



Dr.WEB®

Anti-virus
for Windows

User Manual

Defend what you create

© Doctor Web, 2003-2011. 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 Anti-virus for Windows

Version 7.0

User Manual

14.12.2011

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	7
1.1. About This Manual	9
1.2. Document Conventions	10
1.3. System Requirements	11
1.4. Licensing	12
1.4.1. Key File	12
1.4.2. Get Key File	13
1.4.3. Renewing Registration	15
1.5. How to Test Anti-virus	16
1.6. Detection Methods	17
2. Installing Dr.Web Anti-virus	19
2.1. Installation Procedure	20
2.2. Reinstalling and Removing Dr.Web Anti-virus	30
2.3. Receiving Key Files	31
3. Getting Started	34
3.1. SpIDer Agent	37
3.2. General Settings	40
3.3. License Manager	44
3.4. Quarantine	46
4. Dr.Web Scanner	50
4.1. Scanning Your System	51
4.2. Neutralizing Detected Threats	53
4.3. Scanner Settings	54



4.4. Scanning in Command Line Mode	58
4.5. Console Scanner	59
5. SpIDer Guard	60
5.1. Managing SpIDer Guard	61
5.2. SpIDer Guard Settings	62
6. SpIDer Mail	67
6.1. Managing SpIDer Mail	69
6.2. SpIDer Mail Settings	70
7. Dr.Web for Outlook	77
7.1. Configuring Dr.Web for Outlook	77
7.2. Treat Detection	79
7.2.1. Types of Threats	79
7.2.2. Configuring Actions	79
7.4. Logging	82
7.4.1. Event Log	82
7.4.2. Debug Text Log	83
7.5. Statistics	84
8. Dr.Web Firewall	85
8.1. Training Dr.Web Firewall	85
8.2. Managing Dr.Web Firewall	90
8.3. Firewall settings	92
8.3.1. Application Filter	92
8.3.2. Parent processes	98
8.3.3. Network Interfaces	100
8.3.4. Advanced settings	109
8.3.5. Restoring Defaults	112



8.4. Event Logging	113
8.4.1. Active Applications	113
8.4.2. Application Filter Log	115
8.4.3. Packet Filter Log	118
9. Automatic Updating	120
9.1. Running Updates	120
Appendices	123
Appendix A. Command Line Parameters	123
Appendix B. Computer Threats and Neutralization Methods	128
Appendix C. Naming of Viruses	136
Appendix D. Central Anti-virus Protection	141
Appendix E. Technical Support	143



1. Introduction

Dr.Web Anti-virus for Windows provides multi-level protection of RAM, hard disks, and removable devices against viruses, rootkits, Trojans, spyware, adware, hack tools, and other malicious programs. The module architecture of **Dr.Web Anti-virus** 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®, and Solaris®).

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

Dr.Web Anti-virus 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 them, standard anti-virus components are used.

Dr.Web Anti-virus includes the following components:

- **Dr.Web Scanner for Windows (Scanner)** is an anti-virus scanner with graphical interface. The program runs on user demand or according to a schedule and checks the computer for viruses. There is also a command line version (**Dr.Web Console Scanner for Windows**).
- **SpIDer Guard® for Windows** (also called **Monitor** or **Guard**) is an anti-virus guard. The program resides in the main memory, checks files and memory on the fly, and detects virus-like activity.
- **SpIDer Mail® for Windows (Mail Guard)** is an anti-virus guard for e-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.



- **Dr.Web for Outlook** is a plug-in that checks Microsoft Outlook mail boxes for viruses.
- **Dr. Web Firewall** protects your computer from unauthorized access and prevents vital data from leaking through networks.
- **Dr.Web Updater** allows registered users to receive updates of the virus database and other program files as well as automatically install them.
- **SpIDer Agent** is a utility that lets you set up and manage **Dr. Web Anti-virus** components.

For information on centralized protection, refer to [Appendix D](#).



1.1. About This Manual

This User Manual describes installation and effective utilization of **Dr.Web Anti-virus**.

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

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

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



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://products.drweb.com>.



1.2. Document Conventions

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

Convention	Description
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 Dr.Web products and components.
<u>Green and underlined</u>	Hyperlinks to topics and web pages.
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. In addition, it may indicate a term in position of a definition.
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.

The following abbreviations are used in this User Manual:

- GUI – Graphical User Interface (GUI version of a program, a version that utilizes the GUI)
- OS – operating system
- PC – personal computer
- RAM – Random Access Memory



1.3. System Requirements



Before installing **Dr.Web Anti-virus**:

- Install all critical updates recommended by the operating system developer.
- Uninstall all other anti-virus packages from the computer to avoid possible incompatibility with their resident components.
- If you install **Dr.Web Firewall**, uninstall all other firewalls.

Specification	Requirement
OS	<p>One of the following:</p> <ul style="list-style-type: none">• Microsoft® Windows® 2000 Workstation SP4 with Update Rollup 1• Windows® XP SP2• Windows® Vista• Microsoft® Windows® 7 <p>Both 32-bit and 64-bit versions of operating systems are supported.</p> <p>You may need to download and install certain system components from the official Microsoft website. If necessary, the program will notify you about the components required and provide download links.</p>
Hard disk space	<p>330 MB for Dr.Web Anti-virus components.</p> <p>Files created during installation will require additional space.</p>
CPU	i686 compatible
RAM	minimum 512 MB
Other	Internet connection for updating virus databases and Dr.Web Anti-virus components.



1.4. Licensing

The use rights for the **Dr.Web Anti-virus** are specified in the key file.

To use **Dr.Web Anti-virus**, [obtain](#) and [install](#) a key file.

For more information on licensing and types of key files, visit the [official Doctor Web website](#).

1.4.1. Key File

The key file contains the following information:

- list of components a user is allowed to use
- duration of the license
- other restrictions (i.e., the number of computers on which a program is allowed to be used)

The key file has the .key extension and, by default, should reside in the program's installation folder.



The key file has a write-protected format and must not be edited. Editing the key file renders it invalid. Therefore, it is not recommended to open your key file with a text editor which may accidentally corrupt it.

There are three types of key files:

- *License key file* is purchased with the **Dr.Web** software and allows a user to use the software and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. It also contains information about the user and seller.
- *Demo key file* is used to evaluate **Dr.Web** products. It is completely free, provides full functionality of the software, but has a limited duration – 30 days.



Demo key files for the same computer cannot be obtained more often than once in four months.

- *Temporary key file* is used if you do not install a license or demo key file during installation. This key file provides full functionality of **Dr.Web Anti-virus** components, however, updating is not available until you have installed license or demo key file. Furthermore, the **My Dr.Web** and **Update** items of [SpIDer Agent menu](#) will be inaccessible.

A *valid* license key file satisfies the following criteria:

- License is not expired.
- All anti-virus components required by **Dr.Web Anti-virus** are licensed.
- Integrity of the license key file has not been violated.

If any of the conditions are violated, the license key file becomes *invalid* and **Dr.Web Anti-virus** stops detecting and neutralizing malicious programs.

1.4.2. Get Key File

The key file can be delivered as a .key file or an archive containing such a file.

You can receive key files in one of the following ways:

- [During installation](#), the first update, or later.
- Via manual [product registration](#) on the [official Doctor Web website](#).
- Within the product distribution kit.
- On a separate data carrier provided by the seller.

Key files received [during installation](#) or within the installation kit are installed automatically. You need to [install](#) key files received in any other way.



To acquire key files via manual registration:



To register and download key files, a valid Internet connection is required.

To receive a license key file, a product serial number is required. Without a serial number, you can only receive a demo key file [during installation](#).

1. Launch an Internet browser and go to the site specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number found on the registration card.
4. The license key file is archived and sent to the e-mail address you specified in the registration form. After registration, you can also download the license key file from the registration page. Windows operating systems extract files from ZIP-archives automatically. You do not need to purchase or install additional software.
5. [Install](#) the key file.

To acquire key files during installation:

The key file can be delivered as a .key file or an archive containing such a file. A user can receive a key file via the **Dr.Web Updater** during installation or the first update. The utility registers the program (after the serial number is provided) on the official website and receives the key file. This procedure is available only for **Dr.Web** programs that protect individual workstations. Without a serial number, a user can only receive a demo key file. (See [Receiving key file](#)).

It is recommended to keep the key file until it expires. If you re-install a product or install it on several computers, you do not have to register the serial number again; you can use the key file received



during the first registration.



Demo key file can be used only on that computer on which it was registered.

Subsequent Registration

If a key file is lost, you must register again by inputting the personal data you provided during the previous registration. You may use a different e-mail address in which case the key file will be sent to the address specified.



When recovering a demo key file, you will receive the same key file as you received during the previous registration.

The number of times you can request a key file is limited. One serial number can be registered no more than 25 times. If requests in excess of that number are sent, no key file will be delivered. To receive a lost key file, contact [Technical Support](#), describe your problem in detail and state personal data you entered when you registered the serial number.



If no valid key file is found (either for a license or a demo), the functionality of the program is blocked.

1.4.3. Renewing Registration

When your license expires or the security of your system is reinforced, you may need to update the license. The new license should be registered with the product. **Dr.Web Anti-virus** supports hot license updates without stopping or reinstalling the product.



To renew license key files:

1. Open [License Manager](#). To purchase a new license or renew an existing one, you can also use your personal web page on the **Doctor Web** website. To visit your page, use the **My Dr.Web** option in the **License Manager** or [SpIDer Agent](#) menu.
2. If your current key file is invalid, **Dr.Web Anti-virus** automatically switches to the new license.

1.5. How to Test Anti-virus

The European Institute for Computer Anti-Virus Research (EICAR) Test File helps test the performance of anti-virus programs that detect viruses using signatures.

For this purpose, most anti-virus software vendors generally use a standard test.com program. This program was specially designed to let user test the reaction of newly installed anti-virus tools that detect viruses without compromising the 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 one. Upon detecting this "virus", **Dr.Web Anti-virus for Windows** reports the following: EICAR Test File (Not a Virus!). Other anti-virus tools alert users in a similar way.

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

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

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

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



In [optimal mode](#) **SpIDer Guard** does not detect an EICAR file as malicious software because this file is a DOS application and does not compromise computer security.



1.6. Detection Methods

Dr.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 behaviour:

1. The scans begin with *signature analysis*, which is performed by comparing file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes that is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, **Dr.Web anti-virus solutions** use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures which preserves the correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed in such a way that some entries can be used to detect not just specific viruses but whole classes of threats.
2. On completion of signature analysis, **Dr.Web anti-virus solutions** use the unique **Origins Tracing™** method to detect new and modified viruses that use known infection mechanisms. Thus, **Dr.Web** users are protected against viruses such as notorious blackmailer Trojan.Encoder.18 (also known as gpcod). In addition to detecting new and modified viruses, the **Origins Tracing** mechanism considerably reduces the number of incidents of false triggering of the **Dr. Web** heuristics analyzer.
3. The detection method used by the *heuristics analyzer* is based on certain knowledge about the attributes that characterize malicious code. Each attribute or characteristic has a weight coefficient that determines the level of its severity and reliability. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. As with any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (i.e., it may omit viruses or raise false alarms).

While performing any of the aforementioned checks, **Dr.Web anti-virus solutions** use the most recent information about known malicious software. As soon as **Doctor Web Virus Laboratory**



experts discover new threats, they issue an update on virus signatures, behaviour characteristics, and attributes. 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 update the virus is detected in the list of processes and neutralized.



2. Installing Dr.Web Anti-virus

Before installing the program, we strongly recommend to:

- install all critical updates released by Microsoft for the OS version used on your computer (they are available at the company's updating web site at <http://windowsupdate.microsoft.com>);
- check the file system with the system utilities, and remove the detected defects;
- close all active applications.



Dr.Web Anti-virus is not compatible with other anti-virus software. Installing two anti-virus programs on one computer may lead to a system crash and the loss of important data.

To begin installing **Dr.Web Anti-virus** on your computer, do one of the following:

- Execute the file, if supplied as a single executable file.
- Insert the company disk into the CD/DVD drive. If autorun is enabled, the installation procedure will start automatically. If autorun is disabled, run the executable file of the distribution kit manually.

Follow the dialog windows of the installation wizard. At any stage of the installation (before the files are copied onto the computer), you can return to the previous stage by clicking **Back**. To continue installation, click **Next**. To abort installation, click **Cancel**.



2.1. Installation Procedure



Only a user with administrative privileges can install **Dr.Web Anti-virus**.

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

1. The background mode.
2. The usual mode.

Background Installation

To install **Dr.Web Anti-virus** in the background mode, enter in the command line the executable file name with necessary parameters (these parameters affect logging, reboot after installation, and **Dr. Web Firewall** installation).

Installation	Parameters
No reboot. No logging.	/S /V/qn
Reboot. No logging.	/S /V"/qn REBOOT=Force" or /S /V"/qn REBOOT=F"
No reboot. Logging.	/S /V"/qn /lv* \"<path>\drweb-setup.log\""
Reboot. Logging.	/S /V"/qn /lv* \"<path>\drweb-setup.log\" REBOOT=F" or /S /V"/qn /lv* \"<path>\drweb-setup.log\" REBOOT=Force"
Dr.Web Firewall installation. Reboot.	/S /V"/qn INSTALL_FIREWALL=1 REBOOT=F" or /S /V"/qn INSTALL_FIREWALL=1 REBOOT=Force"



For example, to install **Dr.Web Anti-virus** with logging and reboot after installation, execute the following command:

```
C:\Documents and Settings\drweb-700-win-x86.exe  
/S /V"/qn /lv* \ "%temp%\drweb-setup.  
log\" REBOOT=F"
```

If particular language of the installation is required, use the following additional parameter:

```
/L<language_code>
```

For example,

```
/L1049 /S /V"/qn REBOOT=Force"
```

The list of languages:

Code	Language
1026	Bulgarian
2052	Chinese (Simplified)
1028	Chinese (Traditional)
1033	English
1061	Estonian
1036	French (France)
1031	German
1032	Greek
1038	Hungarian
1040	Italian
1041	Japanese
1062	Latvian
1063	Lithuanian
1045	Polish
2070	Portuguese
1049	Russian



Code	Language
1051	Slovak
1034	Spanish (Traditional Sort)
1055	Turkish
1058	Ukrainian

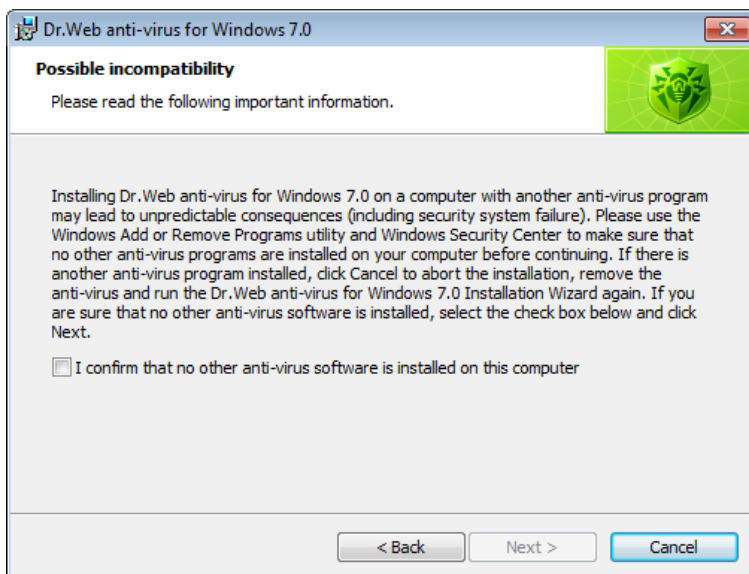


English will be installed in addition to whatever other language is chosen.

Usual Installation

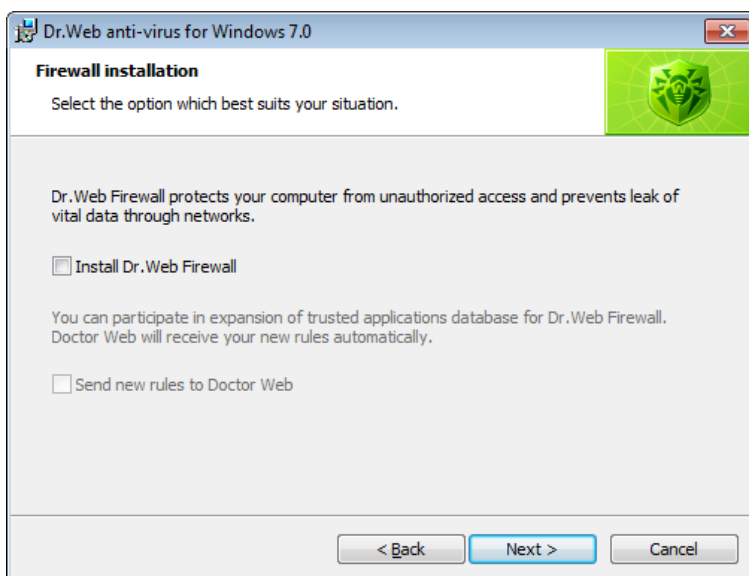
1. Select the language for the installation wizard. Regardless of your choice English language will be installed in addition.
2. In the next window, you will be asked to read the License agreement. To continue installation, you must accept its terms and click **Next**.
3. The installation wizard will inform you of any possible incompatibility between **Dr.Web** and other anti-viruses installed on your computer and offer to uninstall or disable them. If other anti-viruses are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other anti-viruses, and then proceed with installation.

To continue with the installation select the **I confirm that no other anti-virus software is installed on this computer** check box, and click **Next**.

