Dr.WEB®
Security Space Pro

User Manual

Defend what you create

Dr.Web® Security Space Pro
Version 6.0
User Manual
09.03.2010

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

Introduction

Dr.Web® Security Space Pro provides multi-level protection of RAM, hard disks and removable devices against viruses, rootkits, Trojans, spyware, adware, hack tools and other malicious programs. The module architecture of **Dr.Web Security Space Pro** is its significant feature. **Dr.Web** uses the anti-virus engine and virus databases which are common for all its components and different operating environments. At present, in addition to **Dr.Web Security Space Pro**, there are versions of the anti-virus for IBM® OS/2®, Novell® NetWare® and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

Dr.Web is designed as a powerful anti-virus program and regularly shows the best results in independent comparative reviews.

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

Dr.Web can detect and remove undesirable programs (adware, dialers, jokes, riskware, and hacktools) from your computer. For detection of undesirable programs and actions with the files contained in them, standard anti-virus components of **Dr.Web** are used.

Dr.Web Security Space Pro includes the following components (available components may vary depending on the type of license):

- **Dr.Web Scanner for Windows** (**Scanner**) is an anti-virus scanner with graphical interface. The program is run on user demand or according to schedule, and checks the computer for viruses. There is also a command line version (**Dr.Web Console scanner for Windows**).
- **SpIDer Guard® for Windows** (also called **Monitor** or **Guard**) is an anti-virus guard. The program resides in main memory, checks files and memory on the fly, and detects virus-like activity.
- **SpIDer Mail® for Windows** (**Mail Guard**) is a mail anti-virus guard. The program intercepts calls sent from mail clients to mail servers through POP3/SMTP/IMAP4/NNTP protocols

(IMAP4 stands for IMAPv4rev1), 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. **Mail Guard** uses Anti-spam to scan mail for spam messages.

- **SpIDer Gate™** is an anti-virus HTTP-monitor. By default **SpIDer Gate** automatically checks incoming and outgoing HTTP-traffic and blocks all malware objects.
- The **Parental Control** component is used to restrict access to both local and web resources.
- **Dr. Web Firewall** protects your computer from unauthorized access and prevents leak of vital data through networks.
- **Dr.Web Automatic Updating Utility for Windows** (**Updater**) allows registered users to receive updates of the virus database and other files of the program, as well as automatically install them. Moreover, the **Updater** lets registered users renew their license (serial number is required). For unregistered users it allows to register and receive a license or demo key file (see Receiving the Key File).
- **SpIDer Agent** is a ultility which lets you set up and manage components of **Dr.Web**.

To centralize the management of the anti-virus protection at an enterprise level, a special program – **Dr.Web Enterprise Suite** – is supplied. For more details on this program read Appendix E. Internet service providers can organize anti-virus and anti-spam protection of their clients using **Dr.Web AV-Desk**. For more information on this software see Appendix F.

What is This Manual About

This User Manual describes installation and effective utilization of **Dr.Web Security Space Pro**.

You can find detailed description of all the GUI elements in the Help system of **Dr.Web Security Space Pro** which can be accessed from any component.

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

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

In connection with constant development, the program interface can mismatch the images given in this document. You can always find the actual help information on drweb.com.

In connection with constant development, the program interface can mismatch the images given in this document. You can always find the actual help information on http://products.drweb.com.

Document Conventions and Abbreviations

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

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of **Dr.Web** products and components.
Green and underlined	Hyperlinks to topics and web pages.
`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. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign ('+')	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
Exclamation mark	A warning about potential errors or any other important comment.

The following abbreviations are used in this User Manual:

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

System Requirements

Before installing **Dr.Web Security Space Pro**, you should:

- install all critical updates recommended by the OS developer;
- uninstall all other anti-virus packages from the computer to avoid possible incompatibility with their resident components.

Specification	Requirement
OS	One of the following: • Microsoft® Windows® 2000 SP 4 + Update Rollup 1 • Microsoft® Windows® XP • Microsoft® Windows® Vista • Microsoft® Windows® 7 Both 32-bit and 64-bit versions of operating systems are supported.
CPU	i686 compatible.
RAM	512 MB and more
Other	Internet connection for updating of virus databases and **Dr.Web Security Space Pro** components.

Minimum system requirements are similar to those for the corresponding OS's.

You may need to download certain system components from the Microsoft web-site and install them. The program will notify you about the components required and provide direct links.

Licensing

The use rights for the **Dr.Web Security Space Pro** are specified in the key file.

To use **Dr.Web Security Space Pro**, obtain and install a key file.

For more information on licensing and types of key files, visit the official Doctor Web website.

Key File

The key file contains the following information:

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

The key file has the .key extension and, by default, should reside in the installation folder of the program (see Installing Dr.Web Security Space Pro).

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

There are two types of key files:

- *License key file* is purchased with the **Dr.Web** software and allows a user to use it and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. It also contains information about the user and seller.
- *Demo key file* is used for evaluation of **Dr.Web** products. It is

completely free, provides full functionality of the software but has a limited duration.

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

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

If any of the conditions are violated, the license key file becomes *invalid* and **Dr.Web Security Space Pro** stops detecting and neutralizing malicious programs and transmits.

Get Key File

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

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

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

Key files received via the product registration procedure are installed automatically. You need to install key files received in another way.

To acquire key files via manual registration

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

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

---

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

To acquire key files during installation

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

It is recommended to keep the key file until it expires. If you re-install a product or install it on several computers, additional registration of the serial number will not be required because the key file received during the first registration can be used.

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

Subsequent Registration

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

When recovering demo key file, you will receive the same key file as you received during the previous registration. Demo key file for the same computer cannot be received more often then once in 4 months.

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.

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

Renewing registration

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

To renew license key files

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

How to Test Anti-virus

EICAR (European Institute for Computer Anti-Virus Research) Test File helps to test the performance of the anti-virus programs detecting viruses with their signatures.

For this purpose, most of the anti-virus designers at present generally use the standard test.com program. This program was specially designed so that a user, without any risk to his machine, could verify how a newly-installed anti-virus tool will alert on detecting a virus. The test.com program, is not actually a virus, but it is recognized by the majority of anti-virus utilities as if it is a virus. And on detecting this "virus", **Dr.Web® Security Space Pro** reports the following: `EICAR Test File (Not a Virus!)`.

Other anti-virus utilities also alert along somewhat similar lines.

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

The test.com file contains only printable characters and the corresponding string reads as follows:

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

If you create a file with the above line only and save the file as test.com, you will obtain a program, which is the "virus" described above.

Installing Dr.Web Security Space Pro

Before installing the program we strongly recommend to:

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

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

To begin the installation of **Dr.Web Security Space Pro** on your computer, do one of the following:

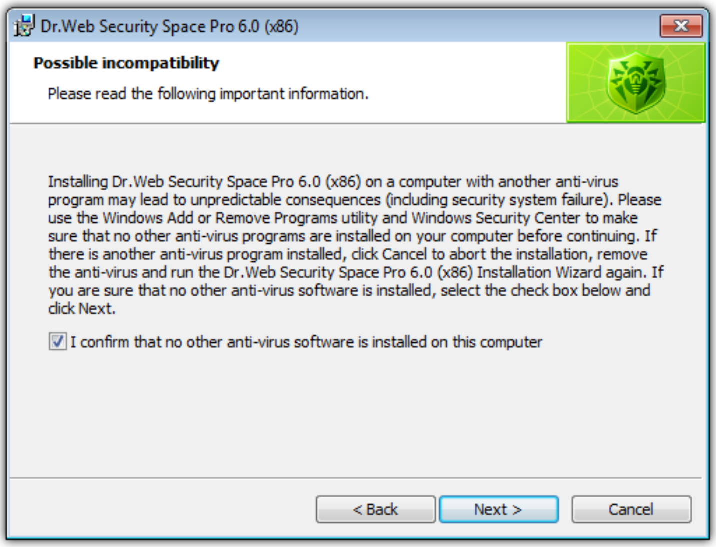
- Execute the file, if supplied as a single executable file.
- Insert the company disk into the CD/DVD drive. If autorun is enabled, installation procedure will start automatically. If autorun is disabled, run the executable file of the distribution kit manually.

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

Installation procedure

Only a user with administrator privileges can install **Dr.Web Security Space Pro**.

1. Select the language for the installation wizard. Regardless of your choice English language will be installed in addition.
2. In the next window you will be offered to read the License agreement. You should accept it and click **Next** in order to continue installation.
3. The installation wizard will inform on possible incompatibility of **Dr.Web** with other anti-viruses installed on your computer and offer to uninstall or disable them. If other anti-viruses are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other anti-viruses and after that continue installation.
   To continue installation select the **I confirm that no other anti-virus software is installed on this computer** check box and click **Next**.



Possible incompatibility

Please read the following important information.

Installing Dr.Web Security Space Pro 6.0 (x86) on a computer with another anti-virus program may lead to unpredictable consequences (including security system failure). Please use the Windows Add or Remove Programs utility and Windows Security Center to make sure that no other anti-virus programs are installed on your computer before continuing. If there is another anti-virus program installed, click Cancel to abort the installation, remove the anti-virus and run the Dr.Web Security Space Pro 6.0 (x86) Installation Wizard again. If you are sure that no other anti-virus software is installed, select the check box below and click Next.

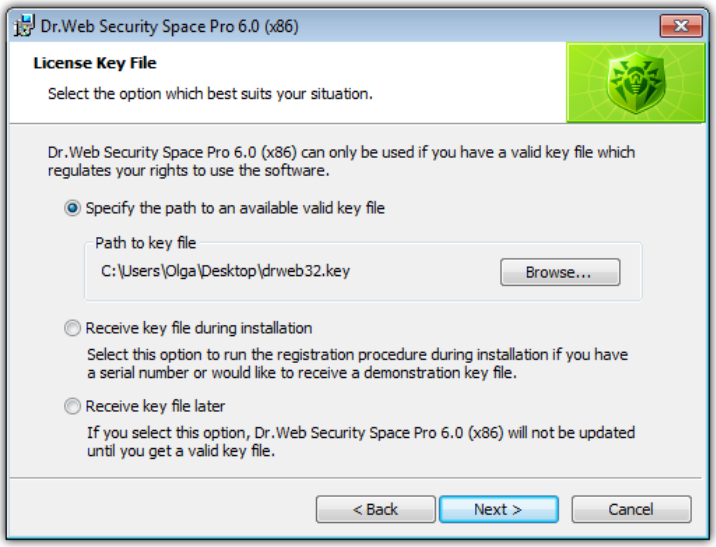
☑ I confirm that no other anti-virus software is installed on this computer

---

Not all anti-viruses can be detected by the installation wizard.

---

4. The installation program will bring up a warning window requesting a key file (license or demo) required for the program's operation. If a key file is present on your hard drive or on removable media, click **Browse**, select the key file and click **Next**.



License Key File

Select the option which best suits your situation.

Dr.Web Security Space Pro 6.0 (x86) can only be used if you have a valid key file which regulates your rights to use the software.

● Specify the path to an available valid key file

Path to key file

C:\Users\Olga\Desktop\drweb32.key

○ Receive key file during installation

Select this option to run the registration procedure during installation if you have a serial number or would like to receive a demonstration key file.

○ Receive key file later

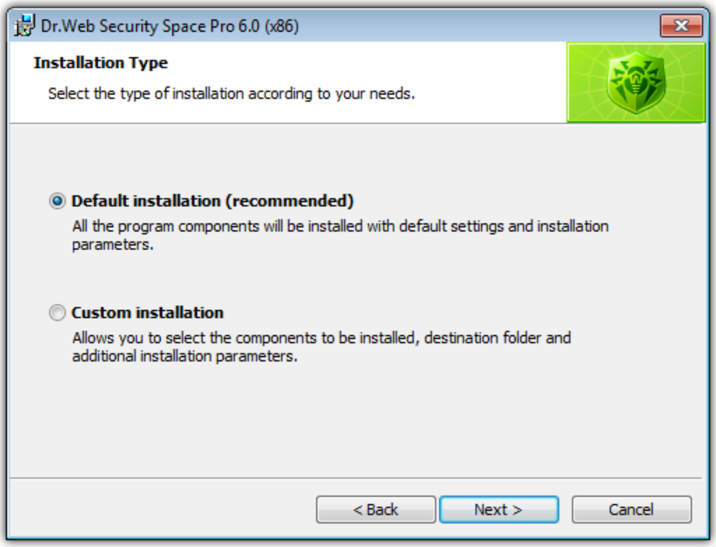
If you select this option, Dr.Web Security Space Pro 6.0 (x86) will not be updated until you get a valid key file.

If no key file is available, but you have a serial number, select **Receive key file during installation**. Otherwise, select **Receive key file later** and click **Next**.

Use only **Dr.Web Security Space Pro** key file. The key file should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

---

5. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components and all secondary programs automatically up to step 10. **Custom Installation** is meant for experienced users. During custom installation you will be asked to select which components should be installed, adjust proxy server settings and some additional installation parameters.



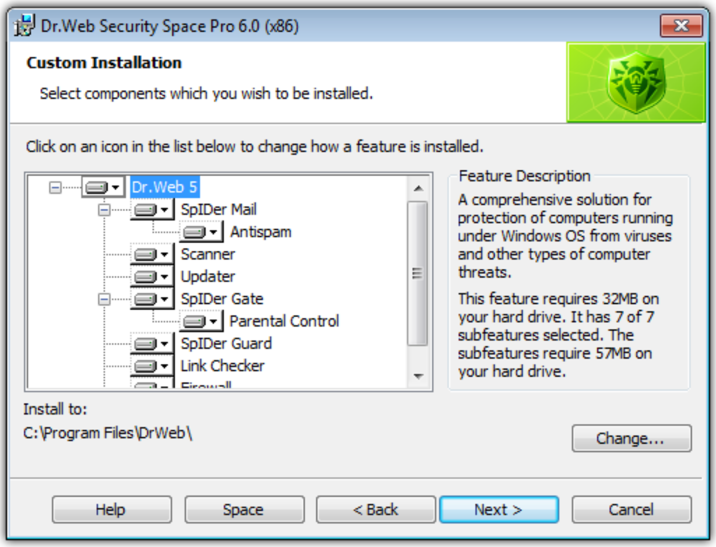
Select the type of installation according to your needs.

● **Default installation (recommended)**
All the program components will be installed with default settings and installation parameters.

○ **Custom installation**
Allows you to select the components to be installed, destination folder and additional installation parameters.

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

6. If you chose default installation type, go to step 10. In case of custom installation, a window for selecting the program components which you wish to install will open. In the hierarchical list select the components you wish to install. You can also change the installation folder if necessary.



Dr.Web Security Space Pro 6.0 (x86)

Custom Installation

Select components which you wish to be installed.

Click on an icon in the list below to change how a feature is installed.

Feature Description

A comprehensive solution for protection of computers running under Windows OS from viruses and other types of computer threats.

This feature requires 32MB on your hard drive. It has 7 of 7 subfeatures selected. The subfeatures require 57MB on your hard drive.

Install to:

C:\Program Files\DrWeb\

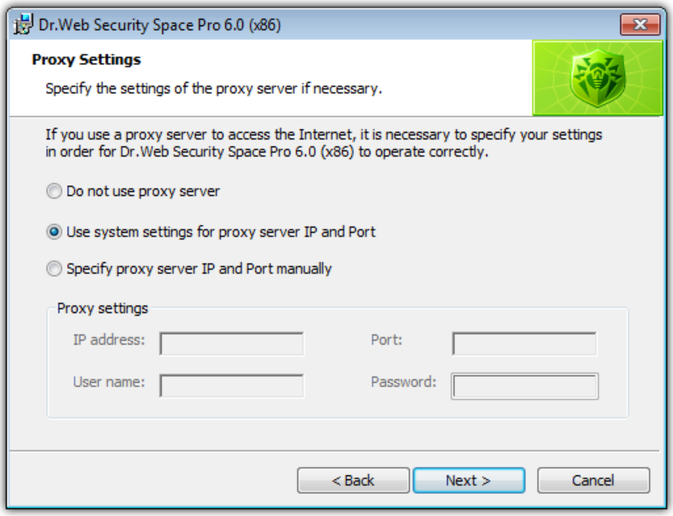
Click **Next** when you finish selecting the necessary components.

7. The window for selecting which shortcuts to **Dr.Web Security Space Pro** should be created will open. Select the necessary options and click **Next**.
8. The window for adjusting proxy server settings will open.

   If you do not use a proxy server, choose **Do not use proxy server**.

   If you use current settings for proxy server, choose **Use system settings for proxy server IP and Port**.

   If you want to specify settings for proxy server, choose **Specify proxy server IP and Port manually**.



Dr.Web Security Space Pro 6.0 (x86)

Proxy Settings

Specify the settings of the proxy server if necessary.

If you use a proxy server to access the Internet, it is necessary to specify your settings in order for Dr.Web Security Space Pro 6.0 (x86) to operate correctly.

○ Do not use proxy server

● Use system settings for proxy server IP and Port

○ Specify proxy server IP and Port manually

Proxy settings

IP address:

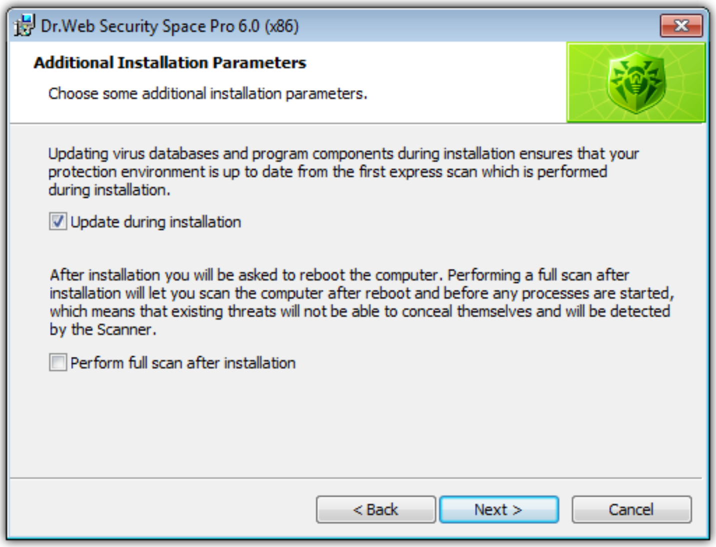
Port:

User name:

Password:

Click **Next**.

