mode](#). Regardless of the operation mode, events are logged.

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

Select the **Allow local connections** check box to allow all applications on your computer to interconnect (i.e., allow unlimited connections between application installed on your computer). For this type of connection, no rules are applied. Clear this check box to apply rules for connections carried out both through the network and within your computer.



After a session under a limited user account (Guest) is open, **Firewall** displays an access error message. **Firewall** status is then displayed as inactive in **SpIDer Agent**. However, **Firewall** is enabled and operates with default settings or settings set earlier in Administrative mode.

Operation modes

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** – mode, when rules for known applications are created automatically (set by default) .
- **Interactive learning mode** – [training 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.

Create rules for known applications automatically

In this mode, rules for known applications are created automatically. U/For other applications you have control over **Firewall** reaction: that is, you can allow or block unknown connections as well as create new rules.

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

This mode is used by default.

Interactive learning mode

In this mode, you have total control over **Firewall** reaction on unknown connection detection, thus training the program while working on computer.

When a user application or operating system attempts to connect to a network, **Firewall** checks whether a filtering rule set for the application is created. If no filtering rule is set for the application, 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 operating system attempts to connect to a network, **Firewall** checks whether a filtering rule set for the application is created. 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.

Allow unknown connections

In this mode, **Firewall** allows all unknown applications to access network resources including the Internet. No notification on access attempt is displayed.

Rules for Applications

Application level filtering helps you 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.



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

This page lists all applications and processes for which there is an [application filter rule set](#). You can



create new filter rule sets as well as edit the existing ones or delete those that are unnecessary. 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 the file of an application for which the rule was created changes (e.g., an update was installed), **Firewall** prompts to confirm that the application is still allowed to access network resources.



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.

In the **New application rule set** (or **Edit 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 the **Applications** page and click **Create** or select an application and click **Edit**.

When **Firewall** is operating in **learning mode**, you can start creating a new rule directly from the windows with notification on an unknown connection attempt.

Launching other applications

To enable or disable launch of other applications, in 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.



Parameter	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.
Rule name	The rule name.
Direction	The direction of the connection: <ul style="list-style-type: none">• Inbound – the rule is applied when someone from the network attempts to connect to an application on your computer.• Outbound – the rule is applied when an application on your computer attempts to connect to the network.• Any – apply the rule regardless of packet transfer direction.
Description	User description of the rule.

3. If necessary, edit the predefined rule set or create a new one.
 - To add a new rule, click **Create**. The rule will be added to the end of the list.
 - To modify a rule, select it and click **Edit**.
 - To copy the selected rule to the list, click **Copy**. The copy is added after the selected rule.
 - To remove the selected rule, click **Delete**.
4. If you selected to create a new rule set or edit the existing one, [adjust the settings](#) in the open window.

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.
Direction	The direction of the connection: <ul style="list-style-type: none">• Inbound – the rule is applied when someone from the network attempts to connect to an application on your computer.• Outbound – the rule is applied when an application on your computer attempts to connect to the network.• Any – apply the rule regardless of packet transfer direction.
Logging	Logging mode: <ul style="list-style-type: none">• Enabled – register events;• Disabled – no information is logged.



Parameter	Description
Rule Settings	
Protocol	<p>The network and transport level protocols used for the connection attempt.</p> <p>The following protocols of the network level are supported:</p> <ul style="list-style-type: none">• IPv4;• IPv6;• IP all – any version of the IP protocol. <p>The following protocols of the transport level are supported:</p> <ul style="list-style-type: none">• TCP;• UDP;• TCP & UDP – TCP or UDP protocol• RAW.
Local address/ Remote address	<p>The IP address of the remote host. You can specify either a certain address (Equals) 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 (Equals) or a port range (In range).</p> <p>To apply the rule for all ports, select Any.</p>

Rules for Networks

On the **Interfaces** page, you can select a rule set to use for filtering packets transmitted through a certain network interface installed on your computer.

To set rule sets for network interfaces

1. In the **Firewall** settings window, select **Interfaces**.
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.
3. Click **OK** to save the changes.

To list all available interfaces, click **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.

To configure rules for interfaces, click **Configure**.

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, select **Interfaces** and click **Configure**. 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, click **Create**.
- To edit an existing set of rules, select the rule set in the list and click **Edit**.
- To add a copy of an existing set of rules, select the rule set and click **Copy**. The copy is added after the selected rule set.
- To delete a selected rule set, click **Delete**.

