Dr.WEB®

# Anti-virus for Windows

## User Manual

**© Doctor Web, 2014. 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 10.0**
**User Manual**
**24.10.2014**

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

**Dr.Web Anti-virus for Windows** provides multilevel protection of RAM, hard disks, and removable devices against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

The module architecture of **Dr.Web 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 Anti-virus** products for Windows, there are versions of anti-virus software for IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Android®, Symbian®, and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

**Dr.Web 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 the programs, anti-virus components of **Dr.Web Anti-virus** are used.

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

- **Dr.Web Scanner** (**Scanner**) is an anti-virus scanner with graphical interface. The program runs on user demand or as scheduled and checks the computer for viruses.
- **Dr.Web Console Scanner** – a command-line version of **Dr.Web Scanner**.
- **SpIDer Guard** is an on-access anti-virus scanner that constantly resides in memory while scanning files and RAM "on the fly" and instantly detects any malicious activity.
- **SpIDer Mail** – the program intercepts calls sent from mail clients to mail servers through POP3/SMTP/IMAP4/NNTP protocols (IMAP4 stands for IMAPv4rev1), and detects and neutralizes mail viruses before a mail message is received by the mail client or before a mail message is sent to the mail server.
- **Dr.Web for Outlook** is a plug-in that checks Microsoft Outlook mail boxes for viruses.
- **Dr.Web Firewall** is a components that protects your computer from unauthorized access and prevents vital data from leaking through networks.
- **Dr.Web Update** 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.

## 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 which can be accessed from any component.

This User Manual describes how to install the program and contains some words of advice on how to use it and solve typical problems caused by virus threats. Mostly, it describes the standard operating modes of the **Dr.Web Anti-virus** 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://download.drweb.com/doc.

## 1.2. Document Conventions

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

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

# 1.3. Detection Methods

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

## Detection Methods

### Signature analysis

The scans begin with signature analysis which is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web** anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

### Origins Tracing™

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

### Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator* – a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

### Heuristic analysis

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

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers **Dr.Web** is aware of, but by also new, previously unexplored programs. While checking packed objects, **Dr.Web** anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious ".

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

# 2. System Requirements

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

- Remove any anti-virus software from your computer to prevent possible incompatibility of resident components.
- If you install **Dr.Web Firewall**, uninstall all other firewalls from your computer
- Install all critical updates released for your operating system. If the operating system is no longer supported, then upgrade to a newer operating system.

**Dr.Web Anti-virus** can be installed and run on a computer which meets the following minimum requirements:

| Component | Requirement |
|---|---|
| CPU | An i686-compatible processor. |
| Operating system | For 32-bit platforms:<br>• Windows® XP with Service Pack 2 or higher<br>• Windows Vista®<br>• Microsoft® Windows® 7<br>• Microsoft® Windows® 8<br>• Microsoft® Windows® 8.1<br>For 64-bit platforms:<br>• Windows Vista®<br>• Microsoft® Windows® 7<br>• Microsoft® Windows® 8<br>• Microsoft® Windows® 8.1<br>You may need to download and install certain system components from the Microsoft official website. If necessary, the program will notify you about the **Dr.Web Anti-virus** components required and provide download links. |
| Free RAM | Minimum 512 MB. |
| Hard disk space | 330 MB for **Dr.Web Anti-virus components.**<br>Files created during installation will require additional space. |
| Resolution | Recommended minimum screen resolution is 800x600. |
| Other | To update **Dr.Web virus databases** and **Dr.Web Anti-virus** components, connection to the Internet is required. |

# 3. Installing the program

Before installing **Dr.Web Anti-virus**, note the system requirements and do the following:

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

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

## 3.1. Installation Procedure

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

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

- The background mode
- The usual mode

### Installation with command-line parameters

To install **Dr.Web Anti-virus** with command-line parameters, enter the executable file name with necessary parameters in the command line (the parameters affect installation in background mode, installation language, restart after installation completes, and installation of **Firewall**):

| Parameter | Description |
|---|---|
| installFirewall | Install **Dr.Web Firewall**. |
| lang | Language used for the installation. The value of this parameter is language code in ISO 639-1 format. |
| reboot | Restart the computer automatically after installation is complete. |
| silent | Installation in background mode. |

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

```
drweb-1000-win.exe /silent yes /reboot yes
```

### Usual Installation

To start usual installation, do one of the following:

- run the file, if the installation kit is supplied as a single executable file;
- insert the company disk into the CD/DVD drive, if the installation kit is supplied on the disk. If autorun is enabled, the installation will start automatically. If autorun is disabled, run the autorun.exe file of the installation kit manually. The window opens and displays the autorun menu. Click **Install**.

Follow the instructions of the Installation Wizard. At any installation step, before the wizard starts copying files to your computer, you can do the following:

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

#### Installing Dr.Web Anti-virus

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

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

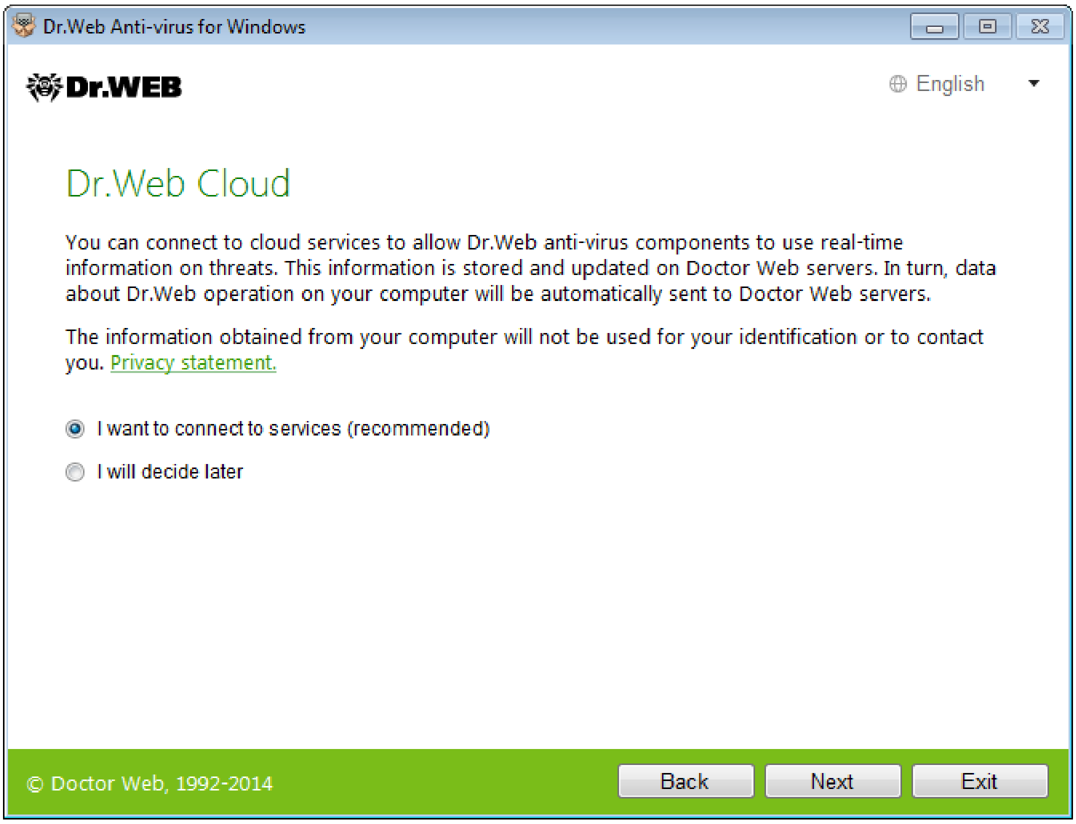
2. Read the license agreement. To continue installation, you must accept its terms and click **Next**.

   Click **Next.**

3. At the next step, you will be offered to install **Dr.Web Firewall**.

   Click **Next.**

4. At this step, you are prompted to connect to **Dr.Web** cloud services that allow the anti-virus components to use the newest information which is stored and updated on **Doctor Web** servers.



Dr.Web Cloud

You can connect to cloud services to allow Dr.Web anti-virus components to use real-time information on threats. This information is stored and updated on Doctor Web servers. In turn, data about Dr.Web operation on your computer will be automatically sent to Doctor Web servers.

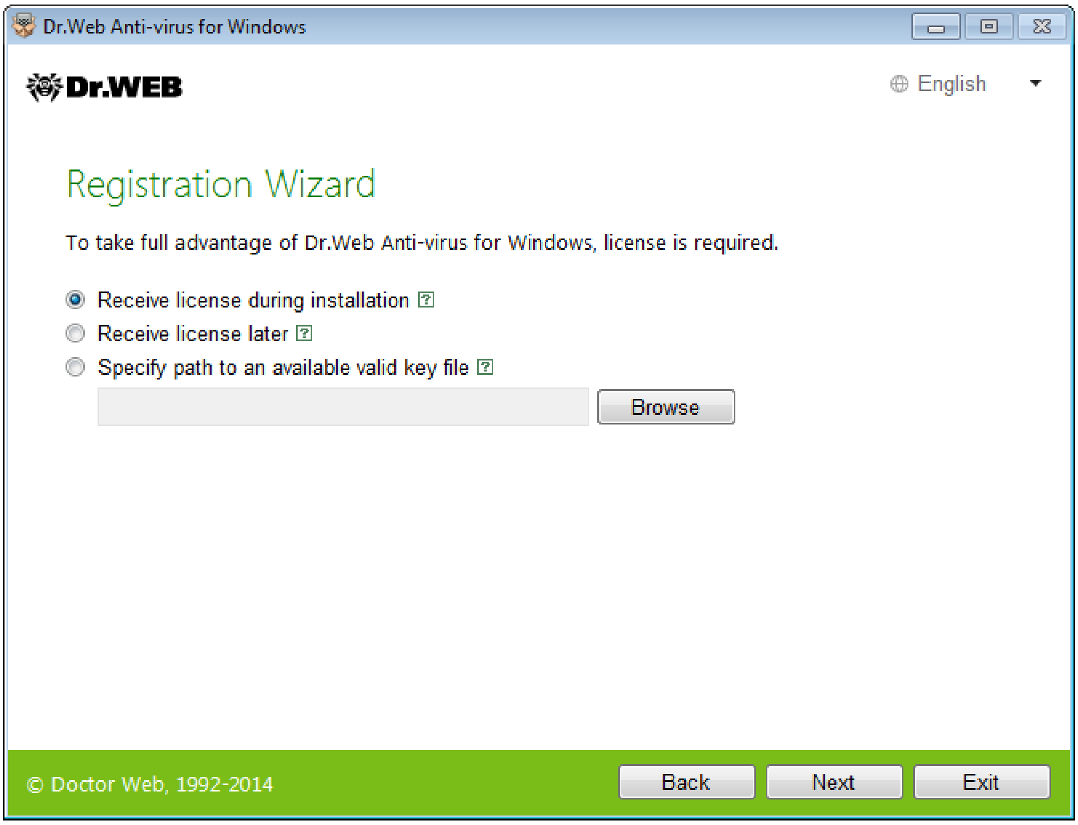
The information obtained from your computer will not be used for your identification or to contact you. Privacy statement.

● I want to connect to services (recommended)

○ I will decide later

   Click **Next.**

5. The Installation Wizard informs you that a license is required for **Dr.Web Anti-virus** operation.



Registration Wizard

To take full advantage of Dr.Web Anti-virus for Windows, license is required.

● Receive license during installation
○ Receive license later
○ Specify path to an available valid key file

Do one of the following:

- if a key file is present on the hard drive or removable media, click **Specify path to an available valid key file** and select the file in the open window. To change the path, click **Browse** and select another key file.
- If you want to receive a key file during the installation, select **Receive license during installation.**
- To continue installation without a license, select **Receive license later.** Updating is not available until you have obtained a key file.

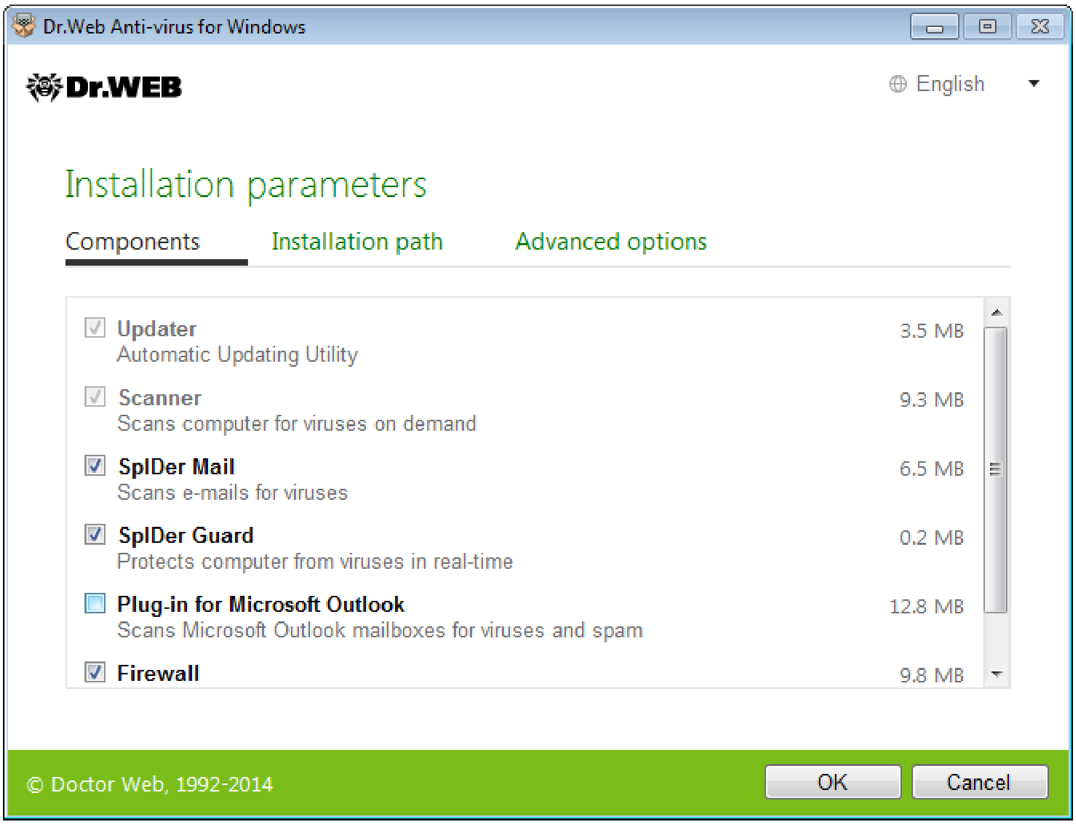
Click **Next.**

6. The window opens notifying you that the product is ready to be installed. To start installation with the default parameters, click **Install**.

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

7. If you selected **Install** at the previous step, go to the description of step 10. Otherwise, the **Installation parameters** window opens.

On the first tab, you can specify the components you want to install.



Dr.Web Anti-virus for Windows

Dr.WEB

English

Installation parameters

Components | Installation path | Advanced options

| | | |
|---|---|---|
| ☑ | **Updater**<br>Automatic Updating Utility | 3.5 MB |
| ☑ | **Scanner**<br>Scans computer for viruses on demand | 9.3 MB |
| ☑ | **SpIDer Mail**<br>Scans e-mails for viruses | 6.5 MB |
| ☑ | **SpIDer Guard**<br>Protects computer from viruses in real-time | 0.2 MB |
| □ | **Plug-in for Microsoft Outlook**<br>Scans Microsoft Outlook mailboxes for viruses and spam | 12.8 MB |
| ☑ | **Firewall** | 9.8 MB |

© Doctor Web, 1992-2014

8. On this tab, you can change the installation path.
9. If you specified a valid key file or selected **Receive license during installation** at step 5, the last page of the window allows you to select **Update during installation** check box to download updates to virus databases and other program components. The window also prompts you to create shortcuts to start **Dr.Web Anti-virus**.