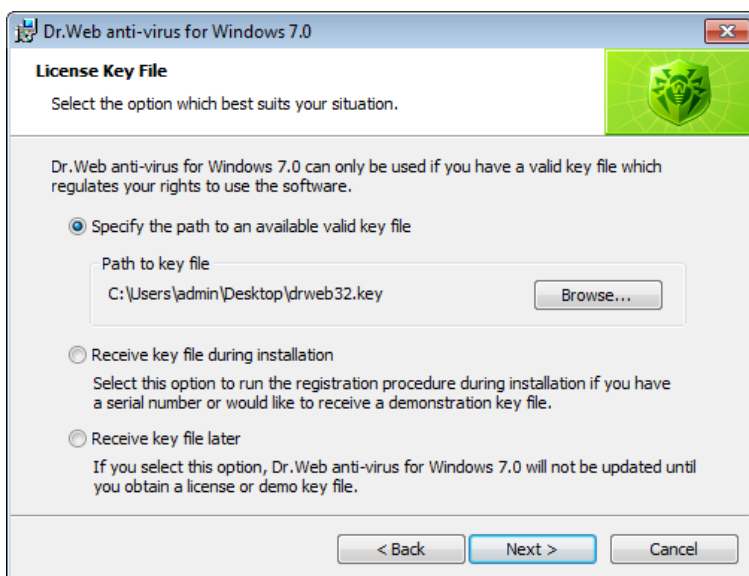


4. In the next window you will be offered to install **Dr.Web Firewall**.

You can also participate in expansion of trusted applications database for **Dr.Web Firewall**. Select the **Send new rules to Doctor Web** checkbox to allow **Dr.Web Firewall** to send created rules to **Doctor Web**.



5. If in the previous step you selected the **Install Dr.Web Firewall** check box, the installation wizard will inform you of any possible incompatibility between **Dr.Web** and other firewalls installed on your computer and offer to uninstall or disable them. If other firewalls are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other firewalls, and then continue with the installation.
To continue installation select the **I confirm that no other firewall is installed on this computer** check box and click **Next**.
6. The installation program will bring up a warning window requesting a **key file** (license or demo) required for the program's operation. If a key file is present on your hard drive or on removable media, click **Browse**, select the key file and click **Next**.

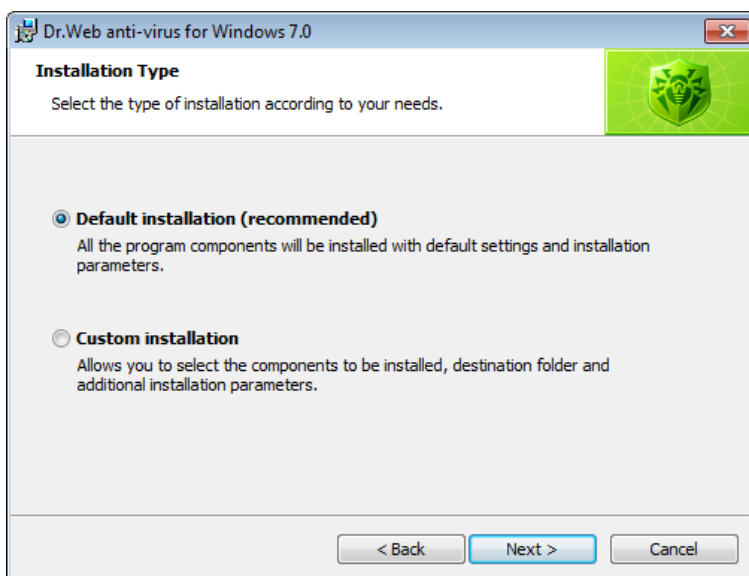


If no key file is available, but you have a serial number, select **Receive key file during installation**. Otherwise, select **Receive key file later** (updating is not available in this mode) and click **Next**.



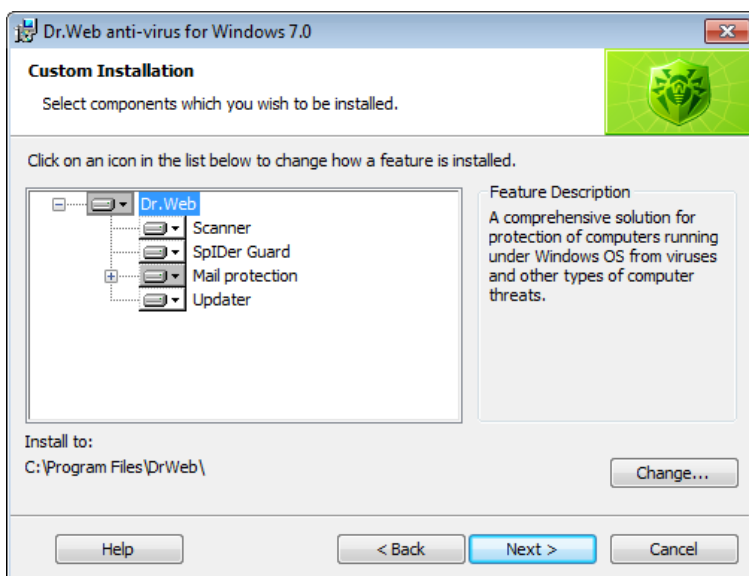
Use only a **Dr.Web Anti-virus** key file which should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

7. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components and all secondary programs automatically up to step 12. **Custom Installation** is meant for experienced users. During custom installation you will be asked to select components for installation and adjust proxy server settings and some additional installation parameters.



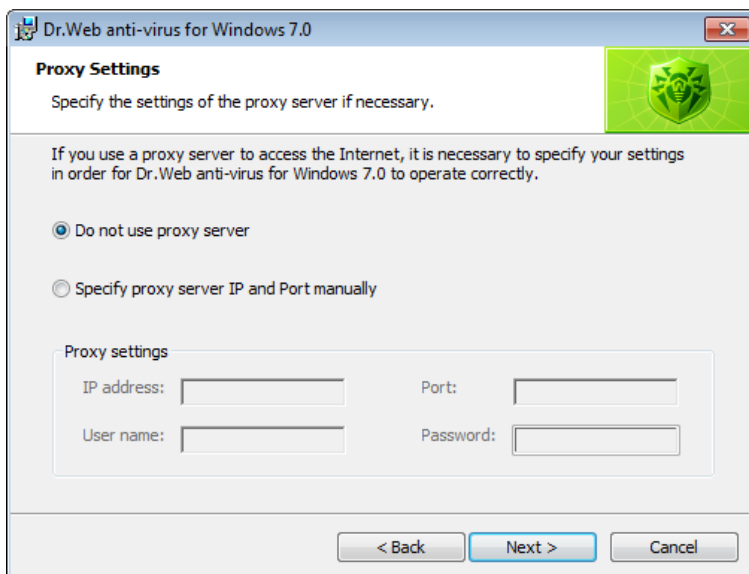
Once you choose the type of installation, click **Next**.

8. If you chose default installation type, go to step 12. In case of custom installation, a window will open that allows you to select – from the hierarchical list – the program components you want install. You can also change the installation folder if necessary.



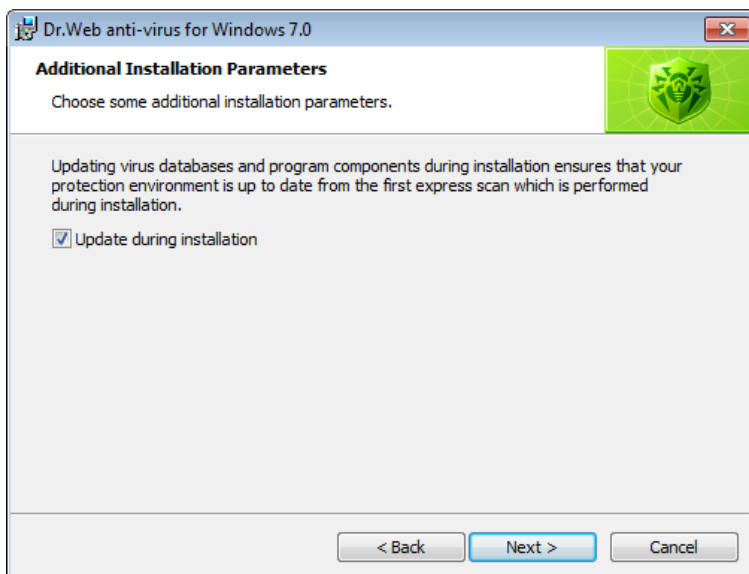
Click **Next** when you finish selecting the necessary components.

9. The window for selecting what shortcuts to **Dr.Web Anti-virus** you want to create will open. Select the necessary options, and click **Next**.
10. The window for adjusting proxy server settings will open.
 - If you do not use a proxy server, choose **Do not use proxy server**.
 - If you want to specify settings for a proxy server, choose **Specify proxy server IP and Port manually**.



Click **Next**.

11. If in step 6 you specified a valid key file or selected **Receive key file during installation**, then to download the latest virus databases and anti-virus components, you may proceed to the next step and select the **Update during installation** checkbox.



12. A window will open, informing you that the program is ready to be installed. Click **Install** to start the installation process or **Back** to change any of the installation parameters.
13. If in step 6 you selected the **Receive key file during installation** option, the installation wizard will launch the [registration procedure](#). To receive the key file, your computer should be connected to the Internet.
14. If in step 11 you selected the **Update during installation** check box, or during default installation, after receiving the key file virus databases and components of **Dr.Web Anti-virus** will be updated automatically.
15. After installation is complete, **Scanner** will perform an [express scan](#). Avert any detected threats, and close **Scanner** after the scanning process.



Scanner is not compatible with Windows Blinds (an application for adjusting Windows GUI). In order for **Dr. Web Anti-virus** to operate correctly you must disable the option to change the **Dr.Web** interface in the Windows Blinds settings. To do this, add drweb32w.exe to the list of excluded applications.

16. The program will ask you to reboot the computer; this is required to complete the installation.

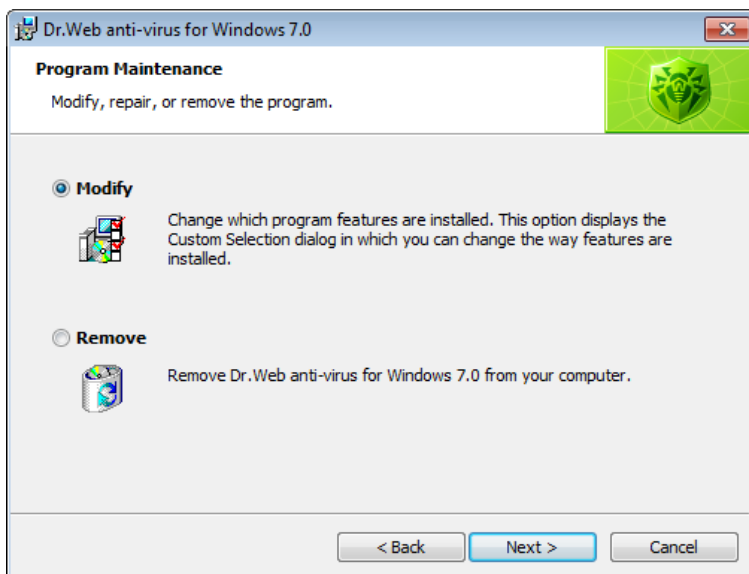
2.2. Reinstalling and Removing Dr.Web Anti-virus

To modify, repair, or remove an installed version of **Dr.Web Anti-virus**, start the [installation wizard](#).

In the opened window:

1. Select **Modify** to change the set of installed components, and click **Next**. The [Custom Installation](#) window will open. To remove all the components, select **Remove**.
2. To remove the **Dr.Web Anti-virus** or to change the set of installed components, you must disable **Self-Protection** by entering the digits shown in the picture or password (if you set **Protect Dr.Web settings by password** flag on **Extended** tab in [SpIDer Agent settings](#)).
3. At the end of the installation, reboot the computer when prompted.

You can start the modification, repair, or removal procedure via the standard Windows utility - **Add/Remove Programs**.



2.3. Receiving Key Files

The registration procedure for a new key file starts automatically during installation or can be launched from the **SpIDer Agent** menu once the installation is complete. This procedure helps you connect to the **official Doctor Web website** and register your installation.

To obtain a key file:

1. During the first step of the procedure, you will be asked to choose what type of key file you would like to obtain - either a license or a demo key file.



Registration Wizard

Step 1
License type

Step 2
User information

Step 3
Obtaining license

In order for Dr.Web product to operate, you need a license key file. To continue, please register and obtain a license or demo key file from Doctor Web servers.

☒ Demo key file

You do not need a serial number to get the 30-day demo key file. Please note that you may receive the demo key file no more frequently than once every 4 months.

☐ License key file. Please enter serial number:

- - -

[What is a key file?](#)

[Where is the serial number?](#)

Back Next Cancel

If you received a serial number when you purchased your **Dr. Web** product, select **License key file**, and enter the serial number. If you want to install the product for demonstration purposes, select **Demo key file**, and go to step 2.



If you have used **Dr.Web Anti-virus for Windows** in the past, you may be eligible for a 150-day extension to your new license. To enable the bonus, enter your registered serial number or provide the license key file.

Click **Next**. The registration data window opens.

2. Fill in all necessary fields in the registration form to receive a key file, and click **Next**.



Registration Wizard

Step 1
License type

Step 2
User information

Step 3
Obtaining license

Registration name:
Mr. Smith ✓

Region:
United Kingdom ✓

City:
London ✓

E-mail address:
mail@mail.com ✓

☒ Subscribe to newsletters

[Privacy statement \(online\)](#)

Back Next Cancel

3. The procedure of receiving the license key will start. If the key file is downloaded successfully, the window displays an appropriate message and duration of the license. Otherwise, an error message will appear.



3. Getting Started

The installation program allows you to install the following **Dr.Web Anti-virus** components on your computer:

- **Scanner** (GUI and console versions)
- **SpIDer Guard**
- **SpIDer Mail**
- **Dr.Web for Outlook**
- **Firewall**
- **Automatic Updating Utility**
- **SpIDer Agent**

The components of **Dr.Web Anti-virus** use common virus databases and anti-virus engine. In addition, uniform algorithms that detect and neutralize viruses in scanned objects are implemented. However, the methods of selecting objects for scanning differ greatly, which allows these components to be used for absolutely different and mutually supplementary PC protection policies.

For example, **Scanner for Windows** scans (on user demand or according to schedule) certain files (e.g., all files, selected logical disks, directories). By default, the main memory and startup files are scanned too. Since it is the user who decides when to launch a task, there is no need to worry about the sufficiency of computational resources needed for other important processes.

SpIDer Guard constantly resides in the main memory of the PC and intercepts calls made to the objects of the file system. The program checks for viruses in files that are being launched, created, or changed on the hard drives and those that are opened on removable media and network drives. Due to a balanced approach to the level of the file system scanning details the program hardly disturbs other processes on the PC. However, this results in insignificant decrease of virus detection reliability.

An advantage of the program is that it provides you with uninterrupted control of the virus situation during the entire time a PC is running. In



addition, some viruses can only be detected by the guard through their specific activity.

SpIDer Mail also constantly resides in the memory. The program intercepts all calls from your mail clients to mail servers via POP3/SMTP/IMAP4/NNTP protocols and scans incoming and outgoing e-mail messages before they are received (or sent) by the mail client.

SpIDer Mail is designed to check all current mail traffic going through a computer. As a result, it becomes more efficient and less resource-consuming to scan mailboxes. For example, you can control attempts at mass distribution of a mail worm's functional copies to the addresses specified in the user address book which is performed via the worm's own mail clients. You can also disable scanning of e-mail files for **SpIDer Guard**, which considerably reduces consumption of computer resources.

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



Ensuring Protection Against Virus Threats

To ensure comprehensive anti-virus protection, we advise you to use the **Dr.Web Anti-virus** components as follows:

- Scan your computer file system with the default (maximum) scanning detail settings.
- Keep default settings of **SpIDer Guard**.
- Perform complete e-mail scanning with **SpIDer Mail**.
- Block all unknown connections with **Dr.Web Firewall**.
- Perform a periodic complete scan of your PC that coincides with when virus database updates are issued (at least once a week).
- Immediately perform a complete scan whenever **SpIDer Guard** has been temporarily disabled and the PC was connected to the Internet or files were downloaded from removable media.




Anti-virus protection can only be effective if you update the virus databases and other program files regularly (preferably every hour). For more information, read [Automatic Updating](#).

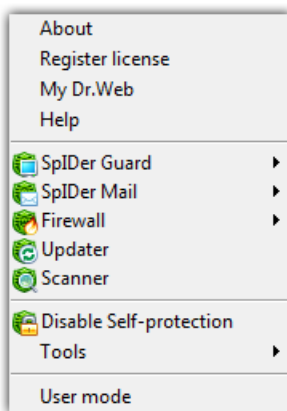


3.1. SpIDer Agent

After **Dr.Web Anti-virus** has been installed, a **SpIDer Agent**  icon is added to the taskbar notification area.

If you hover the mouse cursor over the icon, a pop-up appears with information about the components that are running, the date of last update, and amount of virus signatures in the virus databases. Furthermore, notifications, which are adjusted in the settings (see below), may appear above the **SpIDer Agent**  icon.

The context menu of the icon allows to perform the main management and settings functions of **Dr.Web Anti-virus**.



The **About** item opens a window showing information about your version of **Dr.Web Anti-virus**.

The **Register license** item starts the [registration procedure](#) for receiving a key file from **Doctor Web** servers.

The **My Dr.Web** item opens your personal web page on the **Doctor Web official website**. This page gives information about your license



(e.g., period of usage, serial number), and allows you to renew your license, contact Technical Support, etc.

The **Help** item opens the **Dr.Web Anti-virus** help system.

The **SpIDer Guard**, **SpIDer Mail** and **Update** items allow you to access the management and settings features of the corresponding components.

The **Scanner** item runs **Dr.Web Scanner**.

The **Disable/Enable Self-protection** item allows you to disable/enable protection of **Dr.Web Anti-virus** files, registry keys, and processes from damage and deletion.