To configure additional settings

In the **Packet filter settings** window, use 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 active connections according to the TCP protocol specification. This option helps 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.




Rule Sets

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 rules 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 displays:

Parameter	Description
Enabled	Status of the rule.
Action	The action for Firewall to perform when the packet is intercepted: <ul style="list-style-type: none">• Block packets• Allow packets
Rule name	The rule name.
Direction	The direction of the connection:



Parameter	Description
	<ul style="list-style-type: none">•  – the rule is applied when the 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 is stored in the log: <ul style="list-style-type: none">• Headers only – log the packet header only.• Entire packet – log the whole packet.• Disabled – no information is logged.
Description	The rule description.

Edit rule set

1. If you selected to create or edit an existing rule set on the **Packet filtering settings** page, in the open window specify the name for the rule set.
2. Use the following options to create filtering rules:
 - To add a new rule, click **Create**. The new rule is added to the beginning of the list.
 - To modify a rule, select it and click **Edit**.
 - To copy the selected rule to the list, click **Copy**. The copy is added after the selected rule.
 - To remove the selected rule, click **Delete**.
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 adjusting the settings, click **OK** to save changes or **Cancel** to reject them.



Packets with no rules in a rule set are blocked automatically except 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 **Create** or **Edit**. 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 the packet is intercepted: <ul style="list-style-type: none">• Block packets• Allow packets
Direction	The direction of the connection: <ul style="list-style-type: none">• Inbound – the rule is applied when the packet is received from the network.• Outbound – the rule is applied when the packet is sent into the network from your computer.• Any – apply the rule regardless of packet transfer direction.



Parameter	Description
Logging	The logging mode for the rule. This parameter defines which information is stored in the log: <ul style="list-style-type: none">• Entire packet – log the whole packet.• Headers only – log the packet header only.• Disabled – no information is logged.
Criterion	Filtering criterion. For example, transport or network protocol. To add a filtering criterion, select it from the list and click Add . You can add any number of filtering criteria. For certain headers there are additional criteria available.



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

For example, adding a packet filter rule that allows all packets from a subnetwork, may look as follows:

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 Outlook

Main Functions

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

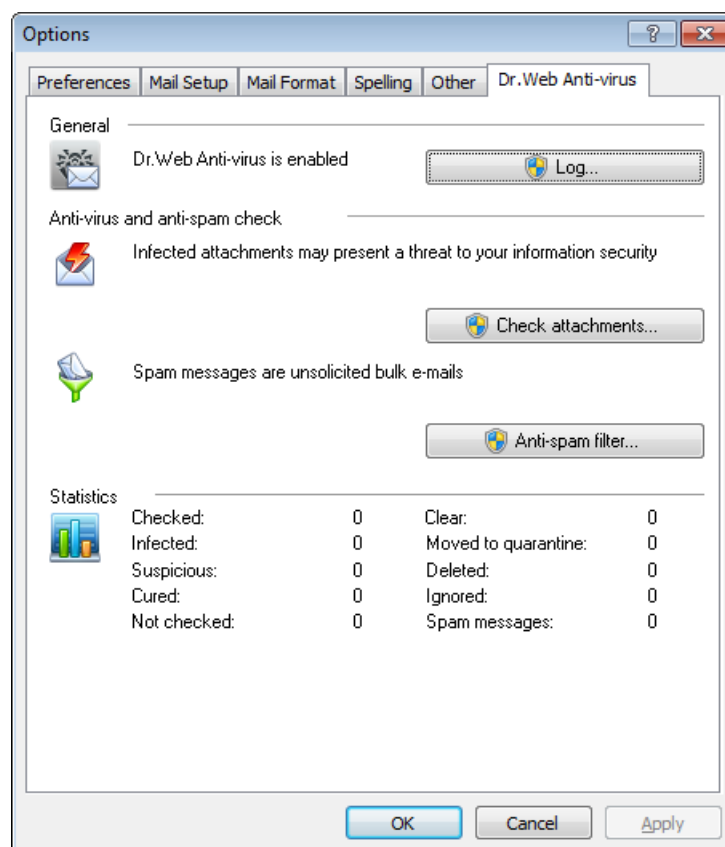
- Anti-virus check of email attachments
- Spam check
- Detection and neutralization of malware
- Heuristic analysis for additional protection against unknown viruses

11.6.1. Configuring Dr.Web for Outlook

You can set up parameters of plug-in operation and view statistics on Microsoft Outlook mail application, in the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select **Dr.Web for 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 specifying program actions on spam detection and creating black and white lists of email addresses.
- [Statistics](#) – allows viewing the number of checked and processed objects.