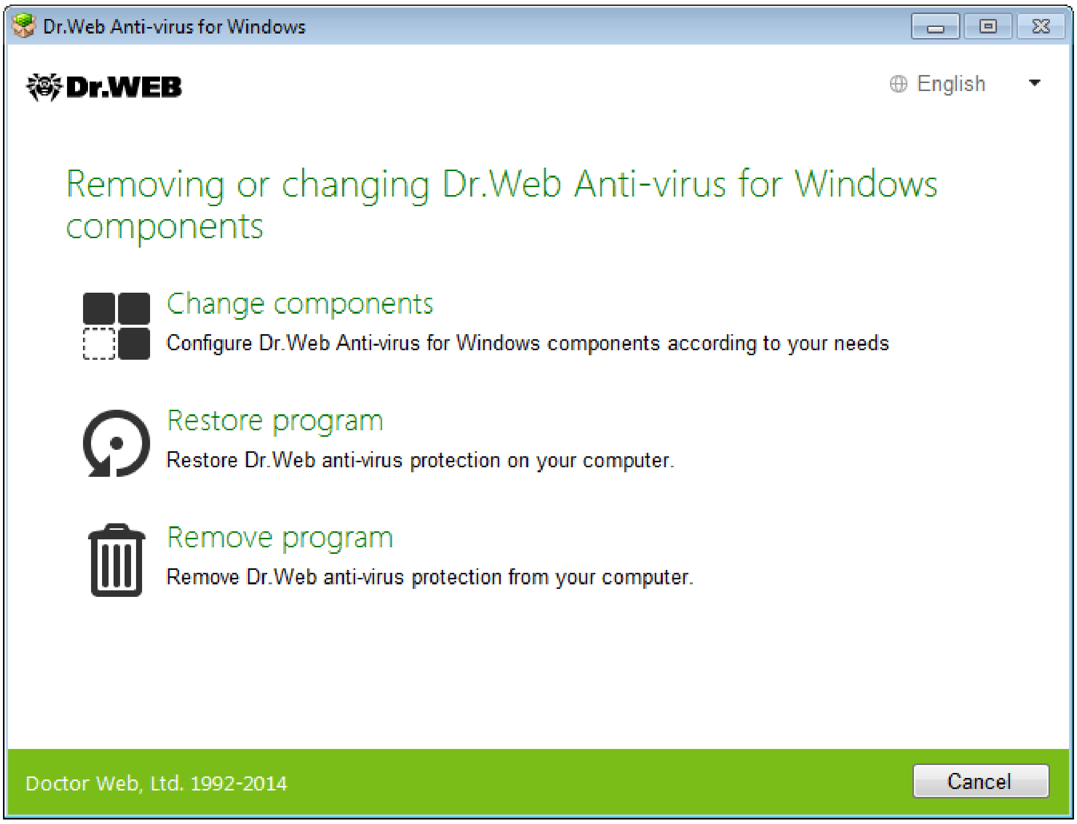
   When you finish adjusting the installation parameters, click **OK.**

10. If you selected **Receive license during installation** at step 5, the procedure of receiving the key file from the Internet via the Registration Wizard starts.
11. If you specified a key file or received it during the installation and selected **Update during installation** check box at step 9, the Wizard updates virus databases and other **Dr.Web Anti-virus** components. Updating starts automatically and does not require any additional actions.
12. Restart your computer after the installation is complete.

## 3.2. Removing or changing the program

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

1. To uninstall **Dr.Web Anti-virus** or change its configuration by adding or removing individual components, select (depending on the operating system):
   - For Windows XP (depending on the presentation of the Start menu):
     - Start menu: **Start** → **Control Panel** → **Add or Remove programs.**
     - Classic Start menu: **Start** → **Settings** → **Control Panel** → **Add or Remove programs.**
   - For Windows Vista (depending on the presentation of the Start menu):
     - Start menu: **Start** → **Control Panel,** then, depending on the Control Panel view:
       - Classic view: **Programs and Features.**
       - Control Panel Home: **Programs** → **Programs and Features.**
     - Classic Start menu: **Start** → **Settings** → **Control Panel** → **Add or Remove programs.**
   - For Windows 7, click **Start** → **Control Panel**, then, according to the Control Panel view:
     - Small/large icons: **Programs and Features.**
     - Category: **Programs** → **Uninstall a program.**
   - For Windows 8 and Windows 8.1, open **Control Panel** in any convenient way: for example, right-click the bottom left corner and select the **Control Panel** item in the shortcut menu. According to the selected **View** option for the Control Panel, click:
     - Small/large icons: **Programs and Features.**
     - Category: **Programs** → **Uninstall a program.**
2. In the open window, select the program. To delete the program completely, click **Uninstall** and go to step 6. To change the configuration of **Dr.Web Anti-virus** by adding or removing certain components, click **Change**. The window of the Installation Wizard opens.



Removing or changing Dr.Web Anti-virus for Windows components

Change components
Configure Dr.Web Anti-virus for Windows components according to your needs

Restore program
Restore Dr.Web anti-virus protection on your computer.

Remove program
Remove Dr.Web anti-virus protection from your computer.

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

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

5. To delete all installed components, select **Remove program**.
6. In the **Parameters** window, select check boxes of those components that you do not want to remove from your system. Saved objects and settings can be used by the program if it is installed again. By default, all options are selected, that is **Quarantine**, **Dr.Web Anti-virus for Windows** settings and **Protected copies of files**. Click **Next**.
7. In the next window, confirm deletion of **Dr.Web Anti-virus**by entering the displayed code and then click **Remove program**.
8. When prompted, restart the computer to complete the procedure.

# 4. Licensing

To use **Dr.Web Anti-virus** for a long period of time, activate a license. You can purchase a license with the product or on the **Doctor Web** official website. A license allows to take advantage of all product features during the whole period. Parameters of the license key file are set in accordance with the software license agreement.

### Key File

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

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

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

A *valid* key file satisfies the following criteria:

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

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

If during **Dr.Web Anti-virus** installation, a key file was not received and no path to it was specified, a *temporary* key file is used. Such a key file provides full functionality of **Dr.Web Anti-virus**. However, on the **SpIDer Agent** menu, **My Dr.Web** and **Update** items are not available until you either activate a license or specify a path to the valid key file via **License Manager**.

It is recommended to keep the key file until the license expires.

## 4.1. Activation method

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

- Using the Registration Wizard during installation or later
- Obtaining the key file during registration on the **Doctor Web** official website
- Specifying the path to the valid key file residing on your computer during installation or in the License Manager window

### Reactivating License

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

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

If you reinstall the product or install it on several computers, if the license allows for that, you will be able to use the previously registered key file. You can use the key file obtained during the first registration.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact technical support describing your problem in detail, stating your personal data input during the registration and the serial number. The key file will be sent by technical support to your email address.

## 4.2. Renewing License

When the license expires or characteristics of the protected system change, you may need to renew or extend the license. If so, you should change the current key file. **Dr.Web Anti-virus** supports hot license update without stopping or reinstalling the product.

**To change a license key file**

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

## 4.3. Registration Wizard

**SpIDer Agent** checks whether you have a key file. If no key file is found, you are prompted to obtain a key file on the Internet.

A key file can be obtained during an installation procedure. For this, select **Receive key file during installation** on step 5 of installation procedure, and activation of the license will start.

You can also obtain a key file by starting activation of the license after the product is installed on your system. For that, do one of the following:

- Click the **SpIDer Agent** icon in the notification area and select **License.**
- In the License Manager window, click **Get new license** and select **from Internet.**

After activation is started, the Registration Wizard window opens.

To activate the license, you need to enter the registration serial number, supplied to you when purchasing **Dr.Web Anti-virus**.

## Starting activation

The first window prompts you to activate license and enter the serial number. Enter it and click **Next.**

If you enter a serial number for activation of a license, the registration data entry window opens.

If you have already been a user of **Dr.Web Anti-virus**, you are eligible for extension of your new license for another 150 days. To enable the bonus, enter your serial number and specify the path to the previous key file in the open window.

## Registration data entry

To register a license, enter personal data (your registration name and email address), select the country and enter the city name. All the fields listed are obligatory and must be filled in.

If you want to receive news of **Doctor Web** by email, select the corresponding check box.

Click **Next.**

## Activation results

If the activation procedure completed successfully, the corresponding message displays where the license validity period is specified. Click **Finish** to proceed to updating the virus databases and other package files. This procedure does not require user intervention.

If activation failed, an error message displays. Click **Network settings** to adjust Internet connection parameters or click **Repeat** to correct invalid data.

# 5. Getting Started

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

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

- – All necessary components are running and protect your computer.
- – **Dr.Web Anti-virus**Self-protection or an important component such as **SpIDer Guard** or **Firewall** is disabled, which compromises security of **Dr.Web** and your computer. Enable Self-protection or the component.
- – an error occurred while starting one of the main **Dr.Web Anti-virus** components. Your computer is at risk of virus infection. Check that you have a valid key file and, if required, install it or contact your anti-virus network administrator;

Various notifications may appear over the **SpIDer Agent** if configured.

The **SpIDer Agent** menu allows to perform the main management and setting functions of **Dr.Web Anti-virus**. To open the menu, click the **SpIDer Agent** icon in the Windows notification area.

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

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

**Register license.** Starts the Registration Wizard for receiving the key file from the **Doctor Web** server.

**Tools**. Opens a submenu providing access to:

- License Manager;
- Data Loss Prevention;
- Anti-virus Network;
- Quarantine Manager;
- Support section.

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

**Updater**. Information about actuality of the components or virus databases. Launches the update.

**Scanner**. Quick access to launching different kinds of scanning.

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

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

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

⚠ To access the component settings and open your personal webpage **My Dr.Web**, you also need to enter the password if you enabled **Protect Dr.Web settings by password** option on the Settings window.

If you forgot your password for the product settings, contact technical support.

## 5.1. How to Test Anti-virus

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

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

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

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

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

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

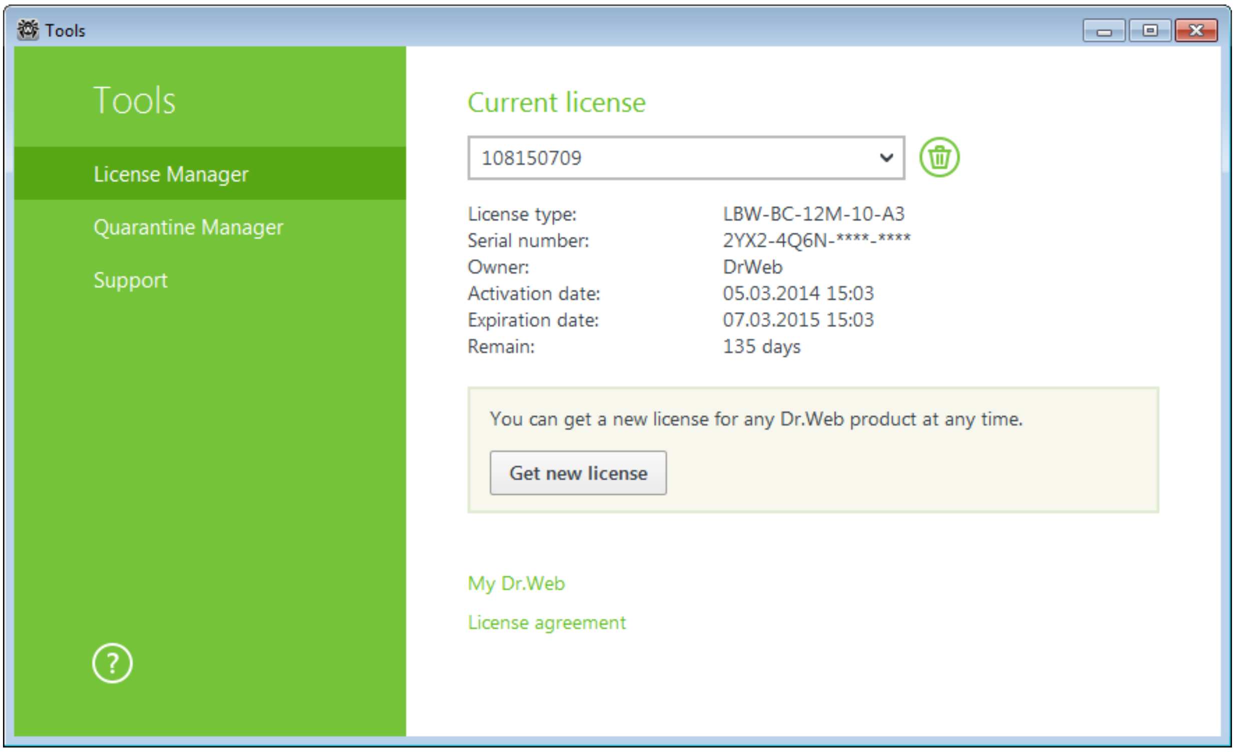
When you attempt to execute an EICAR file while **SpIDer Guard** is running in the optimal mode, the operation is not terminated and the file is not processed as malicious since it does not pose any actual threat to your system. However, if you copy or create such a file in your system, it will be detected by **SpIDer Guard** and moved to **Quarantine** by default.

# 6. Tools

## 6.1. License Manager

This window displays information on **Dr.Web Anti-virus** licenses.

To open this window, click the **SpIDer Agent** icon in the notification area, select **Tools**, and then select **Quarantine Manager**. In the upper part of the window, you can find information about the license you are using.



License type: LBW-BC-12M-10-A3
Serial number: 2YX2-4Q6N-****-****
Owner: DrWeb
Activation date: 05.03.2014 15:03
Expiration date: 07.03.2015 15:03
Remain: 135 days

You can get a new license for any Dr.Web product at any time.

### Obtaining key file

To start the registration procedure for receiving the key file from **Doctor Web** servers, click **Get new license** and select **from Internet** in the drop-down menu. That launches Registration Wizard that will guide you through obtaining the key file.

To enable operation of **Dr.Web Anti-virus**, install the key file on the system.

**My Dr.Web** link opens your personal page of the **Doctor Web** official website with the default Internet browser. This page provides you with information on your license including usage period and serial number and allows to renew the license, contact technical support, and so on.

Click 🗑 to delete the selected license by removing the corresponding key file. The current license cannot be deleted.

⚠ You can delete license only in the administrator mode. This button is not available in user mode.

To enable operation of **Dr.Web Anti-virus**, install a **Dr.Web Anti-virus** key file on the system. The key files received during installation or within the product distribution kit are installed automatically.

By default, the key file is located in the **Dr.Web Anti-virus** installation folder. **Dr.Web Anti-virus** verifies the file regularly. Do not edit or modify the key file to avoid its corruption.

If no valid key file is found, **Dr.Web Anti-virus** components are blocked.

**License Manager** can display a notification above the **SpIDer Agent** icon in the notification area. If necessary, you can configure desktop and email notifications.

## 6.2. Anti-virus Network

**Anti-Virus Network** is not included in **Dr.Web Anti-Virus**. However, you can allow access to **Dr.Web Anti-Virus** on your computer. To allow remote connection, on the **Anti-virus Network** page in the Main settings section select **Enable Remote Control** and specify the password, required to access the anti-virus program.

If you use **Dr.Web Security Space** key file, you can download the corresponding documentation at http://download.drweb.com/doc for more information about **Anti-Virus Network**.

The following items are available to a remote user of your **Dr.Web Anti-Virus**:

- **About**
- Register license
- **My Dr.Web**
- **Help**
- **Tools**
- Updater
- Main Settings

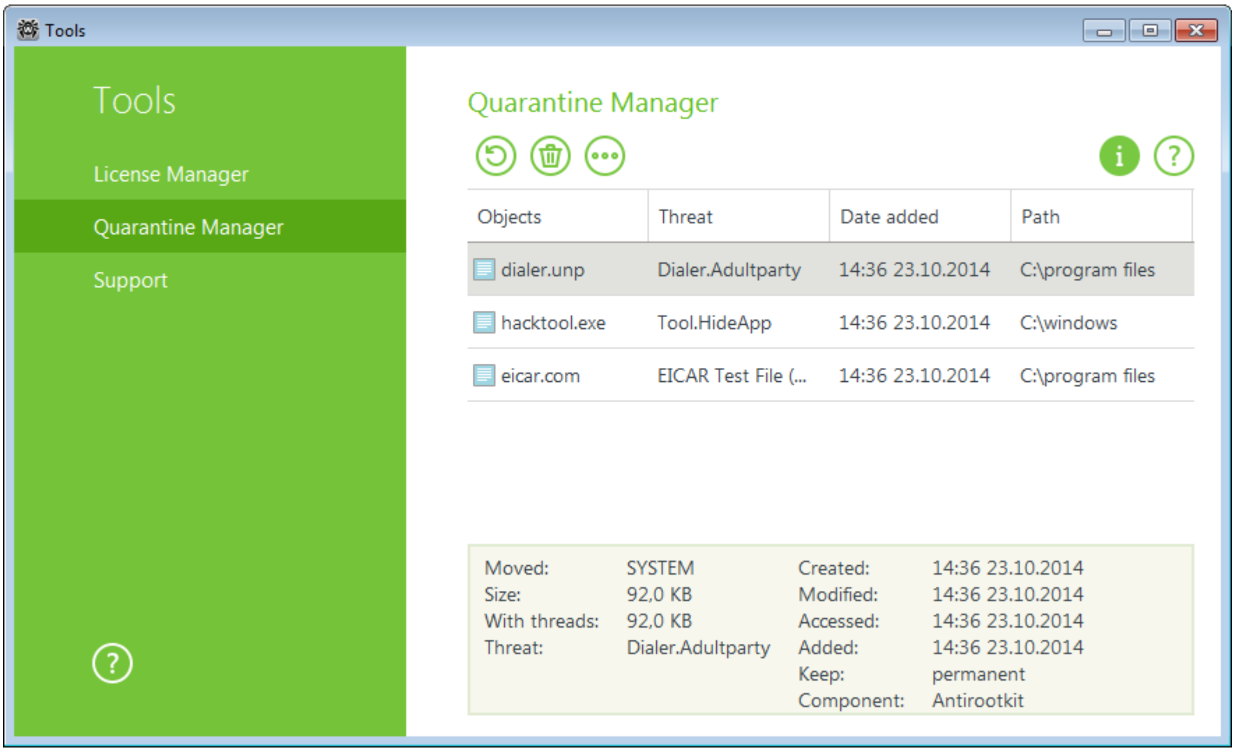
Remote control allows you to view statistics, enable or disable components and modify their settings. **Quarantine** and **Scanner** are not available. **Dr.Web Firewall** settings and statistics are not available either, but it is allowed to enable or disable thw component.