To disable self-protection:

- select **Disable self-protection** in the **SpIDer Agent** menu;
- enter the text displayed in the picture.

The **Enable self-protection** item will appear.



You cannot disable self-protection when in User mode. It is not recommended to disable self-protection.

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

The **Tools** item opens a submenu that provides access to:

- License Manager
- General Settings of **Dr.Web Anti-virus** operation
- Quarantine
- Anti-virus Network
- Report generation wizard.

Before contacting **Doctor Web Technical Support**, generate a report that indicates how your operating system and **Dr.Web Anti-virus** are functioning. To adjust parameters, in the opened window, click **Report settings**. The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% directory.



The **Administrative/User mode** item allows you to switch between full-function **Administrative mode** and restricted **User mode**. In **User mode**, access to settings of components is forbidden, as well as disabling of all components and self-protection. **License Manager** is not available, too. You need administrative rights to switch to **Administrative mode**.



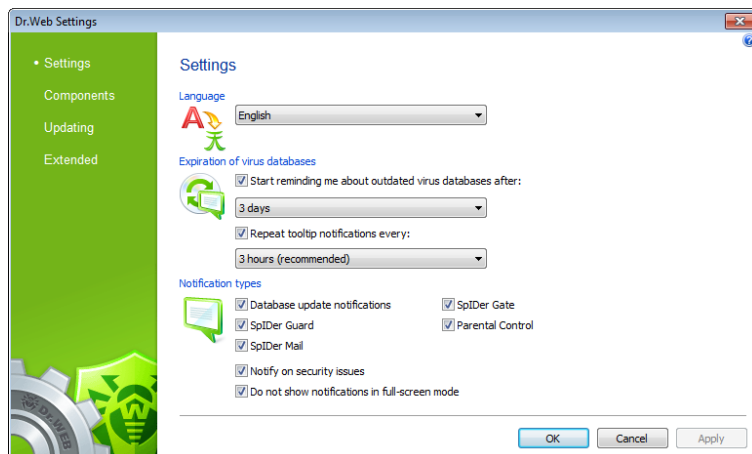
This item displays when you do not have administrative privileges. For instance, this item displays when you log into Microsoft Windows 2000 or Windows XP operating systems as a non-privileged user, or when User Account Control of Windows Vista or Microsoft Windows 7 operating system is enabled. Otherwise, the item is hidden and **Dr.Web Anti-virus** operates in full-function mode all the time.



3.2. General Settings

General settings of **Dr.Web Anti-virus** operation is configured in the **Dr.Web Settings** window. To open this window, click the **SpIDer Agent** icon in the notification area, select **Tools**, and then select **Settings**.

Settings Page



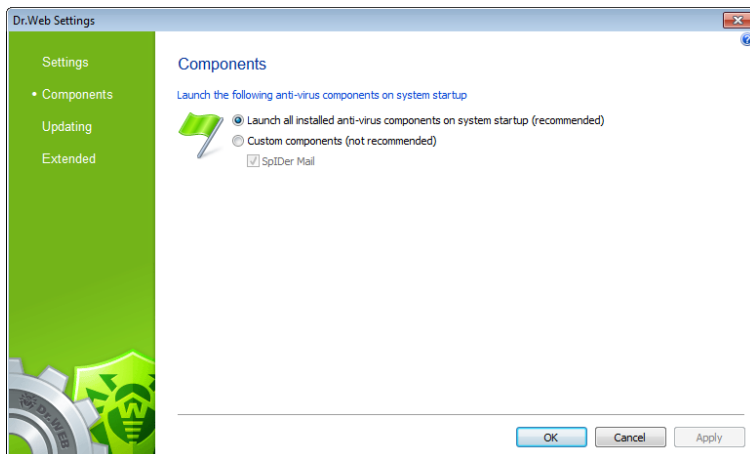
On this page you can specify the language of the **Dr.Web Anti-virus** GUI by selecting the necessary language in the **Language** list. If you choose language that hasn't been installed, **Dr.Web Anti-virus** will suggest to install it.

Also in this window you can select the types of pop-up notifications which appear above the **SpIDer Agent** icon in the taskbar notification area. Components send notifications when a corresponding event happens (i.e. when a threat is detected or an update is performed). Also if your system hasn't been scanned for 7 days, a corresponding notification appears (**Security issue notifications** checkbox).



Components Page

On this page you can configure automatic launching of **Dr.Web Anti-virus** components on system startup.

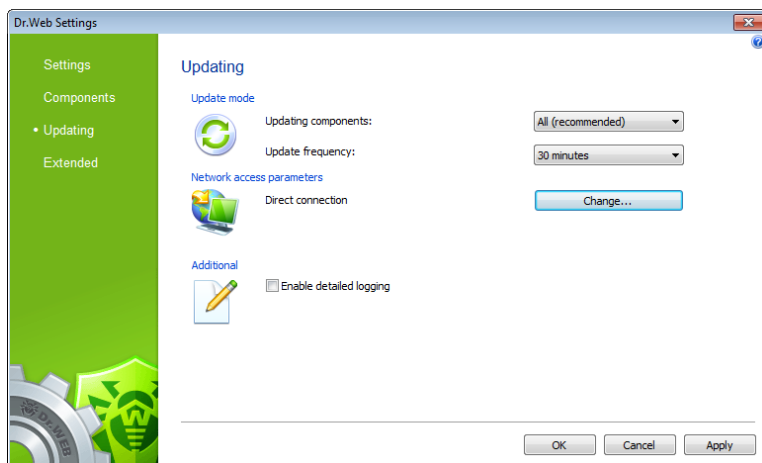


Update Page

On this page you can configure **Dr.Web Anti-virus** update parameters such as components that should be updated and update period.

You can also configure network access. To do this, in the **Network access parameters** click **Change** and select one of the following modes:

- If you use proxy server for Internet connections, select **Direct connection**.
- If you want to specify proxy server settings manually, select **User-defined settings** and enter connection parameters.



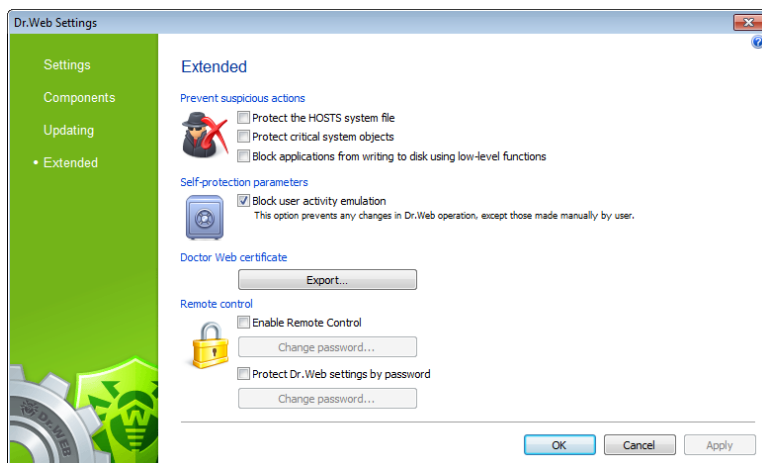
Also you can set the **Enable detailed logging** flag to increase change log detail level. All changes are logged into dwupdater.log, that is located in %allusersprofile%\Application Data\Doctor Web\Logs\ folder (in Windows 7, %allusersprofile%\Doctor Web\Logs\).

Extended Page

On this page, you can specify self-protection parameters and disable miscellaneous operations that may compromise security of your computer.



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.



Doctor Web Certificate

You may need to scan data transmitted in accordance with SSL protocol. For instance, you can set **SpIDer Mail** to receive and send messages via POP3S, SMTPS, or IMAPS. These protocols use encrypted SSL connections. In order for **Dr.Web Anti-virus** to scan such encrypted traffic and maintain transparent integration with some browsers and mail clients that do not refer to the Windows system certificate storage, it may be necessary to import **Doctor Web SSL certificate** into the application certificate storages. To save the certificate from the system storage for future use in third party applications, click **Export** and select a convenient folder.

Password protection


Here you can configure the following options:

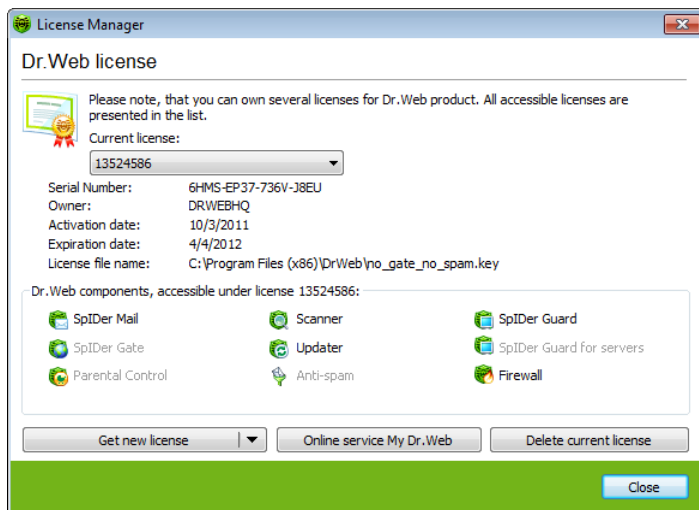
- Allow remote access to **Dr.Web Anti-virus** on your computer and set a password that will be required to connect to your anti-virus from other computers.
- Protect **Dr.Web Anti-virus** settings on your computer with a password. Set a password that will be required to access settings of **Dr.Web Anti-virus**.



3.3. License Manager

License Manager shows information from the **Dr.Web Anti-virus** key files in an understandable form.

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



Selected **Dr.Web Anti-virus** components for your license are specified in the **Dr. Web antivirus components** group box.

The **Online service My Dr.Web** item opens your personal web page on the **official Dr.Web Anti-virus website**. This page gives information about your license (period of usage, serial number), allows to renew your license, contact Technical Support, etc.

To start the registration procedure for receiving the key file from **Doctor Web** servers, click **Get new licence** and select **from Internet** in the drop-down menu. That launches [key file receipt](#).



To add a key file

1. Click **Get new licence**. In the drop-down menu, select **from file**.
2. Select the file in a standard window.
3. **Dr.Web Anti-virus** starts using the key file automatically.

If you received a key file during installation or in the distribution kit complete set, installation of a key file is made automatically and does not demand any additional actions.

To delete a key file from a list, select it and click **Delete current licence**. Last used key cannot be removed.



The **License Manager** item is available in the menu when operation in [Administrative mode](#) only.



3.4. Quarantine

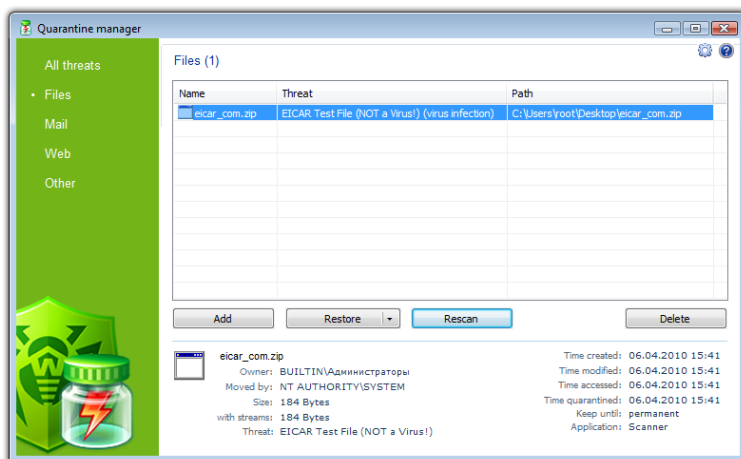
The **Quarantine** section of **Dr.Web Anti-virus** serves for isolation of files that are suspicious as malware. **Quarantine** folders are created separately on each logic disk where suspicious files are found. When infected objects are detected at the portable data carrier accessible for writing, the Quarantine folder will be created on the data carrier and infected objects will be moved to this folder.

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

In the center of the window the table with the quarantine state is displayed. The following columns are included:

- **Name** – name list of the objects in the quarantine
- **Threat** – malware classification, which is assigned by **Dr.Web Anti-virus** during automatic moving to the quarantine
- **Path** – full path of the object before moving to the quarantine

The bottom pane of the window displays detailed information about the selected objects. You can also display this information in the table.



To configure table view:

1. Right-click the header of the table and select **Customize columns**.
2. In the opened window, set the checkboxes next to those items that you want to display in the table, or clear the checkboxes next to those items that you want to hide. You can also do one of the following:
 - To select checkboxes for all items, click **Check all**
 - To clear all checkboxes, click **Uncheck all**
3. Use **Move up** and **Move down** to change position of a column in the table.
4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

The left pane serves to filter the quarantine objects to display. Click the corresponding option to display all quarantine objects or just specified groups: files, mail objects, web pages or all other objects, not classified.

In the quarantine window only the users with access rights to the files can see these that files.



Use the following buttons to manage the quarantine:

- **Add** – add the file to the quarantine. Select the necessary file in the opened file system browser
- **Restore** – remove the file from the quarantine and restore the original location of the file, i.e. restore the file to the folder where it had resided before it was moved to the quarantine



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

In the drop-down menu you can choose **Restore to** – restore the file to the folder specified by the user.


- **Rescan** – scan the file one more time
- **Remove** – delete the file from the quarantine and from the system

Right-click anywhere in the table to access the following options:

- **Submit file(s) to Doctor Web Laboratory** – send files to **Doctor Web Virus Laboratory** for checking
- **Copy hash to clipboard** – copy hash of the file, computed using MD5 or SHA256 function, to clipboard

To manage several objects simultaneously, select necessary objects in the quarantine window and select necessary action in the drop-down menu.

In the bottom of the quarantine window the detailed information about selected items is displayed.

To configure **Quarantine** parameters, click the **Settings**  button in the **Quarantine** window. The **Quarantine** properties window will be opened. In this window you can change the following parameters:

- In the **Set quarantine size** section you can configure the amount of disk space for **Quarantine** folder



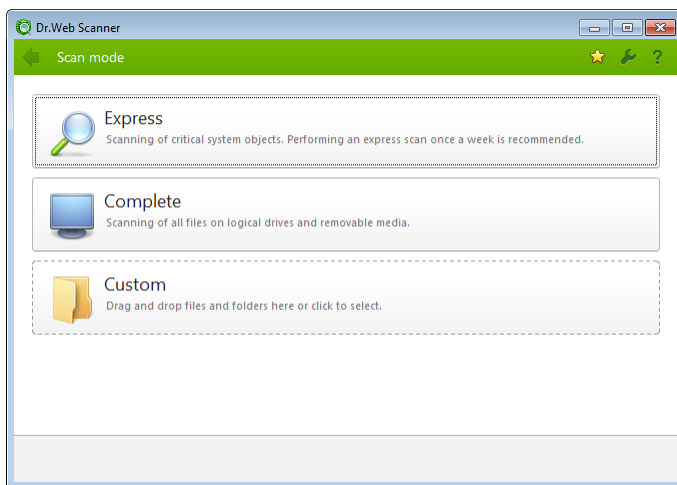
- In the **View** section, you can set the **Show backup files** checkbox to display backup copies of **Quarantine** files in the object table

Backup copies are created automatically during moving files to the **Quarantine**. Even if **Quarantine** files are kept permanently, their backup copies are kept temporarily.



4. Dr.Web Scanner

By default, the program scans 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.





4.1. Scanning Your System

Dr.Web Scanner is installed as a usual Windows application and can be launched by the user.



It is recommended for the scanner to be run by a user with administrator rights because files to which unprivileged users have no access (including system folders) are not scanned.

To launch Scanner:

Do one of the following:

- Click the **Dr. Web Scanner** icon on the Desktop.
- Click the **Scanner** item in the context menu of the **SpIDer Agent** icon in the taskbar notification area (see [SpIDer Agent](#) chapter).
- Click the **Dr.Web Scanner** item in All Programs -> Dr. Web directory of the Windows **Start** menu.
- Run the corresponding command in the Windows command line (read [Command Line Scanning Mode](#)).

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

There are 3 scanning modes: **Express scan**, **Complete scan** and **Custom scan**. Depending on the selected mode, either a list of objects which will be scanned or a file system tree is displayed at the center of the window.

In **Express scan** mode the following objects are scanned:

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

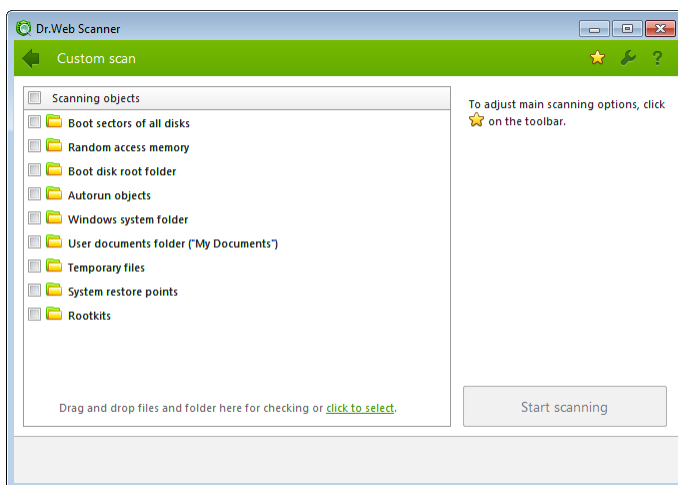


- System temporary folder
- User temporary folder

If scanning process is running under administrative privileges, then in this mode **Scanner** also checks if rootkits are present in the system.

If **Complete 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.