9. The window for adjusting some additional parameters of installation will open.



Additional Installation Parameters

Choose some additional installation parameters.

Updating virus databases and program components during installation ensures that your protection environment is up to date from the first express scan which is performed during installation.

☑ Update during installation

After installation you will be asked to reboot the computer. Performing a full scan after installation will let you scan the computer after reboot and before any processes are started, which means that existing threats will not be able to conceal themselves and will be detected by the Scanner.

☐ Perform full scan after installation

Select the **Update during installation** check box to download the latest virus databases during installation. Select the **Perform full scan after installation** check box to check the file system after your computer is rebooted at the end of the installation.

10. A window informing that the program is ready to be installed will open. Click the **Install** button to start the installation process or **Back** to change any of the installation parameters.
11. If in step 4 you selected the **Receive key file during installation** option, the Updater will launch the registration procedure. To receive the key file your computer should be connected to the Internet.
12. If in step 9 you selected the **Update during installation** check box, after receiving the key file virus databases will be updated automatically.
13. After installation is complete (if the GUI version of the **Scanner** was selected in the list of components which should be installed) the **Scanner** will perform express scan.

Neutralize any detected threats and close the **Scanner** after the scanning process.

Scanner is not compatible with Windows Blinds (an application for adjusting Windows GUI). For correct operation of **Dr.Web Security Space Pro** it is necessary to disable changing of the **Dr.Web** interface in the Windows Blinds settings. To do this, add drweb32w.exe to the list of excluded applications.

---

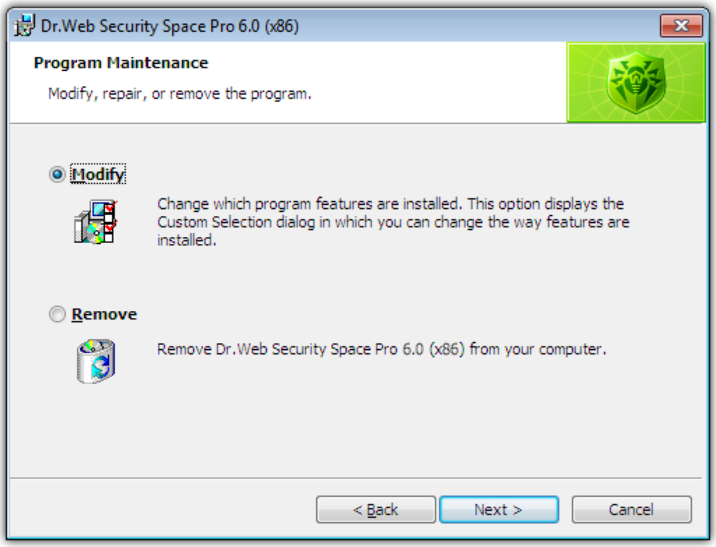
14. The program will ask for a computer reboot which is required to complete the installation.

If you install **Firewall** among other **Dr.Web Security Space Pro** components, the installation wizard will inform on possible incompatibility of **Dr.Web** with other firewalls installed on your computer and offer to uninstall or disable them. If other firewalls are installed on your computer, it is recommended to click **Cancel** and terminate installation, delete or deactivate other firewalls and after that continue installation.
To continue installation select the **I confirm that no other firewall is installed on this computer** check box and click **Next**.

Reinstalling and Removing Dr.Web Security Space Pro

To modify, repair or remove an installed version of **Dr.Web Security Space Pro**, start the installation wizard.

After selecting the language for the installation wizard, the following window will open:


Dr.Web Security Space Pro 6.0 (x86)
Program Maintenance
Modify, repair, or remove the program.
● Modify
Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.
○ Remove
Remove Dr.Web Security Space Pro 6.0 (x86) from your computer.
< Back
Next >
Cancel

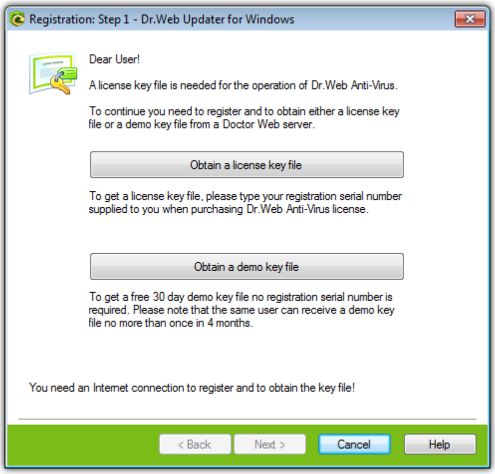
In this window:

- To change the set of installed components select **Modify** and click **Next**. The **Custom Installation** window will open. Subsequent steps beginning from this window are similar to those described in the two previous section.
- To remove all the components select **Remove**. During removal of **Dr.Web Security Space Pro** it is necessary to disable Self Protection. To do this, enter the digits shown on the picture. At the end of the installation, reboot the computer when prompted.

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

Receiving the Key File

At the first step of the procedure you will be offered to choose what type of key file you would like to obtain - either license or demo.



Registration: Step 1 - Dr.Web Updater for Windows

Dear User!

A license key file is needed for the operation of Dr.Web Anti-Virus.

To continue you need to register and to obtain either a license key file or a demo key file from a Doctor Web server.

To get a license key file, please type your registration serial number supplied to you when purchasing Dr.Web Anti-Virus license.

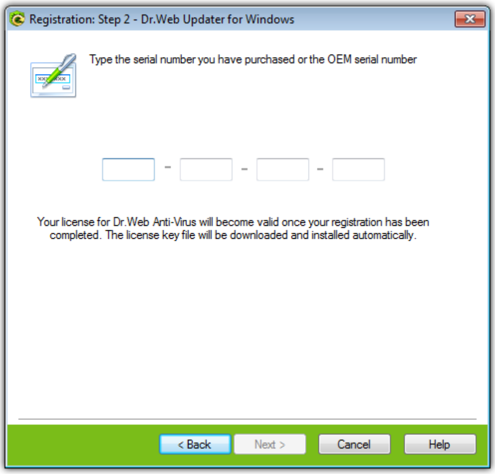
To get a free 30 day demo key file no registration serial number is required. Please note that the same user can receive a demo key file no more than once in 4 months.

You need an Internet connection to register and to obtain the key file!

If you have a serial number, click the **Obtain a license key** file button.

In the opened window enter your serial number and click **Next**.

If you specified the prolongation serial number at the previous step, the window for specifying information about your previous license will open. Enter your old serial number and click **Next**.



Registration: Step 2 - Dr.Web Updater for Windows

Type the serial number you have purchased or the OEM serial number

Your license for Dr.Web Anti-Virus will become valid once your registration has been completed. The license key file will be downloaded and installed automatically.

A window for entering personal data necessary to receive a key file will open. The registration procedure for receiving the demo key file starts from this step.

Fill in the fields of this window and click **Next**.

When the window with the specified information opens check that all the data is correct and click **Next**.

The procedure of receiving the license key will start. The protocol of its operation will be displayed in the information message box. If the license key is successfully downloaded, the location of the file will be indicated. Otherwise, an error message will appear.

Getting Started

By default the installation program installs the following components of **Dr.Web Security Space Pro** on the computer:

- the **Scanner for Windows** environment (GUI and console versions)
- **SpIDer Guard**
- **SpIDer Mail**
- **SpIDer Gate**
- **Parental control**
- **SpIDer Agent**
- **Anti-spam**
- **Link Checker**

The **Automatic Updating Utility** and some other additional utilities are installed obligatory.

The components of **Dr.Web Security Space Pro** use common virus databases and anti-virus engine. Also uniform algorithms for detection and neutralization of viruses in scanned objects are implemented. However, the methods of selecting the objects for scanning differ greatly allowing to use these components for absolutely different and mutually supplementary PC protection policies.

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

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

An advantage of the program is uninterrupted control of the virus situation during the whole PC runtime. Besides, some viruses can only be detected by the guard through their specific activity.

SpIDer Mail also constantly resides in the memory. The program intercepts all calls from your mail clients to mail servers via POP3/ SMTP/IMAP4/NNTP protocols and scans incoming and outgoing e-mail messages before they are received (or sent) by the mail client. **SpIDer Mail** is designed to check all current mail traffic going through a computer. As a result, scanning of mailboxes becomes more efficient and less resource-consuming. For example, it allows to control attempts at mass distribution a mail worm's functional copies to the addresses specified in the user address book which is performed via the worm's own mail clients. This also allows to disable scanning of e-mail files for **SpIDer Guard**, which considerably reduces consumption of computer resources.

An anti-virus HTTP-monitor **SpIDer Gate** by default automatically checks incoming and outgoing HTTP-traffic and blocks all malware objects. HTTP is used by web browsers, download managers and other applications which exchange data with web servers, i.e. which work with the Internet. **SpIDer Gate** resides in the main memory of the computer and automatically launches upon Windows startup. You can change the automatic launch mode by clearing the corresponding check box.

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

To secure comprehensive anti-virus protection, we advise you to use the **Dr.Web Security Space Pro** components as follows:

- scan the PC's file system with the default (maximum) scanning detail settings;
- keep the autorun mode and other default settings of **SpIDer Guard**;

- perform complete e-mail scanning with **SpIDer Mail**;
- perform complete scanning of HTTP-traffic with **SpIDer Gate**;
- perform a periodic complete scan of the PC, coordinated with the time of the virus database updates (at least once a week);
- immediately perform a complete scan in case **SpIDer Guard** was temporary disabled and the PC was connected to the Internet or files were downloaded from removable media.

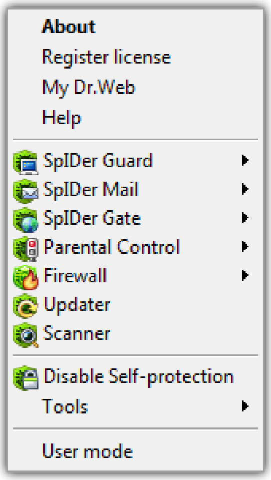
Anti-virus protection can only be effective if you update the virus databases and other files of the program regularly (preferably every hour). For more information read Automatic Updating of the Virus Databases and Other Files of the Program.

SpIDer Agent

After installing **Dr.Web Security Space Pro** a **SpIDer Agent** icon is added to the taskbar notification area.

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

The context menu of the icon allows to perform the main management and settings functions of **Dr.Web Security Space Pro**.



The **About** item opens a window with information about the version of **Dr.Web Security Space Pro**.

The **Register license** item starts the registration procedure for receiving the key file from the **Doctor Web, Ltd.** server.

The **My Dr.Web** item opens your personal web page on the **Doctor Web, Ltd.** web site. This page gives information about your license (period of usage, serial number), allows to renew your license, contact Technical Support, etc.

The **Help** item opens **Dr.Web Security Space Pro** help system.

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

Scanner item runs **Dr.Web Scanner** that automatically starts express scan of your computer.

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

To disable self-protection:

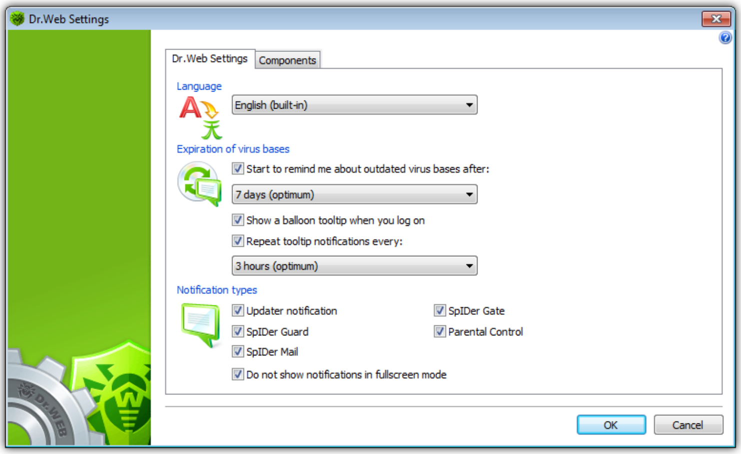
- select **Disable self-protection** in the **SpIDer Agent** menu;
- enter text displayed on the picture.

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

It is not recommended to disable self-protection.

The **Tools** item opens a submenu which contains following items:

- **License Manager** (see License Manager).
- **Settings**. This command displays **SpIDer Agent** settings.



Language

English (built-in)

Expiration of virus bases

☑ Start to remind me about outdated virus bases after:

7 days (optimum)

☑ Show a balloon tooltip when you log on

☑ Repeat tooltip notifications every:

3 hours (optimum)

Notification types

☑ Updater notification

☑ SpIDer Guard

☑ SpIDer Mail

☑ SpIDer Gate

☑ Parental Control

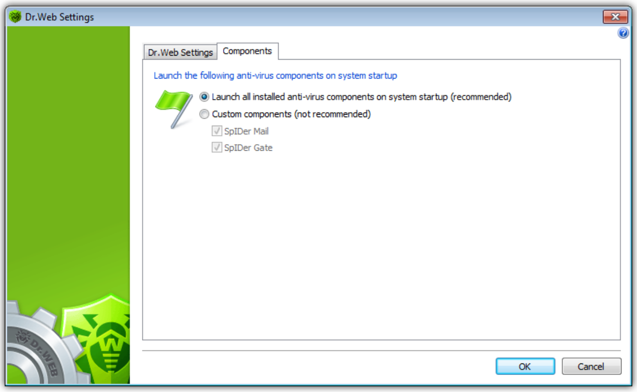
☑ Do not show notifications in fullscreen mode

In the **Dr.Web Settings** tab you can specify the language of the **Dr.Web Security Space Pro** GUI by selecting the necessary language in the **Language** list.

Also in this window you can select the types of pop-up notifications which appear above the **SpIDer Agent** icon in the taskbar notification area. Components send notifications when a corresponding event happens (i.e. when a threat is detected or an update is performed).

In the **Components** tab you can choose one of the following:

- **Launch all installed anti-virus components on system startup (recommended)**.
- **Custom components (not recommended)**. In this mode you can disable automatic launch of **SpIDer Mail** or **SpIDer Gate**.



Launch the following anti-virus components on system startup

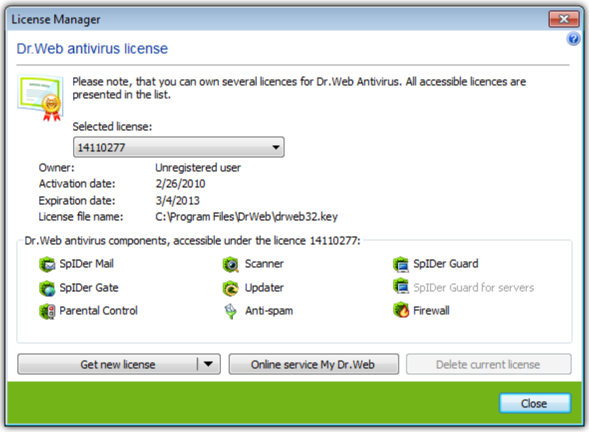
● Launch all installed anti-virus components on system startup (recommended)
○ Custom components (not recommended)
  ☑ SpIDer Mail
  ☑ SpIDer Gate

- **Scheduler.** This command displays the standard Windows Scheduler task which determines the **Dr.Web® Security Space Pro** updating schedule.
- **Quarantine** (see Quarantine).

The **Administrative/User mode** item allows you to switch between full-function **Administrative mode** and restricted **User mode**. In **User mode**, access to to settings of components is forbidden and the **Scheduler** item is also inaccessible. You need administrative rights to switch to **Administrative mode**.

License Manager

License Manager shows information from the **Dr.Web Security Space Pro** key files in an understandable form.



License Manager

Dr.Web antivirus license

Please note, that you can own several licences for Dr.Web Antivirus. All accessible licences are presented in the list.

Selected license: 14110277

Owner: Unregistered user
Activation date: 2/26/2010
Expiration date: 3/4/2013
License file name: C:\Program Files\DrWeb\drweb32.key

Dr.Web antivirus components, accessible under the licence 14110277:

Selected **Dr.Web Security Space Pro** components for your license are specified in the **Dr. Web antivirus components** group box.

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

To start the registration procedure for receiving the key file from the **Doctor Web** server, click the **Get new licence** button and choose **from Internet** in the drop-down menu. That will launch receiving the key file procedure.

To add a key file

1. Press the **Get new licence** button. Choose **from file** in the drop-down menu.
2. Select the file in a standard window.

3. **Dr.Web Security Space Pro** will automatically start to use a key file.

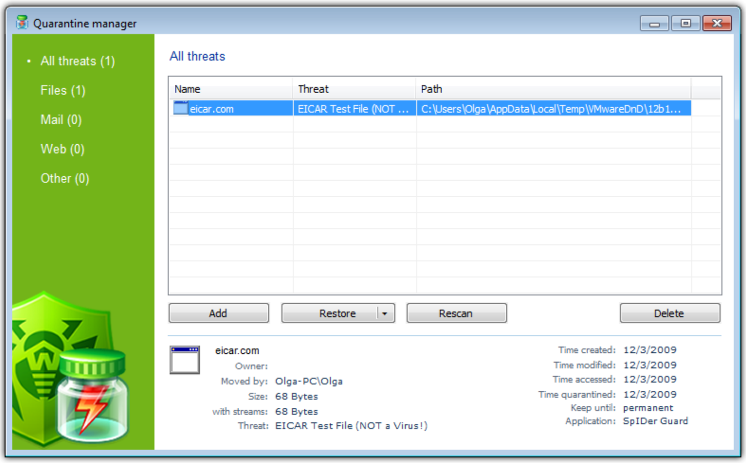
If you received a key file during installation or in the distribution kit complete set, installation of a key file is made automatically and does not demand any additional actions.

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

Quarantine

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

To view and edit the quarantine, select **Quarantine** in the **Tools** submenu of the **SpIDer Agent** context menu. A new window with table that contains quarantine current state opens.