## 6.3. Quarantine Manager

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

Folders of **Quarantine** are created separately on each logical drive where suspicious files are found. The **Quarantine** folder is created on portable data carriers only when they are accessible for writing. Infected objects are moved to appropriate folders and then the quarantined files located on hard drives are encrypted. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss.

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



Quarantine Manager

| Objects | Threat | Date added | Path |
|---|---|---|---|
| dialer.unp | Dialer.Adultparty | 14:36 23.10.2014 | C:\program files |
| hacktool.exe | Tool.HideApp | 14:36 23.10.2014 | C:\windows |
| eicar.com | EICAR Test File (... | 14:36 23.10.2014 | C:\program files |

| | | | |
|---|---|---|---|
| Moved: | SYSTEM | Created: | 14:36 23.10.2014 |
| Size: | 92,0 KB | Modified: | 14:36 23.10.2014 |
| With threads: | 92,0 KB | Accessed: | 14:36 23.10.2014 |
| Threat: | Dialer.Adultparty | Added: | 14:36 23.10.2014 |
| | | Keep: | permanent |
| | | Component: | Antirootkit |

The central table lists the following information on quarantined objects that are available to you:

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

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

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

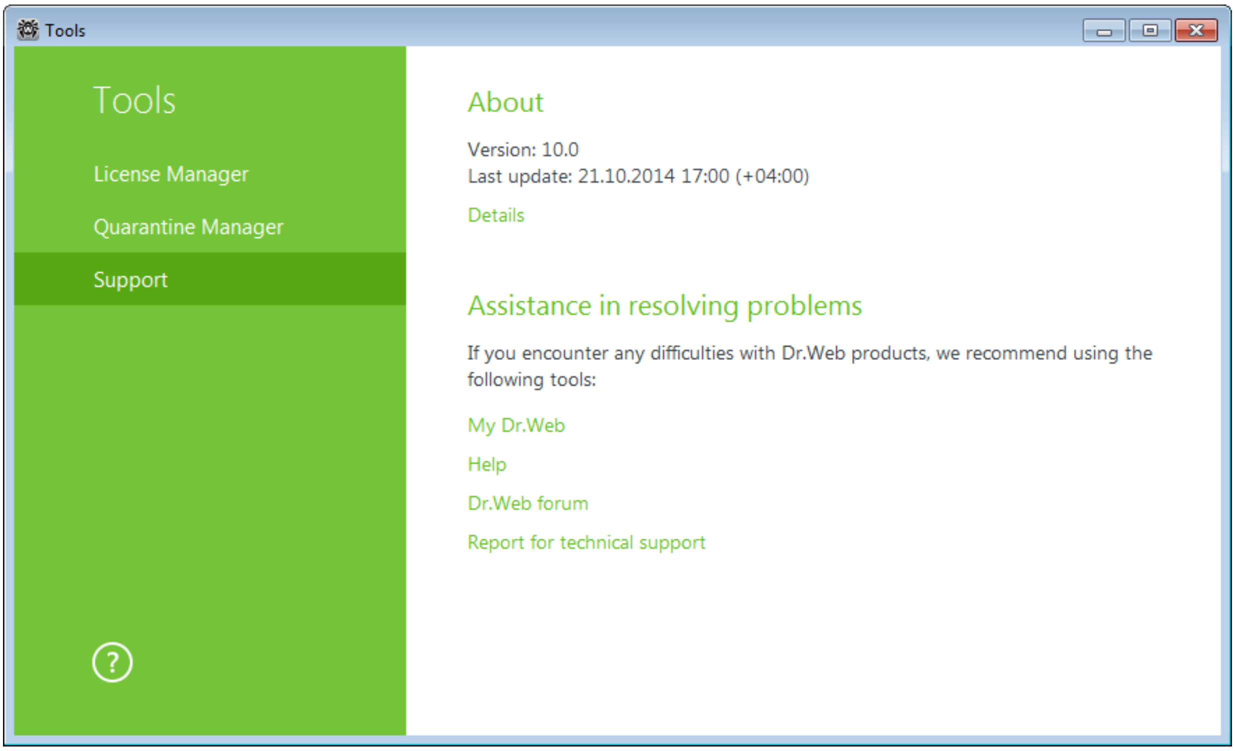
- **Restore –** remove file to the selected folder and specify a new file name;

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

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

## 6.4. Support

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



About

Version: 10.0
Last update: 21.10.2014 17:00 (+04:00)

Details

Assistance in resolving problems

If you encounter any difficulties with Dr.Web products, we recommend using the following tools:

My Dr.Web

Help

Dr.Web forum

Report for technical support

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

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

**Help**. Opens help file.

**Dr.Web forum**. Opens the **Dr.Web** forum at http://forum.drweb.com.

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

If you have not found solution for the problem, you can request direct assistance from **Doctor Web** technical support by filling in the web from in the corresponding section of the support site at http://support.drweb.com/.

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

### 6.4.1. Report

When contacting **Doctor Web** technical support, you can generate a report on your operating system and **Dr.Web Anti-virus** operation.

You need administrative privileges to generate a full report.

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

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

1. Technical information about the operating system:
   - General information about your computer
   - Running processes
   - Scheduled tasks
   - Services, drivers
   - Default browser
   - Installed applications
   - Policies
   - HOSTS file
   - DNS servers
   - MSInfo log
   - system event log
   - system directories
   - registry branches
   - Winsock providers
   - Network connections
   - Dr.Watson logs
   - Performance index
2. Information about **Dr.Web** anti-virus solutions.
3. Information about the following plug-ins:
   - **Dr.Web for IBM Lotus Domino**
   - **Dr.Web for Kerio MailServer**
   - **Dr.Web for Kerio WinRoute**

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

# 7. Update

The anti-virus solutions of **Doctor Web** use **Dr.Web** virus databases to detect malicious software. These databases contain details and signatures for all virus threats known at the moment of the product release. However, new types of computer threats are being constantly developed all over the world, that is why **Dr.Web** virus databases require regular update. With the updates, **Dr.Web Anti-virus** receives information required to detect and block new viruses and sometimes to cure the infected files which were considered unrecoverable before.

From time to time, the updates include enhancements to anti-virus algorithms in the form of executable files and libraries. The experience of **Dr.Web** anti-virus protection helps to fix any bugs in software, and to update support service and documentation.

To ensure the virus databases and software algorithms being most up-to-date, **Doctor Web** provides you with regular updates to virus databases and product components, which are distributed via the Internet. **Dr.Web Update** helps you download and install the updates during the licensed period.

## Update Procedure

Before starting an update, **Dr.Web Update** checks if you have a registered key file in the installation folder. Update of **Dr.Web Anti-virus** is blocked, if no key file is found or if the key file is damaged or expired.

If no key file is found, update of **Dr.Web Anti-virus** is blocked.

If a key file is found, **Dr.Web Update** checks its validity at **Doctor Web** official website (the file can be blocked, if discredited; that is, if its illegal distribution is uncovered). If your key file is blocked due to misuse, **Dr.Web Update** displays an appropriate warning, terminates the update, and blocks components.

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

Successful key file verification initiates an updating process. **Dr.Web Update** automatically downloads and installs all updated files that correspond to your version of **Dr.Web Anti-virus**, and if the subscription terms allow, upgrades **Dr.Web Anti-virus** (when a newer version is released).

After an update of executable files or libraries, a program restart may be required. In such cases, an appropriate warning displays.

A connection to the Internet is required to use **Dr.Web Update**.

## Update start

You can start an update in one of the following ways:

- From the command line
- From the **SpIDer Agent** menu

All necessary parameters can be defined on the **Update** page of **Dr.Web Anti-virus** Main settings.

Click the **SpIDer Agent** icon and select **Update.** This opens a window with information on relevance of **Dr.Web virus databases** and other components as well as the date of their last update.

If necessary, you can start updating by clicking **Update.** If update is not required, close the window.

You can also start an update by using the command line. For this, open the **Dr.Web Anti-virus** installation folder (C:\Program Files\Common Files\Doctor Web\Updater) and run the drwupsrv.exe file. The list of command-line parameters can be found in Appendix A.

If launched automatically, **Dr.Web Update** installs updates silently and logs all changes into the dwupdater.log file located in the %allusersprofile%\Doctor Web\Logs\ folder.

**Dr.Web Update** can display a notification in the notification area. If necessary, you can configure desktop and email notifications.

# 8. Dr.Web Scanner

By default, **Dr.Web Scanner** checks all files for viruses using both the virus database and the heuristic analyzer (a method based on the general algorithms of virus developing allowing to detect the viruses unknown to the program with a high probability). Executable files compressed with special packers are unpacked when scanned. Files in archives of all commonly used types (ACE, ALZIP, AR, ARJ, BGA, 7-ZIP, BZIP2, CAB, GZIP, DZ, HA, HKI, LHA, RAR, TAR, ZIP, etc.), in containers (1C, CHM, MSI, RTF, ISO, CPIO, DEB, RPM, etc.), and in mailboxes of mail programs (the format of mail messages should conform to RFC822) are also checked.

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

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

You can also connect to **Doctor Web** cloud services which allow anti-virus components to use the latest information on threats. This information is stored and updated on **Doctor Web** servers in real-time mode.

## 8.1. Scanning Your System

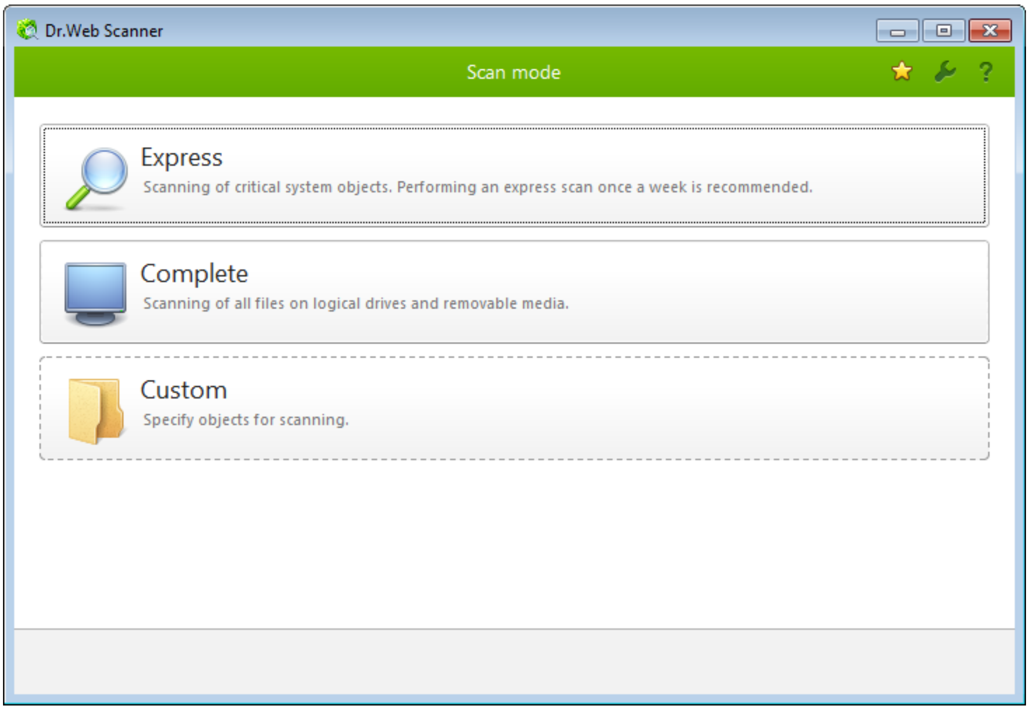
### To launch Scanner

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

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

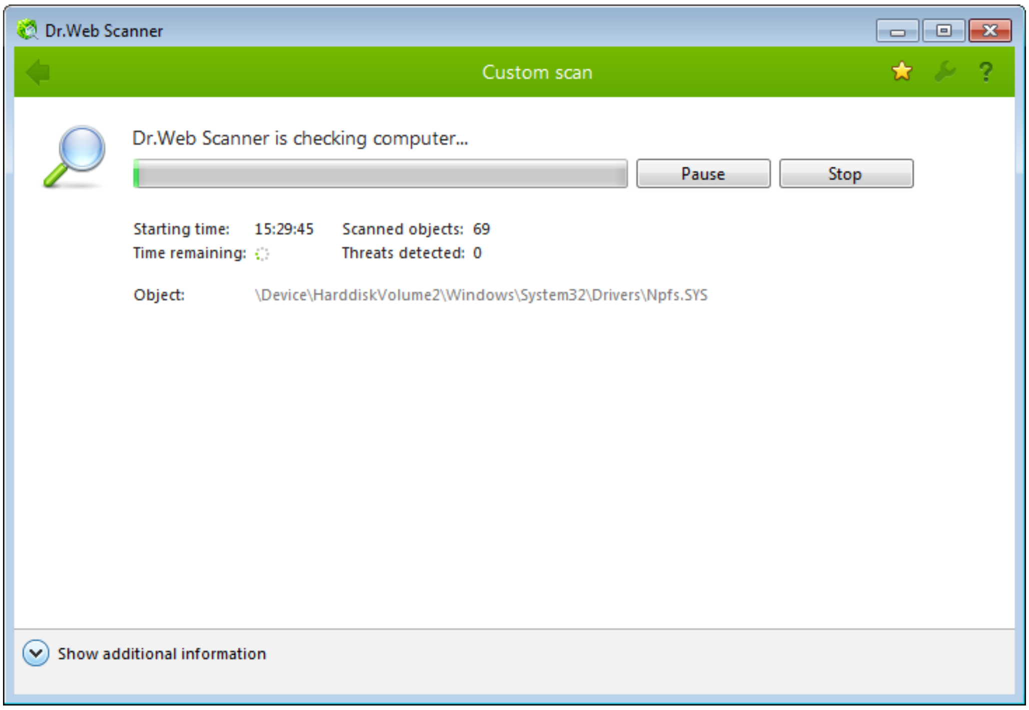
   To launch **Scanner** with default settings to scan a certain file or folder, select **Check with Dr.Web.**

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



Dr.Web Scanner
Scan mode
Express
Scanning of critical system objects. Performing an express scan once a week is recommended.
Complete
Scanning of all files on logical drives and removable media.
Custom
Specify objects for scanning.

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



Dr.Web Scanner is checking computer...

Starting time: 15:29:45
Time remaining:
Scanned objects: 69
Threats detected: 0
Object: \Device\HarddiskVolume2\Windows\System32\Drivers\Npfs.SYS

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

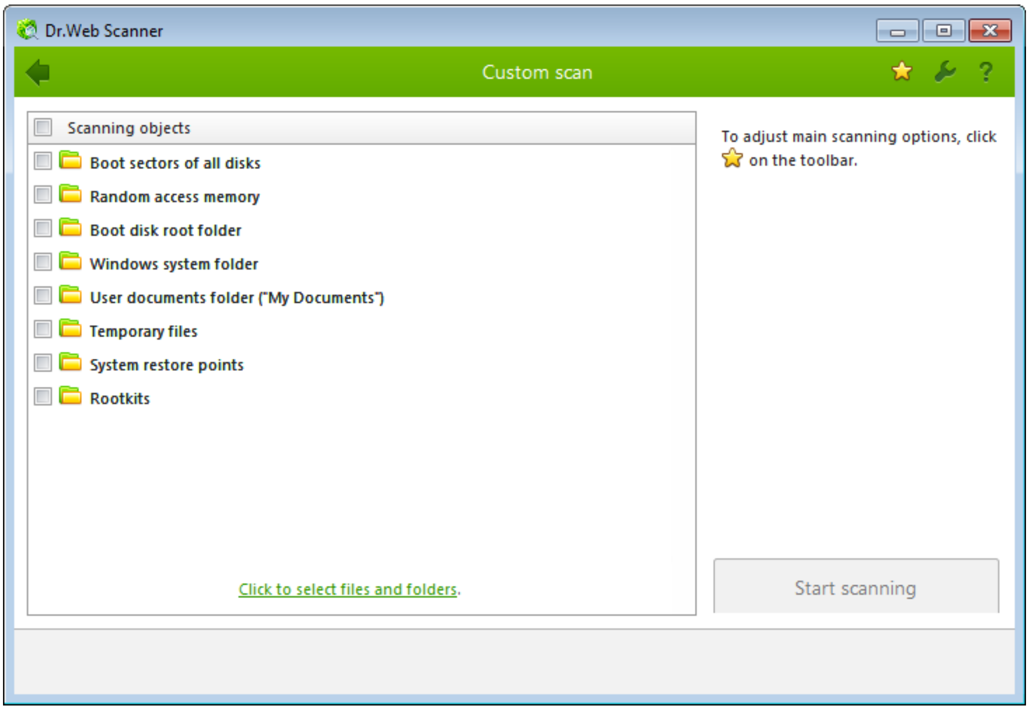
   In *Express* scan mode, **Scanner** checks the following:

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

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

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

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



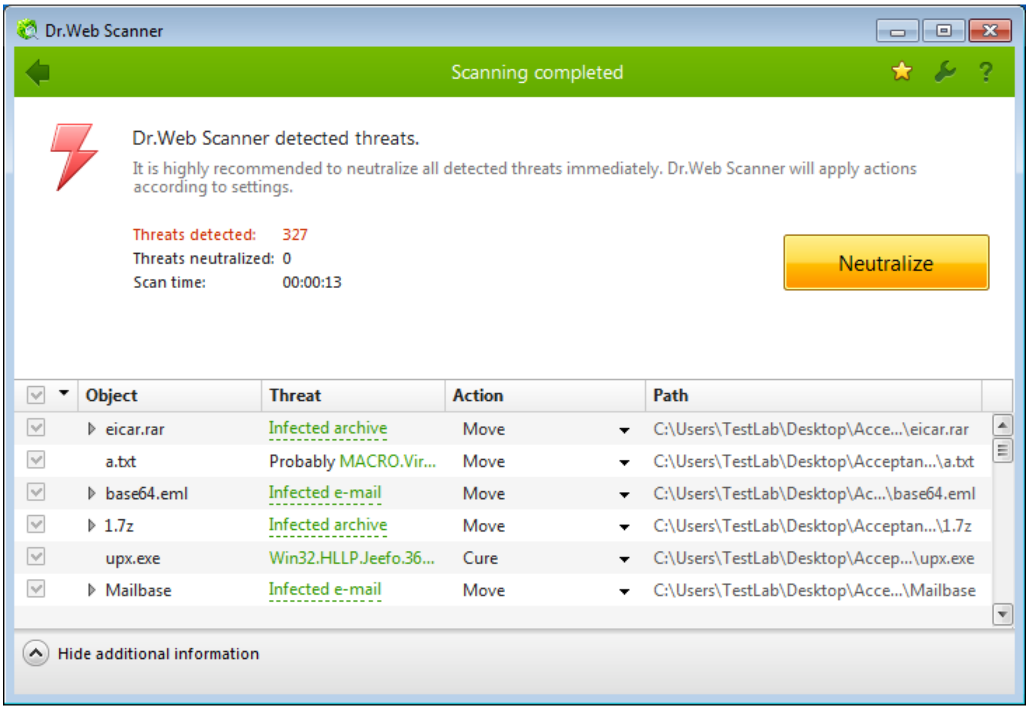
To adjust main scanning options, click ☆ on the toolbar.