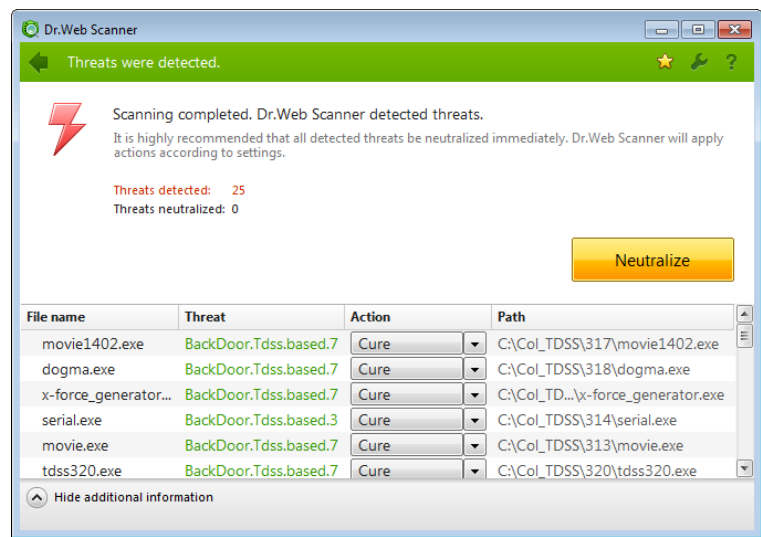
Custom scan mode allows you to select objects for scanning: any folders and files, and such objects as random access memory, autorun objects, boot sectors, etc. To start scanning selected objects, click **Start scanning**.





4.2. Neutralizing Detected Threats

By default, if a known virus or a suspicious object is detected, **Scanner** informs you about it.



To select an action:

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



Suspicious objects are moved to **Quarantine** and should be sent for analysis to the anti-virus laboratory of **Doctor Web**. To send the files, right-click anywhere in the **Quarantine** windows and select **Submit file(s) to Doctor Web Laboratory**.

There are some limitations:



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

The detailed report on the program's operation is saved in dwscanner.log file that resides in the %allusersprofile%\Application Data\Doctor Web\Logs\ folder (in Windows 7, %allusersprofile%\Doctor Web\Logs\).



4.3. Scanner Settings



It is recommended for **Scanner** to be run by a user with administrator privileges because files to which unprivileged users have no access (including system folders) are not scanned.

Default program settings are optimal for most applications and they should not be modified, if there is no special need for it.

To configure Scanner:

1. To open **Scanner** settings, click the **Settings**  icon on the toolbar. This opens the **Dr.Web Scanner settings** window which contains several tabs.
2. Make the necessary changes.
3. For more detailed information on the settings specified in each tab use the **Help**  button.
4. When editing is finished click **OK** to save the changes made or **Cancel** to cancel the changes.

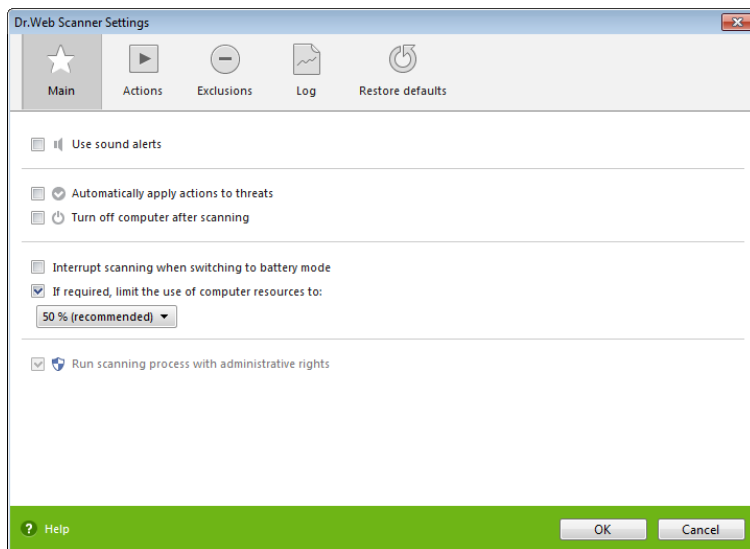


Main Page

On this tab you can set general parameters of **Scanner** operation.

You can enable sound notifications on particular events, set **Scanner** to apply recommended actions to detected threats automatically, and configure **Scanner** interaction with the operating system.

It is recommended to run **Scanner** under an account with administrative privileges. Otherwise, all folders and files that are not accessible to unprivileged user including system folder are not scanned. To run **Scanner** under an administrative account, select the **Run scanning process with administrative rights** checkbox.

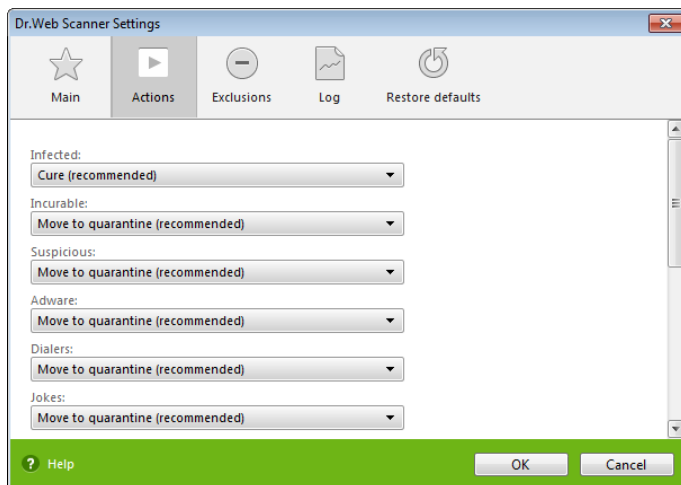




Actions Page

To set reaction on threat detection:

1. Select the **Actions** tab in the **Scanner settings** window.



2. In the **Infected objects** drop-down list, select the program's action upon detection of an infected object.
3. Select the program's action upon detection of an incurable object in the **Incurable objects** drop-down list. The range of actions is the same as those described above but the **Cure** action is not available.



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

4. In the **Suspicious objects** drop-down list select the program's action 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

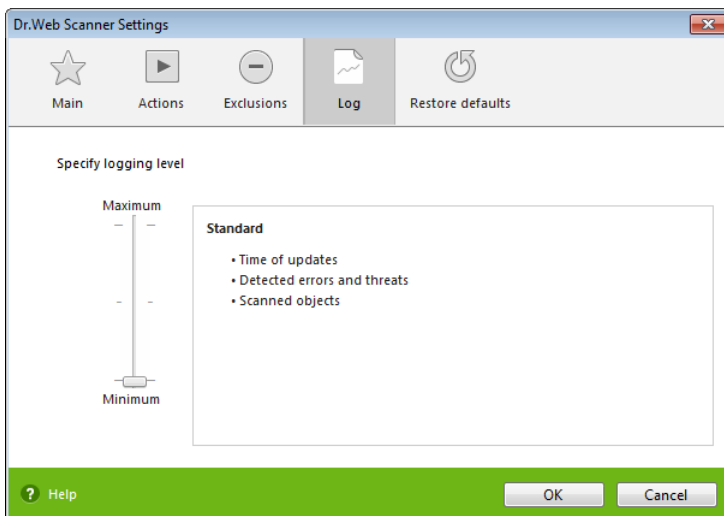


detection of viruses or suspicious codes in file archives, containers and mailboxes, applied to these objects as a whole, are set up.

7. To cure some infected files it is necessary to reboot Windows. You can choose one of the following:
 - **Restart computer automatically.** It can lead to loss of unsaved data.
 - **Prompt restart**

Log Page

In the **Log** page you can set up the parameters of the log file.



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



4.4. 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:

Enter a command in the following format:

```
[<path_to_program>]drweb32w [<objects>] [<switches>]
```

The list of objects for scanning can be empty or contain several elements separated with blanks.

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

- **/FAST** perform an express scan of the system (for more information on the express scan mode see [Scan Modes](#)).
- **/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, boot sectors of all disks and startup objects.

Switches are command line parameters that specify program settings. If no switches are defined, scanning is performed with the settings specified earlier (or with the default settings if you have not changed them).

Each switch begins with a forward slash (/) character and is separated with a blank from other switches.



4.5. Console Scanner

Dr.Web Anti-virus also includes **Console Scanner** that provides advanced settings.



Console Scanner moves suspicious files not to **Quarantine**.

To run Console Scanner:

Enter the following command:

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

The list of objects for scanning can be empty or contain several elements separated with blanks.

Switches are command line parameters that specify program settings. Several parameters are divided by spaces. For the full list of available switches, refer to [Appendix A](#).

Return codes:

- 0 – Scanning was completed successfully, infected objects were not found
- 1 – Scanning was completed successfully, infected objects were detected
- 10 – Invalid keys are specified
- 11 – Key file is not found or does not license **Console Scanner**
- 12 – **Scanning Engine** did not start
- 255 – Scanning was aborted by user



5. SpIDer Guard

By default, **SpIDer Guard** is loaded automatically at every Windows startup and cannot be unloaded during the current Windows session. If necessary, you can [temporarily disable SpIDer Guard](#) (for example, when a task consuming too much processor resources is performed in real time mode).



Only the user with administrator rights can temporarily disable **SpIDer Guard**.

By default, **SpIDer Guard** performs on-access scanning of files that are being created or changed on the HDD and all files that are opened on removable media. It scans these files in the same way as the **Scanner** but with "milder" options. Besides, **SpIDer Guard** constantly monitors running processes for virus-like activity and, if they are detected, blocks these processes.

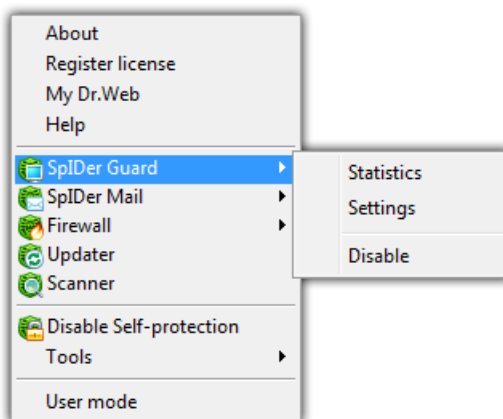
By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web Anti-virus** acts according to actions set on the [Actions tab](#).

You can set the program's reaction to virus events by adjusting the corresponding settings. A user can control it with the help of the **Statistics** window and the log file.



5.1. Managing SpIDer Guard

Main tools for setting and managing in **SpIDer Guard** reside in its menu.



The **Statistics** menu item allows to open the **Statistics** window, where the information on the operation of **SpIDer Guard** during the current session is displayed (the number of scanned, infected or suspicious objects, virus-like activities and actions taken).

The **Settings** menu item gives access to the main part of the program parameters (for details, see [SpIDer Guard Settings](#)).

The **Disable** item allows to temporary disable program functions (for users with administrator rights only).




Access to the **SpIDer Guard** settings is possible only for the user with administrator rights.

To disable **SpIDer Guard**, enter confirmation code.



5.2. SpIDer Guard Settings

The main adjustable parameters of **SpIDer Guard** are in the **Settings** panel. To receive help on parameters specified on a page, select that page and click **Help** .

When you finish editing the parameters click **OK** to save changes or **Cancel** to cancel the changes made.

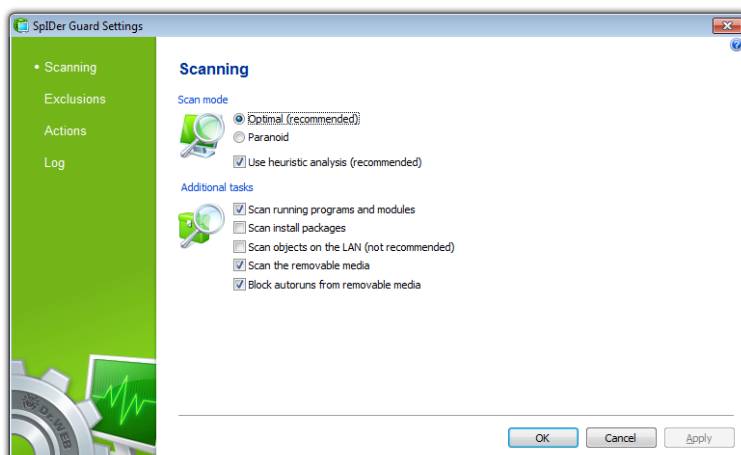
Some of the most frequently changed settings of the program are described below.

Scanning Page

By default, **SpIDer Guard** is set in **Optimal** mode to scan files that are being executed, created or changed on the hard drives and all files that are opened on removable media.

In **Paranoid** mode **SpIDer Guard** scans files that are being opened, created or changed on the hard drives, on removable media and network drives.

Selecting the **Use heuristic analysis** checkbox enables the heuristic analyser mode (a method of virus detection based on the analysis of actions specific for viruses).



Certain external devices (e.g. mobile drives with USB interface) can be identified by the system as hard drives. That is why such devices should be used with utmost care and checked for viruses by the **Scanner** when connected to a computer.

Disabled scanning of archives, even if **SpIDer Guard** is constantly active, means that viruses can still easily penetrate a PC but their detection will be postponed. When the infected archive is unpacked (or an infected message is opened), an attempt to write the infected object on the hard drive will be taken and **SpIDer Guard** will inevitably detect it.

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

- Executables of running processes regardless of their location
- Installation files
- Files on network drives
- Files and boot sectors on removable devices

These parameters are applied in any scan mode.

Also you can select **Block autoruns from removable media** check-



box to disable autoplay option for portable data storages such as CD/DVD, flash memory etc. 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 remove **Block autoruns from removable media** flag.

Exclusions Page

On this page folders and files to be excluded from checking are specified.

In the **Excluded folders and files** field the list of folders and files to be excluded from scanning can be set. These can be the quarantine folder of the anti-virus, some program folders, temporary files (swap files), etc.

To add a file, folder or mask to the list type its name into the entry field and click **Add**. To enter an existing file name or folder you can click **Browse** to the right and select the object in a standard file browsing window.

To remove a file or folder from the list select it in the list and click **Remove**.

Actions Page

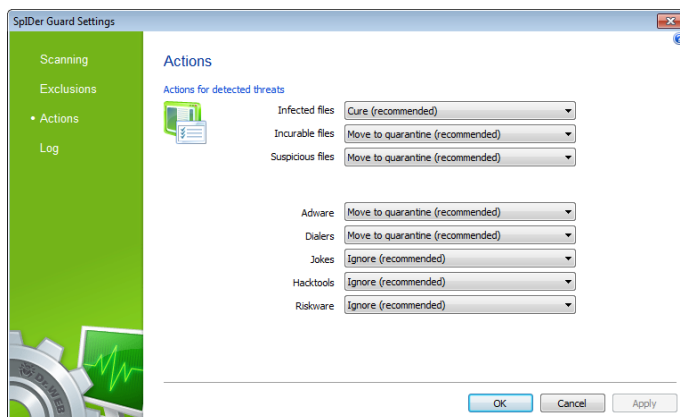
On this page you can adjust **SpIDer Guard** reaction to infected objects.

The **Cure**, **Ignore**, **Delete** and **Move to quarantine** actions are similar to those of the **Scanner**. All actions with files are described in [Appendix B. Computer Threats and Neutralization Methods](#) chapter.



To change the default actions in SpIDer Guard:

1. In the **SpIDer Guard Settings** window select the **Actions** tab.



2. In the **Infected objects** drop-down list choose the program's action upon detection of an infected object. **Cure** action is recommended.
3. In the **Incurable objects** drop-down list choose the program's action upon detection of an incurable object. **Move to quarantine** action is recommended.
4. In the **Suspicious objects** drop-down list choose the program's action upon detection of a suspicious object. **Move to quarantine** action is recommended.
5. In the **Adware** and **Dialers** drop-down lists choose the program's action upon detection of dangerous files. **Move to quarantine** action is recommended.
6. The same procedure is used when setting the program's actions upon detection of objects containing jokes, riskware and hacktools. **Ignore** action is recommended.
7. Click **OK** to apply changes and close the **SpIDer Guard Settings** window.



Log Page

On this page, you can select the mode of keeping records in the log file:

- **Standard** – in this mode, **SpIDer Guard** logs the following most important actions only:
 - Time of updates
 - Time of **SpIDer Guard** starts and stops
 - Detected errors and infections
- **Extended** – in this mode, **SpIDer Guard** logs the most important actions and the following additional data:
 - Names of scanned objects
 - Names of packers
 - Contents of scanned complex objects (archives, mail boxes and file containers)

It is recommended to use this mode when determining objects that **SpIDer Guard** checks most often.

- **Debugging** – in this mode, **SpIDer Guard** logs all details on its activity. This may result in considerable log growth.

The **SpIDer Guard** log is stored in the spiderg3.log file that is located in folder %allusersprofile%\Application Data\Doctor Web\Logs\ (for Windows 7, %allusersprofile%\Doctor Web\Logs). It is recommended to analyze the log file periodically.



6. SpIDer Mail

By default, **SpIDer Mail for Windows** is included into the set of installed components, constantly resides in the memory and automatically reloads at Windows startup. You can disable the automatic launch mode in [SpIDer Agent settings](#).

By default, the program automatically intercepts all calls of any mail programs on your computer to POP3 servers on port 110, to SMTP servers on port 25, to IMAP4 servers on port 143 and to NNTP servers on port 119.

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

By default, the program's reaction upon detection of infected incoming messages, as well as messages that were not scanned (e.g. due to their complicated structure) is as follows:

- Messages infected with a virus are not delivered; the mail program receives an instructions to delete this message; the server receives a notification that the message had been received (this action is called *deletion* of the message).
- Messages with suspicious objects are moved to the quarantine folder as separate files; the mail program receives a notification about this (this action is called *moving* the message).
- Messages that were not scanned and safe messages are passed on.
- All deleted or moved messages are also deleted from the POP3 or IMAP4 server.

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



If an unknown virus distributing through e-mail is detected on the computer, the program can detect signs of a typical "behavior" for such viruses (mass distribution). By default, this option is enabled.