Name	Threat	Path
eicar.com	EICAR Test File (NOT ...	C:\Users\Olga\AppData\Local\Temp\VMwareDnD\12b1...

eicar.com
Owner:
Moved by: Olga-PC\Olga
Size: 68 Bytes
with streams: 68 Bytes
Threat: EICAR Test File (NOT a Virus!)

Time created: 12/3/2009
Time modified: 12/3/2009
Time accessed: 12/3/2009
Time quarantined: 12/3/2009
Keep until: permanent
Application: SpIDer Guard

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

- **Name** – name list of the objects in the quarantine,
- **Threat** – malware classification, which is assigned by **Dr.Web Security Space Pro** during automatic moving to the quarantine.

- **Path** – full path of the object before moving to the quarantine.

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

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

Use the following buttons to manage the quarantine:

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

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

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

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

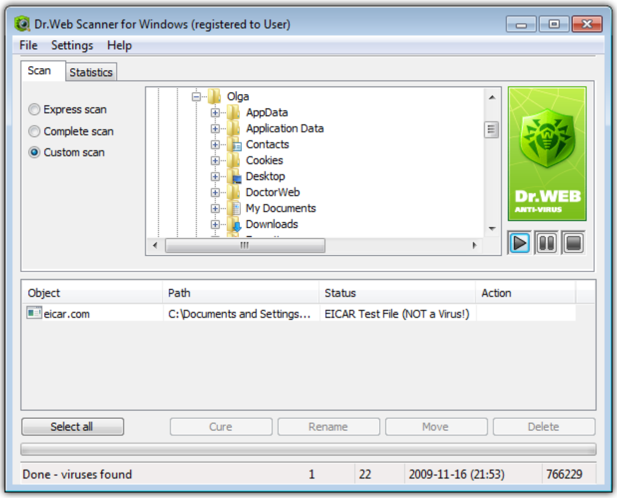
To manage several objects simultaneously, select necessary objects in the quarantine window and select necessary action in the drop-down menu.

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

Using Dr.Web Scanner for Windows

By default, the program scans all files for viruses using both the virus database and the heuristic analyzer (a method based on the general algorithms of virus developing allowing to detect the viruses unknown to the program with a high probability). Executable files compressed with special packers are unpacked when scanned. Files in archives of all commonly used types (Zip, Arj, Lha, Rar and many other), in containers (PowerPoint, RTF and other), and in mailboxes of mail programs (the format of mail messages should conform to RFC822) are also checked.

By default, **Dr.Web Security Space Pro** informs a user about any infected or suspicious objects in a special report field generated at the bottom of the **Scanner** main window (see illustration below). For more information see Adjusting the Scanner Settings.



○ Express scan
○ Complete scan
● Custom scan

Object	Path	Status	Action
eicar.com	C:\Documents and Settings...	EICAR Test File (NOT a Virus!)	

Done - viruses found 1 22 2009-11-16 (21:53) 766229

Launching the Scanner. General Information.

The **Scanner** is installed as a usual Windows application and can be launched by the user or the **Scheduler** command.

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

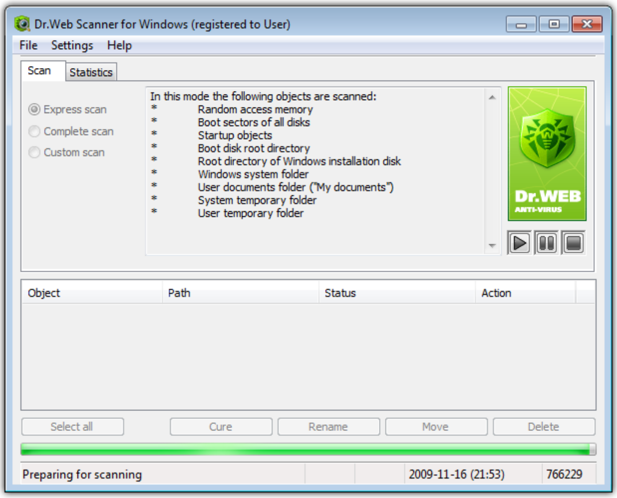
To launch the Scanner do one of the following:

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

You can also run the **Scanner** with default settings to scan a certain file or folder immediately:

- Select **Check by Dr.Web** in the context menu of the file or folder icon (on the Desktop or in Windows Explorer).
- Drag and drop the icon of the file or folder onto the **Scanner** icon or to the main window of the **Scanner** (see illustration below).

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



● Express scan
○ Complete scan
○ Custom scan

In this mode the following objects are scanned:

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

Preparing for scanning | 2009-11-16 (21:53) | 766229

By default, immediately after the **Scanner** performs express scan. Other objects of the file system, that are not scanned during express scan, can be scanned on user demand.

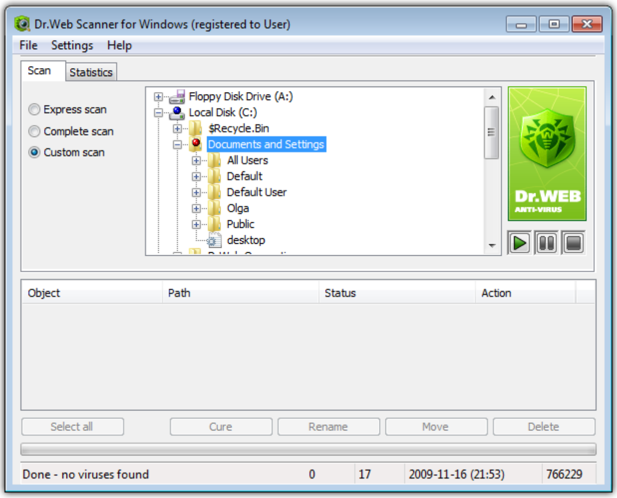
There are 3 scanning modes: **Express scan**, **Complete scan** and **Custom scan**. Depending on the selected mode, either a list of objects which will be scanned or a file system tree is displayed at the center of the window.

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

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

If **Complete scan** mode is selected, random access memory, all hard drives and removable media (including boot sectors of all disks) are scanned.

Custom scan mode allows you to select folders and files for scanning. When this mode is selected, a file system tree will appear in the center of the **Scan** pane. If necessary, you can expand objects in the file system tree down to the level of any folder or file. Select the necessary objects for scanning in the file system tree. The illustration below shows the situation when the Documents and Settings folder on the disk C: is selected for scanning.



○ Express scan
○ Complete scan
● Custom scan

Done - no viruses found 0 17 2009-11-16 (21:53) 766229

To launch scanning of the selected objects, click the ▶ button in the right part of the main window.

When launching the **Scanner** on a portable computer running on battery, a message on the battery state will appear. You can disable this option in the **General** tab of the **Settings** window (for more information see Adjusting the Scanner Settings).

As soon as scanning starts, the ⏸ button in the right part of the window becomes available. Click this button to pause the scanning process. To resume scanning, click the ▶ button. To stop scanning, click the ■ button.

⚠ By default, subfolders in the selected directories and logical drives, as well as boot sectors of all logical drives on which at least one folder or file is selected, and also the main boot sectors of respective physical drives are scanned too.

Actions Upon Detection of a Virus

By default, **Dr.Web Security Space Pro** only reports about infected or suspicious objects. You can try to restore the functionality of an infected object (i.e. cure it) or avert the threat from it if curing is impossible.

To apply actions to detected objects:

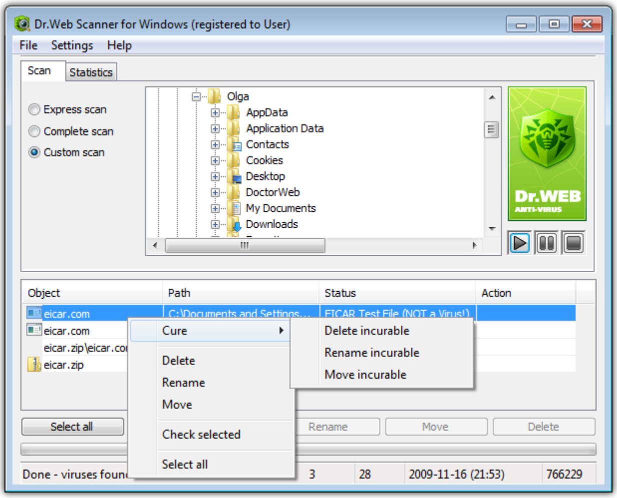
1. Right click the line of the report list with the description of the infected object.

⚠ You can specify an action either for all objects or for specific objects in the report list. To select all objects click the **Select All** button. To select objects in the report list the following keys and combinations of keys are additionally used:

- [Insert] - to select an object.
- [CTRL+A] - to select all objects.
- the asterisk button [*] on numeric keyboard - to select or deselect all.

---

2. Select the action you want to apply in the opened context menu or click the corresponding button at the bottom of the report field.



3. If the **Cure** action is selected, choose another action which should be applied in case curing fails.

The **Rename** action means replacement of a file extension. By default, the first character of the extension is replaced with the # symbol.

The **Move** action means that the object is moved to a folder specified in the program’s settings. By default, it is the infected.!!! subfolder of the program's installation directory.

The **Move** action means that the object is moved to a folder specified in the program’s settings. By default, it is the infected.!!! subfolder of the program's installation directory.

Suspicious objects are moved to infected.!!! folder and should be sent for analysis to the anti-virus laboratory of **Doctor Web, Ltd.** through a specially designed web-form at http://support.drweb.com/sendnew/.

For suspicious objects curing is impossible.

For objects which are not files (boot sectors) moving, renaming and deletion is impossible.

For files inside archives, containers or attachments, no actions are possible.

By default, when the **Delete** action is applied to file archives, containers or mailboxes, the program generates a warning message that the data might be lost.

After the required action is applied, the report with the operation result will be generated in the **Action** column of the report field.

In some cases the specified action cannot be immediately applied to selected files. The **Will be cured after reboot** or **Will be deleted after reboot** text string, depending on the action specified, will appear in the **Action** column of the **Scanner** main window report field. The necessary action will be taken at the next reboot, i.e. it will be a postponed action. That is why, if such objects are found, it is recommended to reboot the system immediately after the scanning process. You can also set up automatic reboot if necessary (for more information see Adjusting the Scanner Settings).

The detailed report on the program's operation is saved as a log file. By default, the log file resides in the program's installation folder in the DoctorWeb subfolder of the %USERPROFILE% directory. The name of the log file is drweb32w.log.

To view the reports on the operation of different anti-virus components select the Logs subfolder in the All Programs -> Dr. Web directory of the Windows Start menu.

Adjusting the Scanner Settings

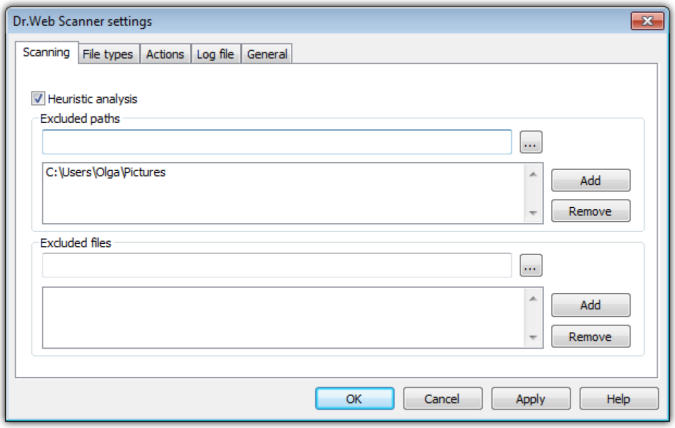
It is recommended for the **Scanner** to be run by a user with administrator privileges because files to which unprivileged users have no access (including system folders) are not scanned.

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

To modify the Scanner settings:

1. To open the **Scanner** settings do one of the following:
   - Select the **Options** item in the menu located at the top of the main window and then choose **Change settings** in the opened submenu.
   - Make sure, that **Scanner** window is active, and press F9

   This will open the **Scanner settings** window which contains several tabs.



☑ Heuristic analysis

Excluded paths

C:\Users\Olga\Pictures

Excluded files

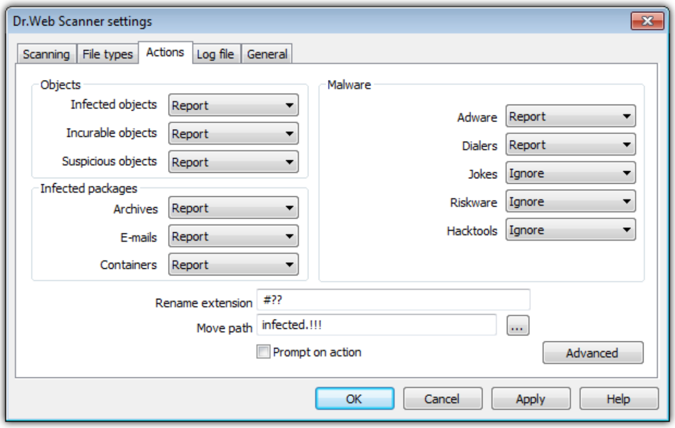
2. Make the necessary changes and click **Apply** when switching to another pane.
3. For more detailed information on the settings specified in each tab use the **Help** button. Also, for the majority of settings specified in the panes, a context help feature is available which is activated by right-clicking an element of the interface.
4. When editing is finished click **OK** to save the changes made or **Cancel** to cancel the changes.

The most frequent changes in default settings are described below.

The default settings of **Dr.Web Security Space Pro** are optimal for scanning on user demand. The program performs full and detailed scanning of the selected objects and informs the user on all infected or suspicious objects, leaving him with the right to decide what action should be taken upon their detection. The objects containing joke programs, riskware or hacktools are excluded: for them the **Ignore** action is specified by default. However, when scanning is performed without the user's assistance, settings for automatic reaction of the program upon detection of infected objects can be applied.

To set the program's reaction upon detection of infected objects:

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



Infected objects: Report
Incurable objects: Report
Suspicious objects: Report
Archives: Report
E-mails: Report
Containers: Report
Adware: Report
Dialers: Report
Jokes: Ignore
Riskware: Ignore
Hacktools: Ignore
Rename extension: #??
Move path: infected.!!!
☐ Prompt on action

2. In the **Infected objects** drop-down list, select the program's action upon detection of an infected object.

The **Cure** action is the best for automatic mode.

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

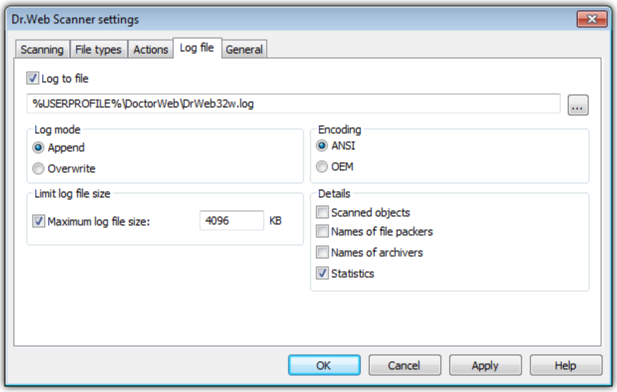
The **Move to** action is the best in most cases.

4. In the **Suspicious objects** drop-down list select the program's action upon detection of a suspicious object (fully similar to the previous paragraph).

It is recommended to keep the default **Report** action.

5. Similar actions should be specified for detection of objects containing Adware, Dialers, Jokes, Riskware and Hacktools.
6. The same way the automatic actions of the program upon detection of viruses or suspicious codes in file archives, containers and mailboxes, applied to these objects as a whole, are set up. The **Report** action is specified by default.
7. Clear the **Prompt on action** check box to enable the specified program's action without prior inquiry.
8. When **Rename** is set as the program's action, the program, by default, will replace the first character of a file name extension with the **#** symbol. If necessary, you can change the renaming mask for file extensions. For this, insert the necessary value into the **Rename extension** entry field.
9. When **Move to** is set as the program's action, the program, by default, will move the file to the infected.!!! subfolder of the program's installation directory. If necessary, you can specify a different name of the folder in the **Move path** entry field.
10. To cure some infected files it is necessary to reboot Windows. You can adjust parameters of rebooting in the **Cure settings** window. To open this window click the **Advanced** button in the bottom right of the **Actions** pane. You can choose one of the following:
    - **Restart automatically, if necessary**. It can lead to loss of unsaved data.
    - **Do not restart automatically**. If you choose this mode, it is recommended to select the **Prompt restart, when necessary** checkbox to restart at any time convenient to you.

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



☑ Log to file

%USERPROFILE%\DoctorWeb\DrWeb32w.log

Log mode
● Append
○ Overwrite

Encoding
● ANSI
○ OEM

Limit log file size
☑ Maximum log file size: 4096 KB

Details
☐ Scanned objects
☐ Names of file packers
☐ Names of archivers
☑ Statistics

Most parameters set by default should be left unchanged. However, you can change the details of logging (by default, the information on infected or suspicious objects is always logged; the information on the scanned packed files and archives and on successful scanning of other files is omitted). You can instruct to log the results of scanning of all files, regardless the result. For this, select the **Scanned objects** check box (this will considerably increase the size of the log file). You can instruct to log the names of archivers (select the **Archivers names** check box) and executable file packers (select the **File packers names** check box).

You can cancel the default restriction set for the maximum size of the log file (clear the **Maximum log file size** check box) or specify your own log file size limit in the entry field next to the check box.

Command Line Scanning Mode

You can run **Dr.Web Scanner for Windows** in the command line mode which allows to specify settings of the current scanning session and the list of objects for scanning as additional parameters. This mode provides automatic activation of the **Scanner** according to schedule.

The launching command syntax is as follows:

[*path_to_program*]`drweb32w` [*objects*] [*keys*]

Dr.Web Console Scanner for Windows can be used instead of **Dr.Web Scanner for Windows**. To do this type the **drwebwcl** command name instead of **drweb32w**.

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

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

- ***** – scan all hard drives
- **C:** – scan drive C:
- **D:\games** – scan files in the specified folder
- **C:\games\*** – scan all files and subfolders of the specified directory

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

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

Several most frequently used switches are listed below. For their full list refer to Appendix A.