4. If you launch a custom scan, you can select objects from the list to be scanned: any files and folders, and such objects as random access memory, boot sectors, and so on. To start scanning selected objects, click **Start scanning**. In full scan or express scan modes, objects cannot be selected manually.
5. When scanning starts, the **Pause** and **Stop** buttons become available. During scanning, you can do the following:
   - To pause scanning, click **Pause.** To resume scanning after pause, click **Resume**.
   - To stop scanning, click **Stop**.

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

## 8.2. Neutralizing Detected Threats

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



Dr.Web Scanner detected threats.

It is highly recommended to neutralize all detected threats immediately. Dr.Web Scanner will apply actions according to settings.

Threats detected: 327
Threats neutralized: 0
Scan time: 00:00:13

| Object | Threat | Action | Path |
|---|---|---|---|
| eicar.rar | Infected archive | Move | C:\Users\TestLab\Desktop\Acce...\eicar.rar |
| a.txt | Probably MACRO.Vir... | Move | C:\Users\TestLab\Desktop\Acceptan...\a.txt |
| base64.eml | Infected e-mail | Move | C:\Users\TestLab\Desktop\Ac...\base64.eml |
| 1.7z | Infected archive | Move | C:\Users\TestLab\Desktop\Acceptan...\1.7z |
| upx.exe | Win32.HLLP.Jeefo.36... | Cure | C:\Users\TestLab\Desktop\Accep...\upx.exe |
| Mailbase | Infected e-mail | Move | C:\Users\TestLab\Desktop\Acce...\Mailbase |

By clicking **Neutralize** you apply actions to the objects selected in the table. **Dr.Web** selects all objects by default once scanning completes. When necessary, you can customize selection of objects to be neutralized by using check boxes next to object names or threat categories from the drop-down menu in the table header.

### To select an action

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

There are the following limitations:

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

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

| Column name | Description |
|---|---|
| Object | This table column contains the name of an infected or suspicious object (it is a file name, if a file is infected, or **Boot sector**, if a boot sector is infected, or **Master Boot Record**, if an MBR of the hard drive is infected). |

| | |
|---|---|
| Threat | In this column, names of viruses or virus modifications are listed as per the internal classification of the **Doctor Web** package (a modification of a known virus is a code resulting from such alteration of a known virus which can still be detected, but cannot be treated with the curing algorithms applied to the initial virus). For suspicious objects, an indication that the object "is possibly infected" and the type of a possible virus according to the classification of the heuristic analyzer is displayed. |
| Action | Click an arrow on this button to select a custom action for a detected threat (by default, **Dr.Web Scanner** offers the most effective action).<br>You can apply the displayed action separately to each threat by clicking this button. |
| Path | The full paths to the corresponding files. |

If you selected **Automatically apply actions to threats** check box on the **Main** page, **Dr.Web Scanner** will neutralize threats automatically.

## 8.3. Scanner Settings

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

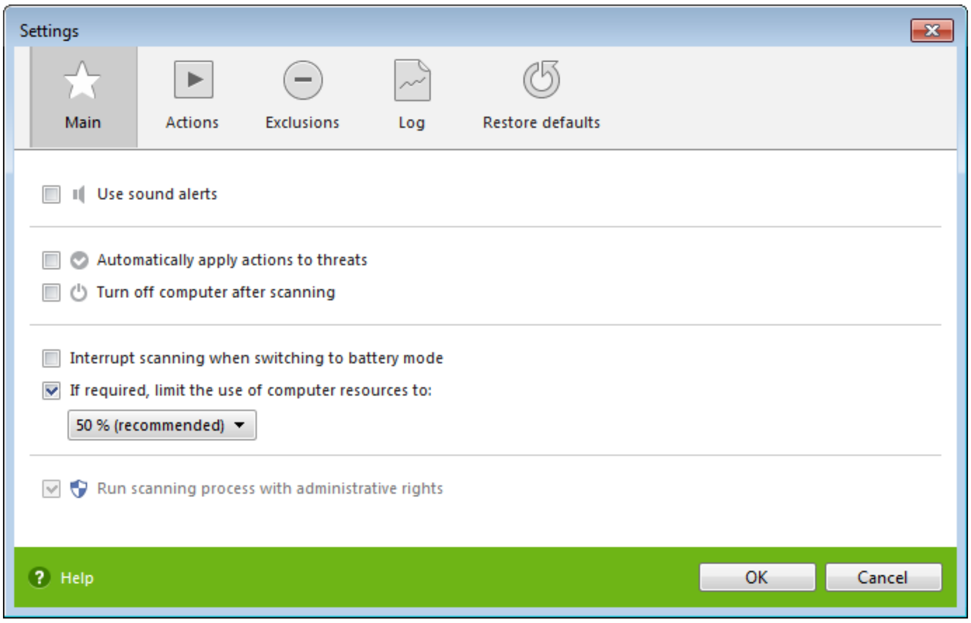
The default settings are optimal for most uses. Do not change them unnecessarily.

**To configure Scanner settings**

1. If **Dr.Web Scanner** is not running, click the **SpIDer Agent** icon and select **Scanner.** The **Dr.Web Scanner** window opens.
2. Click the **Settings** icon on the toolbar. This opens the window which contains several pages:
   - The Main page, where you can configure general parameters of **Dr.Web Scanner** operation
   - The Actions page, where you can configure reaction of the **Dr.Web Scanner** on detection of infected or suspicious files and archives or other malicious objects
   - The Exclusions page, where you can specify files and folders to be excluded from scanning
   - The Log page, where you can set logging options for **Dr.Web Scanner**.
   - The Restore defaults page, where you can restore the **Dr.Web Scanner** settings to their default values
2. Configure options as necessary.
3. For details on settings specified on each page, use the **Help** button.
4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

## Main Page

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



□ Use sound alerts

□ Automatically apply actions to threats

□ Turn off computer after scanning

□ Interrupt scanning when switching to battery mode

☑ If required, limit the use of computer resources to:

50 % (recommended)

☑ Run scanning process with administrative rights

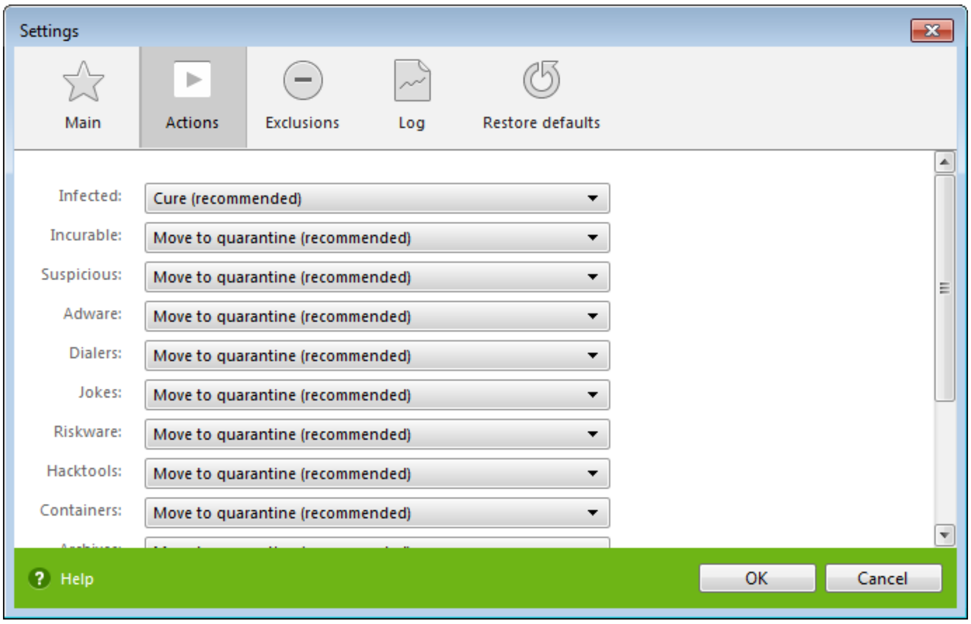
| Option | Description |
|---|---|
| Use sound alerts | Enable **Dr.Web Scanner** to use sound alerts for every event. |
| Automatically apply actions to threats | Select to enable **Dr.Web Scanner** to apply actions to detected threats automatically. |
| Turn off computer after scanning | Select to turn off the computer after scanning. If **Automatically apply actions to threats** is selected, **Dr.Web Scanner** will apply the specified actions to detected threats. |
| Interrupt scanning when switching to battery mode | Select to interrupt scanning when switching to battery mode. |
| If required, limit the use of computer resources to | Select to limit the use of computer resources by **Dr.Web Scanner** to the specified percent. If no other tasks are running on the computer, computer resources are used at maximum. |

You can also set these parameters in the **Dr.Web Scanner** Main window or Custom Scan Settings window. To set the parameters, click ☆ icon on the toolbar.

## Actions Page

### To set reaction to threat detection

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



Infected: Cure (recommended)
Incurable: Move to quarantine (recommended)
Suspicious: Move to quarantine (recommended)
Adware: Move to quarantine (recommended)
Dialers: Move to quarantine (recommended)
Jokes: Move to quarantine (recommended)
Riskware: Move to quarantine (recommended)
Hacktools: Move to quarantine (recommended)
Containers: Move to quarantine (recommended)

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

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

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

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

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

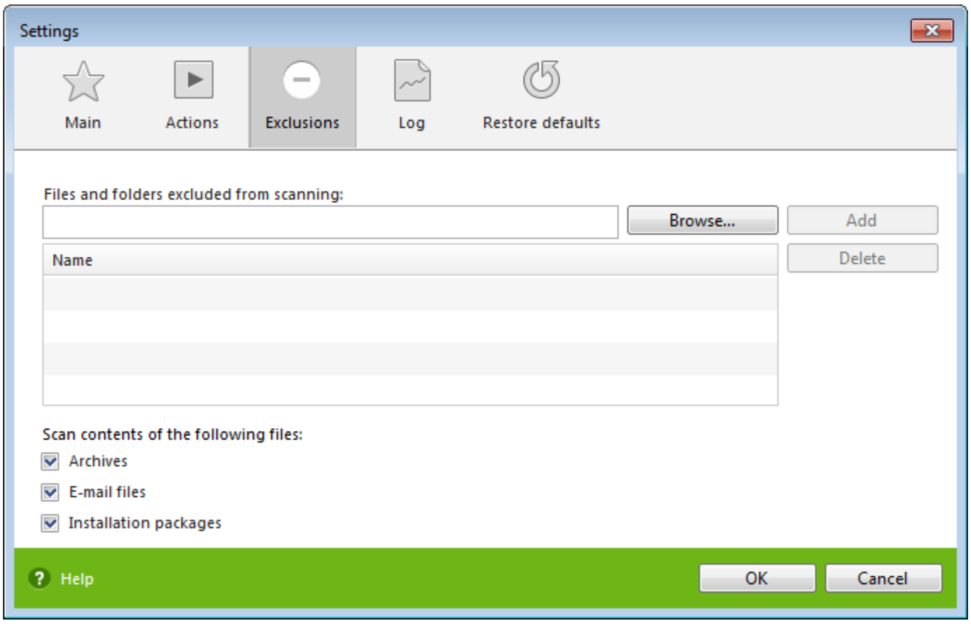
The best action for curable threats (e.g., files infected with known viruses) is curing, since it allows to restore the infected file completely. It is recommended to move other threats to quarantine in order to prevent loss of potentially valuable data. You can select one of the following actions:

| Action | Description |
|---|---|
| Cure | Instructs to restore the original state of an object before infection. If the object is incurable, or an attempt of curing fails, the action set for incurable viruses is applied.<br>This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects (archives, email attachments, file containers). Trojan programs are deleted on detection.<br>This is the only action available for boot sectors. |
| Move to Quarantine | Instructs to move the object to a specific folder for isolation.<br>This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector. |
| Delete | Instructs to delete the object.<br>This action is not available for boot sectors. No action is performed on malicious objects for which you selected this action, if they are detected in a boot sector. |
| Ignore | Instructs to skip the object without performing any action or displaying a notification.<br>The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware. |

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

## Exclusions Page

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



Files and folders excluded from scanning:

Scan contents of the following files:

- ☑ Archives
- ☑ E-mail files
- ☑ Installation packages

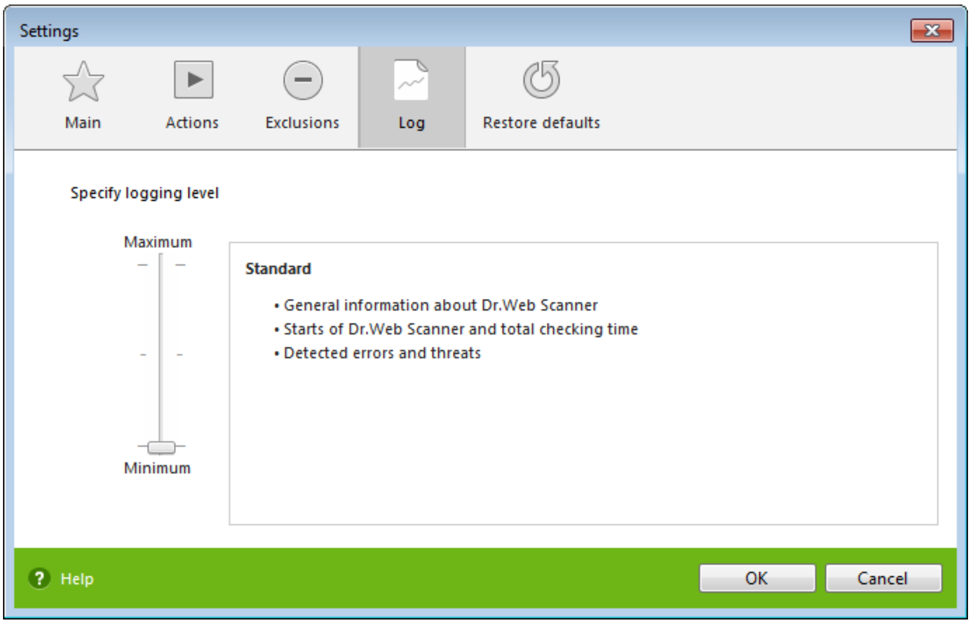
Here you can list names or masks for the files to be excluded from scanning. All files with the names which match the name or mask specified will be excluded from scanning (this option is appropriate for temporary files, swap files, etc.).

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

## Log Page

On this page, you can specify the logging mode.