The default program settings are optimal for a beginner, provide maximum protection level and require minimum user interference. But some options of mail programs are blocked (for example, sending a message to many addresses might be considered as mass distribution and mail will not be scanned for spam), useful information (from their safe text part) becomes unavailable if messages are automatically destroyed. Advanced users can modify mail scanning parameters and the program's reactions to virus events.

In certain cases automatic interception of POP3, SMTP, IMAP4 and NNTP connections is impossible; in such situation the program allows to set up manual interception of connections.

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

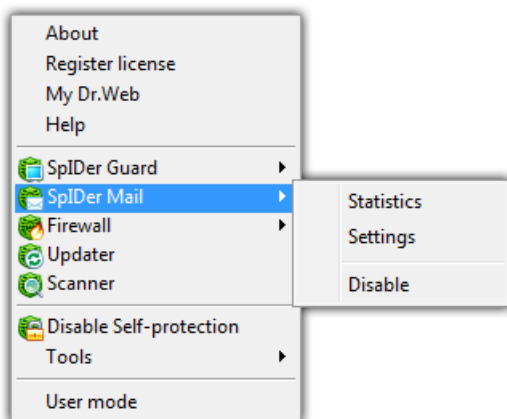
- Not all formats of popular mailboxes are supported by **Dr.Web Scanner**. In this case, when using **SpIDer Mail**, the infected messages are not even delivered to mailboxes.
- The **Scanner** does not check the mailboxes at the moment of the mail receipt, but either on user demand or according to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

Thus, with all the components in their default settings, **SpIDer Mail** detects viruses and suspicious objects distributed via e-mail first and does not let them infiltrate into your computer. Its operation is rather resource-sparing; scanning of e-mail files can be performed without other components.



6.1. Managing SpIDer Mail

SpIDer Mail can be managed via the **SpIDer Mail** item in the context menu of the **SpIDer Agent** icon (see [SpIDer Agent](#)).



If the **Settings** menu item is selected, a window with **SpIDer Mail** settings will open (read [Adjusting Certain Program Settings](#)).



User should have administrator rights to change settings of the **SpIDer Mail** interface.


If the **Statistics** menu item is selected, a window with information on the program's operation during current session (the number of scanned, infected, suspicious objects and taken actions) will open.

The **Disable/Enable** item allows to start/stop **SpIDer Mail**.



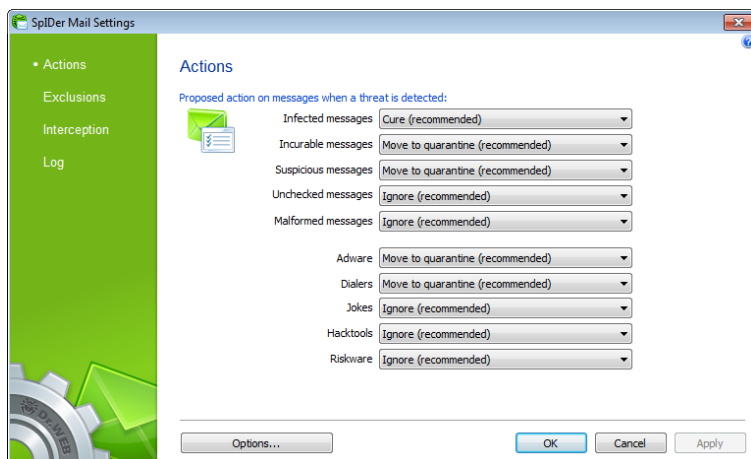
6.2. SpIDer Mail Settings

To modify **SpIDer Mail** settings open the settings window as described in [Managing SpIDer Mail](#).

When editing the settings, use the program's help system (general help for each page is generated by pressing the Help  button; there is also a context prompt for certain elements of the interface).

When adjusting is finished, click **OK**.

Most default settings are optimal for the majority of situations. The most frequently used parameters, except the default ones are described below.





To configure default actions:

1. In the **Infected messages** drop-down list choose the program's action upon detection of an infected message (**Cure** action is recommended).
2. In the **Incurable messages** drop-down list choose the program's action upon detection of an incurable message (**Move to quarantine** action is recommended). Other actions with moved files are described in [Neutralizing Detected Threats](#).
3. In the **Suspicious messages** drop-down list choose the program's action upon detection of a suspicious message. (**Move to quarantine** action is recommended).
4. In the **Non checked messages** and **Malformed messages** drop-down lists choose the program's action upon detection of a non-checked or malformed message. (**Ignore** action is recommended).
5. In the **Adware** and **Dialers** drop-down lists choose the program's action upon detection of adware and dilers. (**Move to quarantine** action is recommended).
6. The same procedure is used when setting the program's actions upon detection of messages containing jokes, riskware and hacktools. (**Ignore** action is recommended).
7. Click **OK** to apply changes and close the **SpIDer Mail Settings** window.



Protection against suspicious messages can be disabled if a PC is additionally protected by a constantly loaded **SpIDer Guard** component.

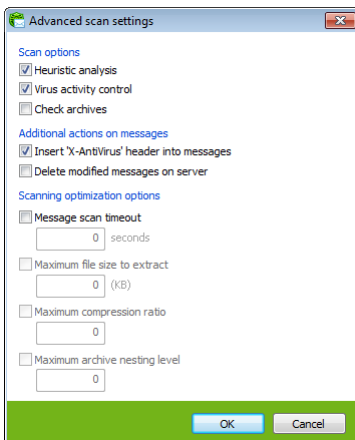
Additionally, you can increase the default level of reliability of anti-virus protection by selecting the **Move to quarantine** option in the **Not checked messages** drop-down list. Files with moved messages should be checked by the scanner.

Experienced users can disable the mode when the deleted or moved messages are immediately deleted from the POP3/IMAP4 server, and delete such messages manually or using more advanced settings of the mail program. For this, clear the **Delete modified messages on**



server check box in advanced settings.

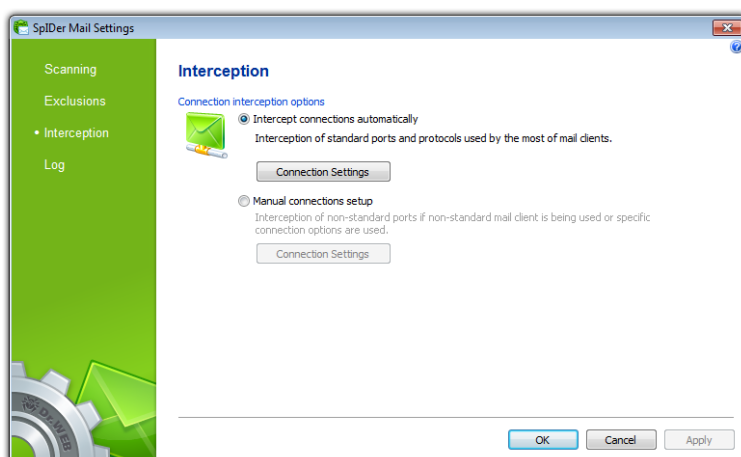
To get access to advanced settings, click **Options**



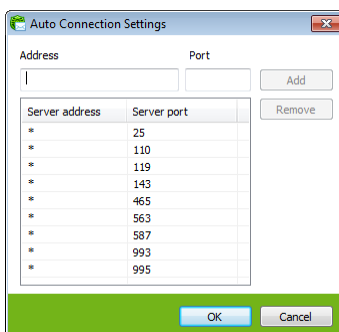
Interception Page

By default, **SpIDer Mail** automatically intercepts e-mail traffic of all user applications on your computer. You can disable mail traffic scanning for certain programs on the **Exclusions** page. For this, add the necessary applications to the list of exclusions.

The interception parameters of connections are set up on the **Interception** page.



By default, interception is carried out automatically. The list of intercepted addresses can be viewed in an additional window. To open it, click **Parameters**.



By default, the list of automatically intercepted messages includes all IP addresses (specified by the asterisk * symbol) and the following ports: 143 (standard IMAP4 port), 119 (standard NNTP port), 110 (standard POP3 port) and 25 (standard SMTP port).

To remove an element from the list, select it and click **Remove**.

To add a server or a group of servers to the list, specify its address (IP



address or domain name) in the **Address** field and the called port number into the **Port** field and click **Add**.



The **localhost** address is not intercepted if the asterisk (*) is specified. If necessary, this address should be specified in the interception list explicitly.

To set up manual interception

1. On the **Interception** page, select **Manual connections setup** and click **Parameters**. A window for setting up manual connections opens.

The dialog box titled "Manual connections settings" contains a table with three columns: "SpIDer Mail port", "Server address", and "Server port". The first row has the value "7000" in the "SpIDer Mail port" column. To the right of the table are "Add" and "Remove" buttons. At the bottom of the dialog are "OK" and "Cancel" buttons.

SpIDer Mail port	Server address	Server port
7000		

2. Make up a list of resources (POP3/SMTP/IMAP4/NNTP servers) connections to which should be intercepted. Number them one after another starting from 7000. Hereinafter these numbers will be called **SpIDer Mail ports**.
3. For every resource input the appropriate number into the **SpIDer Mail** port entry field, a domain name or IP address of the server into the **Server address** entry field and the port number to which a connection is made into the **Server port** entry field and click **Add**.
4. Repeat these actions for each resource.
5. Click **OK**.



In the settings of the mail client, instead of the address and port of POP3/SMTP/IMAP4/NNTP server, specify the address localhost: port_SpIDer_Mail, where port_SpIDer_Mail is the address assigned to an appropriate POP3/SMTP/IMAP4/NNTP server.

Secure Connections

You can enable scanning of data transmitted via secure protocols such as POP3S, SMTPS, or IMAPS. To check such data, select the **Check encrypted traffic (POP3S/SMTPS/IMAPS)** checkbox under **Secure Connections**. If your client application (a mail client) that uses secure connections does not refer to the default Windows system certificate storage, then you need to [export](#) Doctor Web SSL certificate.

Log Page

On this page, you can select the mode of keeping records in the log file:

- **Standard** – (Suitable for most cases) in this mode, **SpIDer Mail** logs the following most important actions only:
 - Time of updates
 - Time of **SpIDer Mail** starts and stops
 - Detected errors and infections
- **Extended** – in this mode, **SpIDer Mail** logs the most important actions and the following additional data:
 - Mail interception parameters
 - Names of scanned objects
 - Names of packers
 - Contents of scanned complex objects (archives, mail boxes and file containers)
- **Debugging** – in this mode, **SpIDer Mail** logs all details on its activity. This may result in considerable log growth and reduce system performance.



The **SpIDer Mail** log is stored in the netfilter.log file that is located in folder %allusersprofile%\Application Data\Doctor Web\Logs\ (for Windows 7, %allusersprofile%\Doctor Web\Logs\). It is recommended to analyze the log file periodically.



7. Dr.Web for Outlook

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

- Anti-virus check of e-mail attachments transferred via SMTP, POP3 and HTTP protocols.
- Check of e-mail attachments transferred via SSL encrypted connections.
- Detection and neutralizing of malicious objects.
- Malware detection.
- Heuristic analysis for additional protection against unknown viruses.

7.1. Configuring Dr.Web for Outlook

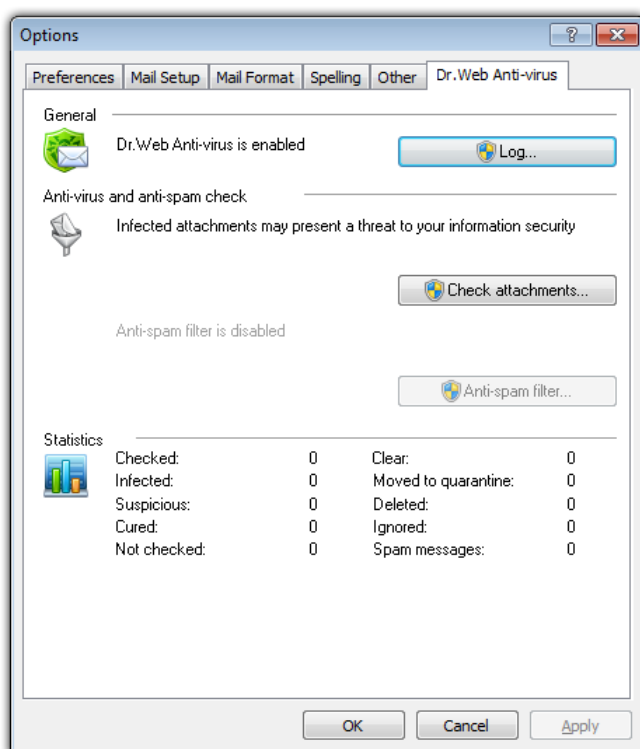
You can configure **Dr.Web for Outlook** plug-in operation and review statistics at the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (for Microsoft Outlook 2007, in the **Tools** → **Options** → **Dr.Web Anti-virus** tab).



The **Dr.Web Anti-virus** tab of Microsoft Outlook parameters are active only if user has permissions to change these settings.

On **Dr.Web Anti-Virus** tab, the current protection status is displayed (enabled/disabled) and it provided the access to the following program functions:

- [Log](#) – allows to configure the program logging.
- [Check attachments](#) – allows to configure the e-mails check and to specify the program actions for the detected malicious objects.
- [Statistics](#) – allows to review the number of checked and processed objects.





7.2. Treat Detection

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

7.2.1. Types of Threats

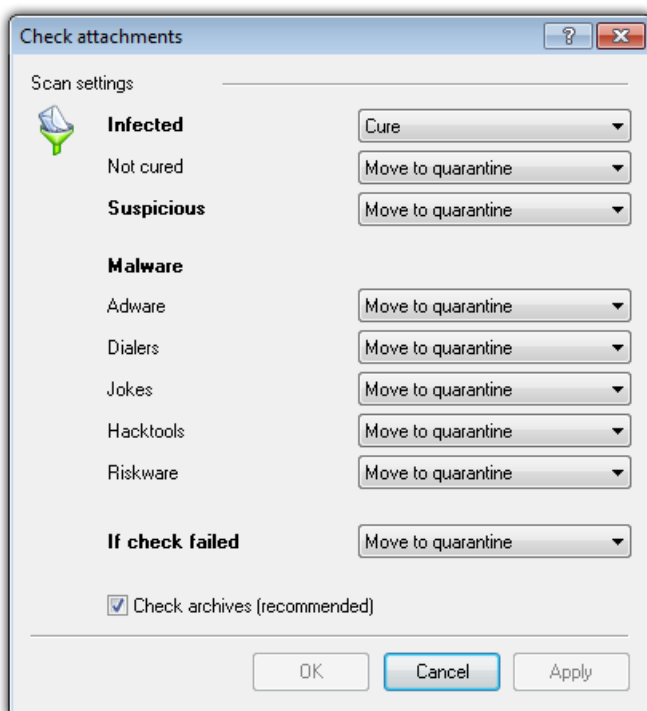
Dr.Web for Outlook detects the following computer security threats in the mail:

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

7.2.2. Configuring Actions

Dr.Web for Outlook allows to specify reaction to detection of infected or suspicious files and malicious objects during e-mail attachments check.

To configure the virus check of e-mail attachments and to specify the program actions for the detected malicious objects, in the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (in the **Tools** → **Options** → **Dr.Web Anti-virus** tab for Microsoft Outlook 2007), click **Check attachments**.



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

To set actions on virus threats detection, use the following options:

- The **Infected** drop-down list sets the reaction to the detection of a file infected with a known 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 a reaction of the heuristic analyzer).



- In the **Malware** section, set the reaction to the detection of types of unsolicited software such as:
 - Dialers
 - Jokes
 - Riskware
 - Hakctools
- The **If checked failed** drop-down list allows to configure actions, if attachment can not be checked, e.g. if attached file is corrupted or password protected.
- The **Check archives (recommended)** flag allows to enable or disable checking of attached archived files. Set this flag, to enable checking, clear – to disable.

For different types of objects, actions are assigned separately.

The following actions for detected virus threats are provided:

- **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.



7.4. Logging

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

- [Windows Event Log](#)
- [Text Dr.Web debug log](#)

7.4.1. Event Log

Dr.Web for Outlook registers the following information in the Windows Event Log:

- Plug-in starts and stops.
- License key file parameters: license validation, license expiration date (information is written during program launch, during program operating and when key file is changed).
- License errors: the key file is absent, permissions for usage of program modules is absent in the key file, licence is blocked, the key file is corrupted (information is written during program launch and during program operating).
- Parameters of program modules: Scanner, engine, virus bases (information is written during program launch and modules update).
- Information on threats detection.
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration).

To view Event Log:

1. On the **Control Panel**, select **Administrative Tools** → **Event Viewer**.
2. In the tree view, select **Application**. The list of events, registered in the log by user applications, will be opened. The source of **Dr.Web for Outlook** messages is the **Dr.Web for Outlook** application.



7.4.2. Debug Text Log

The following information can be registered in the **Dr.Web for Outlook** text log:

- License validity status
- Malware detection reports per each detected malicious object
- Read-write errors or errors while scanning for archives or password-protected files
- parameters of program modules: **Scanner**, engine, **Dr.Web virus databases**
- Core failures
- License expiration notifications (A message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)



Enabling the program logging in the Log file decreases server performance, therefore it is recommended to enable logging only in case of errors occurrence in operation of **Dr.Web for Outlook**.

To configure logging:

1. On **Dr.Web Anti-virus** tab, click **Log**. The window of log settings will open.
2. Specify the detailing level (0 - 5) for logging:
 - level **0** corresponds to disable logging
 - level **5** means the maximum level of details for the program logging

By default, logging is disabled.

3. Specify the maximum log file size (in kilobytes).
4. Click **OK** to save changes.

To view program log:

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



7.5. Statistics

In the Microsoft Outlook mail application, in the **Service** → **Parameters** → **Dr.Web Anti-virus** tab (in the **Tools** → **Options** → **Dr.Web Anti-virus** tab for Microsoft Outlook 2007), statistic information about total number of objects, which have been checked and treated 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 can not be checked or error has occurred during scan.
- **Clear** – number of messages, which are not infected.