/cu – cure infected objects.

/icm – move incurable files (to the default folder).
/icr – rename (by default).

/qu – close the scanner window after session is finished.

/go – no prompts on actions should be generated.

Two last parameters are especially useful for automatic launch of the **Scanner** according to schedule.

By default, the console version of the **Scanner for Windows** uses the same settings as the GUI-version of the **Scanner**. The parameters set via the graphical interface of the **Scanner** (for more information see Adjusting the Scanner Settings) are used for scanning in command line mode unless different parameters were set as switches. Some settings of the **Scanner** can only be specified in the program's configuration file (read Appendix B for more details).

SpIDer Guard for Windows

By default, **SpIDer Guard** is loaded automatically at every Windows startup and cannot be unloaded during the current Windows session. If it is necessary to temporarily disable **SpIDer Guard** (for example, when a task consuming too much processor resources is performed in real time mode), select the **Disable** item in the menu of **SpIDer Guard** item (read SpIDer Agent).

Only the user with administrator rights can temporarily disable the guard.

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

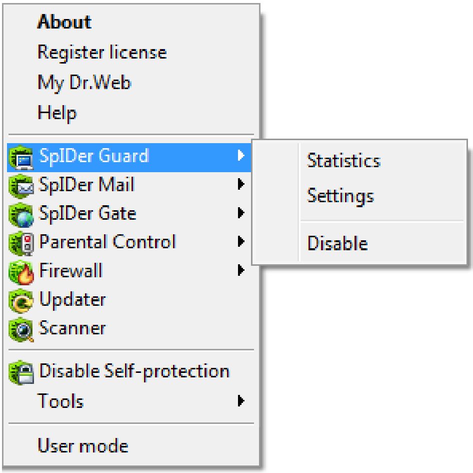
By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web Security Space Pro** acts according to actions set on Actions tab.

You can set the program’s reaction to virus events by adjusting the corresponding settings; in this case, the guard will act in the background. A user can control it with the help of the **Statistics** window (read about this window below) and the log file.

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

Managing the Guard

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



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

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

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

The **Disable** item allows to temporary disable program functions except for completion of background processes and checks (for users with administrator rights only).

Main Parameters of the SpIDer Guard

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

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

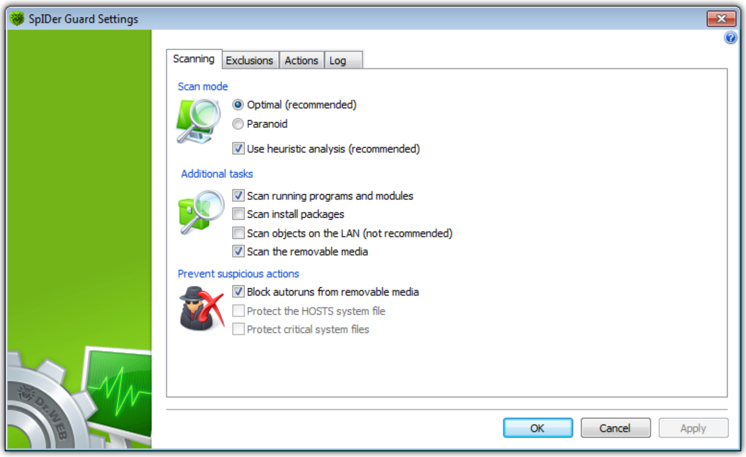
Some of the most frequently changed settings of the program are described below.

Scanning Tab

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

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

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



Scan mode

● Optimal (recommended)
○ Paranoid

☑ Use heuristic analysis (recommended)

Additional tasks

☑ Scan running programs and modules
☐ Scan install packages
☐ Scan objects on the LAN (not recommended)
☑ Scan the removable media

Prevent suspicious actions

☑ Block autoruns from removable media
☐ Protect the HOSTS system file
☐ Protect critical system files

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

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

Exclusions Tab

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

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

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

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

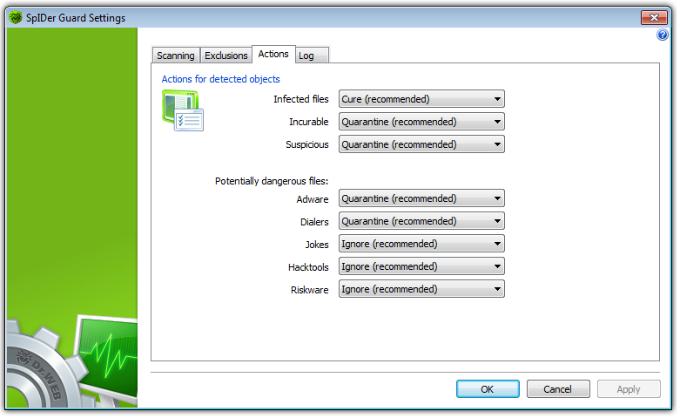
Actions Tab

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

The **Cure**, **Ignore**, **Delete** and **Quarantine** actions are similar to those of the **Scanner**.

To change the default actions in SpIDer Guard:

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



Actions for detected objects

Infected files: Cure (recommended)
Incurable: Quarantine (recommended)
Suspicious: Quarantine (recommended)

Potentially dangerous files:
Adware: Quarantine (recommended)
Dialers: Quarantine (recommended)
Jokes: Ignore (recommended)
Hacktools: Ignore (recommended)
Riskware: Ignore (recommended)

2. In the **Infected objects** drop-down list choose the program's action upon detection of an infected object. **Cure** action is recommended.
3. In the **Incurable objects** drop-down list choose the

program's action upon detection of an incurable object. **Quarantine** action is recommended. Other actions with moved files are described in Actions Upon Detection of a Virus chapter.

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

SpIDer Mail

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

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

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

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

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

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

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

SpIDer Mail uses Dr.Web Anti-spam which allows to scan mail for spam messages. By default, this option is enabled. (For information on settings of the spam filter refer to Adjusting Certain Program Settings).

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

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

SpIDer Guard and the **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 **SpIDer Guard** and the **Scanner**. In this case, when using **SpIDer Mail**, the infected messages are not even delivered to mailboxes.
- By default **SpIDer Guard** does not check mailboxes. If this option is enabled, it considerably degrades the system’s performance.
- The **Scanner** does not check the mailboxes at the moment of the mail receipt, but either on user demand or according to schedule. Furthermore, this action is rather resource-consuming and takes a lot of time

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

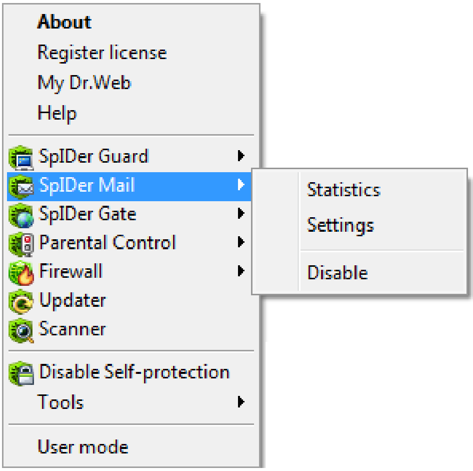
Anti-spam

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

- **Heuristic analysis** – a highly intelligent technology that empirically analyzes all parts of a message: header, message body, and attachments, if any.
- **Detection of evasion techniques** – this advanced anti-spam technology allows detecting evasion techniques adopted by spammers to bypass anti-spam filters.
- **HTML-signature analysis** – messages containing HTML code are compared with a list of known patterns from the anti-spam library. Such comparison, in combination with the data on sizes of images typically used by spammers, helps protect users against spam messages with HTML-code linked to online content.
- **Semantic analysis** – the words and phrases of a message – both visible to the human eye and hidden – are compared with words and phrases typical of spam using a special dictionary.
- **Anti-scamming** – scam (as well as pharming messages) is the most dangerous type of spam including so-called "Nigerian" scams, loan scams, lottery and casino scams and false messages from banks and credit organizations. A special module of **Dr.Web Anti-spam** is used to filter scams.
- **Technical spam** – bounces are delivery-failure messages sent by a mail server. Such messages are also sent by a mail worm. Therefore bounces are as unwanted as spam.

Managing SpIDer Mail

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



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

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

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

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

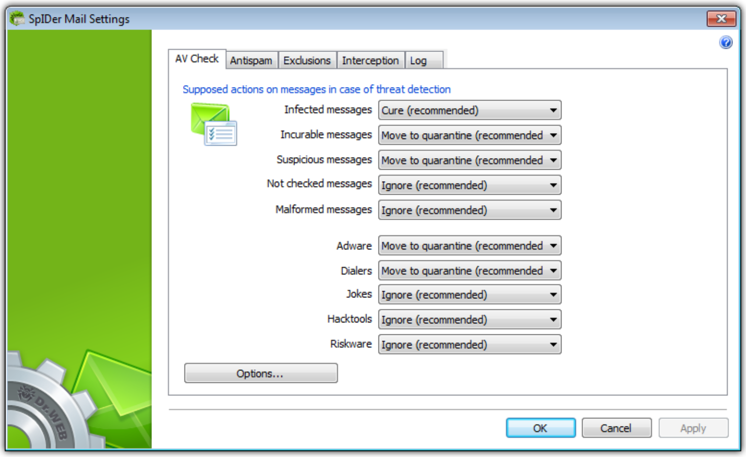
Adjusting Certain Program Settings

To modify **SpIDer Mail** settings open the settings window as described in Managing SpIDer Mail.

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

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

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



Supposed actions on messages in case of threat detection

Infected messages: Cure (recommended)
Incurable messages: Move to quarantine (recommended
Suspicious messages: Move to quarantine (recommended
Not checked messages: Ignore (recommended)
Malformed messages: Ignore (recommended)

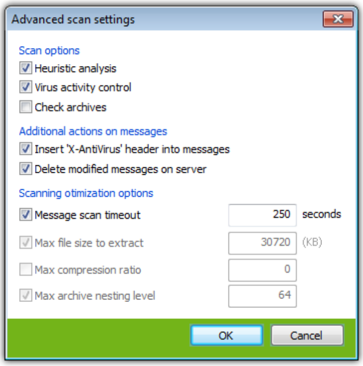
Adware: Move to quarantine (recommended
Dialers: Move to quarantine (recommended
Jokes: Ignore (recommended)
Hacktools: Ignore (recommended)
Riskware: Ignore (recommended)

To change the default actions in SpIDer Mail:

1. In the **Infected messages** drop-down list choose the program’s action upon detection of an infected message (**Cure** action is recommended).

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

To get access to advanced settings click the **Options** button.



Advanced scan settings

Scan options

☑ Heuristic analysis

☑ Virus activity control

☐ Check archives

Additional actions on messages

☑ Insert 'X-AntiVirus' header into messages

☑ Delete modified messages on server

Scanning otimization options

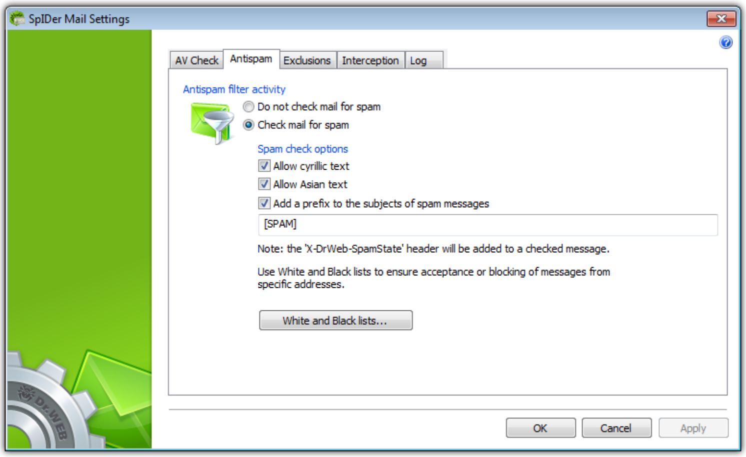
☑ Message scan timeout 250 seconds

☑ Max file size to extract 30720 (KB)

☐ Max compression ratio 0

☑ Max archive nesting level 64

Settings of the spam filter can be set in the **Antispam** tab.



Antispam filter activity

○ Do not check mail for spam

● Check mail for spam

Spam check options

☑ Allow cyrillic text

☑ Allow Asian text

☑ Add a prefix to the subjects of spam messages

[SPAM]

Note: the 'X-DrWeb-SpamState' header will be added to a checked message.

Use White and Black lists to ensure acceptance or blocking of messages from specific addresses.

White and Black lists...

By default **SpIDer Mail** scans incoming messages for spam. To disable the spam filter, choose the **Do not check mail for the spam** mode.

The following headers will be added to all scanned messages:

- `X-DrWeb-SpamState: Yes/No`. **Yes** shows that the message is spam. **No** means that **SpIDer Mail** does not regard the message as spam.
- `X-DrWeb-SpamVersion: version`. **version** is the version of **Anti-spam** library.

During installation with standard parameters, a rule for Outlook Express (versions 5 and 6) named **DRWEB-VR-ANTISPAM RULE** is created. This rule moves all messages that contain prefix **[SPAM]** in their subjects to the **Deleted** folder.

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

Selecting the **Add a prefix to the subjects of spam messages** check box instructs **SpIDer Mail** to add a special prefix to subjects of spam messages. This prefix can be specified in the field below. Use of the prefix will allow you to create filter rules for spam in e-mail clients which do not support filtering by headers (e.g. MS Outlook Express).

Selecting the **Allow Cyrillic text** check box instructs the spam filter to analyze messages with Cyrillic encoding. If the check box is not selected, it is highly possible that messages with Cyrillic encoding will be regarded as spam.

Functioning of the **Allow Asian text** check box is the same as the one described above but for East Asian encodings.

In the **White list** and **Black list** fields, white and black lists of senders' addresses are specified.

- If a sender's address is on the white list, the message is not scanned for spam. But if the domain names of recipient and sender coincide and this domain name is on the white list with the asterisk (*****) symbol, the message and its contents will be scanned for spam.
- If a sender's address is on the black list, the message will be automatically regarded as spam.

Addresses must be divided by a semicolon (**;**). The asterisk (*****) symbol can stand for a part of address (for example, ***@domain.org** denotes all addresses with the **domain.org** domain name).

If the spam filter regards certain messages as spam by mistake, you are advised to forward such messages to special e-mail addresses for analysis. Messages which are wrongly regarded as spam should be forwarded to vrnonspam@drweb.com, and unblocked spam messages should be forwarded to vrspam@drweb.com. Forward messages as attachments; do not include them to the message body.

To change the set of detected unsolicited programs, select the check boxes in the **Check for** section of the **Scan** pane against the types of unsolicited programs you wish to be detected, and clear the check boxes against the types of programs you do not wish to be detected.

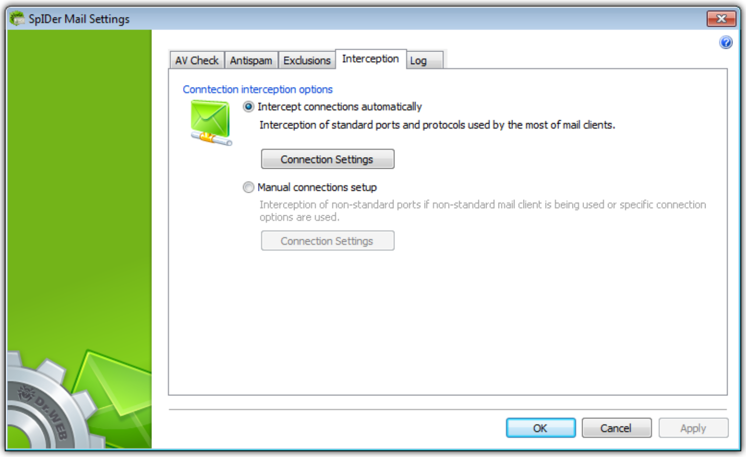
Protection against suspicious messages can be disabled if a PC is additionally protected by a constantly loaded **SpIDer Guard** component.

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

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

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

The interception parameters of connections are set up in the **Interception** pane.



Conntection interception options

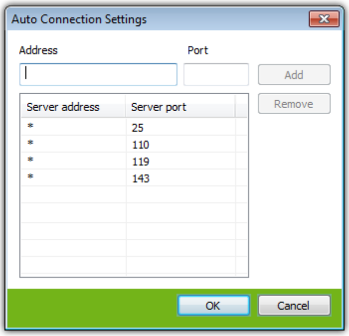
● Intercept connections automatically

Interception of standard ports and protocols used by the most of mail clients.

○ Manual connections setup

Interception of non-standard ports if non-standard mail client is being used or specific connection options are used.

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



Server address	Server port
*	25
*	110
*	119
*	143

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

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

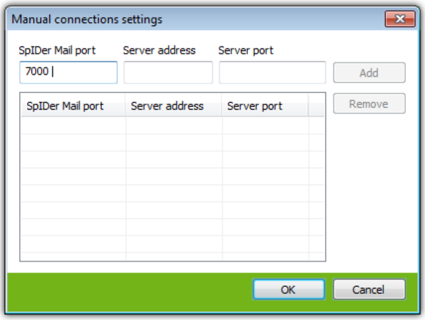
To add a server or a group of servers to the list, specify its address (IP address or domain name) in the **Address** field and the called port number into the **Port** field and click **Add**.

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

If automatic interception is impossible (the program will inform about it, if the **Test interception functionality at every starting** check box is selected), the interception should be set manually.

To set up manual interception:

1. In the previously mentioned **Interception** pane for setting up the mode of interception select the **Manual connections setup** radio button and click the **Parameters** button. A window for setting up manual connections will open.



SpIDer Mail port: 7000

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

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

SpIDer Gate

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

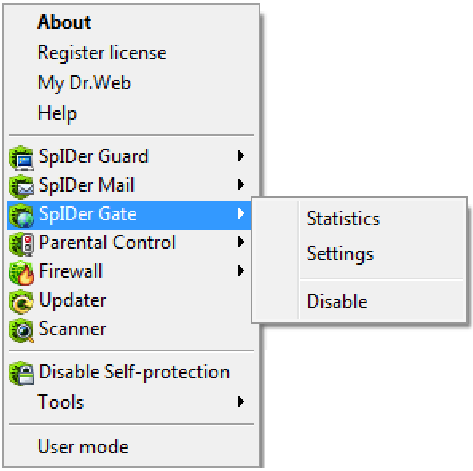
You can adjust the **SpIDer Gate** settings to completely disable monitoring of incoming or outgoing traffic, compose a list of applications whose HTTP-traffic should always be checked or exclude certain applications from being monitored.