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



Specify logging level

**Standard**

- General information about Dr.Web Scanner
- Starts of Dr.Web Scanner and total checking time
- Detected errors and threats

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

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

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

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

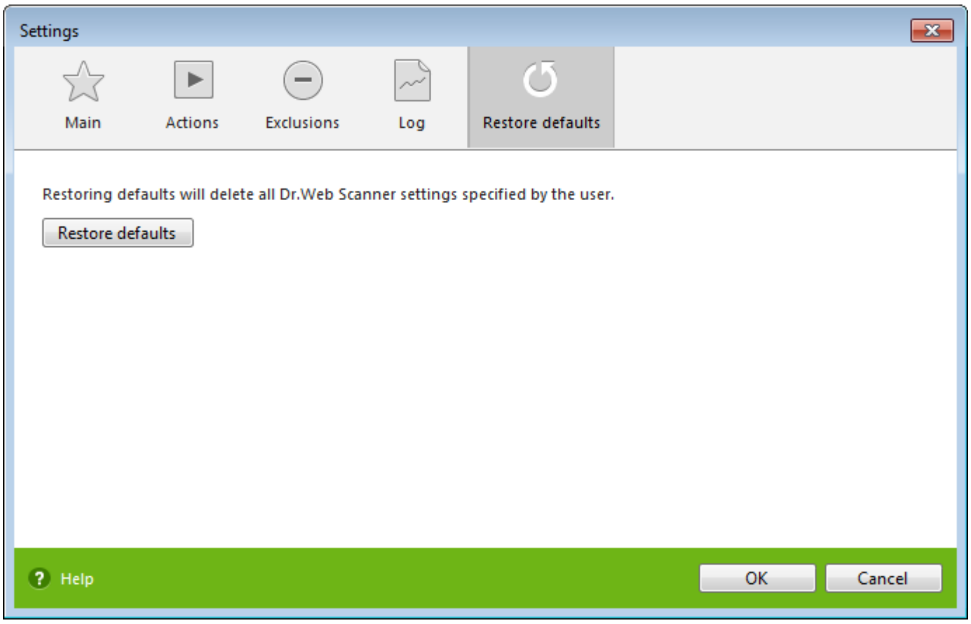
After scanning, if the log file size exceeds the limit, the content is reduced to:

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

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

## Restore Defaults Page

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



Restoring defaults will delete all Dr.Web Scanner settings specified by the user.

## 8.4. 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. Automatic activation of the **Scanner** according to schedule is performed in this mode.

### To run scanning from command line

For that purpose, use the following command:

[<*path_to_program*>]`dwscanner` [<*switches*>] [<*objects*>], where

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

The list of objects for scanning can be empty or contain several elements separated by spaces. The most commonly used examples of specifying the objects for scanning are given below:

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

## 8.5. Console Scanner

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

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

**To run Console Scanner**

The command syntax to launch **Console Scanner** is as follows:

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

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

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

After the operation is complete **Console Scanner** returns one of the following codes:

0 – scanning completed successfully; infected objects were not found
1 – scanning completed successfully; infected objects were detected
10 – invalid keys are specified
11 – key file is not found or does not support **Console Scanner**
12 – **Scanning Engine** did not start
255 – scanning was aborted by user request

## 8.6. Automatic Launch of Scanning

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

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

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

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

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

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

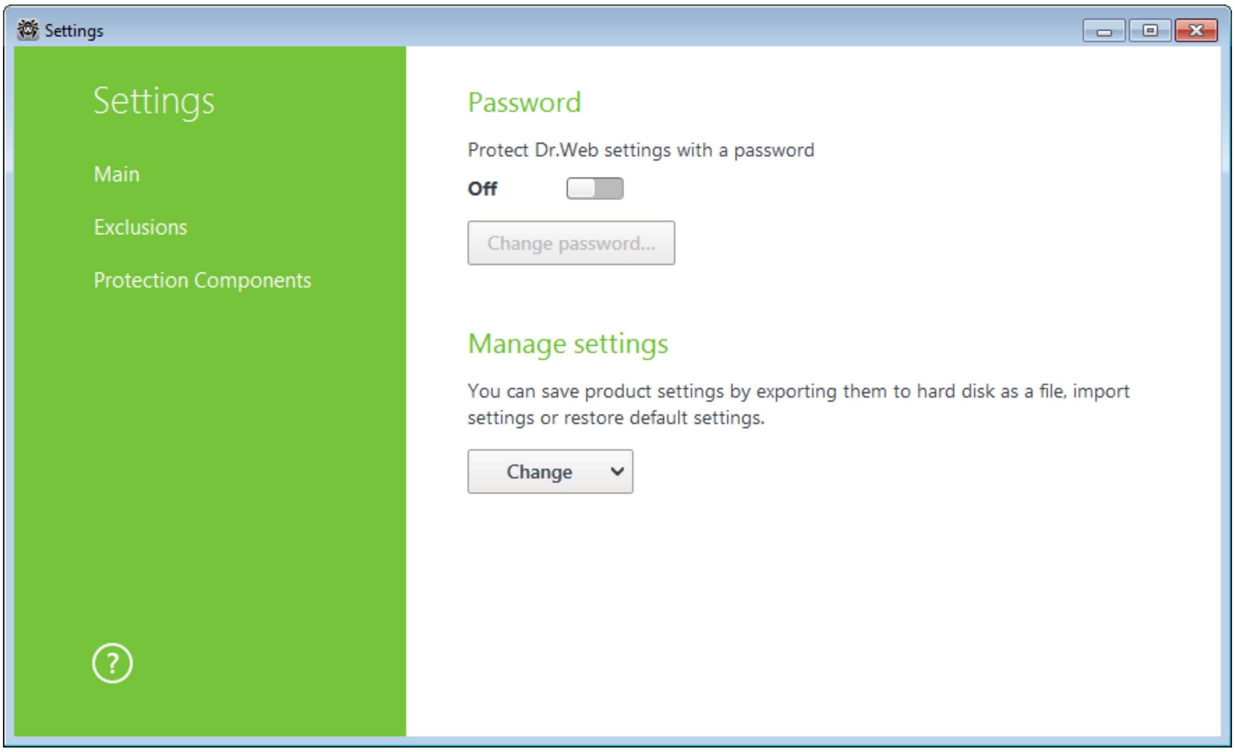
# 9. Settings

Managing settings is available only when having administrative privileges.

### Password protection

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

If you forgot your password for the product settings, contact technical support.



Password

Protect Dr.Web settings with a password

Off

Manage settings

You can save product settings by exporting them to hard disk as a file, import settings or restore default settings.

### Manage settings

To restore default settings, select **Reset settings** in the drop-down list.

If you want to use settings of **Dr.Web** anti-virus that you already configured on another computer, select **Export** in the drop-down list.

If you want to use your settings on other computers, select **Import** in the drop-down list. Then apply them on the same page of another anti-virus.

# 10. Main Settings

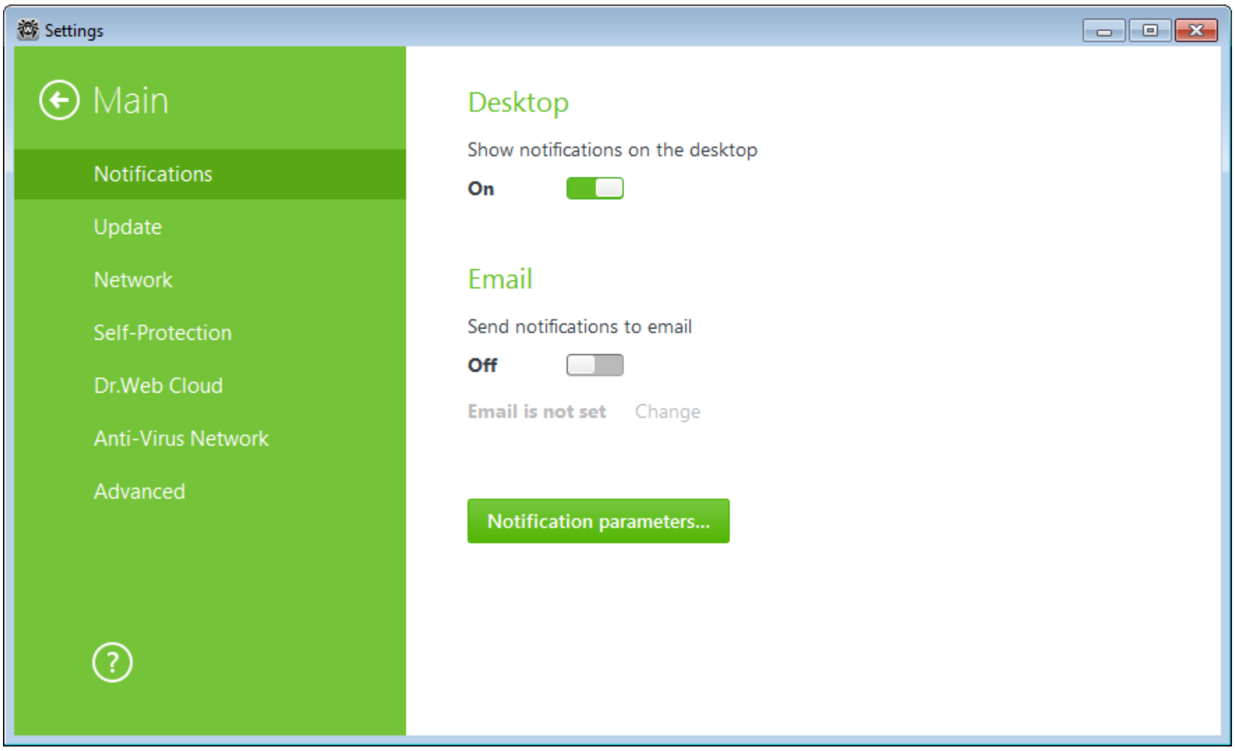
To access the main **Dr.Web Anti-virus** settings, you are prompted to enter the password if you enabled **Protect Dr.Web settings by password** option on the Settings window.

**Dr.Web Anti-virus** settings are available when run with administrative privileges.

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

## 10.1. Notifications

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



Desktop

Show notifications on the desktop

On

Email

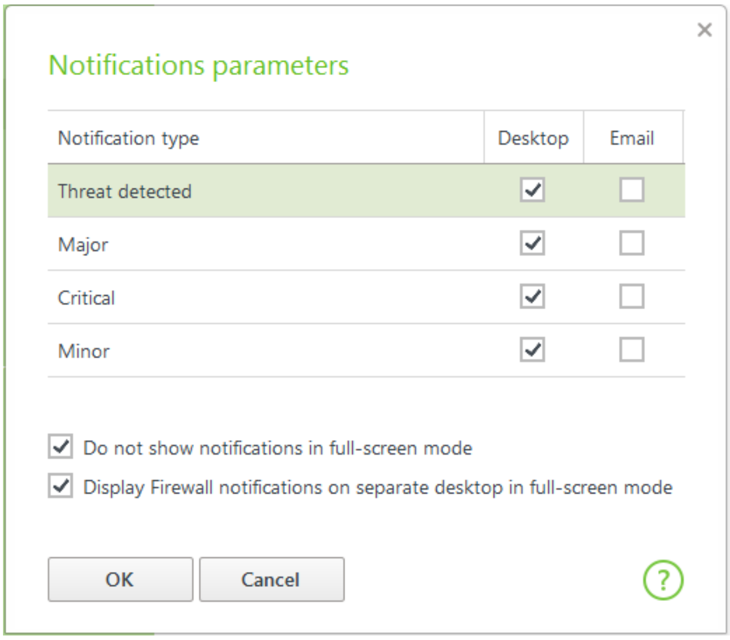
Send notifications to email

Off

Email is not set    Change

**Pop-up notifications**

1. Enable the **Show notifications on the desktop** option to get pop-up notifications.
2. Click **Notification parameters.** The window listing available notifications opens.



Notifications parameters

| Notification type | Desktop | Email |
|---|---|---|
| Threat detected | ☑ | □ |
| Major | ☑ | □ |
| Critical | ☑ | □ |
| Minor | ☑ | □ |

☑ Do not show notifications in full-screen mode

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

3. Select types of notifications that you want to receive and select the corresponding check boxes. To display pop-up notifications, select check boxes in the **Desktop** column. To receive mail notifications, select the check boxes in the **Email** column.
4. If necessary, configure additional parameters:

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

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

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

### To configure email notifications

1. Enable the **Send notifications to email** option.
2. Make sure that all the necessary email notifications in the **Notification parameters** window are selected.
3. Click **Change.** The window with email parameters opens.
4. Specify the following parameters:

| Option | Description |
|---|---|
| Email address | Enter an email address where to send the notifications. |
| SMTP Server | Enter the outgoing (SMTP) server for **Dr.Web Anti-virus** to use when sending email notifications. |
| Port | Enter the port for **Dr.Web Anti-virus** to use when connecting to the mail server. |
| Login | Enter the login for **Dr.Web Anti-virus** to use when connecting to the mail server. |

| Option | Description |
|---|---|
| Password | Enter the password for the login which is used when connecting to the mail server. |
| Security | Select the security level for connections to the mail server. |
| Authentication | Select the authentication method to be used when connecting to the mail server. |

5. Click **Test** to send a test message using the provided connection parameters. If you do not receive the message within several minutes, check the provided connection details.
6. After editing, click **OK** to save the changes or **Cancel** to cancel them.

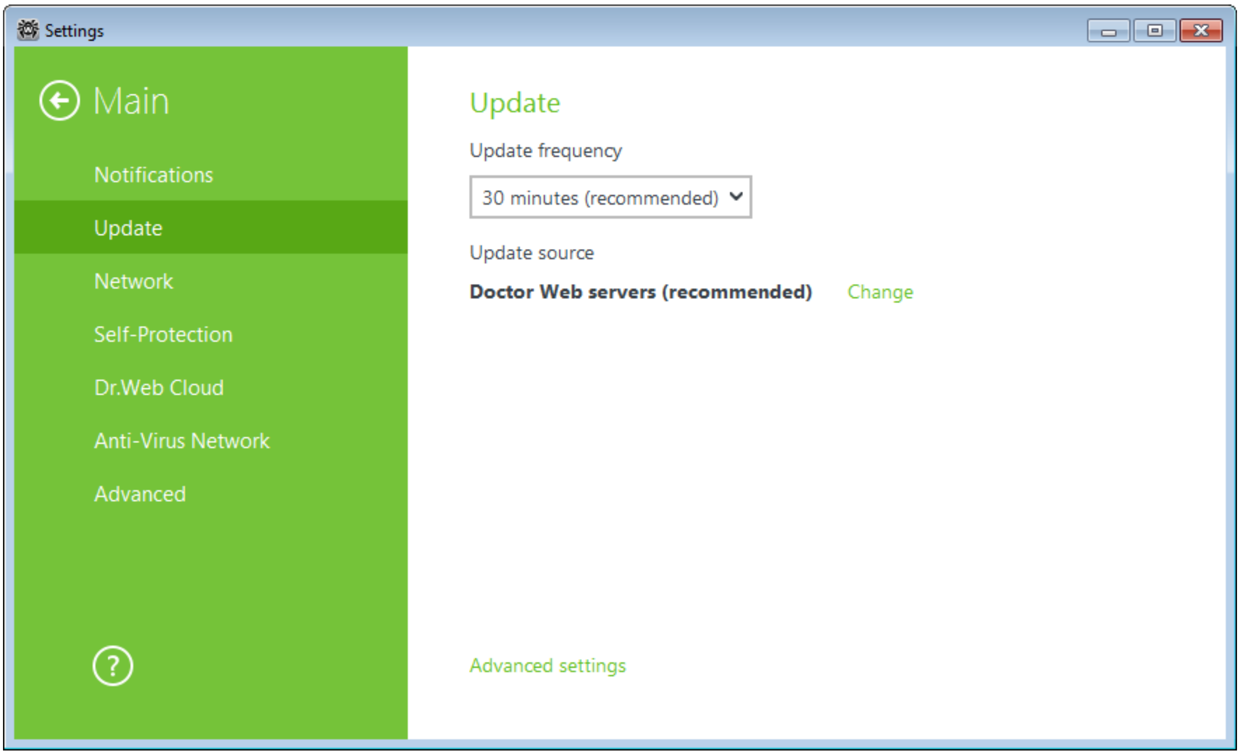
### Suspending notifications

To disable sending email notifications, clear the **Send notifications by email** check box.

To disable all types of notifications, clear the **Enable notifications** check box.

## 10.2. Update

On this page, you can configure protection of **Dr.Web Anti-virus** itself. You can also configure update parameters such as components that should be updated, an updating source, update period, proxy server, and update mirror.



Update

Update frequency

30 minutes (recommended)

Update source

Doctor Web servers (recommended) Change

### General update settings

**Update frequency**. Specify the frequency to check for updates. The default value (30 minutes) is optimal to keep information on threats current.

**Update source.** Specify the update source that suits you best by clicking the **Change** button.

- **Doctor Web servers (recommended)**. This source is selected by default.
- **Local or network folder –** update from local or network folder where updates have been copied. To specify the path to the folder, click **Browse** and select the required folder, or enter the address manually. Enter the user name and password if necessary.
- **Anti-virus Network –** updates are to be downloaded from a local network computer if Dr.Web product is installed and update mirror is created on it.

### Advanced settings

**Updating components**. You can choose one of the following ways of downloading the update:

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

### Update Mirror

To allow other local network computers with installed **Dr.Web** products to use your computer as an update source, click **Change** under the **Update mirror** and in the open window select **Create update mirror. Specify the path to the folder, where updates will be copied. If your computer is connected to several networks, you can specify** IP address available to computers of only one network. You can also specify the port for HTTP connections.