11.6.2. Threat Detection

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

Types of Threats

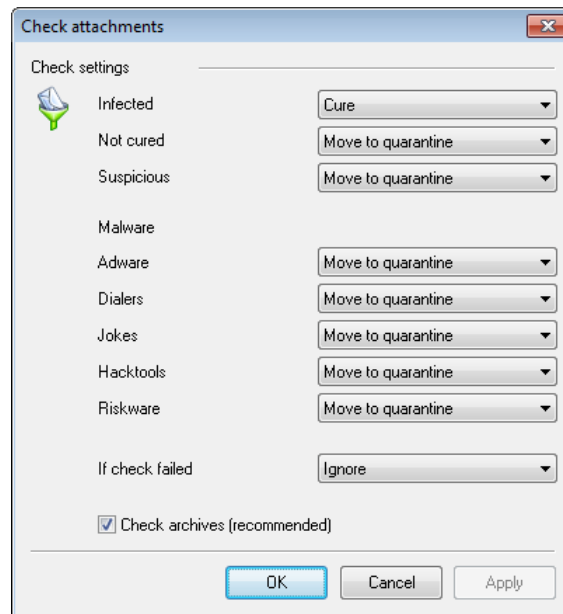
Dr.Web for Outlook detects the following malicious objects:

- Infected objects
- Bomb viruses in files or archives
- Adware
- Hacktools
- Dialer programs
- Joke programs
- Riskware
- Spyware
- Trojan horses (Trojans)
- Computer worms and viruses

Configuring Actions

Dr.Web for 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, in the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select **Dr.Web for Outlook**, then click the **Add-in Options** button) 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 accounting data of system administrator.
- If UAC is disabled: administrator can change program settings; user does not have the permission 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 checked failed** drop-down list allows to configure actions if the attachment cannot be checked, e.g. 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. Set 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) – means, that the action specified for incurable objects will be performed.
- **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 Outlook checks emails for spam by means of **Dr.Web Anti-spam** and filters the messages according to the user-defined [settings](#).

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

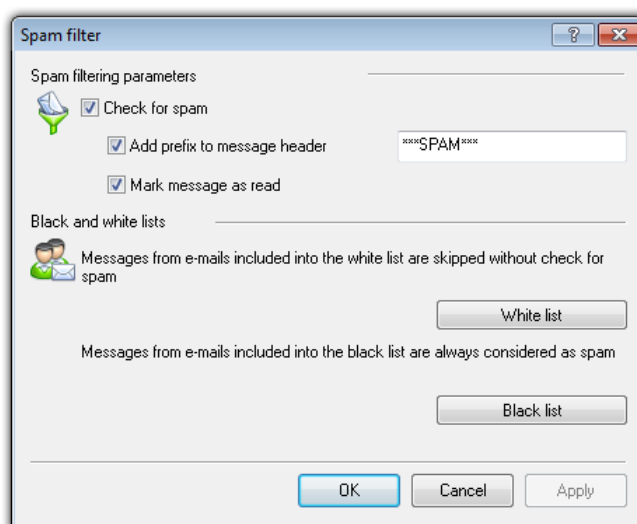


The **Spam filter** window is available only for users with administrative privileges.

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 accounting data of system administrator.
- If UAC is disabled: administrator can change program settings; user does not have the permission change program settings.

Configuring Spam Filter



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 add special text to the spam message header by setting the **Add prefix to message header** check box. The added prefix text is specified to the right of the flag. The default prefix is *****SPAM*****.
- The checked messages can be marked as read in the message options. To mark messages as read on spam check, select the **Mark message as read** check box. By default, this check box is selected.
- You can also configure [black and white lists](#) for message filtering.