By default **SpIDer Gate** blocks all malware objects.

SpIDer Gate resides in the main memory of the computer and automatically launches upon Windows startup. You can disable the automatic launch mode in SpIDer Agent settings.

Managing SpIDer Gate

SpIDer Gate can be managed via the **SpIDer Gate** item in the context menu of the **SpIDer Agent** icon (see SpIDer Agent).



The **Settings** item provides access to the major part of adjustable parameters of the program.

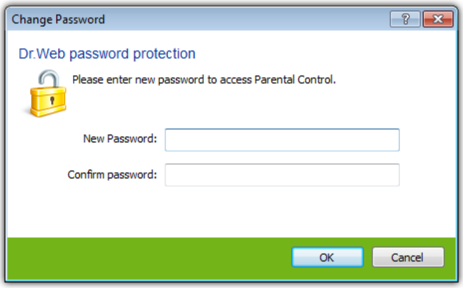
The **Statistics** item opens a window containing information about the **SpIDer Gate** performance within the current session.

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

SpIDer Gate Settings

The default settings are optimal for most cases. They should not be changed without necessity.

Access to **SpIDer Gate** settings is password-protected. At the first start a dialog window will open. You will be offered to enter new password.



Change Password

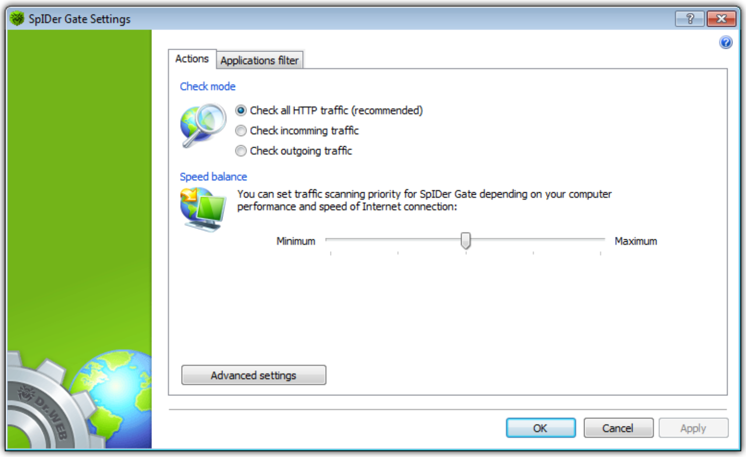
Dr.Web password protection

Please enter new password to access Parental Control.

To change the SpIDer Gate Settings:

1. Enter the password which was specified when the **SpIDer Gate Settings** window was opened for the first time. To change this password click the **Change password** button.
2. Make necessary changes in the tabs of the **SpIDer Gate Settings** window.
3. For more information about settings in a tab, click the ? button.
4. Click **Apply** to save changes immediately.
5. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Actions Tab



Check mode

● Check all HTTP traffic (recommended)

○ Check incomming traffic

○ Check outgoing traffic

Speed balance

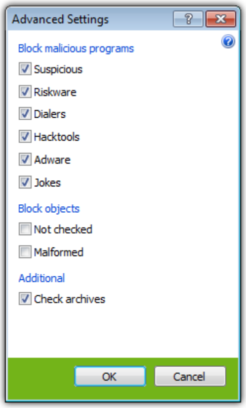
You can set traffic scanning priority for SpIDer Gate depending on your computer performance and speed of Internet connection:

Minimum — Maximum

In the **Check mode** group you can choose type of the checked HTTP-traffic.

On the same tab you can adjust **Speed balance** – distribution of resources depending on traffic scanning priority.

To get access to advanced settings click the **Advanced settings** button in **Actions** tab.



Block malicious programs
☑ Suspicious
☑ Riskware
☑ Dialers
☑ Hacktools
☑ Adware
☑ Jokes

Block objects
☐ Not checked
☐ Malformed

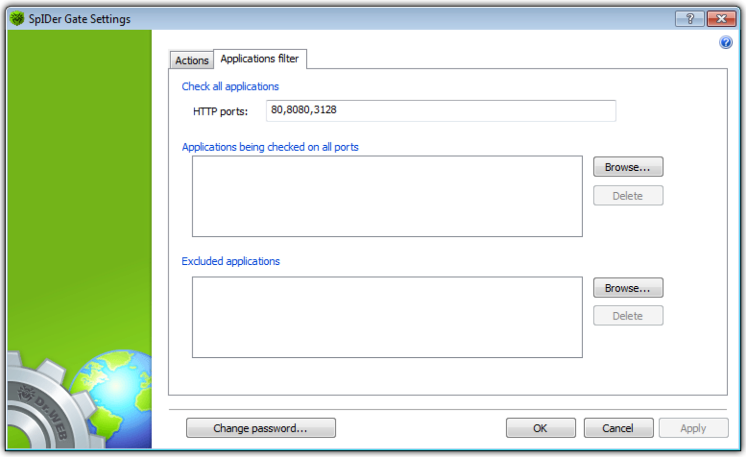
Additional
☑ Check archives

In the opened dialog window you can block malicious programs and objects, and also enable or disable archives checking. By default, the blocking of malicious programs and the archives checking are enabled.

Application Filter Tab

By default monitoring of HTTP-traffic is enabled. On the **Application Filter** tab you can set up which applications to include or exclude from monitoring.

SpIDer Gate checks HTTP-traffic which goes through ports specified in the top part of the tab. By default ports 80, 8080 and 3128 are specified; these ports are often used by applications to transfer data through HTTP. If you are aware that an application on your computer uses another port for HTTP then add it to the **HTTP ports** field.



HTTP ports: 80,8080,3128

Add applications, whose network activity should be checked with extreme caution, to the **Applications being checked on all ports** list. These are web browsers, download managers and most newly installed software.

Add applications, whose network activity should not be checked at all, to the **Excluded applications** list. You should only add applications which you trust to this list.

To add an application to a list, click the **Browse** button and select the application in a standard window.

To delete an application from a list, select it and click **Delete**.

Parental Control

The **Parental Control** component is used to restrict access to both local and web resources.

By restricting access to the local file system you can maintain the integrity of important files, protect them from viruses and secure the confidentiality of stored data. It is possible to restrict access to separate files or folders on local drives and external data carriers. You can also completely restrict access to any kinds of external data carriers.

By controlling access to web resources you can restrict a user to view undesirable web sites (e.g. pornography, violence, gambling, etc.) or allow access only to certain web sites, specified in the **Parental Control** settings.

Access to the **Parental Control** settings is password-protected.

Parental Control Settings

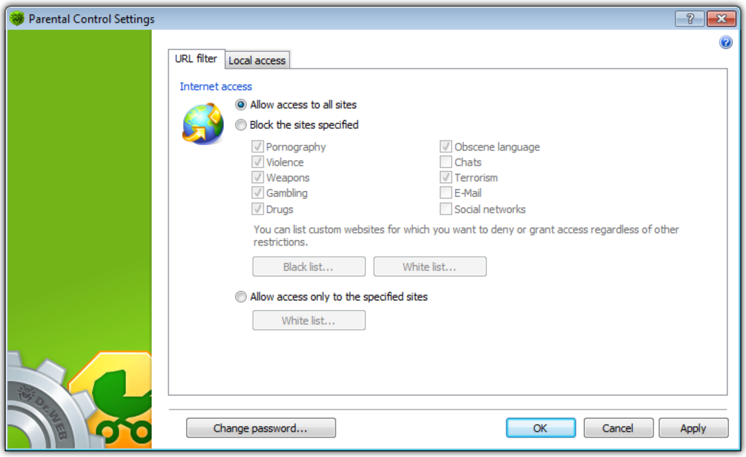
The default settings are optimal for most cases. They should not be changed without necessity.

To change the settings of the Parental Control component:

1. Enter the password which was specified when the **Parental Control Settings** window was opened for the first time. To change this password click the **Change password** button.
2. Make necessary changes in the tabs of the **Parental Control Settings** window.
3. For more information about settings in a tab, click the ? button.

4. Click **Apply** to save changes immediately.
5. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

On the **URL filter** tab you can adjust access to web resources.



Internet access

● Allow access to all sites

○ Block the sites specified

☑ Pornography
☑ Violence
☑ Weapons
☑ Gambling
☑ Drugs
☑ Obscene language
☐ Chats
☑ Terrorism
☐ E-Mail
☐ Social networks

You can list custom websites for which you want to deny or grant access regardless of other restrictions.

Black list... White list...

○ Allow access only to the specified sites

White list...

To set access to web resources:

In URL filter tab choose one of the modes:

- **Allow access to all sites**. There are no restrictions in this mode.
- **Block the sites specified**. In this mode you can select the types of blocked web sites. Besides, you can set lists of blocked and allowed web-sites regardless of restrictions by categories.
- **Allow access only to specified sites**. In this mode access to all resources except those in **White list** will be restricted.

Lists of web sites in all categories are constantly updated by the Automatic Updating Module along with virus databases.

Add the domain names which should be blocked to the **Address bar content** list.

To create a list of domain names:

- Enter a domain name (or part of it) into the field.

  If you wish to add a specific web site, enter its full address (e.g. **www.example.com**). Access to all resources on that web site will be allowed/restricted.

  If you wish to allow/restrict access to web sites, which contain certain text in their address name, enter that text into the field (e.g. **example** means that access to **example**.com, **example**.test.com, test.com/**example**, test.**example**222.ru, etc. will be allowed/restricted).

  If the string contains the "." symbol, it will be considered a domain name. In this case all resources on the domain will be filtered. If the string also contains the "/" symbol (e.g. **example.com/test**), then the part to the left of it will be considered the domain name and the part to the right will be allowed/restricted on the domain (e.g. **example.com/test**11, template.**example.com/test**22, etc. will be filtered).

- Click the **Add** button. The address will be added to the list above.

  The address may be converted to a more simple structure (e.g. **http://www.example.com** will be converted to **www.example.com**).

To delete a web resource from the list, select it and click **Delete**.

Firewall

Dr.Web® Firewall protects your computer from unauthorized access and prevents leak of vital data through networks.

Dr.Web Firewall monitors connection attempts and data transfer and helps you block unwanted or suspicious connections both on network and application levels.

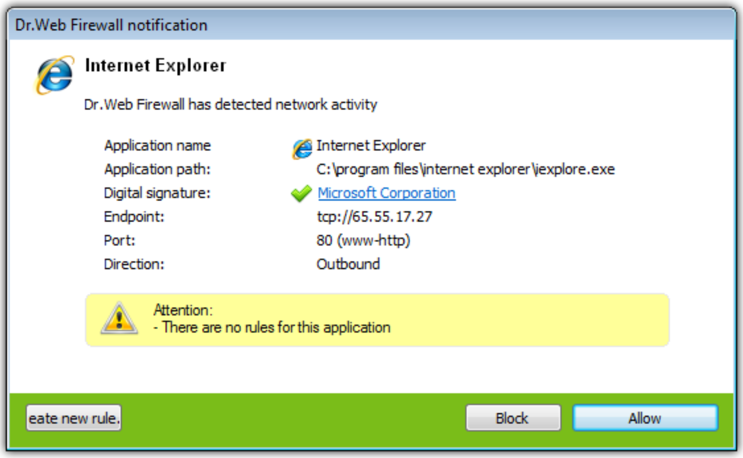
Main Features

Dr.Web Firewall provides you with the following features:

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

Training Dr.Web Firewall

By default, once installation completes **Dr.Web Firewall** starts learning usual behaviour of your operating system by intercepting all new (unknown to the firewall) connection attempts and prompting you to select the necessary action.



Dr.Web Firewall notification

Internet Explorer

Dr.Web Firewall has detected network activity

Application name	Internet Explorer
Application path:	C:\program files\internet explorer\iexplore.exe
Digital signature:	✓ Microsoft Corporation
Endpoint:	tcp://65.55.17.27
Port:	80 (www-http)
Direction:	Outbound

Attention:
- There are no rules for this application

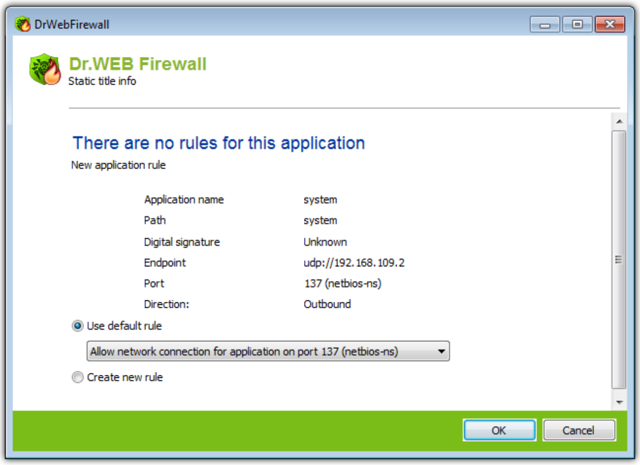
You can either select a temporary solution, or create a rule which will be applied each time **Dr.Web Firewall** detects this type of connection.

To process connection attempts

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

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

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



DrWebFirewall

Dr.WEB Firewall

Static title info

There are no rules for this application

New application rule

Application name	system
Path	system
Digital signature	Unknown
Endpoint	udp://192.168.109.2
Port	137 (netbios-ns)
Direction:	Outbound

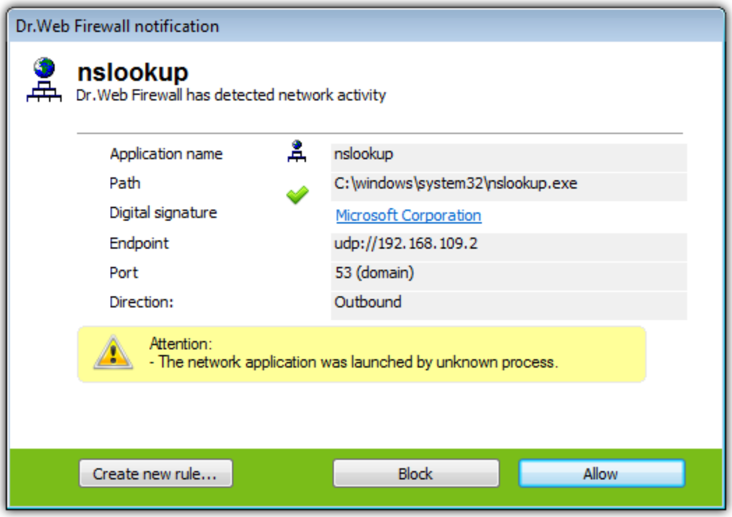
● Use default rule

Allow network connection for application on port 137 (netbios-ns)

○ Create new rule

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

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



nslookup

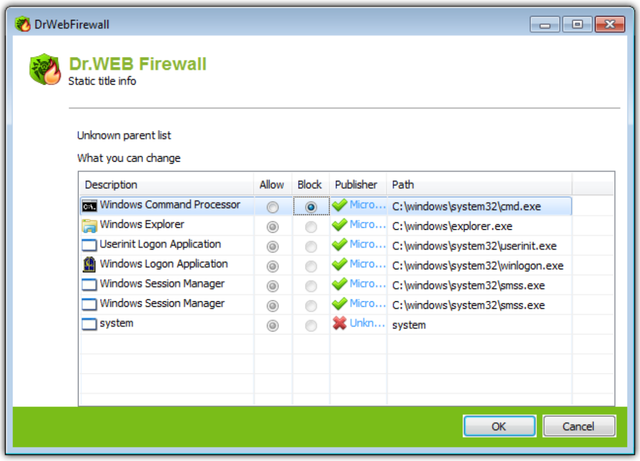
Dr.Web Firewall has detected network activity

Application name	nslookup
Path	C:\windows\system32\nslookup.exe
Digital signature	✓ Microsoft Corporation
Endpoint	udp://192.168.109.2
Port	53 (domain)
Direction:	Outbound

Attention:
- The network application was launched by unknown process.