## 10.3. Network

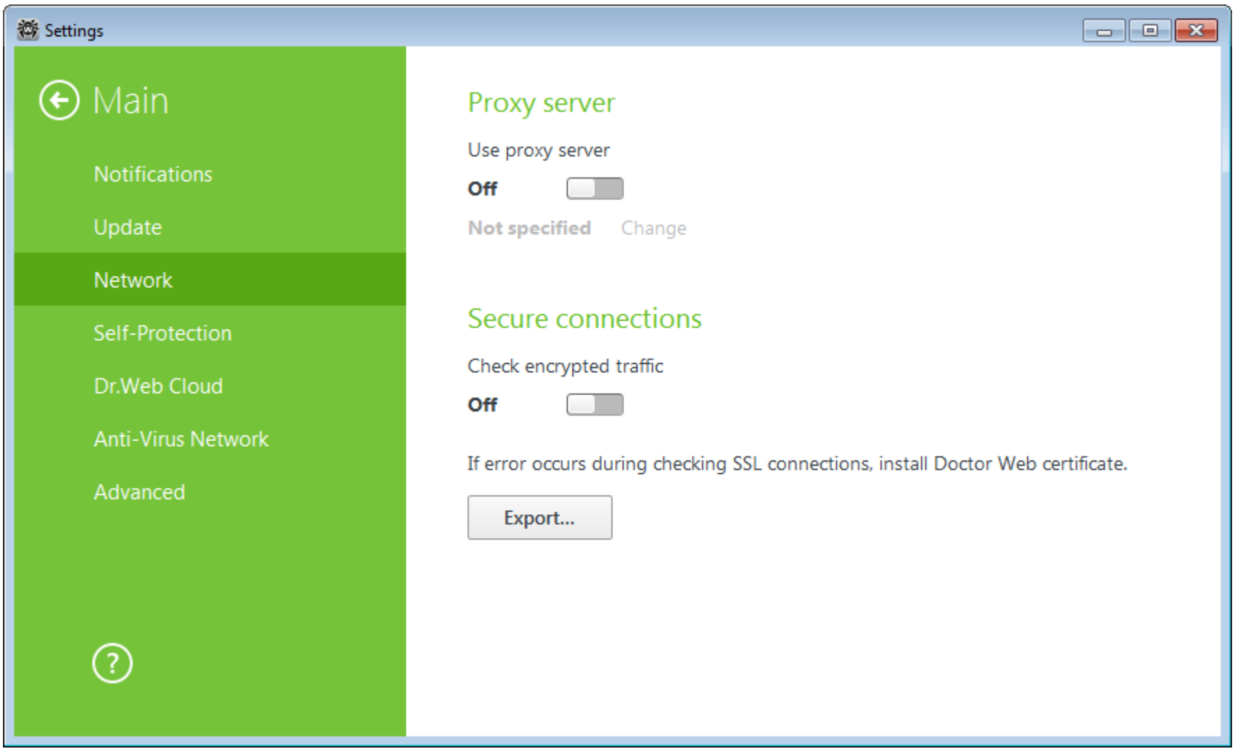
### Proxy Server

By default, all components use direct connection mode. If necessary, you can enable use of a proxy server and specify its connection settings. To do that, click **Change.** The window with proxy server parameters opens.

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

### Secure Connections

You can enable scanning of data transmitted over secure protocols. To check such data, select the **Check encrypted traffic** check box. If your client application that uses secure connections does not refer to the default Windows system certificate storage, then you need to export the certificate.



Proxy server

Use proxy server

Off

Not specified Change

Secure connections

Check encrypted traffic

Off

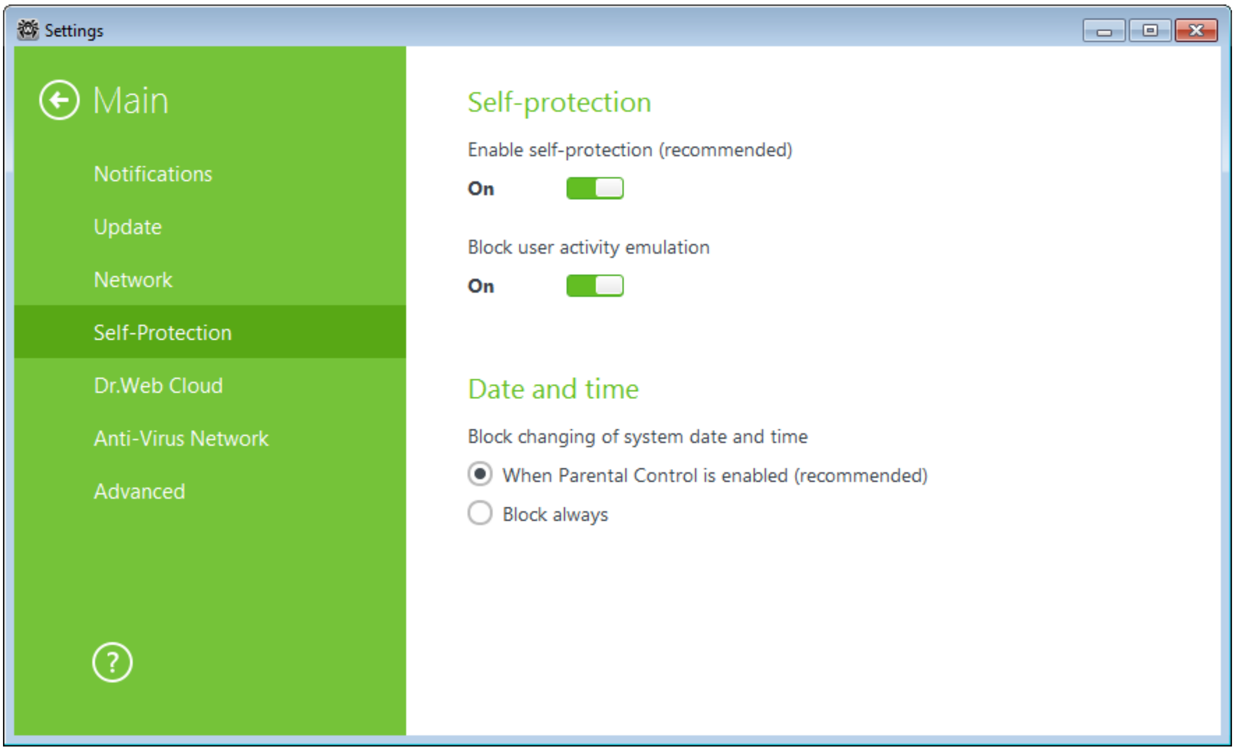
If error occurs during checking SSL connections, install Doctor Web certificate.

### Doctor Web Certificate

You may need to scan data transmitted in accordance with SSL protocol. For instance, you can configure **SpIDer Gate** to check encrypted data transferred over HTTPS protocol and configure **SpIDer Mail** to check messages sent over POP3S, SMTPS, or IMAPS. In order for **Dr.Web** 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.

## 10.4. Self-protection

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



Self-protection

Enable self-protection (recommended)

On

Block user activity emulation

On

Date and time

Block changing of system date and time

● When Parental Control is enabled (recommended)

○ Block always

The **Enable Self-protection** option allows to protect **Dr.Web Anti-virus** files, registry keys, and processes from damage or deletion. It is not recommended to disable Self-protection.

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

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

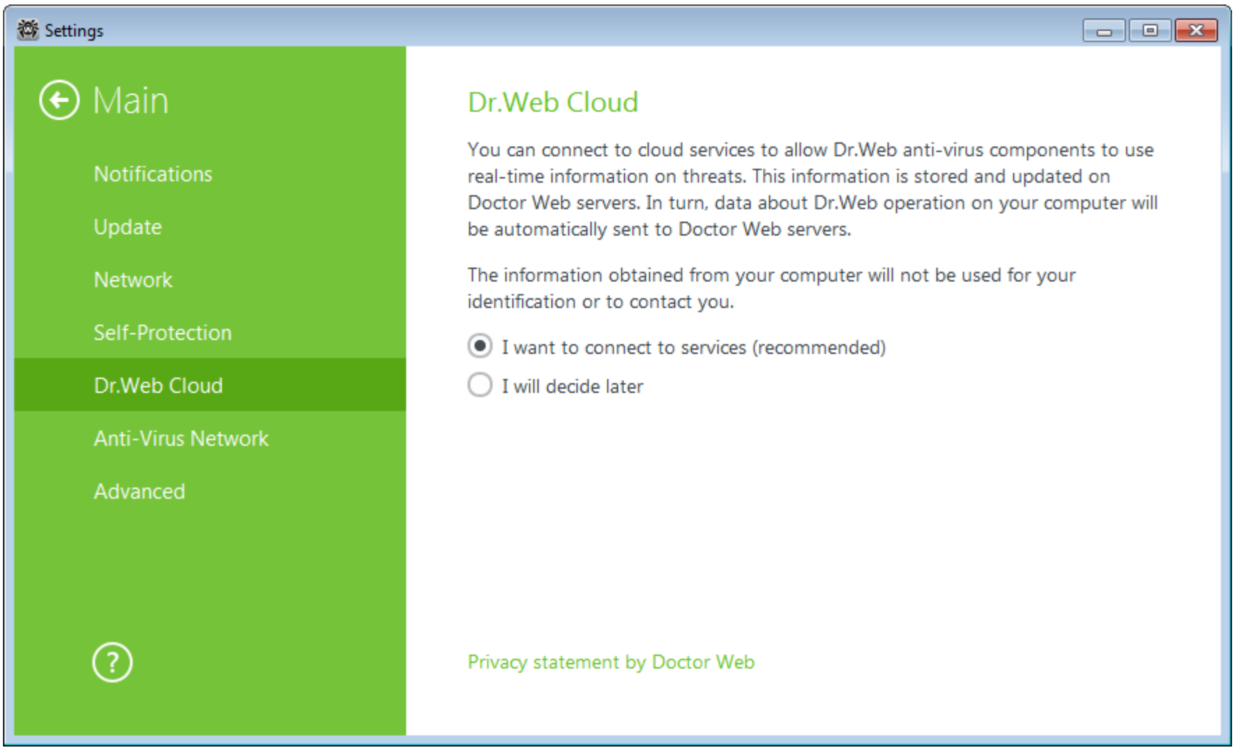
The **Block user activity emulation** option allows to prevent any automatic changes in **Dr.Web Anti-virus** operation, including execution of scripts that emulate user interaction with **Dr.Web Anti-virus** and are launched by the user.

The **Block changing of system date and time** option allows to prevent manual and automatic changes of the system date and time as well as of the time zone. This restriction is set for all system users. You can configure notification parameters so that to be informed on attempt to change the system time.

To restrict access to **Dr.Web Anti-virus** settings on your computer, enable the **Protect Dr.Web settings with a password** option in the Settings section.

## 10.5. Dr.Web Cloud

On this page, you can connect to **Doctor Web** cloud services and take part in **Dr.Web** quality improvement program.



Dr.Web Cloud

You can connect to cloud services to allow Dr.Web anti-virus components to use real-time information on threats. This information is stored and updated on Doctor Web servers. In turn, data about Dr.Web operation on your computer will be automatically sent to Doctor Web servers.

The information obtained from your computer will not be used for your identification or to contact you.

● I want to connect to services (recommended)

○ I will decide later

Privacy statement by Doctor Web

### Cloud Services

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

Depending on update settings, information on threats used by anti-virus components may become out of date. Cloud services can reliably prevent users from viewing unwanted websites and protect your system from infected files.

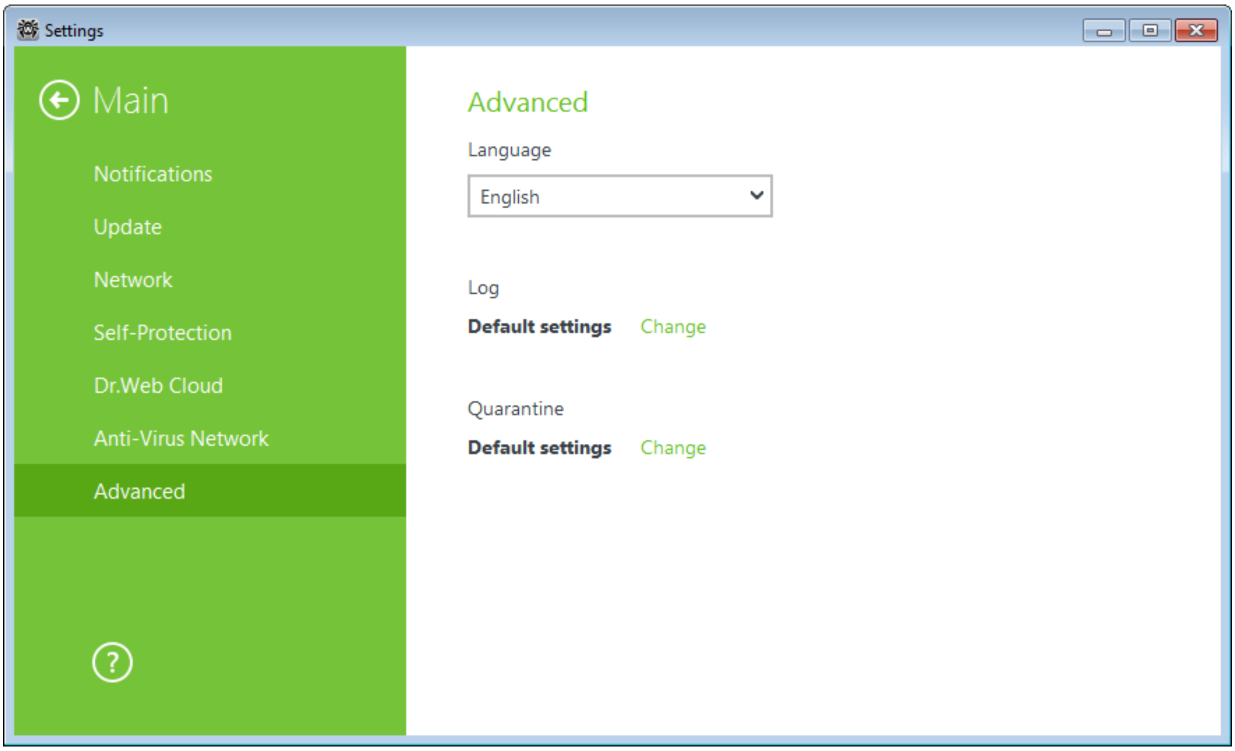
### Software Quality Improvement Program

If you participate in the software quality improvement program, impersonal data about **Dr.Web Anti-virus** operation on your computer will be periodically sent to the **Doctor Web** servers, for example, information on created rule sets for **Dr.Web Firewall**. Received information is not used to identify or contact you.

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

## 10.7. Advanced

On this page, you can configure additional settings.



Advanced

Language: English

Log
Default settings Change

Quarantine
Default settings Change

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

### Log settings

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

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

| Component | Information |
|---|---|
| **SpIDer Guard** | Time of updates and **SpIDer Guard** starts and stops, virus events, names of scanned files, names of packers and contents of scanned complex objects (archives, email attachments, file containers).<br>It is recommended to use this mode to determine the most frequent objects scanned by **SpIDer Guard**. If necessary, you can add these objects to the list of exclusions in order to increase computer performance. |
| **SpIDer Mail** | Time of updates and **SpIDer Mail** starts and stops, virus events, connection interception settings, names of scanned files, names of packers and contents of scanned archives.<br>It is recommended to use this mode when testing mail interception settings. |
| **Dr.Web Firewall** | **Dr.Web Firewall** does not log its operation in the standard mode. When you enable detailed logging, **Firewall** collects data on network packets (pcap logs). |
| **Dr.Web Updater** | List of updated **Dr.Web Anti-virus** files and their download status, date and time of updates, and details on auxiliary script execution and **Dr.Web Anti-virus** component restart. |

| Component | Information |
|---|---|
| **Dr.Web Services** | Information on **Dr.Web** components, changing of component settings, component starts and stops, preventive protection events, connections to anti-virus network. |

### Memory dump creation

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

### Enabling detailed logging

Logging detailed data on **Dr.Web Anti-virus** operation may result in considerable log file growth and increase in process load. It is recommended to use this mode only when errors occur in component operation or by request of **Doctor Web** technical support.

1. To enable detailed logging for a **Dr.Web Anti-virus** component, select the corresponding check box.
2. By default, detailed logging is enabled until the first restart of the operating system. If it is necessary to log component activity before and after the restart, select the **Continue detailed logging after restart (not recommended)** check box.
3. Save the changes.

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

## Quarantine settings

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

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

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

### To empty Quarantine

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

Use **Advanced** settings to select the isolation mode for infected objects detected on portable data carriers. By default, detected threats are moved to the folder on this data carrier without being encrypted. The **Quarantine** folder is created on portable data carriers only when they are accessible for writing. The use of separate folders and omission of encryption on portable data carriers prevents possible data loss.