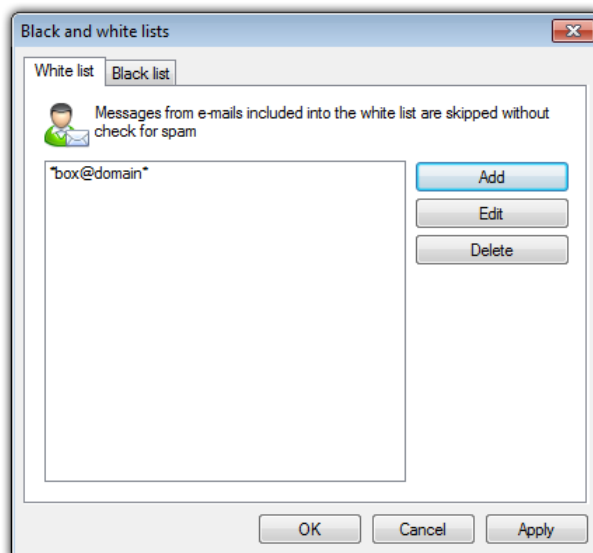
If spam filter defines certain messages incorrectly, you are advised to forward such messages to your anti-virus network administrator. Forward messages as attachments: do not include them in the message body.



Using Black and White Lists

Black and white lists are used for messages filtration.

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



To add addresses

1. Click **Add**.
2. In the **Edit list** window, enter the address (see [white](#) and [black](#) lists filling methods).
3. Click **OK** in the **Edit list** window.

To change addresses

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

To delete addresses

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

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

White List

If the sender's address is on the white list, the message is not scanned for spam. But, if domain name of receiver and sender addresses are matched, and this domain name is specified in the white list using a special asterisk character (*), this message will be checked for spam. Details



- To add a certain sender, enter the full email address (for example, `friend@mail.com`). 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 addresses are available:

- `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, specify 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, specify an asterisk (*) instead of the domain name in the address. For example, if you want to receive messages from all senders with the "someone" mailbox, enter `name@*`.

Black List

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

- To add a definite 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 as spam messages sent from any email address within a domain, 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 as spam messages sent from an email address with a certain user name from any domain, specify an asterisk character (*) instead of the domain name in the address. For example, if you enter `someone@*`, 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. Logging

Dr.Web for 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 the **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 by user applications, will open. The source of **Dr.Web for Outlook** messages is **Dr.Web for Outlook**.

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 the logging settings opens.
2. To set the maximum detalization for the logging, enable the **Detailed logging** flag. By default, logging is set to regular mode.



The maximum detalization 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 Outlook** occurs.

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



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

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 accounting data of system administrator.
- If UAC is disabled: administrator can change program settings; user does not have the permission change program settings.



To view program log

To open the text log, click **Show in folder**. The folder, where the text log is located, opens.

11.6.5. Statistics

In the Microsoft Outlook mail application, on the **Tools** → **Options** → **Dr.Web Anti-virus** page (for Microsoft Outlook 2010, in the **Files** → **Options** → **Add-ins** section select **Dr.Web for 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 to quarantine** – number of objects which 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%\DoctorWeb folder.