Then the number of the following categories of treated objects is specified:

- **Moved to quarantine** – number of objects, which have been moved to [Quarantine](#).
- **Deleted** – number of objects, deleted from the system.
- **Skipped** – number of objects, skipped without changes.

By default, statistics file is `drwebforoutlook.stat` file that is located in the `%USERPROFILE%\DoctorWeb` folder (for Windows 7, `C:\Users\<username>\DoctorWeb`). To clear statistics, delete this file.



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



8. Dr.Web Firewall

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

Main Features

Dr.Web Firewall provides you with the following features:

- Control and filtration of all incoming and outgoing traffic
- Access control on application level
- Network level packet filtering
- Fast selection of rule sets
- Event logging

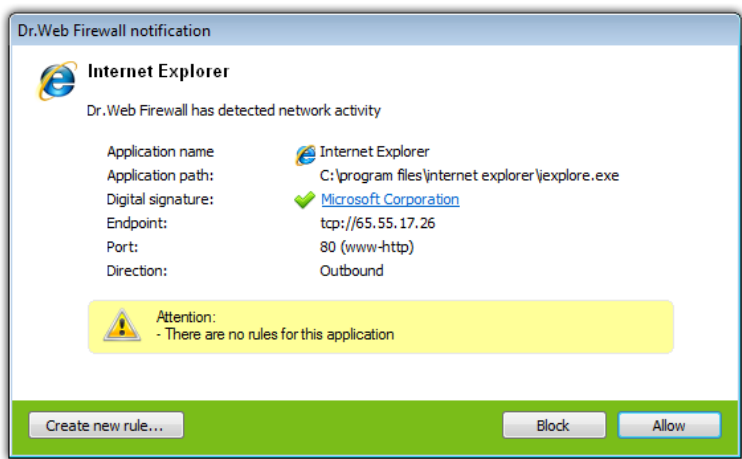
8.1. Training Dr.Web Firewall

By default, once installation completes **Dr.Web Firewall** starts learning usual behaviour 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 **Dr.Web Firewall** detects this type of connection.



When running under limited user account (Guest) **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.



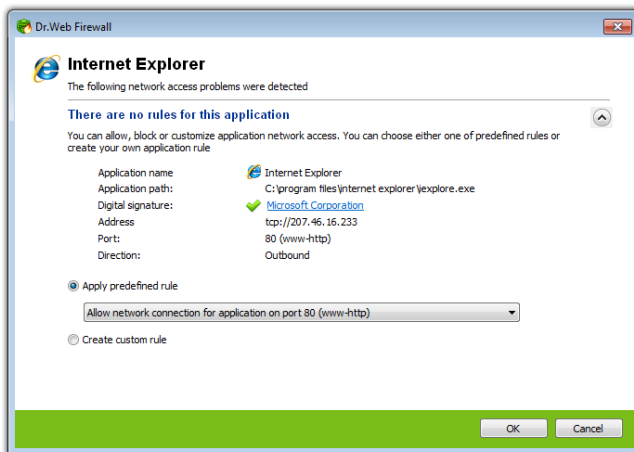
To process connection attempts

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

Information	Description
Application name	The name of the application. Ensure that the Path to the application executable file corresponds to its usual location.
Application path	The full path to the application executable file and its name.
Digital signature	Digital signature of the application.
Endpoint	The protocol used and the network address the application is trying to connect to.
Port	The network ports used for the connection attempt.
Direction	Connection type.

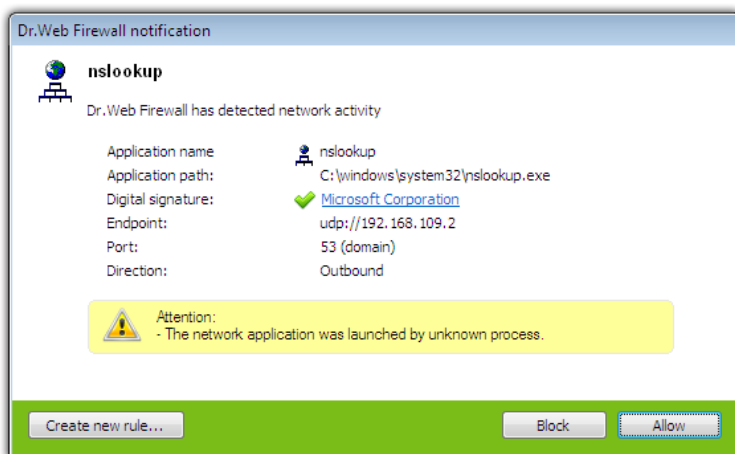


2. Once you make a decision, select an appropriate action:
 - To block this connection once, select **Block**
 - To allow this connection once, select **Allow**
 - To open a window where you can create a new application filter rule, select **Create new rule**. In the opened window you can either choose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



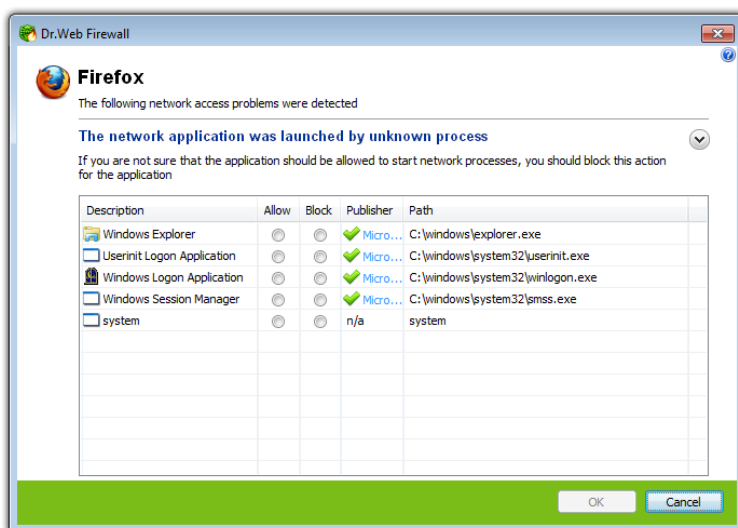
3. Click **OK**. **Dr.Web Firewall** executes the selected action and closes the notification window.

In cases when connection was initiated by a trusted application (an application with existing rules), but this application was run by an unknown parent process, a corresponding notification will be prompted:



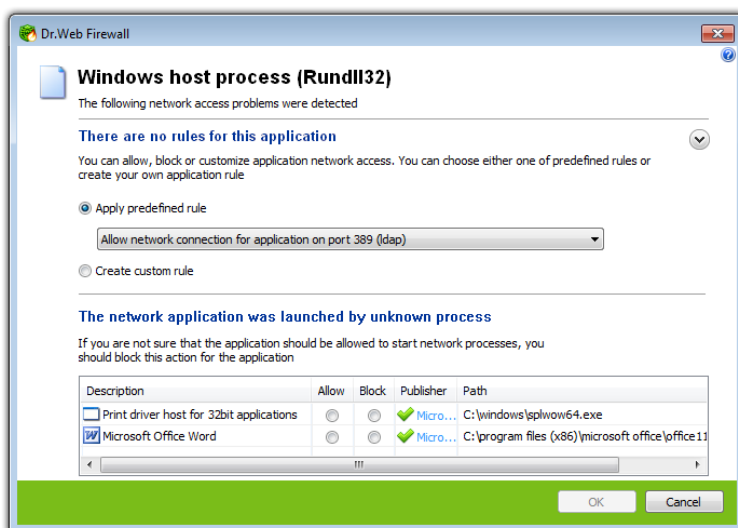
To set parent processes rules

1. Consider the information about parent process displayed in the notification.
 - To block this connection once, select **Block**
 - To allow this connection once, select **Allow**
 - To open a window where you can create a new application filter rule, select **Create new rule**. In the opened window you can either choose one of the predefined rules or create your rule for parent process.



2. Click **OK**. **Dr.Web Firewall** executes the selected action and closes the notification window.

When unknown process was run by another unknown process, a notification will display corresponding details. If you click **Create new rule**, the new window will appear, allowing you to create new rules for this application and its parent process:



You need administrative rights to create rules.

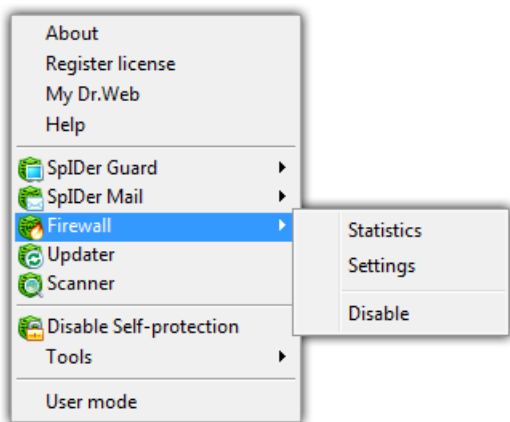
8.2. Managing Dr.Web Firewall

Dr.Web Firewall installs as a network component and loads on Windows startup. If necessary, you can suspend **Dr.Web Firewall** operation, review its statistics, or change settings.




After a session under 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.

You can configure and manage **Dr.Web Firewall** using **SpIDer Agent**.



To manage Dr.Web Firewall

- 1. Right-click the **SpIDer Agent** icon .
- 2. Select **Firewall**, then select a required item:

Item	Select to
Statistics	Display information on events which Dr.Web Firewall handled.
Settings	Access adjustable Dr.Web Firewall settings. On the Restore Defaults page you can restore all settings to their default values.
Disable	Suspend Dr.Web Firewall operation. This operation is available for users with administrative privileges only.
Enable	Resume Dr.Web Firewall operation. This item is available when Dr.Web Firewall is disabled only.



To disable **Dr.Web Firewall**, enter confirmation code.

Settings and **Disable/Enable** items are not available in **User mode**.



8.3. Firewall settings



You need administrative rights to access **Dr.Web Firewall** settings.

To start using **Dr.Web Firewall**, do the following:

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

Dr.Web Firewall loads on Windows startup and starts [logging](#) events. By default, **Dr.Web Firewall** operates in [learning](#) mode.



If any problems occur with Internet Connection Sharing (i.e. access to the Internet is blocked for computers that are connected to a host computer), on the host computer specify [packet filter rule](#) that allows all packets from the subnet, according to your local configuration.

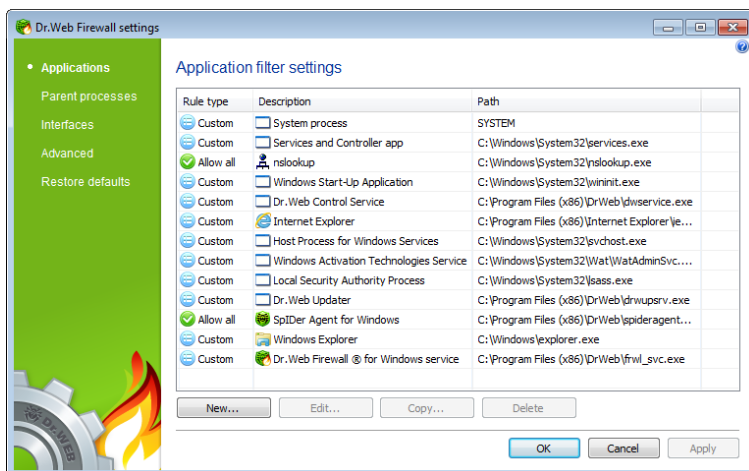
8.3.1. Application Filter

Application level filtering helps you control access of various application and processes to network resources. You can create rules for both system and user applications.

The **Application filter settings** page lists all applications and processes for which there is an [application filter rule set](#). Each application is explicitly identified by the path to its executable file. **Dr.Web 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).



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



To configure rule sets

In the **Dr.Web Firewall** settings window, select the **Applications** page and do one of the following:

- to add a new set of rules, click **New**.
- to edit an existing set of rules, select the rule set in the list and click **Edit**.
- to add a copy of existing set of rules, select the rule set and click **Copy**. The copy is added after the selected rule set.
- to delete all rules for an application, select the appropriate rule set and click **Delete**.



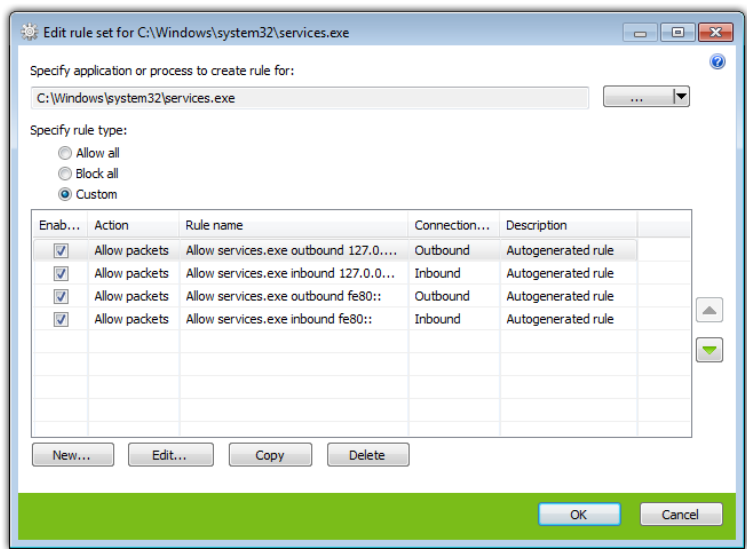
If the application file, for which the rule was created, changes (e.g., due to update installation) then **Dr.Web Firewall** asks to confirm that the application is still allowed to access network resources.

Application Rules

The **New application rule set** (or **Edit rule set**) window lists types of the filtering rule for application or process, and also a rule set, if the **Custom** type is selected. You can change rule type, configure the list



by adding new rules for the application 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:

Column	Description
Enabled	Execution states for the rule.
Action	The action for Dr.Web Firewall to perform when the connection attempt is detected: <ul style="list-style-type: none">• Block packets• Allow packets
Rule name	The rule name.
Connection type	The party which initiates the connection: <ul style="list-style-type: none">• Inbound – the rule is applied when someone from the network attempts to connect to the application on your computer.



Column	Description
	<ul style="list-style-type: none">• Outbound – the rule is applied when the application on your computer attempt to connect to the network.• Any – the rule is applied regardless of who initiate the connection.
Description	The rule description.

To configure rules

1. If you select to create a new or edit an existing set of application filter rules on the **Application filter settings** page, in the opened window specify the application for which you want the rules to apply:
 - To add a set of rules for a user program, click the **Select**  button and select the application executable file.
 - To add a set of rules for a process, click arrow on the **Select**  button, choose **running application** and select the process.
2. Specify rule type:
 - **Allow all** – all connections will be allowed;
 - **Block all** – all connections will be blocked;
 - **Custom** – in this mode you can create a set of rules, that will allow or block different connections.
3. If you chose **Custom** type, create filtering rules using the following options:
 - To add a new rule, click **New**. The new rules is added to the end of the list.
 - To modify a rule, select it and click **Edit**.
 - To add a copy of a rule, select the rule and click **Copy**. The copy is added after the selected rule.
 - To delete a rule, select it and click **Delete**.
4. If you selected to create or edit a rule, [configure rule settings](#) in the opened window.
5. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.



- When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Rule Settings

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

Edit rule DrWEB Firewall Settings Application/http

General

Rule name: DrWEB Firewall Settings Application/http

Description: Allows to connect to CRL distribution points via http. This is used to verify securit

State: Enabled Connection type: Outbound

Action: Allow packets

Rule settings

Outbound address: Any Outbound port: Equal 80 www-http

TCP

OK Cancel

To add or edit a rule:

- Configure the following parameters:

Parameter	Description
General	
Rule name	The rule name.
Description	The rule description.
State	One of the following execution states for the rule: <ul style="list-style-type: none">Enabled – apply rule for all matching connection attempts.



Parameter	Description
	<ul style="list-style-type: none">• Disabled – do not apply the rule yet.
Connection type	<p>The party which initiates the connection:</p> <ul style="list-style-type: none">• Inbound – apply the rule when someone from the network attempts to connect to the application on your computer.• Outbound – apply the rule when the application on your computer attempt to connect to the network.• Any – apply the rule regardless of who initiate the connection.
Action	<p>The action for Dr.Web Firewall to perform when the connection attempt is detected:</p> <ul style="list-style-type: none">• Block packets• Allow packets
Rule Settings	
Protocol	<p>The network and transport level protocols used for the connection attempt.</p> <p>Dr.Web Firewall supports the following network level protocols:</p> <ul style="list-style-type: none">• IPv4• IPv6• IP all – any version of IP protocol <p>Dr.Web Firewall supports the following transport level protocols:</p> <ul style="list-style-type: none">• TCP• UDP• TCP & UDP – TCP or UDP protocol

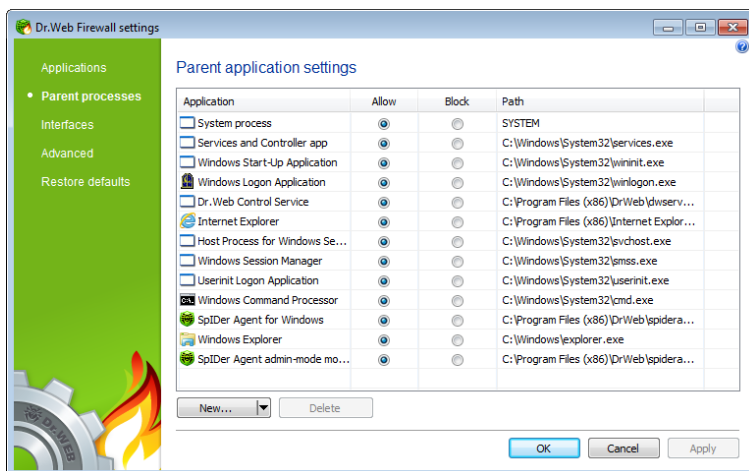


Parameter	Description
Inbound/Outbound address	<p>The IP address of the remote host. You can specify either a specific address (Equals) or several IP addresses using a range (In range), specific subnetwork mask (Mask), or masks of all subnetworks, in which your computer has network addresses (MY_NETWORK).</p> <p>To apply the rule for all remote hosts, select Any.</p>
Inbound/Outbound port	<p>The port used for 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>

2. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

8.3.2. Parent processes

To allow or forbid processes or applications to run other applications you have to set up appropriate rules on **Parent processes** page.