# 11. Exclusions

## 11.1. Files and Folders

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

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

**Configuring list of exclusions**

1. To add a file or folder to the exclusion list, do one of the following:
   - To add an existing file or folder, click ⊕. In the open window, click **Browse** and select it in the standard dialog window. You can enter the full path to the file or folder, or edit the path in the field before adding it to the list.
   - To exclude all files or folders with a particular name, enter the name without path.
   - To exclude a group of files or folders, enter the mask of their names.
2. Click **OK.** The file or folder will appear in the list.
3. To list other files and folders, repeat steps 1 to 2. To remove a file or folder from the list, select the corresponding item and click 🗑**.**

Examples:

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

## 11.2. Programs and Processes

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

**To configure list of exclusions**

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

# 12. Protection components

## 12.1 SpIDer Guard

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

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

Files within archives and mailboxes are not checked. If a file within an archive or email attachment is infected, the malicious object will be detected and neutralized by **SpIDer Guard** immediately when you try to extract archived files or download the attachment. To prevent spread of viruses and other malicious objects with email, use **SpIDer Mail**.

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

You can also connect to **Doctor Web** cloud services which allow anti-virus components to use the latest information on threats. This information is stored and updated on **Doctor Web** servers in real-time mode.

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

### 12.1.1. Configuring SpIDer Guard

To access the **SpIDer Guard** settings, you are prompted to enter the password if you enabled **Protect Dr.Web settings by password** option on the Settings window.

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

#### Background Rootkit Scanning

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

If this option is enabled, **Dr.Web Anti-rootkit** constantly resides in memory. In contrast to on-the-fly scanning of files by **SpIDer Guard**, scanning for rootkits includes checking of autorun objects, running processes and modules, Random Access Memory (RAM), MBR/VBR disks, computer BIOS system and other system objects.

One of the key features of the **Dr.Web Anti-rootkit** is delicate attitude towards consumption of system resources (processor time, free RAM and others) as well as consideration of hardware capacity.

When **Dr.Web Anti-rootkit** detects a threat, it notifies you on that and neutralizes the malicious activity.

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

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

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

## Actions

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

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

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

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

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

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

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

**SpIDer Guard** does not check complex objects. No action is performed on such objects or files within them.

Copies of all processed objects are stored in Quarantine.

## Scan Mode

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

| Option | Description |
|---|---|
| Optimal (recommended) | This scan mode is used by default.<br>In this mode, **SpIDer Guard** scans objects only when one of the following actions is traced:<br>• For objects on hard drives, an attempt to execute a file, create a new file or add a record to an existing file or boot sector.<br>• For objects on removable devices, an attempt to access file or boot sectors in any way (write, read, execute). |
| Paranoid | In this mode, **SpIDer Guard** scans files and boot sectors on hard or network drives and portable data storages at any attempt to access them (create, write, read, execute). |

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

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

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

In any mode, objects on removable media and network drives are scanned only if the corresponding check boxes in the **Additional tasks** group are selected.

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

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

## Additional Tasks

The settings of this group allow to specify parameters for scanning objects "on-the-fly" and are always applied regardless of the selected **SpIDer Guard** operation mode. You can also select **Block autoruns from removable media** check box to disable autoplay option for portable data storages such as CD/ DVD, flash memory, and so on.This option helps to protect you computer from viruses transmitted via removable media.

In this 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

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

## 12.2. SpIDer Mail

**SpIDer Mail** is an anti-virus mail scanner that installs by default and monitors data exchange between mail clients and mail servers made via POP3, SMTP, IMAP4, or NNTP (IMAP4 stands for IMAPv4rev1) protocols..

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

### Mail Processing

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

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

- Malicious code is removed from infected messages, then messages are delivered as usual. This action is called curing the message.
- Messages with suspicious objects are moved to **Quarantine** as separate files; the mail client receives a notification about this.
- Unchecked messages are passed as those that are not infected.
- All deleted or moved messages are saved on a POP3 or IMAP4 server.

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

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

- Not all formats of popular mailboxes are supported by **Scanner**. When using **SpIDer Mail**, the infected messages are even not delivered to mailboxes.
- **Scanner** does not check the mailboxes at the moment of the mail receipt, but either on user demand or according to schedule.

Thus, when all anti-virus components are operating with their default settings, **SpIDer Mail** detects viruses and suspicious objects distributed via email first and prevents them from infiltrating into your computer. **SpIDer Mail** operation is rather resource-sparing; scanning of email files can be performed without other components.

## 12.2.1. Configuring SpIDer Mail

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

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

### Scan Options

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

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

### Actions

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

The **SpIDer Mail** reactions are similar to those of **Dr.Web Scanner**. You can select one of the following actions applied by **SpIDer Mail** to detected threats:

| Action | Description |
|---|---|
| Cure | Instructs to try to restore the original state of the message before infection. If the message is incurable, or the attempt of curing fails, the action set for incurable message is applied.<br>Available for Infected messages only except Trojan programs that are deleted on detection. This is action is not applicable to files within archives. |
| Delete | Instructs to delete the message. The message is not sent to recipient; the mail client receives a notification about this. |
| Move to Quarantine | Instructs to move the message to the special Quarantine folder. The message is not sent to the recipient; the mail client receives a notification about this. |
| Ignore | Instructs to pass the message to the mail client as usual, i.e. without performing any action. |

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

To increase security above the default level, you may select the **Move to quarantine** action for **Unchecked messages**, and then scan the moved file with **Dr.Web Scanner**.

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

After performing reaction you configured, **SpIDer Mail** can display a notification in the notification area. If necessary, you can configure desktop and email notifications.

## Actions on Messages

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

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

## Scanning Optimization Options

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

## Scanning archives

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

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

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

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

## 12.3. Dr.Web Firewall

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

**Firewall** provides you with the following features:

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

### 12.3.1. Training Firewall

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

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

**To set application rules**

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

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

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

You need administrative privileges to create a rule.

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

**To set parent process rules:**

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

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

## 12.3.2. Configuring Firewall

⚠ To access the **Firewall** settings, you are prompted to enter the password if you enabled **Protect Dr.Web settings by password** option on the Settings window.

To start using **Firewall**, do the following:

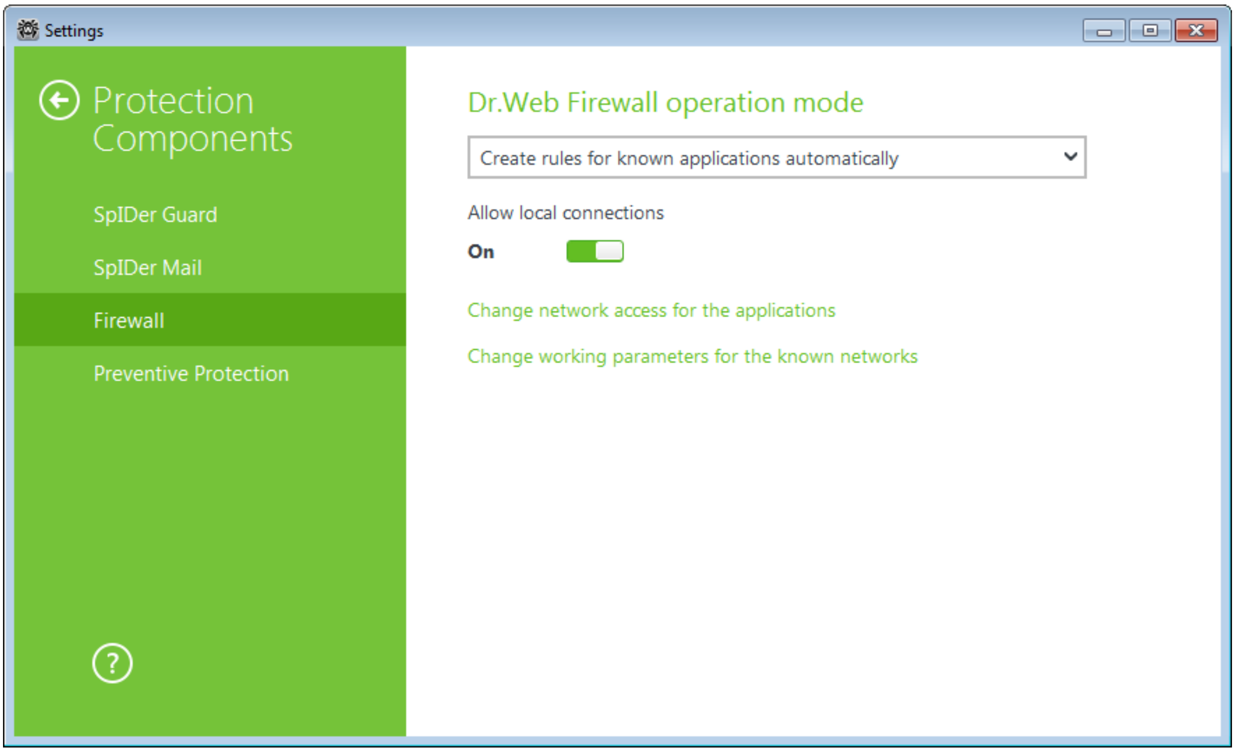
- Select the operation mode
- List authorized applications
- Configure parameters for known networks

By default, **Firewall** operates in training mode. Regardless of the operation mode, events are logged.

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

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

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



Settings

Protection Components

Dr.Web Firewall operation mode

Create rules for known applications automatically

Allow local connections

On

Change network access for the applications

Change working parameters for the known networks

## Operation modes

Select one of the following operation modes:

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

### Create rules for known applications automatically

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

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

This mode is used by default.

### Interactive learning mode

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

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

#### Block unknown connections

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

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

#### Allow unknown connections

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

### Rules for Applications

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

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

This page lists all applications and processes for which there is an application filter rule set. You can create new filter rule sets as well as edit the existing ones or delete those that are unnecessary. Each application is explicitly identified by the path to its executable file. **Firewall** uses the `SYSTEM` name to indicate the rule set applied to the operating system kernel (the system process for which there is no unique executable file).

If the file of an application for which the rule was created changes (e.g., an update was installed), **Firewall** prompts to confirm that the application is still allowed to access network resources.

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

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

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

To open this window, in the **Firewall** settings window, select the **Applications** page and click **Create** or select an application and click **Edit**.

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

## Launching other applications

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

- **Allow** – if you want to enable the application to run other processes;
- **Block** – if you want to disable the application to run other processes;
- **Not specified** – if you want to use the settings specified for the selected operation mode of **Firewall**.

## Access to network resources

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

| Parameter | Description |
|---|---|
| Enabled | Status of the rule. |
| Action | The action for **Dr.Web Firewall** to perform when an attempt to connect to the Internet is detected:<br>• **Block packets –** block the connection;<br>• **Allow packets –** allow the connection. |
| Rule name | The rule name. |
| Direction | The direction of the connection:<br>• **Inbound –** the rule is applied when someone from the network attempts to connect to an application on your computer.<br>• **Outbound –** the rule is applied when an application on your computer attempts to connect to the network.<br>• **Any –** apply the rule regardless of packet transfer direction. |
| Description | User description of the rule. |

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

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

### To create a rule

Configure the following parameters:

| Parameter | Description |
|---|---|
| **General** | |
| Rule name | The name of the created/edited rule. |
| Description | The rule description. |
| Action | The action for **Dr.Web Firewall** to perform when an attempt to connect to the Internet is detected:<br>• **Block packets –** block the connection;<br>• **Allow packets –** allow the connection. |
| State | Rule status:<br>• **Enabled –** the rule is applied for all matching connections.<br>• **Disabled –** the rule is temporary not applied. |
| Direction | The direction of the connection:<br>• **Inbound –** the rule is applied when someone from the network attempts to connect to an application on your computer.<br>• **Outbound –** the rule is applied when an application on your computer attempts to connect to the network.<br>• **Any –** apply the rule regardless of packet transfer direction. |
| Logging | Logging mode:<br>• **Enabled –** register events;<br>• **Disabled –** no information is logged. |
| **Rule Settings** | |
| Protocol | The network and transport level protocols used for the connection attempt.<br>The following protocols of the network level are supported:<br>• **IPv4**;<br>• **IPv6**;<br>• **IP all –** any version of the IP protocol.<br>The following protocols of the transport level are supported:<br>• **TCP**;<br>• **UDP**;<br>• **TCP & UDP** – TCP or UDP protocol<br>• **RAW**. |
| Local address/<br>Remote address | The IP address of the remote host. You can specify either a certain address (**Equals**) or several IP addresses using a range (**In range**), specific subnet mask (**Mask**), or masks of all subnets, in which your computer has a network address (**MY_NETWORK**).<br>To apply the rule for all remote hosts, select **Any**. |
| Local port/<br>Remote port | The port used for the connection. You can specify either a specific port number (**Equals**) or a port range (**In range**).<br>To apply the rule for all ports, select **Any**. |

## Rules for Networks

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

**To set rule sets for network interfaces**

1. In the **Firewall** settings window, select **Interfaces**.
2. For the required interface, select the appropriate rule set. If the appropriate rule set does not exist, you can create a new set of packet filtering rules.
3. Click **OK** to save the changes.

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

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

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

Thus, packet filtering provides you with more general mechanisms to control access to network than the application level filtering.

**Firewall** uses the following predefined rule sets:

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

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

**To set rule sets for network interfaces**

In the **Firewall** settings window, select **Interfaces** and click **Configure.** On this page you can:

- Configure sets of filtering rules by adding new rules, modifying existing ones or deleting them.
- Configure additional filtering settings.

**To configure rule sets**

Do one of the following:

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

**To configure additional settings**

In the **Packet filter settings** window, use the following options:

| Option | Description |
|---|---|
| Use TCP stateful packet filtering | Select this check box to filter packets according to the state of existing TCP connections. **Firewall** will block packets that do not match active connections according to the TCP protocol specification. This option helps protect your computer from DoS attacks (denial of service), resource scanning, data injection, and other malicious operations. |

| Option | Description |
|---|---|
| | It is also recommended to enable stateful packet filtering when using complex data transfer protocols (FTP, SIP, etc.).<br>Clear this check box to filter packets without regard to the TCP session state. |
| Management of fragmented IP packets | Select this check box to ensure correct processing of large amounts of data. The maximum transmission unit (MTU) may vary for different networks, therefore large IP packets may be fragmented. When this option is enabled, the rule selected for the first fragment of a large IP packet is applied to all other fragments.<br>Clear this check box to process fragmented packets independently. |

## Rule Sets

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

For each rule in the set, the following information displays:

| Parameter | Description |
|---|---|
| Enabled | Status of the rule. |
| Action | The action for **Firewall** to perform when the packet is intercepted:<br>• **Block packets**<br>• **Allow packets** |
| Rule name | The rule name. |
| Direction | The direction of the connection:<br>• ⇦ – the rule is applied when the packet is received from the network.<br>• ⇨ – the rule is applied when a packet is sent into the network from your computer.<br>• ⇆ – the rule is applied regardless of packet transfer direction. |
| Logging | The logging mode for the rule. This parameter defines which information is stored in the log:<br>• **Headers only –** log the packet header only.<br>• **Entire packet –** log the whole packet.<br>• **Disabled –** no information is logged. |
| Description | The rule description. |

### Edit rule set

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

Packets with no rules in a rule set are blocked automatically except packets allowed by Application Filter rules.

## Packet Filter Rule Sets

### To add or edit a rule

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

| Parameter | Description |
|---|---|
| Rule name | The name of the created/edited rule. |
| Description | The rule description. |
| Action | The action for **Firewall** to perform when the packet is intercepted:<br>• **Block packets**<br>• **Allow packets** |
| Direction | The direction of the connection:<br>• **Inbound –** the rule is applied when the packet is received from the network.<br>• **Outbound –** the rule is applied when the packet is sent into the network from your computer.<br>• **Any –** apply the rule regardless of packet transfer direction. |
| Logging | The logging mode for the rule. This parameter defines which information is stored in the log:<br>• **Entire packet –** log the whole packet.<br>• **Headers only –** log the packet header only.<br>• **Disabled –** no information is logged. |
| Criterion | Filtering criterion. For example, transport or network protocol. To add a filtering criterion, select it from the list and click **Add.** You can add any number of filtering criteria. For certain headers there are additional criteria available. |

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

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

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

# 12.4. Dr.Web for Outlook

## Main Functions

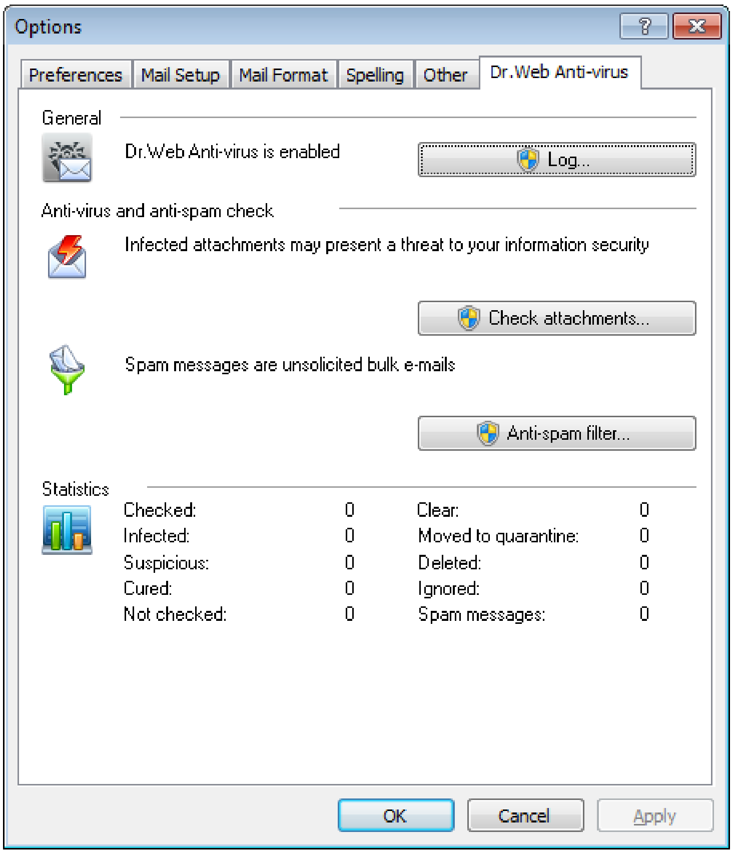
**Dr.Web for Outlook** plug-in performs the following functions:

- Anti-virus check of email attachments
- Check of email attachments transferred over encrypted SSL connections
- Detection and neutralization of malware
- Heuristic analysis for additional protection against unknown viruses

## 12.4.1. Configuring Dr.Web for Outlook

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

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



Dr.Web Anti-virus is enabled

Infected attachments may present a threat to your information security

Spam messages are unsolicited bulk e-mails

| | | | |
|---|---|---|---|
| Checked: | 0 | Clear: | 0 |
| Infected: | 0 | Moved to quarantine: | 0 |
| Suspicious: | 0 | Deleted: | 0 |
| Cured: | 0 | Ignored: | 0 |
| Not checked: | 0 | Spam messages: | 0 |

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

- Log – allows to configure the program logging.