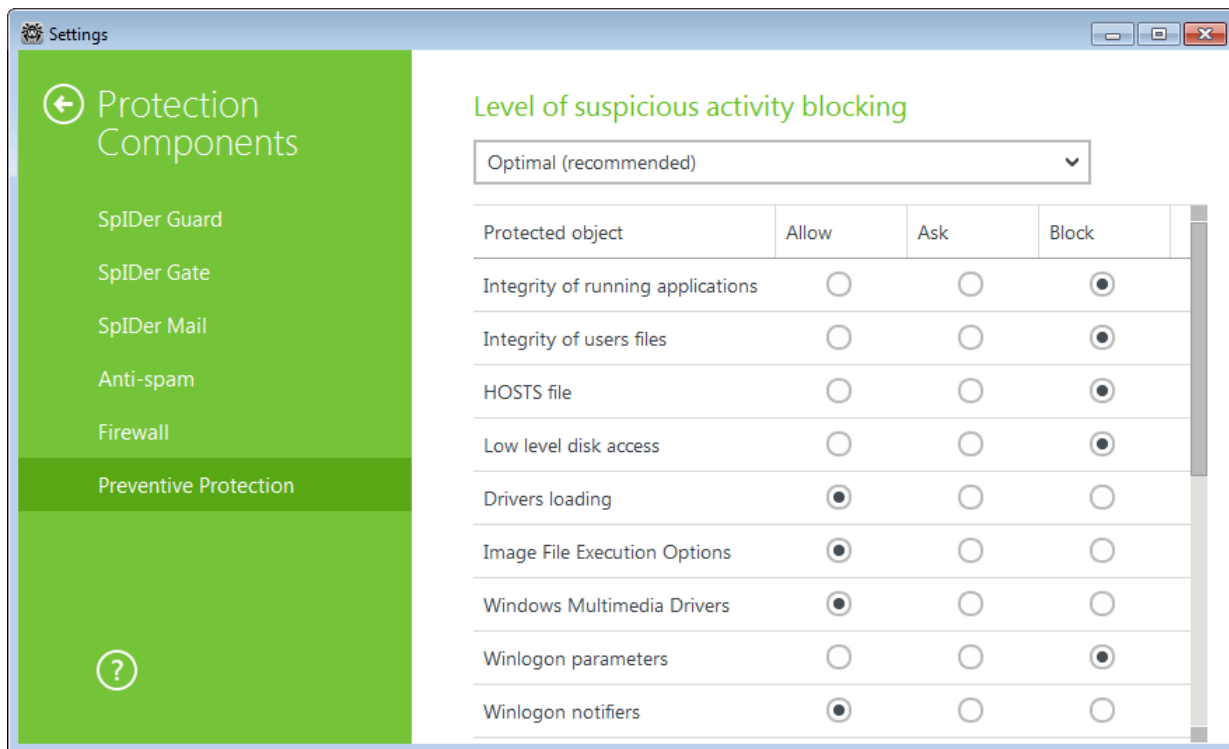


The drwebforoutlook.stat statistics file is individual for each system user.



11.7. Preventive Protection Page

On this page, you can configure **Dr.Web** reaction to such actions of other programs that can compromise security of your computer.



Preventive Protection Level

In the **Optimal** mode, **Dr.Web** disables automatic changes to system objects, modification of which 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** mode. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.



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

When required to have total control of access to critical Windows objects, you can select the **Paranoid** mode. 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 exclusion list of SpIDer Guard 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 exclusion list of SpIDer Guard 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 avoiding the file system.
Drivers loading	Block applications from loading new or unknown drivers.
Critical Windows objects	<p>Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).</p> <p>File Execution Options:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>User Drivers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Winlogon registry keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Winlogon notifiers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Windows registry startup keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib <p>Executable file associations:</p> <ul style="list-style-type: none">• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) <p>Software Restriction Policies (SRP):</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer <p>Browser Helper Objects for Internet Explorer (BHO):</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>Autorun of programs:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\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• SYSTEM\ControlSetXXX\Control\SafeBoot\Network <p>Session Manager parameters:</p> <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows



System services:

- System\CurrentControlXXX\Services



If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), disable the corresponding options in this group.



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



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 with blanks 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 – check archives. Option is enabled by default.

/ARC: <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: <level> – maximum archive nesting level. By default: unlimited.

/ARS: <size> – maximum archive size. If the archive size exceeds the limit, scanner neither unpacks nor scans the archive (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 checked (in KB). By default: unlimited.

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

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

/E: <engines> – perform scanning in specified number of threads.

/FAST – perform an express scan of the system. (For **Scanner** only.)

/FL: <path> – scan files 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 data carriers (including boot sectors). (For **Scanner** only.)



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

`/H` or `/?` – show brief help. (For **Console Scanner** only.)

`/HA` – use heuristic analysis to detect unknown threats. Option is enabled by default.

`/KEY:<keyfile>` – specify a license key file. It is necessary to use this parameter if your key file is stored outside of the **Dr.Web** installation folder where the scanner executables reside. By default, the `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 check for rootkits. (For **Scanner** only.)

`/LN` – resolve shell links. Option is disabled by default.

`/LS` – use LocalSystem account rights. Option is disabled by default.

`/MA` – check mail files. Option is enabled by default.

`/MC:<limit>` – set the maximum number of cure attempts to 'limit'. Number of attempts is unlimited by default.

`/NB` – do not backup cured or deleted files. Option is disabled by default.

`/NI[:X]` – limits usage of system resources at scanning and priority of the scanning process (%). By default: unlimited.

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

`/NT` – check NTFS streams. Option is enabled by default.

`/OK` – display the full list of scanned objects and mark clean files with `Ok`. Option is disabled by default.

`/P:<prio>` – priority of the current scanning task:

`0` – the lowest.

`L` – low

`N` – normal. Default priority.

`H` – high

`M` – maximal.