To set parent processes rules:

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



Dr.WEB Firewall

Static title info

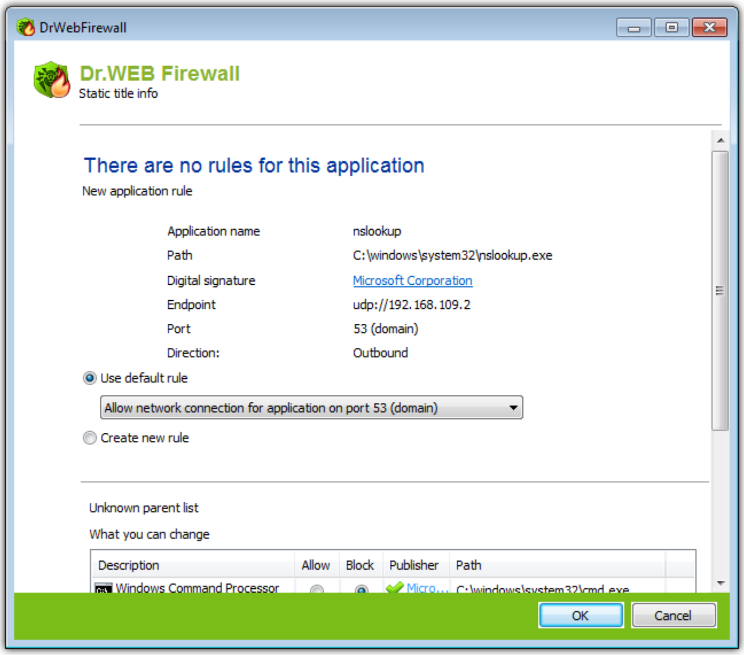
Unknown parent list

What you can change

Description	Allow	Block	Publisher	Path
Windows Command Processor	○	●	✓ Micro…	C:\windows\system32\cmd.exe
Windows Explorer	●	○	✓ Micro…	C:\windows\explorer.exe
Userinit Logon Application	●	○	✓ Micro…	C:\windows\system32\userinit.exe
Windows Logon Application	●	○	✓ Micro…	C:\windows\system32\winlogon.exe
Windows Session Manager	●	○	✓ Micro…	C:\windows\system32\smss.exe
Windows Session Manager	●	○	✓ Micro…	C:\windows\system32\smss.exe
system	●	○	✗ Unkn…	system

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

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



There are no rules for this application

New application rule

Application name	nslookup
Path	C:\windows\system32\nslookup.exe
Digital signature	Microsoft Corporation
Endpoint	udp://192.168.109.2
Port	53 (domain)
Direction:	Outbound

● Use default rule

Allow network connection for application on port 53 (domain)

○ Create new rule

Unknown parent list

What you can change

Description	Allow	Block	Publisher	Path
Windows Command Processor	○	●	✓ Micro...	C:\windows\system32\cmd.exe

Firewall settings

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

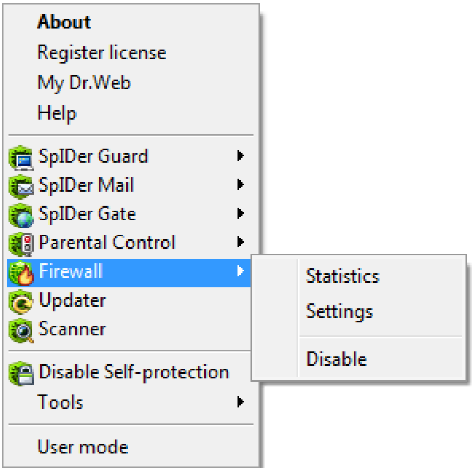
- Select operation mode
- List authorized applications

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

Managing Dr.Web Firewall

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

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



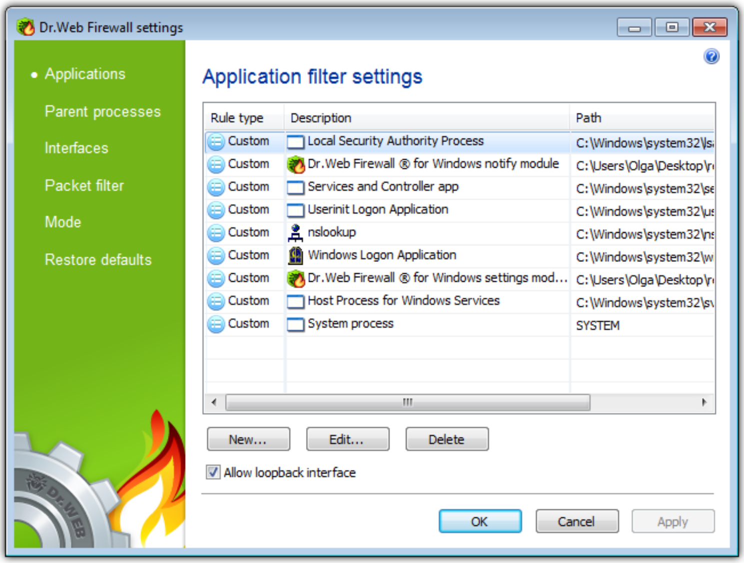
To manage Dr.Web Firewall

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

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

Application Filter

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



Rule type	Description	Path
Custom	Local Security Authority Process	C:\Windows\system32\ls
Custom	Dr.Web Firewall ® for Windows notify module	C:\Users\Olga\Desktop\
Custom	Services and Controller app	C:\Windows\system32\se
Custom	Userinit Logon Application	C:\Windows\system32\u
Custom	nslookup	C:\Windows\system32\n
Custom	Windows Logon Application	C:\Windows\system32\w
Custom	Dr.Web Firewall ® for Windows settings mod...	C:\Users\Olga\Desktop\
Custom	Host Process for Windows Services	C:\Windows\system32\s
Custom	System process	SYSTEM

☑ Allow loopback interface

The **Application filter settings** page lists all applications and processes for which there is an application filter rule set. Each application is explicitly identified by the path to its executable file. **Dr.Web Firewall** uses the SYSTEM name to indicate the rule set applied to the operating system kernel (the system process for which there is no unique executable file).

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

On this page, you can:

- Create a set of rules for an application
- Modify an existing application ruleset
- Delete all filtering rules for an application

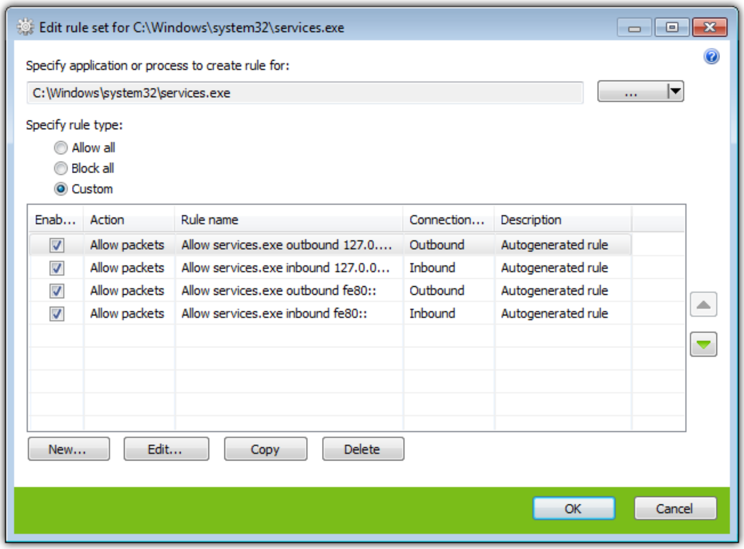
To configure advanced settings

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

Option	Description
Allow loopback interface	Select this checkbox 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 will be applied. Clear this checkbox to apply rules for connections carried out both through the network and within your computer.

Application Rules

The **New application rule set** (or **Edit rule set**) window lists types of the filtering rule for application or process, and also a rule set, if the **Custom** type is selected. You can change rule type, configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.



Edit rule set for C:\Windows\system32\services.exe

Specify application or process to create rule for:

C:\Windows\system32\services.exe

Specify rule type:

- ○ Allow all
- ○ Block all
- ● Custom

Enab...	Action	Rule name	Connection...	Description
☑	Allow packets	Allow services.exe outbound 127.0....	Outbound	Autogenerated rule
☑	Allow packets	Allow services.exe inbound 127.0.0...	Inbound	Autogenerated rule
☑	Allow packets	Allow services.exe outbound fe80::	Outbound	Autogenerated rule
☑	Allow packets	Allow services.exe inbound fe80::	Inbound	Autogenerated rule

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

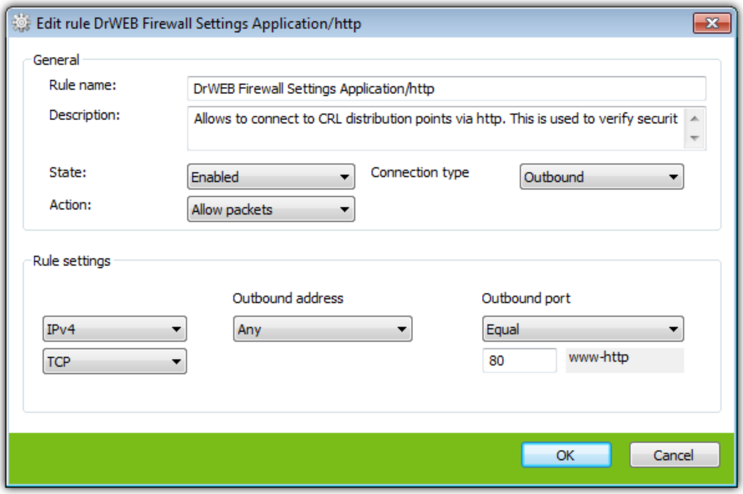
Column	Description
Action	The action for **Dr.Web Firewall** to perform when the connection attempt is detected: • **Block packets** • **Allow packets**
Rule name	The rule name.
Enabled	Execution states for the rule.
Connection type	The party which initiates the connection: • **Inbound** – the rule is applied when someone from the network attempts to connect to the application on you computer. • **Outbound** – the rule is applied when the application on your computer attempt to connect to the network. • **Any** – the rule is applied regardless of who initiate the connection.
Description	The rule description.

To configure rule sets

1. In the **Dr.Web Firewall** settings window, the **Applications** page and do one of the following:
   - to add a new set of rules, click **New**.
   - to edit an existing set of rules, select the rule set in the list and click **Edit**.
   - to delete all rules for an application, select the appropriate rule set and click **Delete**.
2. If you select to create a new or edit an existing set of application filter rules, in the opened window specify the application for which you want the rules to apply:
   - to add a set of rules for a user program, click ... ▼ and select the application executable file.
   - to add a set of rules for a process, click arrow on the ... ▼ button, choose **running application** and select the process.
3. Specify rule type:
   - **Allow all** - all connections will be allowed;
   - **Block all** - all connections will be blocked;
   - **Custom** - in this mode you can create a set of rules, that will allow or block different connections.
4. If you chose **Custom** type, create filtering rules using the following options:
   - to add a new rule, click **New**. The new rules is added to the end of the list.
   - to modify a rule, select it and click **Edit**.
   - to add a copy of a rule, select the rule and click **Copy**. The copy is added after the selected rule.
   - to delete a rule, select it and click **Delete**.
5. If you selected to create or edit a rule, in the opened window, then configure rule settings.
6. Use the arrows next to the list to change the order of rules. The rules are applied according to their order in the set.
7. When you finish adjusting the settings, click **OK** to save changes or **Cancel** to reject them.

Rule Settings

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



Rule name: DrWEB Firewall Settings Application/http

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

State: Enabled

Connection type: Outbound

Action: Allow packets

IPv4

TCP

Outbound address: Any

Outbound port: Equal

80 www-http

To add or edit a rule

1. Configure the following parameters:

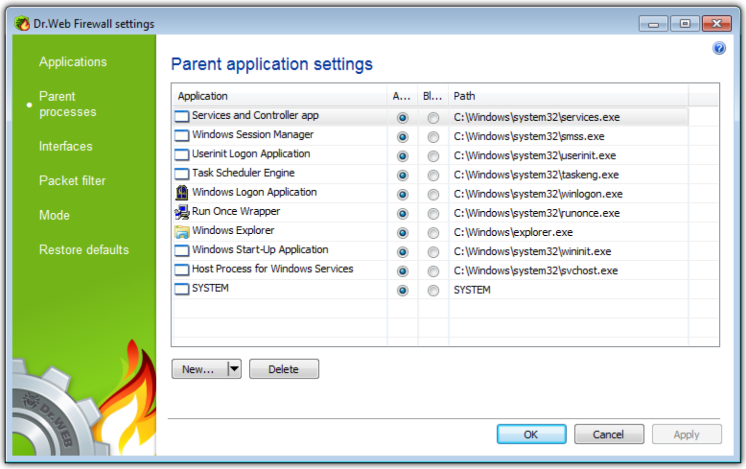
Parameter	Description
General	
Rule name	The rule name.
Description	The rule description.
State	One of the following execution states for the rule: • **Enabled** – apply rule for all matching connection attempts. • **Disabled** – do not apply the rule yet.

Connection type	The party which initiates the connection: - **Inbound** – apply the rule when someone from the network attempts to connect to the application on you computer. - **Outbound** – apply the rule when the application on your computer attempt to connect to the network. - **Any** – apply the rule regardless of who initiate the connection.
Action	The action for **Dr.Web Firewall** to perform when the connection attempt is detected: - **Block packets** - **Allow packets**
Rule Settings	
Protocol	The network and transport level protocols used for the connection attempt. **Dr.Web Firewall** supports the following network level protocols: - **IPv4** - **IPv6** - **IP all** – any version of IP protocol **Dr.Web Firewall** supports the following transport level protocols: - **TCP** - **UDP** - **TCP & UDP** – TCP or UDP protocol
Inbound/ Outbound address	The IP address of the remote host. You can specify either a specific address (**Equals**) or several IP addresses using a range (**In range A:B**) or subnetwork mask (**Mask**). To apply the rule for all remote hosts, select **Any**.
Inbound/ Outbound port	The port used for connection. You can specify either a specific port number (**Equals**) or a port range (**In range A:B**). To apply the rule for all ports, select **Any**.

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

Parent processes

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



Application	A...	Bl...	Path
Services and Controller app	●	○	C:\Windows\system32\services.exe
Windows Session Manager	●	○	C:\Windows\system32\smss.exe
Userinit Logon Application	●	○	C:\Windows\system32\userinit.exe
Task Scheduler Engine	●	○	C:\Windows\system32\taskeng.exe
Windows Logon Application	●	○	C:\Windows\system32\winlogon.exe
Run Once Wrapper	●	○	C:\Windows\system32\runonce.exe
Windows Explorer	●	○	C:\Windows\explorer.exe
Windows Start-Up Application	●	○	C:\Windows\system32\wininit.exe
Host Process for Windows Services	●	○	C:\Windows\system32\svchost.exe
SYSTEM	●	○	SYSTEM

To add rule for parent process:

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

Packet Filter

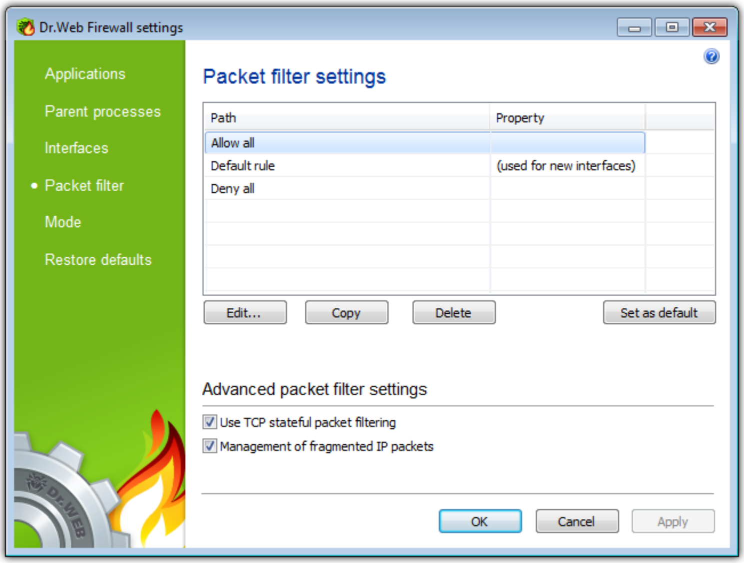
Packet filtering allows you to control access to network regardless of which program initiates connection. **Dr.Web Firewall** applies these rules to network packets transmitted through network interfaces of your computer.

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

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

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

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



Path	Property
Allow all	
Default rule	(used for new interfaces)
Deny all	

Advanced packet filter settings

☑ Use TCP stateful packet filtering

☑ Management of fragmented IP packets

To set rulesets for network interfaces

In the **Dr.Web Firewall** settings window, select **Packet filter** section. On this page you can:

- Configure sets of filtering rules by adding new rules, modifying or deleting existing ones, or changing order of rules execution.
- Select a default filtering rule.
- Configure general filtering settings.

To set default rules

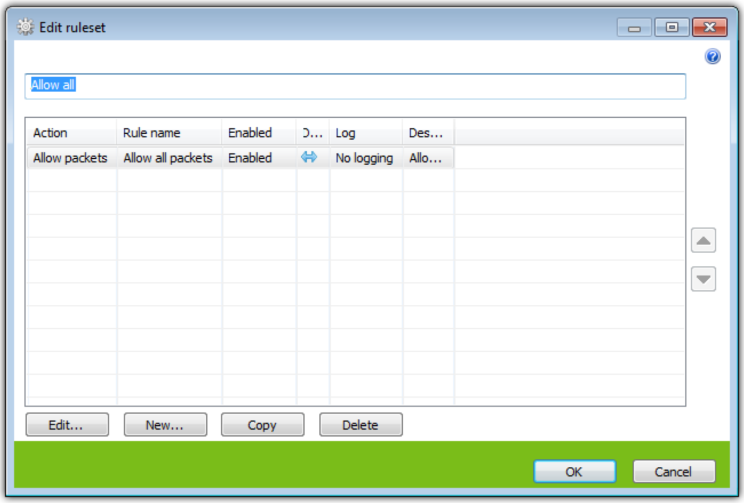
In the list, select the ruleset you want to use for new network interfaces installed on your computer and click **Set as default**.

To configure general settings

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

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

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



Allow all

Action	Rule name	Enabled	D...	Log	Des...
Allow packets	Allow all packets	Enabled	⇔	No logging	Allo...

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

Column	Description
Action	The action for **Dr.Web Firewall** to perform when the packet is intercepted: - **Block packets** - **Allow packets**
Rule name	The rule name.
State	One of the following execution states for the rule: - **Enabled** - the rule is applied for all matching packets. - **Disabled** - the rule is not applied.
Direction	The packet sender: - ⇦ – the rule is applied when packet is received from the network. - ⇨ – the rule is applied when packet is sent into the network from your computer. - ⇔ – the rule is applied regardless of packet transfer direction.

Column	Description
Log	The logging mode for the rule. This parameter defines which information is stored in the **Dr.Web Firewall** log: • **Log headers** – the packet header only. • **Entire packet** – the whole packet. • **No logging** - no information is logged.
Description	The rule description.