- Check attachments – allows to configure email check and to specify program actions on detection of malicious objects.
- Statistics – allows viewing the number of checked and processed objects.

## 12.4.2. Threat Detection

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

### Types of Threats

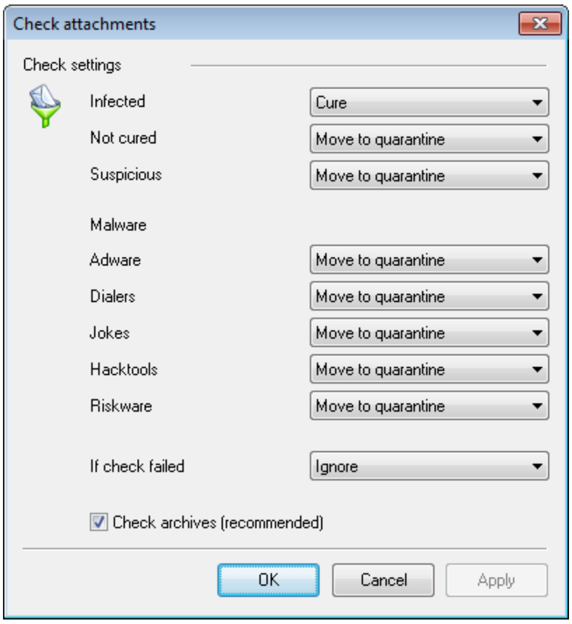
**Dr.Web for Outlook** detects the following malicious objects:

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

### Configuring Actions

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

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



Check attachments

Check settings

Infected: Cure

Not cured: Move to quarantine

Suspicious: Move to quarantine

Malware

Adware: Move to quarantine

Dialers: Move to quarantine

Jokes: Move to quarantine

Hacktools: Move to quarantine

Riskware: Move to quarantine

If check failed: Ignore

☑ Check archives (recommended)

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

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

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

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

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

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

For different types of objects, actions are specified separately.

**The following actions for detected virus threats are available:**

- **Cure** (only for infected objects) – instructs to try to restore the original state of an object before infection.
- **As incurable** (only for infected objects) – means, that the action specified for incurable objects will be performed.
- **Delete –** delete the object.
- **Move to quarantine** – move the object to the special Quarantine folder.
- **Skip –** skip the object without performing any action or displaying a notification.

## 12.4.3. Logging

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

- Windows Event Log
- Debug Text Log

### 7.4.1. Event Log

The following information is registered in the Windows Event Log:

- Program starts and stops.
- Key file parameters: license validation, license expiration date (information is logged on program startup, while the program is running, and when the key file is changed).
- Parameters of program modules: scanner, engine, virus databases (information is logged on program startup and module update).
- License errors: the key file is absent, permissions for program module usage is absent in the key file, the license is blocked, the key file is corrupted (information is logged on program startup and while the program is running).
- Information on threat detection.
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration).

**To view Windows Event Log**

1. Open the **Control Panel** of the operating system.
2. Select **Administrative Tools** → **Event Viewer**.
3. In the tree view, select **Application**. The list of events, registered in the log by user applications, will open. The source of **Dr.Web for Outlook** messages is **Dr.Web for Outlook**.

### 7.4.2. Debug Text Log

The following information is registered in the debug log:

- License validity status
- Information on threat detection
- Read/write errors or errors occurred while scanning archives or password-protected files
- parameters of program modules: scanner, engine, virus databases
- Core failures
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)

**Configure logging**

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

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

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

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

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

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

**To view program log**

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

## 12.4.4. Statistics

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

These scanned objects are classified as follows:

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

Then the number of processed objects is specified:

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

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

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

## 12.5. Preventive Protection Page

On this page, you can configure **Dr.Web Anti-virus** reaction to such actions of other programs that can compromise security of your computer. You can also protect your important data from unwanted changes.

### Preventive Protection Level

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

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

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

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

| Protected object | Description |
|---|---|
| Integrity of running applications | This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security. Processes that are added to the exclusion list of SpIDer Guard are not monitored. |
| Integrity of user files | This option allows detection of processes that modify user files with the known algorithm which indicates that the process may compromise computer security. Processes that are added to the exclusion list of SpIDer Guard are not monitored.To protect your data from modification, you can enable creation of protected copies that contain important data. |
| HOSTS file | The operating system uses the HOSTS file when connecting to the Internet. Changes to this file may indicate virus infection. |
| Low level disk access | Block applications from writing on disks by sectors avoiding the file system. |
| Drivers loading | Block applications from loading new or unknown drivers. |
| Critical Windows objects | Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).<br>File Execution Options:<br>• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options<br>User Drivers:<br>• Software\Microsoft\Windows NT\CurrentVersion\Drivers32<br>• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers<br>Winlogon registry keys:<br>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL<br>Winlogon notifiers:<br>• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify |

| | |
|---|---|
| | Windows registry startup keys:<br>• Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib<br>Executable file associations:<br>• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)<br>• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys)<br>Software Restriction Policies (SRP):<br>• Software\Policies\Microsoft\Windows\Safer<br>Browser Helper Objects for Internet Explorer (BHO):<br>• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects<br>Autorun of programs:<br>• Software\Microsoft\Windows\CurrentVersion\Run<br>• Software\Microsoft\Windows\CurrentVersion\RunOnce<br>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx<br>• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup<br>• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup<br>• Software\Microsoft\Windows\CurrentVersion\RunServices<br>• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce<br>Autorun of policies:<br>• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run<br>Safe mode configuration:<br>• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal<br>• SYSTEM\ControlSetXXX\Control\SafeBoot\Network<br>Session Manager parameters:<br>• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows<br>System services:<br>• System\CurrentControlXXX\Services |

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

If necessary, you can configure desktop and email notifications on preventive protection actions.

# Appendices

## Appendix A. Command Line Parameters

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

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

The switches are listed alphabetically.

## Scanner and Console Scanner Parameters

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

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

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

`/AR` – check archives. Option is enabled by default.

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

`/ARL:`*<level>* – maximum archive nesting level. By default: unlimited.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

`/KEY:`*<keyfile>* – specify a license key file. It is necessary to use this parameter if your key file is stored outside of the **Dr.Web** installation folder where the scanner executables reside. By default, the drweb32.key or another suitable file from the C:\Program Files\DrWeb\ folder is used).

`/LITE` perform a basic scan of random access memory and boot sectors of all disks as well as run a check for rootkits. (For **Scanner** only.)

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

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

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

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

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

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

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

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

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

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

*0* – the lowest.
*L* – low
*N* – normal. Default priority.
*H* – high
*M* – maximal.

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

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

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

`/QNA` – double quote file names.

`/QR[:[d][:p]]` – delete quarantined files on drive <*d*> (logical_drive_letter) that are older than <*p*> (number) days. If <*d*> and <*p*> are not specified, all quarantined files on all drives are deleted. (For **Console Scanner** only.)

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

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

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

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

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

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

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

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

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

`/RPCP:`*<protocol>* – use specified RPC protocol. Possible protocols: lpc, np, tcp. (For **Console Scanner** only.)

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

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

`/SLS` – show logs on the screen. Option is enabled by default. (For **Console Scanner** only.)

`/SPN` – show names of packers. Option is disabled by default.

`/SPS` – display scan progress on the screen. Option is enabled by default. (For **Console Scanner** only.)

`/SST` – display object scan time. Option is disabled by default.

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

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

`/TR` – check system restore points.

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

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

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

Action for different objects ('C' – cure, 'Q' – move to quarantine, 'D' – delete, 'I' – ignore, 'R' – inform. 'R' is available for **Console Scanner** only. 'R' is set by default for all objects in **Console Scanner**):

- `/AAD`:<*action*> – action for adware. (possible: DQIR)
- `/AAR`:<*action*> – action for infected archives. (possible: DQIR)
- `/ACN`:<*action*> – action for infected installation packages. (possible: DQIR)
- `/ADL`:<*action*> –action for dialers. (possible: DQIR)
- `/AHT`:<*action*> –action for hacktools. (possible: DQIR)
- `/AIC`:<*action*> – action for incurable files. (possible DQR)
- `/AIN`:<*action*> – action for infected files. (possible CDQR)
- `/AJK`:<*action*> – action for jokes. (possible: DQIR)
- `/AML`:<*action*> – action for infected email files (possible: QIR)
- `/ARW`:<*action*> – action for riskware. (possible: DQIR)
- `/ASU`:<*action*> – action for suspicious files. (possible: DQIR)

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

| | |
|---|---|
| `/AC-` | option is clearly disabled, |
| `/AC`, `/AC+` | option is clearly enabled. |

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

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

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

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

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

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

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

## Dr.Web Update Command Line Parameters

### Common options

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

### init command parameters

| Parameter | Description |
|---|---|
| -s [ --version ] arg | Version name. |
| -p [ --product ] arg | Product name. |
| -a [ --path ] arg | Product directory path. This directory will be used as the default directory for all components included in the product. **Dr.Web Update** will search for a key file in this directory. |
| -n [ --component ] arg | Component name and installation folder specified as follows:*<name>*, *<install path>*. |
| -u [ --user ] arg | Username for proxy server. |
| -k [ --password ] arg | Password for proxy server. |
| -g [ --proxy ] arg | Proxy server for updating. *<address>*:*<port>*. |
| -e [ --exclude ] arg | Component name that will be excluded from the product during installation. |

### update command parameters

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

| Parameter | Description |
|---|---|
| | - normal-failed – try to update all components including damaged from the current revision to the newest or specified<br>- update-revision – try to update all components of the current revision to the newest if exists<br>- normal – update all components. |
| -g [ --proxy ] arg | Proxy server for updating. *<address>:<port>*. |
| -u [ --user ] arg | Username for proxy server. |
| -k [ --password ] arg | Password for proxy server. |
| --param arg | Pass additional parameters to the script.<br>*<Name>: <value>*. |
| -l [ --progress-to-console ] | Print information about downloading and script execution to the console. |

### exec command parameters

| Parameter | Description |
|---|---|
| -s [ --script ] arg | Execute this script. |
| -f [ --func ] arg | Execute this function in the script. |
| -p [ --param ] arg | Pass additional parameters to the script.<br>*<Name>: <value>*. |
| -l [ --progress-to-console ] | Print information about script execution to the console. |

### getcomponents command parameters

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

### getrevisions command parameters

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

### uninstall command parameters

| Parameter | Description |
|---|---|
| -n [ --component ] arg | Name of the component that is to be uninstalled. |
| -l [ --progress-to-console ] | Print information about command execution to the console. |
| --param arg | Pass additional parameters to the script.<br>*<Name>: <value>*. |
| -e [ --add-to-exclude ] | Components to be deleted. Update of this components will not be performed. |

### keyupdate command parameters

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

### download command parameters

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

## Return codes

The values of the return code and corresponding events are as follows:

| Return code value | Event |
|---|---|
| 0 | OK, no virus found. |
| 1 | Known virus detected. |
| 2 | Modification of known virus detected. |
| 4 | Suspicious object found. |
| 8 | Known virus detected in file archive, mail archive, or container. |
| 16 | Modification of known virus detected in file archive, mail archive, or container. |
| 32 | Suspicious file found in file archive, mail archive, or container. |
| 64 | At least one infected object successfully cured. |
| 128 | At least one infected or suspicious file deleted/renamed/moved. |

The actual value returned by the program is equal to the sum of codes for the events that occurred during scanning. Obviously, the sum can be easily decomposed into separate event codes.

For example, return code `9 = 1 + 8` means that known viruses were detected, including viruses in archives, mail archives or containers; curing and others actions were not executed; no other "virus" events occurred during scanning.

# Appendix B. Computer Threats and Neutralization Methods

With the development of computer technologies and network solutions malicious programs (malware) of different kinds, meant to strafe users, become more and more widespread. Their development began together with computer science and facilities of protection against them progressed alongside. Nevertheless, there is still no common classification for all possible threats due to their unpredictable development character and constant improvement of applicable technologies.

Malicious programs can be distributed through the Internet, local area networks, email and portable data mediums. Some of them rely on the user's carelessness and lack of experience and can be run in completely automatic mode. Others are tools controlled by a computer cracker and they can harm even the most secure systems.

This chapter describes all of the most common and widespread types of malware, against which products of **Doctor Web** are aimed.

## Classification of Computer Threats

### Computer Viruses

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

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

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

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

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

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

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

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

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

## Computer Worms

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

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

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

## Trojans

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

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

## Rootkits

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

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

## Hacktools

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

## Spyware

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

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

## Adware

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

## Jokes

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

## Dialers

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

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

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

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

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

## Actions Applied to Threats

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

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

# Appendix C. Naming of Viruses

When **Dr.Web** components detect a threat, the notification in the user interface and the report file contain a name of the threat sample given by the specialists of the **Dr.Web** Virus Laboratory. These names are formed according to certain principles and reflect a threat's design, classes of vulnerable objects, distribution environment (OS and applications) and some other features. Knowing these principles may be useful for understanding software and organizational vulnerabilities of the protected system. The full and constantly updated version of this classification is available at http://vms.drweb.com/classification/.

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

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

## Prefixes

### Affected Operating Systems

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

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

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

### Macrovirus Prefixes

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

- `WM` – Word Basic (MS Word 6.0-7.0)
- `XM` – VBA3 (MS Excel 5.0-7.0)
- `W97M` – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- `X97M` – VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- `A97M` – databases of MS Access'97/2000

- `PP97M` – MS PowerPoint presentations
- `O97M` – VBA5 (MS Office'97), VBA6 (MS Office 2000); this virus infects files of more than one component of MS Office

## Development Languages

The `HLL` group is used to name viruses written in high level programming languages, such as C, C++, Pascal, Basic and others.

- `HLLW` – worms
- `HLLM` – mail worms
- `HLLO` – viruses overwriting the code of the victim program
- `HLLP` – parasitic viruses
- `HLLC` – companion viruses

The following prefix also refers to development language:

- `Java` – viruses designed for the Java virtual machine

## Trojan Horses (Trojans)

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

- `PWS` – password stealing Trojan
- `Backdoor` – Trojan with RAT-function (*Remote Administration Tool* – a utility for remote administration)
- `IRC` – Trojan which uses Internet Relay Chat channels
- `DownLoader` – Trojan which secretly downloads different malicious programs from the Internet
- `MulDrop` – Trojan which secretly downloads different viruses contained in its body
- `Proxy` – Trojan which allows a third party user to work anonymously in the Internet via the infected computer
- `StartPage` (synonym: `Seeker`) – Trojan which makes unauthorized replacement of the browser’s home page address (start page)
- `Click` – Trojan which redirects a user’s browser to a certain website (or websites)
- `KeyLogger` – a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- `AVKill` – terminates or deletes anti-virus programs, firewalls, etc.
- `KillFiles`, `KillDisk`, `DiskEraser` – deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- `DelWin` – deletes files vital for the operation of Windows OS
- `FormatC` – formats drive C (synonym: `FormatAll` – formats all drives)
- `KillMBR` – corrupts or deletes master boot records (MBR)
- `KillCMOS` – corrupts or deletes CMOS memory

## Tool for Attacking Vulnerabilities

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

### Tools for Network Attacks

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

### Script Viruses

Prefixes of viruses written in different scrip languages:

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

### Malicious Programs

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

### Miscellaneous

- `Generic` – this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.
- `Silly` – this prefix was used to name simple featureless viruses the with different modifiers in the past.

## Suffixes

Suffixes are used to name some specific virus objects:

- `generator` – an object which is not a virus, but a virus generator.

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

© Doctor Web, 2014