`/PAL:<level>` – maximum pack level. If a nesting level is greater than the specified value, SpIDer Mail proceeds unpacking and scanning the archive until this limit is exceeded. The nesting level is 1000 by default.

`/QL` – list files quarantined on all disks. (For **Console Scanner** only.)

`/QL:<logical_drive_name>` – list files quarantined on the specified drive (letter). (For **Console Scanner** only.)

`/QNA` – double quote file names.

`/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 **Dr.Web Scanner** once scanning completes whether the detected threats are neutralized or not. (For **Scanner** only.)

/RA: <file.log> – append the specified file with the current scanning report. By default, logging is disabled.

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

/RP: <file.log> – rewrite the specified file with the current scanning report. By default, logging is disabled.

/RPC: <sec> – Dr.Web 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: 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 names of packers. 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.

/TB – check boot sectors including master boot record (MBR) of the hard drive.

/TM – check processes in memory including Windows system control area.

/TR – check system restore points.

/W: <sec> – maximum time to scan (sec.). By default, the time is unlimited.

/WCL – drwebwcl compatible output. (For **Console Scanner** only.)

/X:S[:R] – set power state ShutDown/Reboot/Suspend/Hibernate with reason 'R' (for shutdown/reboot).



Action 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 email files (possible: QIR)
- /ARW: <action> – action for riskware. (possible: DQIR)
- /ASU: <action> – action for suspicious files. (possible: DQIR)

Several parameters can have modifiers that explicitly enable or disable options specified by these keys. For example:

/AC– option is clearly disabled,
/AC, /AC+ option is clearly enabled.

These modifiers can be useful if option was enabled or disabled by default or was set in configuration file earlier. Keys with modifiers are listed below:

/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 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.