To add rule for parent process

1. Choose parent process:
 - To add new rule for an application click **New** and browse for program executable
 - To add new rule for an already running process click arrow on **New**, choose running application and select process
2. Set appropriate action:
 - **Block** to prevent application from running other processes
 - **Allow** to permit application to run other processes

New process is blocked by default.



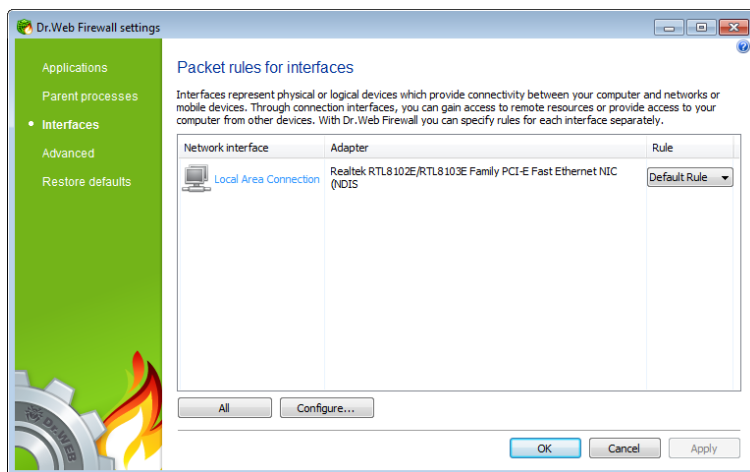
When there is a rule for a parent process and the executable for this parent process has been changed (e.g. after update), then **Firewall** prompts you to reconfirm the rule and approve further launched of applications by this parent process.



8.3.3. Network Interfaces

On the **Interfaces** page you can select a rule set to use for filtering packets transmitted through different network interfaces.

On the **Packet rules for interfaces** page, you can select a packet filtering ruleset to use for each network interface installed on your computer.



To define rule sets for network interfaces:

1. In the **Dr.Web Firewall** settings window, select **Interfaces**.
2. For an interface of interest, select the appropriate ruleset. If the ruleset does not exist, you can [create](#) a new set of packet filtering rules.
3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.

To list all available interfaces, click **All**. This opens a windows where you can selected interfaces that should be listed in the table permanently. Active interfaces are listed in the table automatically.

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



Packet Filter

Packet filtering allows you to control access to network regardless of which program initiates connection. **Dr.Web Firewall** applies these rules to network packets transmitted through [network interfaces](#) of your computer.

Packet filtering allows you to control access to networks on a lower level than the [application filter](#) thus providing you with more flexible options.

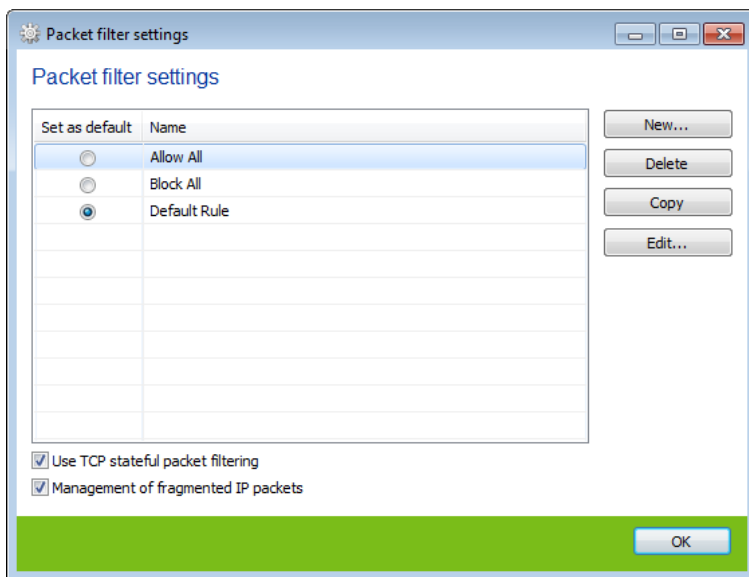
Dr.Web Firewall provides you the following default filtering rule sets:

- **Allow all** – this rule set configures **Dr.Web Firewall** to pass through all packets.
- **Deny all** – this rule set configures **Dr.Web Firewall** to block all packets.
- **Default rule** – this set includes rules describing the most popular system configurations and preventing common network attacks. This rule set is used by default for new [network interfaces](#).

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

To set rulesets for network interfaces:

1. In the **Dr.Web Firewall** settings window, select **Packet filter** page.
2. Do one of the following:
 - [Configure](#) sets of filtering rules by adding new rules, modifying or deleting existing ones, or changing order of their execution.
 - [Select](#) a default filtering rule.
 - [Configure](#) general filtering settings.



To configure sets of filtering rules:

Do one of the following:

- To add a new rule set, click **New**. The new rule set is added to the beginning of the list.
- To edit an existing set of rules, select the rule set in the list and click **Edit**.
- To add a copy of 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 set default rules:

In the list, select the ruleset you want to use for new network interfaces installed on your computer and click **Set as default**.

To configure general settings

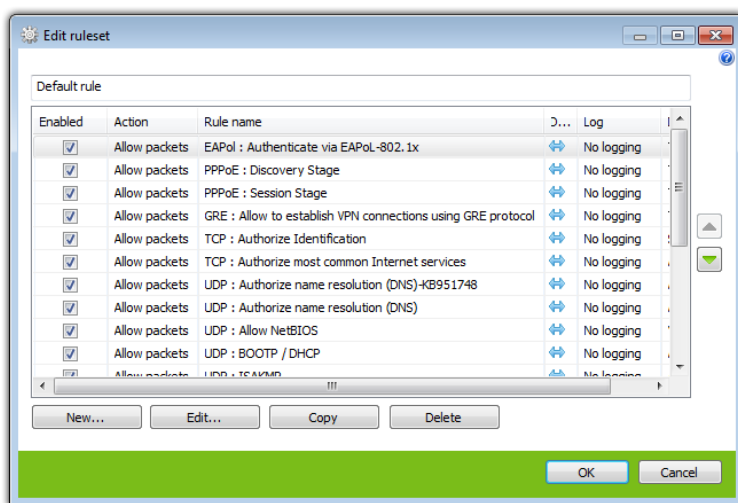
On the **Packet Filter settings**, use the following options:



Option	Description
Use TCP stateful packet filtering	<p>Select this checkbox to filter packets according to the state of existing TCP connections. Dr. Web 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.</p> <p>It is also recommended to enable stateful packet filtering when using complex data transfer protocols such as FTP, SIP, etc.</p> <p>Clear this checkbox to filter packets without regard to state of TCP sessions.</p>
Management of fragmented IP packets	<p>Select this checkbox 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 received fragmented. When this option is enabled, Dr.Web Firewall applies the rule selected for the first fragment of a large IP packet to all other fragments.</p> <p>Clear this checkbox to process fragmented packets independently.</p>

Packet Filter Rulesets

The **New packet ruleset** (or **Edit ruleset**) window lists packet filtering rules for the selected rule set. You can configure the list by adding new rules for the application 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:

Column	Description
Enabled	Execution states for the rule.
Action	The action for Dr.Web 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 packet sender: <ul style="list-style-type: none">• – the rule is applied when packet is received from the network.• – the rule is applied when packet is sent into the network from your computer.• – the rule is applied regardless of packet transfer direction.
Log	The logging mode for the rule. This parameter defines which information is stored in the Dr.Web Firewall log:



Column	Description
	<ul style="list-style-type: none">• Log headers – the packet header only.• Entire packet – the whole packet.• No logging - no information is logged.
Description	The rule description.

You can configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.

To configure rulesets

1. If you select to create or edit an existing rule set on the **Packet filtering settings** page, in the opened window, specify the name for the rule set.
2. Use the following options to create filtering rules:
 - to add a new rule, click **New**. The new rules is added to the beginning of the list.
 - to modify a rule, select it and click **Edit**.
 - to add a copy of a rule, select the rule and click **Copy**. The copy is added after the selected rule.
 - to delete a rule, select it and click **Delete**.
3. If you selected to create or edit a rule, [configure rule settings](#) in the opened 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.

Packet Filter Rules

To add or edit a rule:

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



Edit packet rule

Action:

Direction:

Rule name:

Description:

Logging:

OK Cancel

2. Configure the following parameters:

Parameter	Description
Action	The action for Dr.Web Firewall to perform when the packet is intercepted: <ul style="list-style-type: none">• Block packets• Allow packets
Direction	The packet sender: <ul style="list-style-type: none">• Inbound – apply the rule when packet is received from the network.• Outbound – apply the rule when packet is sent into the network from your computer.• Any – apply the rule regardless of packet transfer direction.
Packet header	Packet header. E.g. transport or network protocol.








Parameter	Description
Logging mode	The logging mode for the rule. This parameter defines which information is stored in the Dr.Web Firewall log: <ul style="list-style-type: none">• Log headers – log packet headers only.• Entire packet – log whole packets.• No logging – do not log any information.
Rule name	The rule name.
Description	The rule description.

3. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

To configure extended filtering parameters:

Use the following options:

- To add a new higher (or lower) level packet header, click the **Add**  button on the right (or left) of a packet header.
- To configure a field within the header, click the corresponding **Browse**  button.
- To remove a header or a field within a header, click the corresponding **Remove**  button.

The **Add**  and **Browse**  buttons are inactive, when the corresponding action is not available. For instance, when there is not criteria for filtering by header fields for the selected packet header, or filtering by higher (or lower) level headers is not possible.

Example:

Adding a packet filter that allows all packets from a sub-network, may look as follows:



Edit packet rule

Action:

Direction:

☐ Ethernet

☐ Local MAC

☐ IPv4

☐ Remote IP

Rule name:

Description:

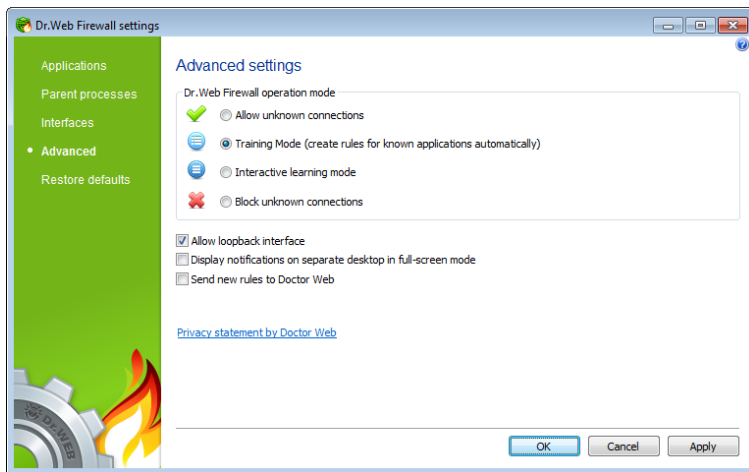
Logging:

If you do not specify any fields within the IPv4 header, then the rule will be passed for any packet that contains an IPv4 header and was sent from a physical address of the local computer.



8.3.4. Advanced settings

On the **Advanced settings** page, you can select a default action, which **Dr.Web Firewall** should execute when it detects a new (unknown to the firewall) connection attempt, and configure advanced settings. These rules are applied on the application level.



To set operation mode:

1. In the **Dr.Web Firewall** settings window, select **Mode**.
2. Select one of the following operation modes:
 - Interactive **learning mode**
 - (Default) **Training mode (create rules for known applications automatically)** – learning mode, when rules for known applications are created automatically
 - **Block unknown connections** – restricted access mode, when all unknown connections are blocked. For known connections, **Dr.Web Firewall** applies the appropriate rules
 - **Allow unknown connections** – free access mode, when all unknown applications are permitted to access networks



3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.

Learning Mode

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

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering rule set for the application. If there are no filtering rules, **Dr.Web Firewall** prompts you to select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

Training Mode

In this mode, rules for known applications are created automatically. For other applications you have control over **Dr.Web Firewall** reaction.

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering rule set for the application. If there are no filtering rules, **Dr.Web Firewall** prompts you to select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

This mode is used by default.

Restricted Access Mode

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

When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering ruleset for the



application. If there are no filtering rules, **Dr.Web Firewall** blocks network access for the application without displaying any notification to the user. If there are filtering rules for the application, **Dr.Web Firewall** processes the connection according to the specified actions.

Free Access Mode

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

To configure advanced settings:

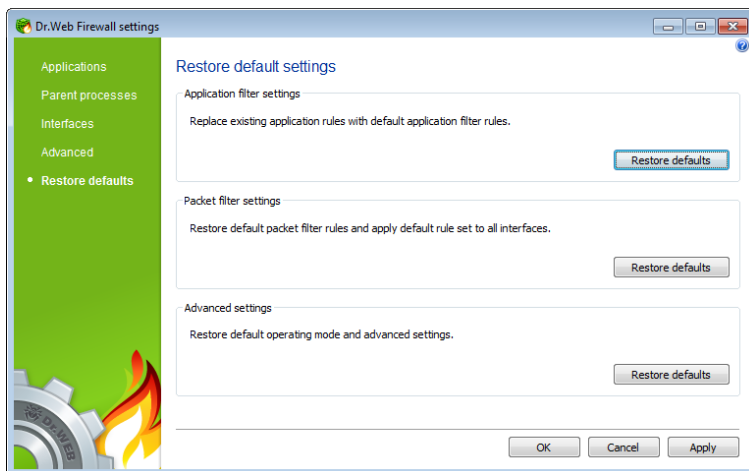
On the **Application filter settings** page, use the following option:

Option	Description
Allow loopback interface	<p>Select this checkbox 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 will be applied.</p> <p>Clear this checkbox to apply rules for connections carried out both through the network and within your computer.</p>
Display notifications in full-screen mode	<p>Select this checkbox to display notifications on a separate desktop when some application is running in full screen mode on your computer (a game or a movie).</p> <p>Clear this checkbox to display notification on the same desktop where an application is running in the full screen mode.</p>



8.3.5. Restoring Defaults

On the **Restore default settings** page, you can restore **Dr.Web Firewall** settings to their default values recommended by **Doctor Web**.



To restore default settings:

1. In the **Dr.Web Firewall** settings window, select **Restore defaults**.
2. Do one of the following:
 - To restore default application filter settings, in the **Application filter settings** section, click **Restore defaults**.
 - To restore default packet filter settings, in the **Packet filter settings** section, click **Restore defaults**.
 - To set the default **Dr.Web Firewall** operation mode, in the **Advanced settings** section, click **Restore defaults**.
3. Click **OK** to save changes, or click **Cancel** to close the window without saving changes.




8.4. Event Logging

Dr.Web Firewall registers connection attempts and network packets in the following logs:

- [Application Filter Log](#) (**Application journal**), which contains information on network connection attempts from various applications and rules applied to process each attempt.
- [Packet Filter Log](#) (**Packet Filter journal**), which contains information on network packets processed by **Firewall**, rules applied to process the packets, and network interfaces used to transmit the packets. Details level depends on settings of each packet application rule.

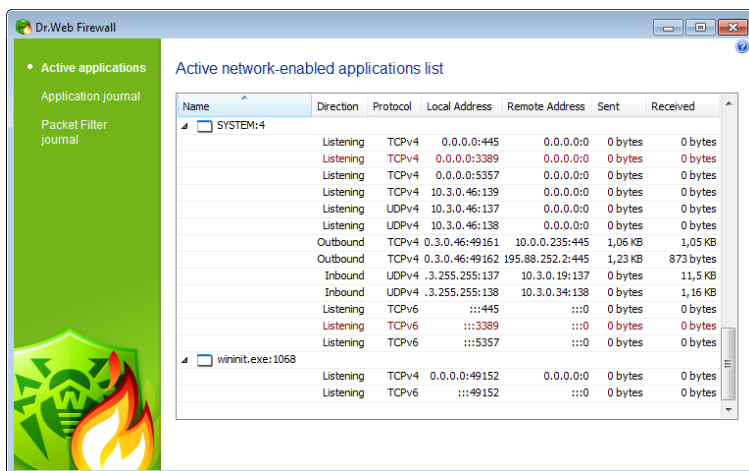
The **Active applications** page displays [applications](#) currently connected to a network.

To open logs:

1. Click the **SpIDer Agent** icon .
2. Select **Firewall**, then select **Statistics**.

8.4.1. Active Applications

The list of active applications displays information on programs accessing network resources at the moment.



For each application, the following information on active connection is available:

Column	Description
Name	The name of the application.
Direction	The party which initiated the connection: <ul style="list-style-type: none">• Inbound – the rule is applied when someone from the network attempted to connect to the application on your computer.• Outbound – the rule is applied when the application on your computer attempted to connect to the network.• Listening – the rule is applied when the application on your computer is awaiting for a connection attempt from the network.
Protocol	The protocol used to transmit data.
Local address	The protocol and host address from which comes an attempt to connect.



Column	Description
Remote address	The protocol and host address to which the connection is attempted.
Sent	The number of bytes sent through this connection.
Received	The number of bytes received through this connection.

In the active connections statistics window you can terminate any active process by right-clicking the process in the table and selecting **Terminate process**.