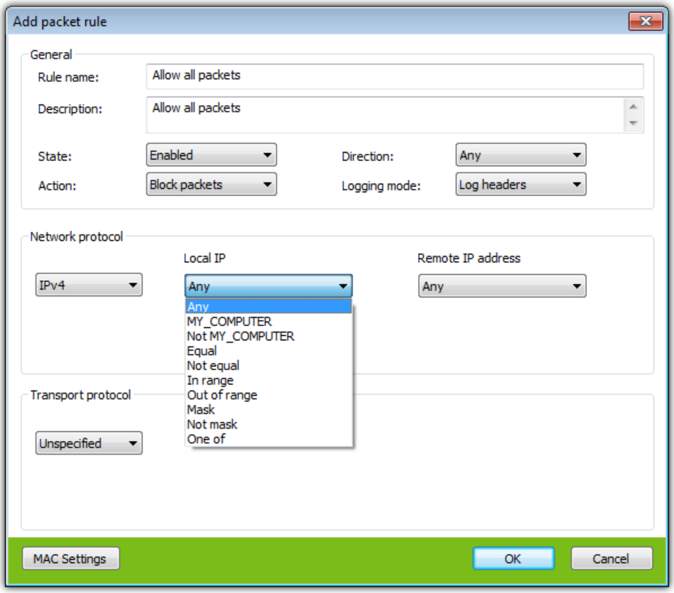
You can configure the list by adding new rules for the application or modifying existing rules and the order of their execution. The rules are applied according to their order in the set.

To configure rulesets

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

To add or edit a rule

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



Add packet rule

General

Rule name: Allow all packets

Description: Allow all packets

State: Enabled

Direction: Any

Action: Block packets

Logging mode: Log headers

Network protocol: IPv4

Local IP: Any

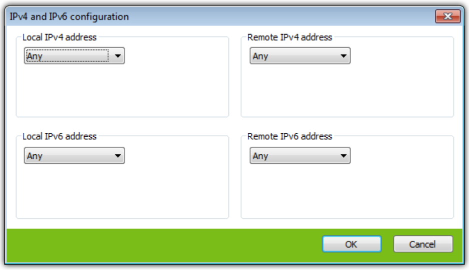
Remote IP address: Any

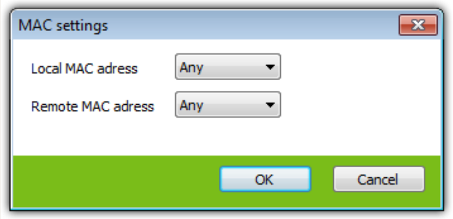
Transport protocol: Unspecified

2. Configure the following parameters:

Parameter	Description
General	
Rule name	The rule name.
Description	The rule description.
State	One of the following execution states for the rule: • **Enabled** – apply the rule for all matching packets.

Parameter	Description
	- **Disabled** – do not apply the rule yet.
Direction	The packet sender: - **Inbound** – apply the rule when packet is received from the network. - **Outbound** – apply the rule when packet is sent into the network from your computer. - **Any** – apply the rule regardless of packet transfer direction.
Action	The action for **Dr.Web Firewall** to perform when the packet is intercepted: - **Block packets** - **Allow packets**
Logging mode	The logging mode for the rule. This parameter defines which information is stored in the **Dr.Web Firewall** log: - **Log headers** – log packet headers only. - **Entire packet** – log whole packets. - **No logging** – do not log any information.
Network Level Protocol	
Protocol	Select one of the following network level protocols: - **IPv4** - Internet Protocol version 4 - **IPv6** - Internet Protocol version 6 - **IP all** - Internet Protocol of any version - **ARP** - Address Resolution Protocol - **EAPoL-802.1x** - Extensible Authentication Protocol (the IEEE 802.1X standard) - **PPPoE -** Point-to-point protocol over Ethernet To apply the rule for all protocols, select **Unspecified**.

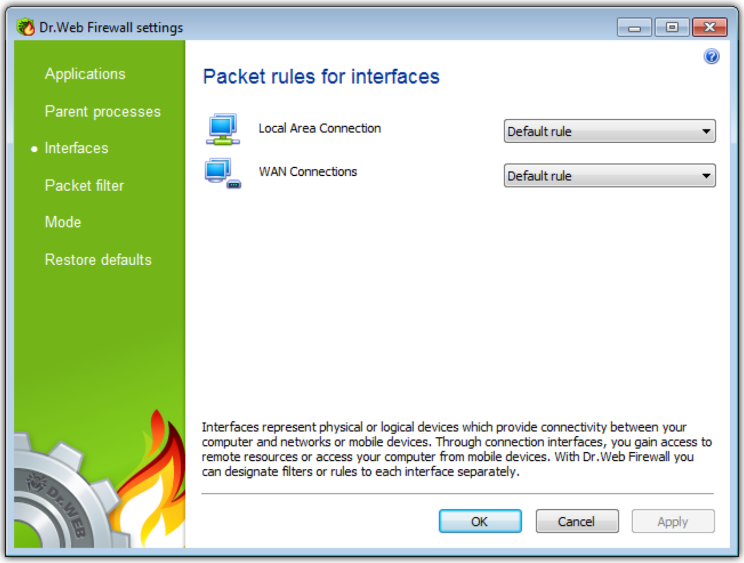
Parameter	Description
Local IP	(Available for **IPv4**, **IPv6**, or **IP all** protocols only) Select the comparison method and enter the IP address of your computer.
Remote IP	(Available for **IPv4** or **IPv6** protocols only) Select the comparison method and enter the IP address of the remote host.
Change ✎	(Available for **IP all** protocol only) Click to view the IP protocols configuration window.  IPv4 and IPv6 configuration Local IPv4 address Any Remote IPv4 address Any Local IPv6 address Any Remote IPv6 address Any OK Cancel Configure the following parameters: • **Local IPv4 address** – select the comparison method and enter your IPv4 address. • **Remote IPv4 address** – select the comparison method and enter the IPv4 address of the remote host. • **Local IPv6 address** – select the comparison method and enter your IPv6 address. • **Remote IPv6 address** – select the comparison method and enter the IPv6 address of the remote host.
Transport Level Protocol	
Protocol	Select one of the following transport level protocols: • **TCP** • **UDP**

Parameter	Description
	- **ICMPv4** – available for the IPv4 network level protocol only. - **ICMPv6** – available for the IPv6 network level protocol only. - **IGMP** – available for the IPv4 network level protocol only. - **GRE** – available for the IPv4 network level protocol only. - **SIPP-ESP** To apply the rule for all protocols, select **Unspecified**. For **ARP** or **EAPoL-802.1x** protocols, you cannot select a transport level protocol (**Unspecified**).
MAC Settings	Click to view MAC address filtering options.  MAC settings Local MAC adress: Any Remote MAC adress: Any Configure the following parameters: - **Local MAC address** – the MAC address of your network card. - **Remote MAC address** – the MAC address of the remote computer.

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

Network Interfaces

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



Packet rules for interfaces

Local Area Connection: Default rule

WAN Connections: Default rule

Interfaces represent physical or logical devices which provide connectivity between your computer and networks or mobile devices. Through connection interfaces, you gain access to remote resources or access your computer from mobile devices. With Dr.Web Firewall you can designate filters or rules to each interface separately.

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

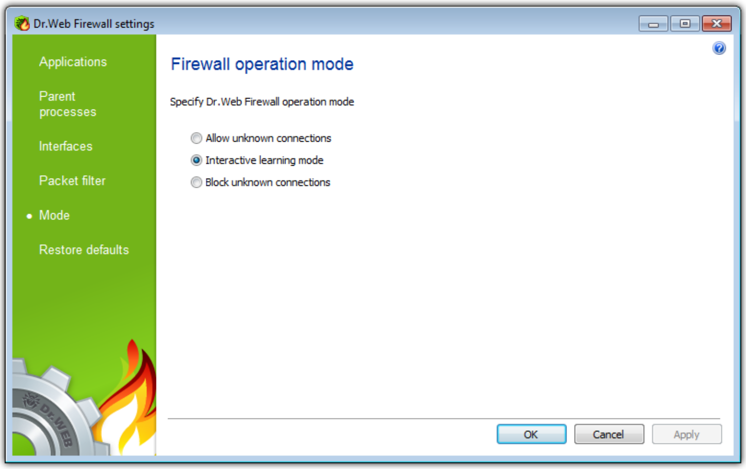
To set rulesets for network interfaces

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

Operation Modes

Operation modes set **Dr.Web Firewall** on application level connection.

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



Firewall operation mode

Specify Dr.Web Firewall operation mode

○ Allow unknown connections
● Interactive learning mode
○ Block unknown connections

To set operation mode

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

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

Learning Mode

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

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

This mode is used by default.

Restricted Access Mode

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

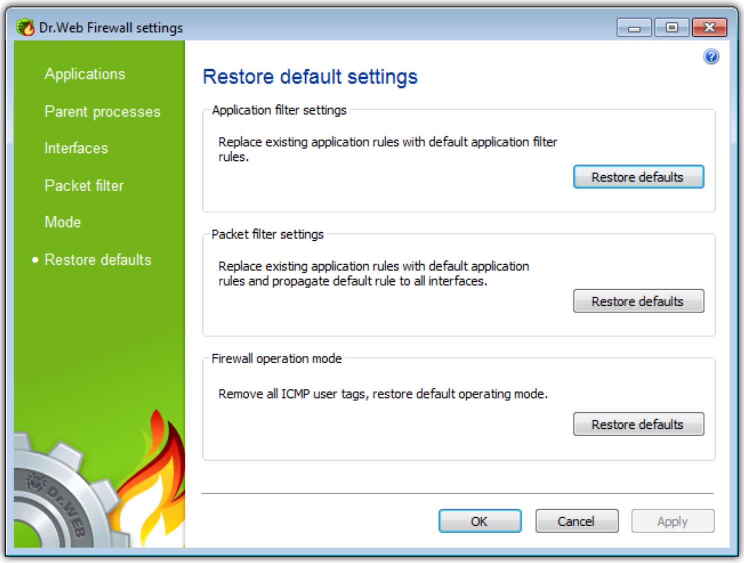
When a user application or operating system attempts to connect to a network, **Dr.Web Firewall** checks if there is a filtering ruleset for the application. If there are no filtering rules, **Dr.Web Firewall** blocks network access for the application without displaying any notification to the user.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

Free Access Mode

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

Restoring Defaults

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



Restore default settings

Application filter settings

Replace existing application rules with default application filter rules.

Packet filter settings

Replace existing application rules with default application rules and propagate default rule to all interfaces.

Firewall operation mode

Remove all ICMP user tags, restore default operating mode.

To restore default settings

1. In the **Dr.Web Firewall** settings window, select **Restore defaults**.
2. Do one of the following:
   - To restore default application filter settings, in the **Application filter settings** section, click **Restore defaults**.
   - To restore default packet filter settings, in the **Packet filter settings** section, click **Restore defaults**.
   - To set the default **Dr.Web Firewall** operation mode, in the **Firewall operation mode** section, click **Restore defaults**.

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

Event Logging

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

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

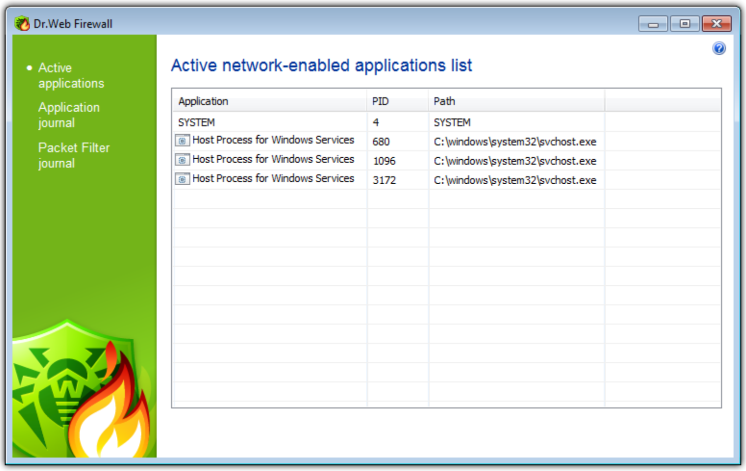
The **Active applications** page displays applications currently connected to a network.

To open journals:

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

Active Applications

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



Active network-enabled applications list

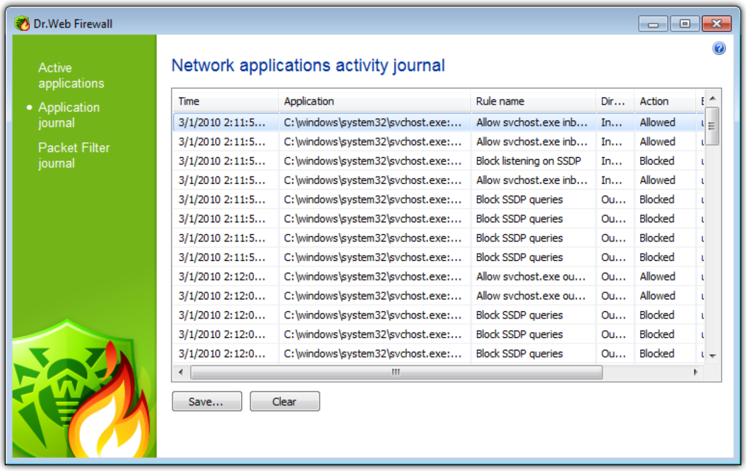
Application	PID	Path
SYSTEM	4	SYSTEM
Host Process for Windows Services	680	C:\windows\system32\svchost.exe
Host Process for Windows Services	1096	C:\windows\system32\svchost.exe
Host Process for Windows Services	3172	C:\windows\system32\svchost.exe

Column	Description
Application	The application description if available in the operating system.
PID	The identification number of the application process.
Path	The full path to the application executable file.

If necessary, use the process PID to terminate the application manually.

Application Filter Log

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



Network applications activity journal

Time	Application	Rule name	Dir...	Action
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Allow svchost.exe inb...	In...	Allowed
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Allow svchost.exe inb...	In...	Allowed
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Block listening on SSDP	In...	Blocked
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Allow svchost.exe inb...	In...	Allowed
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:11:5...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:12:0...	C:\windows\system32\svchost.exe:...	Allow svchost.exe ou...	Ou...	Allowed
3/1/2010 2:12:0...	C:\windows\system32\svchost.exe:...	Allow svchost.exe ou...	Ou...	Allowed
3/1/2010 2:12:0...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:12:0...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked
3/1/2010 2:12:0...	C:\windows\system32\svchost.exe:...	Block SSDP queries	Ou...	Blocked

Column	**Description**
Time	The date and time of the connection attempt.
Application	The full path to the application executable file, its name and process identification number (PID).
Rule name	The name of the rule applied.
Direction	The party which initiated the connection: • **Inbound** – someone from the network attempted to connect to the application on you computer. • **Outbound** – the application on your computer attempted to connect to the network. • **Any** – the rule was applied regardless of who initiated the connection.
Action	The action **Dr.Web Firewall** performed when the connection attempt was detected: • **Block packets** • **Allow packets**
Endpoint	The protocol, IP-address and the port used for the connection.

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

To save application filter log

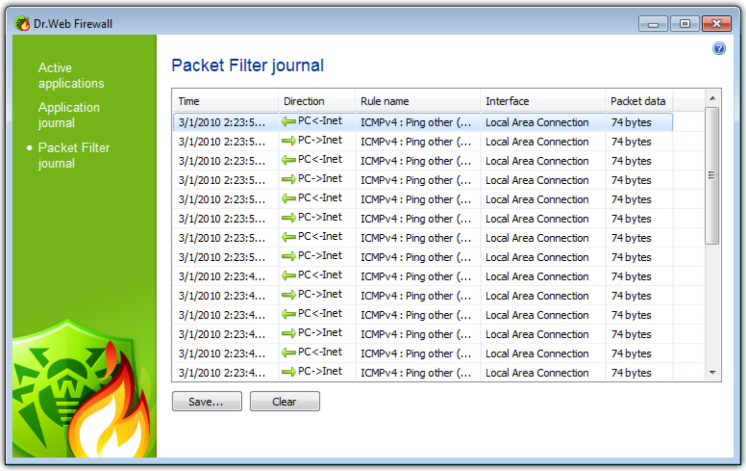
Click **Save**, then enter the file name where to store the log.

To clear application filter log

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

Packet Filter Log

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



Packet Filter journal

Time	Direction	Rule name	Interface	Packet data
3/1/2010 2:23:5...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:5...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC<-Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes
3/1/2010 2:23:4...	PC->Inet	ICMPv4 : Ping other (...	Local Area Connection	74 bytes

Column	Description
Time	The date and time when the packet was processed.
Direction	The packet sender: • ⇦ – the packet was transmitted from the network to your computer. • ⇨ – the packet was transmitted from your computer to the network. • ⬅ – the packet sent from the network to your computer was blocked. • ➡ – the packet sent from your computer to the network was blocked.
Rule name	The name of the applied rule.
Interface	The interface used to transmit the packet.
Packet data	Packet details. The **Logging mode** setting of the rule determines the amount of stored data.

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

To save packet filter log

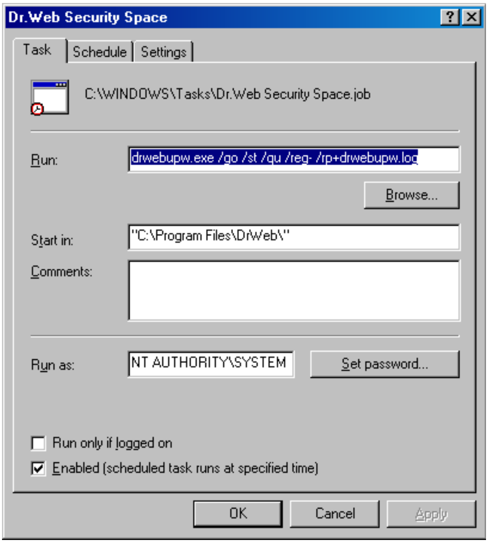
Click **Save**, then enter the file name where to store the log.

To clear packet filter log

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

Automatic Launch of Tasks for Scanning and Updating in Dr.Web

If **Dr.Web Security Space Pro** is installed on computers operated by Microsoft Windows XP, a task to update the virus databases and other files of the package is automatically created in the system scheduler (the Scheduled Tasks directory). To view the parameters of this task, select **Scheduler** in the **Tools** submenu of**SpIDer Agent** context menu. Settings for Windows XP are described below. In Windows Vista/7 the **Scheduler** item will open Task Scheduler.