Example of using command-line switches with **Console Scanner**:

```
[<path_to_file>]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 `dwscanner` command name instead of `dwscancl`.

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 is defined depending on 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 is defined depending on settings on the Server side.

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

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

The switch is specified with the `/pwd` switch for automatic authorization on the Server. If authorization parameters are not set, authorization decision is defined on the Server side.

`/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>` – installer language. 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 set, after the launch of the local installation, installer automatically uses the `drwcsd.pub` public key from 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 the 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 switch is specified with the `/id` switch for automatic authorization on the Server. If authorization parameters are not set, authorization decision is defined on the Server side.

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

- `yes` – register the **Dr.Web Agent** in the list of installed programs.



- `no` – do not register the **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 has not responded after the specified attempts number is reached, it is assumed what the Server is not 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 the **Dr.Web Agent** installation will be performed and to which the **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 the **Dr.Web Agent** installation performs in the graphical mode

`/timeout <time>` – waiting limit of each reply when searching 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

Computer Viruses

This type of malicious programs is characterized by the ability to implement its code into the executable code of other programs. Such implementation is called infection. In most cases the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data on the system. Viruses which infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file are called file viruses.

Some viruses infect boot records of diskettes and partitions or master boot records of fixed disks. Such viruses are called boot viruses. They take very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shutdown occurs.

Macroviruses are viruses which infect documents used by the Microsoft Office and some other applications which allow macro commands (usually written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft Word macros can automatically initiate upon opening (closing, saving, etc.) a document.

A virus which has the ability to activate and perform the tasks assigned by the virus writer only when the computer reaches a certain state (e.g. a certain date and time) is called a memory-resident virus.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are developed.

Encrypted viruses, for instance, cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure), which can be used as a virus signature.

Polymorphic viruses also encrypt their code, but besides that they generate a special decryption procedure which is different in every copy of the virus. This means that such viruses do not have byte signatures.



Stealth viruses perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of a program before infecting it and then plant these “dummy” characteristics which mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases it is assembler, high-level programming languages, scripting languages, etc.) or according to the affected operating systems.

Computer Worms

Worms have become a lot more widespread than viruses and other malicious programs recently. Like viruses they are able to reproduce themselves and spread their copies but they do not infect other programs. A worm infiltrates the computer from the worldwide or local network (usually via an attachment to an email) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user’s action or in an automatic mode, choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm’s body). Many of them have an infectious part (the shellcode), which loads into the main memory (RAM) and then downloads the worm’s body as an executable file via the network. If only the shellcode is present in the system, the worm can be rid of by simply restarting the system (at which the RAM is erased and reset). However, if the worm’s body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (that is, do not cause any direct damage) due to their intensive distribution.

Trojans

This type of malicious program cannot reproduce or infect other programs. A Trojan substitutes a high-usage program and performs its functions (or imitates the programs operation). At the same time it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for another person to access the computer without permission (for example, to harm the computer of a third party).

A Trojan’s masking and malicious facilities are similar to those of a virus and it can even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or email attachments), which are launched by a user or a system task.

Rootkits

It is a type of malicious program used to intercept system functions of an operating system in order to conceal itself. Besides, a rootkit can conceal tasks of other programs, registry keys, folders, and files. It can be distributed either as an independent program or a component of another malicious program. A rootkit is basically a set of utilities, which a cracker installs on a system to which she had just gained access.

There are two kinds of rootkits according to the mode of operation: *User Mode Rootkits (UMR)* which operate in user mode (intercept functions of the user mode libraries) and *Kernel Mode Rootkits (KMR)* which operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).



Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners which detect vulnerabilities in firewalls and other components of the computer's protection system. Besides hackers, such tools are used by administrators to check the security of their networks. Occasionally, common software which can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Spyware

This type of malicious programs is designed to perform monitoring of the system and send the gathered information to a third party – creator of the program or some other person concerned. Among those who may be concerned are: distributors of spam and advertisements, scam-agencies, marketing agencies, criminal organizations, industrial espionage agents, etc.

Spyware is secretly loaded to your system together with some other software or when browsing certain HTML pages and advertising windows. It then installs itself without the user's permission. Unstable browser operation and decrease in system performance are common side effects of spyware presence.

Adware

Usually this term is referred to a program code implemented into freeware programs which perform forced display of advertisements to a user. However, sometimes such codes can be distributed via other malicious programs and show advertisements in Internet browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of malicious programs does not deal any direct damage to the system. Joke programs usually just generate message boxes about errors that never occurred and threaten to perform actions which will lead to data loss. Their purpose is to frighten or annoy a user.

Dialers

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

All the above programs are considered malicious because they pose a threat to the user's data or his right of confidentiality. Programs that do not conceal their presence, distribute spam and different traffic analyzers are usually not considered malicious, although they can become a threat under certain circumstances.

Among other programs there is also a class of riskware programs. These were not intended as malicious, but can potentially be a threat to the system's security due to their certain features. Riskware programs are not only those which can accidentally damage or delete data, but also ones which can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP servers, etc.

**Below is a list of various hacker attacks and Internet fraud:**

- *Brute force attack* – performed by a special Trojan horse program, which uses its inbuilt password dictionary or generates random symbol strings in order to figure out the network access password by trial-and-error.
- *DoS attack* (denial of service) or *DDoS attack* (distributed denial of service) – a type of network attack, which verges on terrorism. It is carried out via a huge number of service requests sent to a server. When a certain number of requests is received (depending on the server's hardware capabilities) the server becomes unable to cope with them and a denial of service occurs. DDoS attacks are carried out from many different IP addresses at the same time, unlike DoS attacks, when requests are sent from one IP address.
- *Mail bombs* – a simple network attack, when a big email (or thousands of small ones) is sent to a computer or a company's mail server, which leads to a system breakdown. There is a special method of protection against such attacks used in the **Dr.Web** products for mail servers.
- *Sniffing* – a type of network attack also called "passive tapping of network". It is unauthorized monitoring of data and traffic flow performed by a packet sniffer – a special type of non-malicious program, which intercepts all the network packets of the monitored domain.
- *Spoofing* – a type of network attack, when access to the network is gained by fraudulent imitation of connection.
- *Phishing* – an Internet fraud technique, which is used for stealing personal confidential data such as access passwords, bank and identification cards data, etc. Fictitious letters supposedly from legitimate organizations are sent to potential victims via spam mailing or mail worms. In these letters victims are offered to visit phony web sites of such organizations and confirm the passwords, PIN codes and other personal information, which is then used for stealing money from the victim's account and for other crimes.
- *Vishing* – a type of Phishing technique, in which war dialers or VoIP is used instead of emails.

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 the virus laboratory **Doctor Web** for analysis.
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 the **Dr.Web** 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 with 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.

- HLLW – worms
- HLLM – mail worms
- HLLQ – 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 Horses (Trojans)

`Trojan` – a general name for different Trojan horses (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's 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

- **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 to name simple featureless viruses the with different modifiers 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.