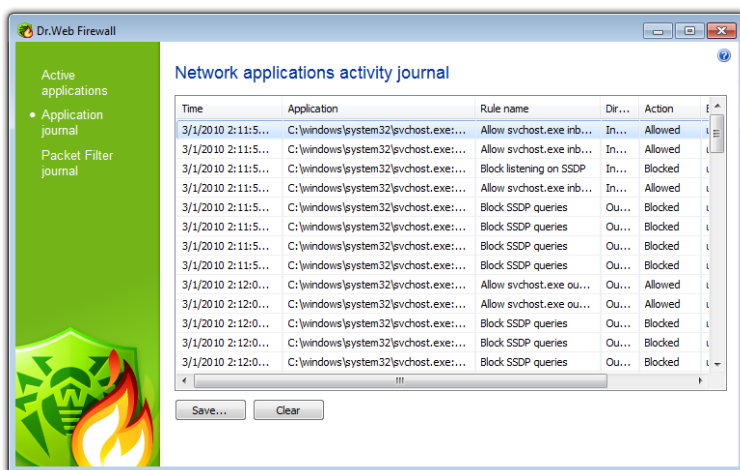


To terminate any active process you need administrative privileges. Otherwise, you can terminate only those processes that are run under your account .

From the context menu you can also block an active or unblock a disabled connection. The blocked connections are marked with red in the table.

8.4.2. Application Filter Log

The application filter log stores information on all attempts of applications installed on your computer to connect to a network.



Column	Description
Time	The date and time of the connection attempt.
Application	The full path to the application executable file, its name and process identification number (PID).
Rule name	The name of the rule applied.
Direction	The party which initiated the connection: <ul style="list-style-type: none">• Inbound – someone from the network attempted to connect to the application on your computer.• Outbound – the application on your computer attempted to connect to the network.• Any – the rule was applied regardless of who initiated the connection.
Action	The action Dr.Web Firewall performed when the connection attempt was detected: <ul style="list-style-type: none">• Block packets• Allow packets
Endpoint	The protocol, IP-address and the port used for the connection.



On this page you can save the information to a file or clear the log.

To save application filter log:

Click **Save**, then enter the file name where to store the log.

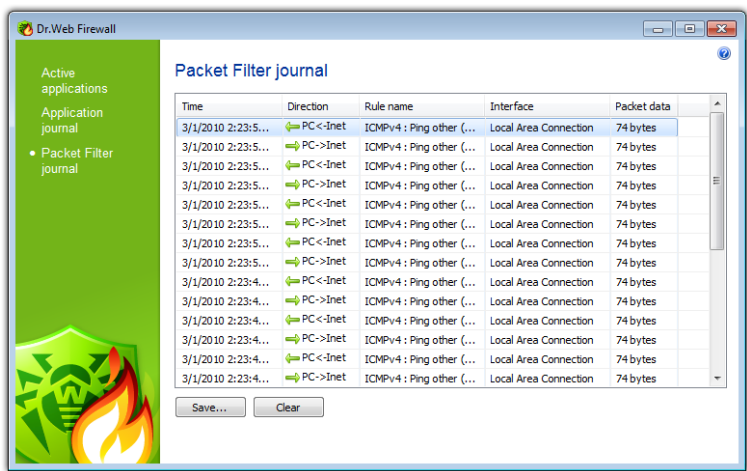
To clear application filter log:

Click **Clear**. All information will be deleted from the log.



8.4.3. Packet Filter Log

The packet filter log stores information on packets transmitted through all network interfaces installed on you computer, if **Log headers** or **Entire packet** logging mode was set for these packets. If **No logging** mode was set for a packet, no information is stored.



Column	Description
Time	The date and time when the packet was processed.
Direction	The packet sender: <ul style="list-style-type: none">→ – the packet was transmitted from the network to your computer.← – the packet was transmitted from your computer to the network.→ – the packet sent from the network to your computer was blocked.→ – the packet sent from your computer to the network was blocked.
Rule name	The name of the applied rule.



Column	Description
Interface	The interface used to transmit the packet.
Packet data	Packet details. The Logging mode setting of the rule determines the amount of stored data.

On this page you can save the information to a file or clear the log.

To save packet filter log:

Click **Save**, then enter the file name where to store the log.

To clear packet filter log:

Click **Clear**. All information will be deleted from the log.



9. Automatic Updating

Anti-virus solutions of **Doctor Web** use **Dr.Web virus databases** to detect computer threats. These databases contain details and signatures for all virus threats known at the moment of the product release. However, modern virus threats are characterized by high-speed evolvment and modification. Within several days and sometimes hours, new viruses and malicious programs emerge. To mitigate the risk of infection during the licensed period, **Doctor Web** provides you with regular updates to virus databases and product components, which are distributed via the Internet. With the updates, **Dr.Web Anti-virus** receives information required to detect new viruses, block their spreading and sometimes cure infected files which were incurable before. From time to time, the updates also include enhancements to anti-virus algorithms and fix bugs in software and documentation.

Dr.Web Updater helps you download and install the updates during the licensed period.

9.1. Running Updates

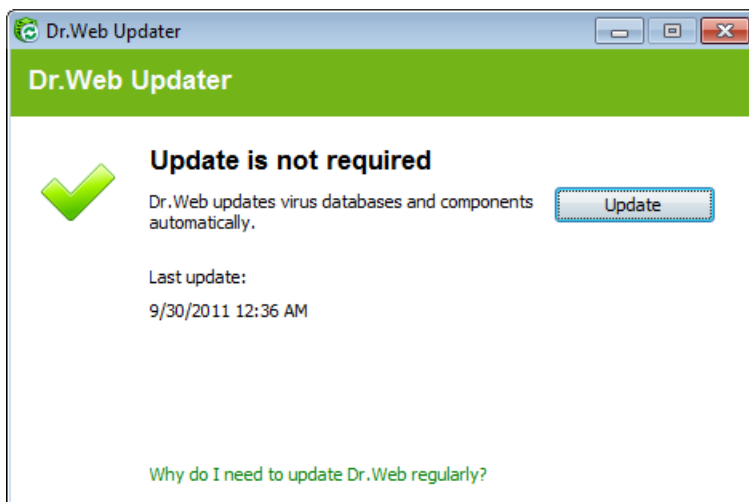
You can run **Updater** in one of the following ways:

- From the command line by running drwupsrv.exe file located in the **Dr.Web Anti-virus** installation folder
- By selecting **Update** in the **SpIDer Agent** menu

On launching, **Updater** displays a window with information on relevance of **Dr.Web virus databases** and **Dr.Web Anti-virus** components. If necessary, you can start an update process. Update parameters can be configured on the **Update** page of **Dr.Web Anti-virus** settings.



If launching **Dr.Web Updater** automatically, changes are logged into dwupdater.log file that is located in the %allusersprofile%\Application Data\Doctor Web\Logs\ folder (in Windows 7, %allusersprofile%\Doctor Web\Logs\).



Update Procedure

Before starting an update, **Updater** checks if you have a [key file](#) registered (license or demo). If no key file is found, **Updater** suggests you to obtain a key file on the Internet through the user registration procedure.

If the key file is found, **Updater** checks its validity at **Doctor Web** servers (the file can be blocked, if discredited, i.e. its illegal distribution is uncovered). If your key file is blocked due to misuse, **Updater** displays an appropriate warning, terminates the update, and blocks Dr. Web components.

If the key is blocked, contact the dealer from which you purchased **Dr. Web Anti-virus**.



After the key file is successfully verified, **Updater** downloads and installs all updated files automatically according to your version of **Dr. Web Anti-virus**. If your subscription terms allow upgrade to newer software versions, **Updater** also downloads and installs a new version of **Dr.Web Anti-virus** when released.

After an update of **Dr.Web Anti-virus** executable files or libraries, a program restart may be required. In such cases, **Updater** displays an appropriate warning.



Scanner, **SpIDer Guard** and **SpIDer Mail** start using the updated databases automatically.

When the **Updater** is launched in the command line mode, the command line parameters can be used (see [Appendix A](#)).



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. The switches can set the parameters unavailable in the configuration file and have a higher priority then the parameters which are specified in it.

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

Console Scanner Parameters

/AA – apply actions to detected threats automatically. (Only for **Scanner**).

/AR – test archive files. Option is enabled by default.

/AC – test containers. Option is enabled by default.

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

/ARC:<ratio> – maximum archive object compression. If the compression rate of the archive exceed the limit, **Console Scanner** neither unpacks, not scans the archive (*unlimited*).

/ARL:<level> – maximum archive level (*unlimited*).

/ARS:<size> – maximum archive size. if the archive size exceed the limit, **Scanner** neither unpacks, nor scans the archive (*unlimited*, KB).

/ART:<size> – minimim archive object matched by **/ARC**. minimum size of file inside archive beginning from which compression ratio



check will be performed (*unlimited*, KB).

/ARX:<size> – maximum archive object size (*unlimited*, KB).

/BI – show virus bases info. Option is enabled by default.

/DR – recursive scan directory. Option is enabled by default.

/E:<engines> – maximum **Dr.Web** engines to use.

/FAST – perform an express scan of the system (for more information on the express scan mode see [Scan Modes](#)). (Only for **Scanner**).

/FL:<path> – scan files listed in the specified file.

/FM:<masks> – scan files matched 'masks'. By default all files are scanned.

/FR:<regexpr> – scan files matched expression. By default all files are scanned.

/FULL – perform a full scan of all hard drives and removable data carriers (including boot sectors). (Only for **Scanner**).

/H or **/?** – show this message. (Only for **Console Scanner**).

/HA – use heuristic analysis. Option is enabled by default.

/KEY:<keyfile> – use 'keyfile' as activation key (by default drweb32.key or other suitable from C:\Program Files\DrWeb\).

/LITE – perform a basic scan of random access memory, boot sectors of all disks and startup objects. **Scanner** also runs a check on rootkits. (Only for **Scanner**).

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

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

/MA – test e-mail like files. Option is enabled by default.



/MC:*<limit>* – set maximum cure attempts number to 'limit' (*unlimited by default*).

/NB – don't backup curing/deleting files. Option is disabled by default.

/NI[:X] – nice mode 0-100, low resource usage (*unlimited, %*).

/NOREBOOT – cancel reboot and shutting down after scanning. (Only for **Scanner**).

/NT – test NTFS streams. Option is enabled by default.

/OK – show OK for clean files. Option is disabled by default.

/P:*<prio>* – test priority:

O – the lowest,

L – low,

N – general. Priority by default,

H – the highest,

M – maximal.

/PAL:*<level>* – maximum pack level. Value is 1000 by default.

/RA:*<file.log>* – add report into file.log. No report by default.

/RP:*<file.log>* – write report into file.log. No report by default.

/RPC:*<secs>* – **Dr.Web Scanning Engine** connection timeout. Timeout is 30 seconds by default. (Only for **Console Scanner**).

/RPCD – use dynamic RPC identification. (Only for **Console Scanner**).

/RPCE – use dynamic RPC endpoint. (Only for **Console Scanner**).

/RPCE:*<name>* – use specified RPC endpoint. (Only for **Console Scanner**).

/RPCH:*<name>* – use specified host name for remote call. (Only for **Console Scanner**).



/RPCP:<name> – use specified RPC protocol. Possible protocols: lpc, np, tcp. (Only for **Console Scanner**).

/QL – list quarantined files on all disks. (Only for **Console Scanner**).

/QL:<drive> – list quarantined files on drive 'drive' (*letter*). (Only for **Console Scanner**).

/QR[:[d]][:p]] – delete quarantined files on drive 'd' (*letter*) older than 'p' days (*number*). Unspecified 'd' – all drives, unspecified 'p' – 0 days. (Only for **Console Scanner**).

/QNA – double quote file names always.

/QUIT – **Scanner** checks the objects specified in the command line (files, disks, directories) and then automatically terminates. (Only for **Scanner**).

/REP – go follow repase points. Option is disabled by default.

/SCC – show content of compound objects. Option is disabled by default.

/SCN – show container name. Option is disabled by default.

/SPN – show packer name. Option is disabled by default.

/SLS – show log on screen. Option is enabled by default. (Only for **Console Scanner**).

/SPS – show progress on screen. Option is enabled by default. (Only for **Console Scanner**).

/SST – show file scan time. Option is disabled by default.

/TB – test boot sectors. Option is disabled by default.

/TM – test processes in memory. Option is disabled by default.

/TS – test system startup processes. Option is disabled by default.



/TR – test system restore points directories. Option is disabled by default.

/W:<sec> – maximum time to scan (*unlimited*, sec).

/WCL – drwebwcl compatible output. (Only for **Console Scanner**).

/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 only for **Console Scanner**. **R** is set by default for all objects in **Console Scanner**):

/AAD:X – action for adware (**R**, possible DQIR).

/AAR:X – action for infected archive files (**R**, possible DQIR).

/ACN:X – action for infected container files (**R**, possible DQIR).

/ADL:X – action for dialers (**R**, possible DQIR).

/AHT:X – action for hacktools (**R**, possible DQIR).

/AIC:X – action for incurable files (**R**, possible DQR).

/AIN:X – action for infected files (**R**, possible CDQR).

/AJK:X – action for jokes (**R**, possible DQIR).

/AML:X – action for infected e-mail files (**R**, possible QIR).

/ARW:X – action for riskware (**R**, possible DQIR).

/ASU:X – action for suspicious files (**R**, possible DQIR).

Several parameters can have modifiers that clearly 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:

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

For **/FL** parameter "-" modifier directs to scan paths listed in specified file and then delete this file.

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

Example of using command line parameters 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, type the `dwscanner` command name instead of `dwscancl`.

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, e-mail 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 shut-down 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 e-mail) 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 (i.e. do not cause any direct damage) due to their intensive distribution.

Trojan horses (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, e.g. 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 e-mail 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.

Joke programs

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 e-mail (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 e-mails.



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:

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 (i.e. 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 more effective curing and file recovery algorithms compared to other anti-virus manufacturers.

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 of **Doctor Web** for analysis.

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. E.g. curing of a computer worm implies deletion of all its functional copies.

Block, rename – these actions can also be used for neutralizing malicious programs. However, fully operable copies of these programs remain in the file system. In case of the Block action all access attempts to or from the file are blocked. The Rename action means that the extension of the file is renamed which makes it inoperative.



Appendix C. Naming of Viruses

Specialists of the **Dr.Web Virus Laboratory** give names to all collected samples of computer threats. 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. 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 and constantly updated version of this classification is available at the [Dr.Web web site](#).

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. Below is a list of all prefixes and suffixes used in **Dr. Web** divided into groups.

Prefixes

Affected operating systems

The prefixes listed below are used for naming viruses infecting executable files of certain OS's:

- 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
- HLLO – viruses overwriting the code of the victim program,
- HLLP – parasitic viruses
- HLLC – companion viruses

The following prefix also refers to development language:

- Java – viruses designed for the Java virtual machine

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

Trojan horses

- 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 web site (or sites)
- 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
- FormatAll – formats all drives
- KillMBR – corrupts or deletes master boot records (MBR)
- KillCMOS – corrupts or deletes CMOS memory



Tools for network attacks

- Nuke – tools for attacking certain 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) – 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)

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

- Exploit – a tool exploiting known vulnerabilities of an O S or application to implant malicious code or perform unauthorized actions.
- 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:

- Origin – this suffix is added to names of objects detected using the *Origins Tracing* algorithm.
- 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.



Appendix D. Central Anti-virus Protection

Solutions for central protection from **Doctor Web** help automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one anti-virus network which security is monitored and managed from central server by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

Logical Structure of Anti-virus Networks

Solutions for central protection from **Doctor Web** use client-server model (see picture below).

Workstations and servers are protected by *local anti-virus components* (agents, or clients) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.

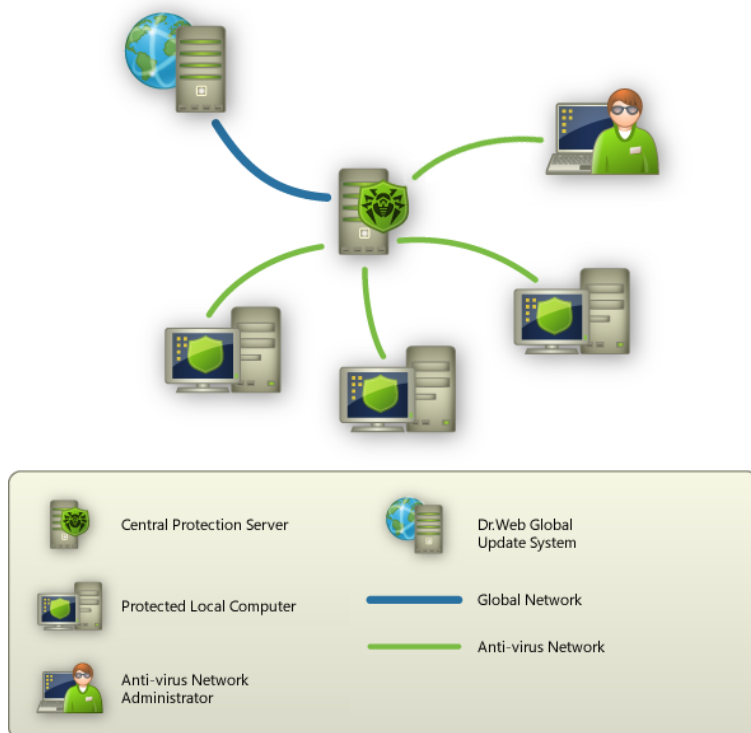
Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.

Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to



central protection server from remote computers) and configure operation of local anti-virus components when necessary.



Local anti-virus components are not compatible with other anti-virus software including versions of **Dr.Web Anti-virus** that do not support operation in central protection mode. Installing two anti-virus programs on one computer may lead to system crash and loss of important data.



Appendix E. Technical Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website at <http://support.drweb.com/>.

If you encounter any issues installing or using company products, take advantage of the following **Doctor Web** support options:

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

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 official **Doctor Web** website at <http://company.drweb.com/contacts/moscow>