C:\WINDOWS\Tasks\Dr.Web Security Space.job

Run: drwebupw.exe /go /st /qu /reg- /rp+drwebupw.log

Start in: "C:\Program Files\DrWeb\"

Comments:

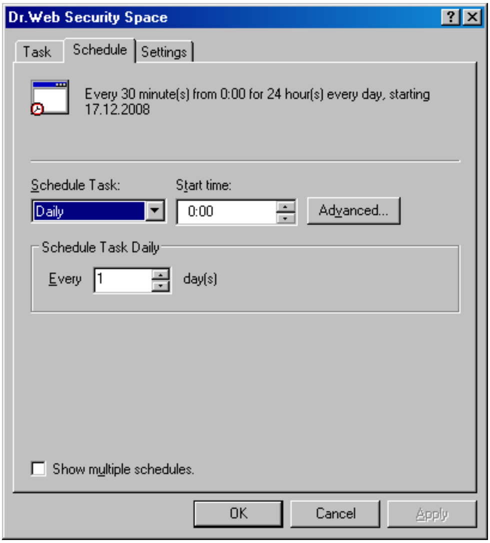
Run as: NT AUTHORITY\SYSTEM

☐ Run only if logged on

☑ Enabled (scheduled task runs at specified time)

In the **Task** tab the full name of the executable file and the command line parameters of the task are specified. The **Enabled** check box instructs to perform the task (if the check box is cleared the task is saved to the folder, but is not performed).

In the **Schedule** tab the schedule according to which a task will be run automatically is made.



Every 30 minute(s) from 0:00 for 24 hour(s) every day, starting 17.12.2008

Schedule Task: Daily

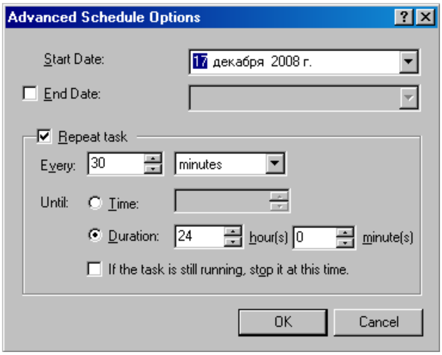
Start time: 0:00

Schedule Task Daily

Every 1 day(s)

☐ Show multiple schedules.

Click **Advanced**. The **Advanced Schedule Options** window will open.



Start Date: 17 декабря 2008 г.

☐ End Date:

☑ Repeat task

Every: 30 minutes

Until: ○ Time:

● Duration: 24 hour(s) 0 minute(s)

☐ If the task is still running, stop it at this time.

You can set your own tasks for anti-virus updating and scanning, delete or edit tasks. Consult the Help system and Windows documentation for more details on the system scheduler operation.

Automatic Updating

Modern computer viruses are characterized by the high-speed distribution. Within several days, and sometimes hours, a newly emerged virus can infect millions of computers around the world.

Developers of the anti-virus constantly supplement the virus databases with new records. When such updates are installed, the anti-virus can detect new viruses, block their distribution and, in some cases, cure the infected files.

From time to time the anti-virus algorithms implemented as executable files and program libraries are being updated. The field experience of the anti-virus helps to correct the detected program errors; the help system and documentation are being improved.

To speed up and facilitate the receipt and installation of the virus database updates and other files a special component – **Dr.Web Automatic Updating Utility for Windows** (**Updater**) – was created.

General Information

The operation of the **Updater** is governed by the structure of the virus databases and by the method of updating the virus databases and the program on the whole:

- The program includes the main virus database (drwebase.vdb) and its extensions (files drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb and drw50004.vdb). They all contain virus signatures known at the moment of the release of the given version of the program (for more details on the version read below).
- Once in a week the weekly add-ons are released – these are files with the virus records for detection and neutralization of viruses detected since the previous week’s add-on’s release. The weekly add-ons are files which look like this: drwXXXYY.vdb, where XXX is the current anti-virus version number

(without a separating full stop), and YY is the number of the weekly add-on. The weekly add-ons are numbered beginning from 05, i.e. the first add-on of the database in the anti-virus version 5.0 is called drw50005.vdb.

- If necessary (usually several times per day), hot add-ons with virus records for detection and neutralization of viruses detected since the last weekly add-ons are released. This add-on is the file called drwtoday.vdb. In the end of a day all the virus records from this file are included in drwdaily.vdb accumulative add-on. In the end of a weekend drwdaily.vdb contents are issued as the next weekly add-on.
- The program includes additional databases of malicious programs drwnasty.vdb and drwrisky.vdb. The records for detection of adware and dialers are included into the drwnasty.vdb virus database. The records for detection of joke programs, riskware and hacktools are included into the drwrisky.vdb virus database.
- From time to time cumulative add-ons for malicious programs database are released. Hot add-ons of these databases can be released much more rarely than for the main virus base.
- Also, files with lists of web sites which are blocked by **Parental Control** are occasionally released.
- From time to time the updates of other files are released independently to the virus database updates.
- From time to time fundamental updates of the anti-virus protection programs are released. This is a new anti-virus version release. All the virus records known up to this moment are included into the new main virus database. Old virus databases are deleted when the new version is installed.

Thus, for example, when version number 5.0 is installed and several weekly add-ons are received, the structure of the virus databases will be as follows:

- the main virus database – drwebase.vdb
- extensions of the main virus database – drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb and drw50004.vdb
- weekly add-ons – drw50005.vdb, drw50006.vdb etc.
- hot add-on – drwtoday.vdb

- accumulative add-on – drwdaily.vdb
- additional databases of malicious programs – drwnasty.vdb and drwrisky.vdb
- cumulative add-ons to malicious programs database – dwn50001.vdb, dwn50002.vdb etc. and dwr50001.vdb, dwr50002.vdb etc.
- hot add-ons of the additional databases of malicious programs – dwntoday.vdb and dwrtoday.vdb

The most convenient way to receive and install the updates of the virus databases and the program is to use the **Updater** described below.

To use the **Updater** you should have an Internet connection.

User should have administrator rights to update components of **Dr.Web**.

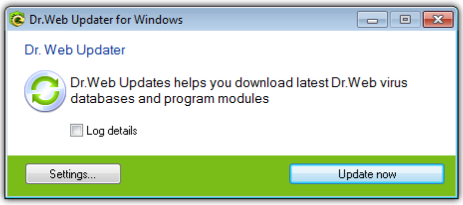
Launching and Using the Automatic Updating Utility

The **Automatic Updating Utility** (**Updater**) can be launched in one of the following ways:

- automatically, according to schedule (read Automatic Launch of Tasks for Scanning and Updating in Dr.Web);
- from the command line by activating the drwebupw.exe executable file from the program's installation folder;
- by selecting the **Update** item in the context menu of the **SpIDer Agent** icon;
- by selecting the **Update** item of the **File** menu in the main window of the **Scanner** (read Using Dr.Web Scanner for Windows);
- by pressing F8 in the active **Scanner** window.

If you launch **Dr.Web Updater** from **SpIDer Agent** menu or from the command line, the dialog window will open. You can launch update or set necessary parameters. Also you can set the **Log details** flag to increase change log detail level. All changes are logged into drwebupw.log file, that is located in %USERPROFILE%\DoctorWeb folder (in Windows 7, C:\Users\<*username*>\DoctorWeb).

If launching **Dr.Web Updater** automatically, changes are logged into drwebupw.log file, that is located in DrWeb folder of the installation folder.

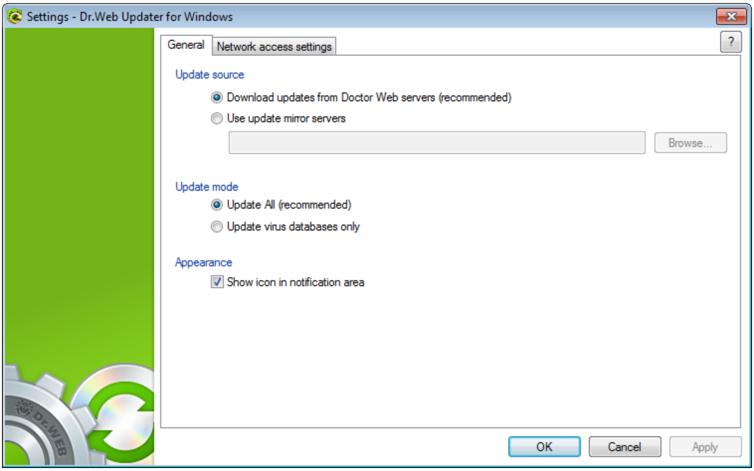


Dr.Web Updates helps you download latest Dr.Web virus databases and program modules

☐ Log details

Settings

To adjust update settings press the **Settings** button.



Settings - Dr.Web Updater for Windows

Update source

● Download updates from Doctor Web servers (recommended)

○ Use update mirror servers

Update mode

● Update All (recommended)

○ Update virus databases only

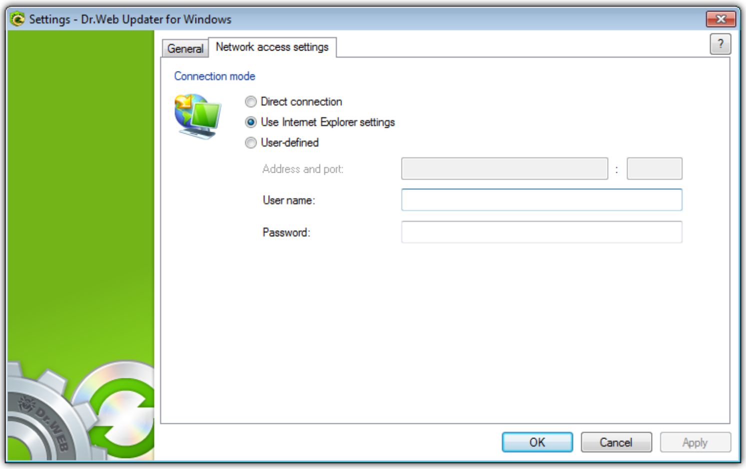
Appearance

☑ Show icon in notification area

On the **General** tab you can set the following parameters:

- **Update source**. **Dr.Web Updater** can download updates from **Doctor Web** servers (recommended) or mirror servers. If you use mirrors, set up necessary parameters;
- **Update mode**. You can choose one of the following:
    - **Update all (recommended)**. In this mode all **Dr.Web Security Space Pro** components, virus databeses and anti-virus engine will be updated;
    - **Update virus databases only**. In this mode **Dr.Web Security Space Pro** components will not be updated;
- **Appearance**. By default, notifications are displayed when update is finished. You can disable this option.

On the **Network access settings** tab you can set up network access.



If you do not use a proxy server, choose **Direct connection**.

If you use current settings for proxy server, choose **Use Internet Explorer settings**.

If you want to specify settings for proxy server, choose **User defined** and set up necessary parameters.

Launching Update

When launching update, the program checks the presence of the license key file in the installation folder, and, if it fails to find it, it tries to receive it via the Internet at www.drweb.com (this is described at the end of the License Key File section). If no key file is found, the updating is impossible.

If the key file is found, the program checks its validity at www.drweb.com (the file can be blocked, if discredited, i.e. its illegal distribution is uncovered). If the key file is blocked, the updating is not done and the components of the program can be blocked; a correspondent message is generated to a user.

If the key is blocked, contact the dealer you have purchased **Dr.**

Web Security Space Pro.

After the key file is successfully checked, the updating is performed. The program automatically downloads all updated files, according to your version of **Dr.Web Security Space Pro**, and, if your subscription terms allow, the new program version (if it is released).

The **Scanner** can use the updated databases after the next restart. **SpIDer Guard** and **SpIDer Mail** periodically check the state of the databases and download the updates of the databases automatically. In this case **SpIDer Guard** generates a prompt message on the update if the **Acknowledge=Yes** mode is enabled.

When the **Updater** is launched from the **Scheduler** or in the command line mode, the command line parameters can be used (read Appendix A).

Appendices

Appendix A. Additional Command Line Parameters of the Anti-virus

Introduction

Additional command line parameters (switches) are used to set parameters for programs which can be launched by opening an executable file. This relates to scanners of all versions (read Using Dr.Web Scanner for Windows and Command Line Scanning Mode) and to the **Updater** (read Automatic Updating of the Virus Databases and Other Files of the Program). The switches can set the parameters unavailable in the configuration file and have a higher priority then the parameters which are specified in it.

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

The command line parameters for the scanner and for the automatic updating module are listed below. If a switch has modifications then they are specified as well.

The Scanner command line parameters

/? – display short help on the program.

/@<*file_name***>** or **/@+<***file_name***>** instructs to scan objects listed in the specified file. Each object is specified in a separate line of the list-file. It can be either a full path with the file name or the boot string which means that scanning of boot sectors should be performed. For the GUI-version of the scanner the file names with mask and directory names should be specified there. The list-file can be prepared manually in any text editor; it can also be made automatically by applications using the scanner to check certain files. After the scanning is made, the scanner deletes the list-file, if used without the + character.

/AL – to scan all files in the given device, or in the given folder, regardless the extensions or the internal format.

/AR – to scan files inside the archives. At present, the scanning of archives (without curing) created by the ARJ, ZIP, PKZIP, ALZIP, RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE, etc. archivers, as well as of MS CAB-archives – Windows Cabinet Files and ISO-images of optical disks (CD and DVD) is available. As it is specified (/AR) the switch instructs to inform a user if an archive with infected or suspicious files is detected. If the switch is supplemented with the D, M or R modifier, other actions are taken: **/ARD** – delete; **/ARM** – move (by default, to the infected.!!! directory); **/ARR** – rename (by default, the first symbol of extension is replaced by the # character). The switch may end with the N modifier, and in this case the name of the archiver after the name of the archived file will not be printed.

/CN – to set action for containers (HTML, RTF, PowerPoint) with infected or suspicious objects. As specified (**/CN**) the switch instructs to report such containers to a user. If D, M or R modifiers are added to the switch, a different action is applied: **/CND** – delete; **/CNM** – move (by default, to the infected.!!! directory); **/CNR** – rename (by default, the first symbol of extension is replaced by the **#** character). The switch may end with the N modifier, and in such case a message with the container type will not be printed.

/CU – actions with infected files and boot sectors of drives. The curable objects are cured and the incurable files are deleted without additional D, M or R modifiers (if different action is not specified by the **/IC** parameter). Other actions taken towards infected files: **/CUD** – delete; **/CUM** – move (by default, to the infected.!!! directory); **/CUR** – rename (by default, the first symbol of extension is replaced by the # character).

/DA – to scan the computer once a day. The next check date is logged into the configuration file and that is why it should be accessible for writing and subsequent rewriting.

/EX – to scan files with extensions listed in the configuration file by default, or, if unavailable, these are EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

If an element of the list of scanned objects contains the explicit file extension, and it is used with special characters ***** and **?**, all files specified in this element of the list, and not only those matching this list of extensions, will be scanned.

/FAST – perform an express scan of the system (for more information on the express scan mode see Launching the Scanner. General Information.)

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

/GO – batch mode of the program. All questions implying answers from a user are skipped; solutions implying a choice are taken automatically. This mode is useful for automatic scanning of files, for example, during a daily (or weekly) check of the hard disk.

/HA – to perform heuristic scanning of files and search for unknown viruses in them.

/ICR, **/ICD** or **/ICM** – what to do with infected files which cannot be cured, **/ICR** – rename, **/ICD** – delete, **/ICM** – move.

/INI:<*path***>** – use alternative configuration file with specified name or path.

/LNG:<*file_name***>** or **/LNG** – use alternative language resources file (DWL file) with specified name or path, and, if the path is not specified, – the inbuilt (English) language.

/ML – scan files of e-mail format (UUENCODE, XXENCODE, BINHEX and MIME). As it is specified (**/ML**) the switch instructs to inform a user if an infected or suspicious object is detected in a mail archive.

If the switch is supplemented with the D, M or R modifier, other actions are taken: **/MLD** - delete; **/MLM** – move (by default, to the infected.!!! directory); **/MLR** – rename (by default, the first symbol of extension is replaced by the # character). The switch may end with the N modifier. In this case the "Mail archive" message will not be displayed.

/MW – actions with all types of unsolicited programs. As it is specified (**/MW**) the switch instructs to inform a user. If the switch is supplemented with the D, M, R or I modifier, other actions are taken: **/MWD** – delete; **/MWM** – move (by default, to the infected.!!! directory); **/MWR** – rename (by default, the first symbol of extension is replaced by the **#** character); **/MWI** – ignore. Actions with some types of unsolicited programs are specified by the **/ADW**, **/DLS**, **/JOK**, **/RSK**, **/HCK** switches.

/NI – not to use parameters specified in **drweb32.ini** configuration file.

/NR – do not create a log file.

/NS – disable interrupting of a computer scanning. With this switch specified, a user will not be able to interrupt scanning by pressing [ESC].

/OK – display full list of scanned objects and mark the uninfected with **Ok**.

/PF – prompt on, if multiple floppies are scanned.

/PR – prompt for confirmation before action.

/QU – the scanner checks the objects specified in the command line (files, disks, directories) and then automatically terminates (for the GUI version of the scanner only).

/RP<*file_name*> or **/RP+<*file_name*>** – log to a file the name of which is specified in the switch. If no name is specified, log to a default file. If the + character is present, the file is appended. If there is no character, a new one is created.

/SCP:<*n*> – sets the priority of the scanning process, where <n>

is a number ranging from 1 to 50.

/SD – scan subdirectories.

/SHELL – for the GUI version of the scanner. The switch disables the splash screen display, scanning of the memory and autorun files. This mode allows to use the GUI version of the scanner instead of the console version to scan only those objects which are listed in the command line parameters.

/SO – enables sounds.

/SPR, **/SPD** or **/SPM** – what to do with suspicious files, **/SPR** – rename, **/SPD** – delete, **/SPM** – move.

/SS – save the mode specified during the current program launch in the configuration file when the program terminates.

/ST – sets stealth mode of the GUI version of the scanner. The program operates without any windows opened and self-terminates. But, if during scanning virus objects were detected, the scanner window will be opened after the scanning made. Such scanner mode presupposes, that the list of the scanned objects is specified in the command line.

/TB – scan boot sectors and master boot records (MBR) of the hard drive.

/TM – search for viruses in main memory (including Windows system area, available for scanners for Windows only).

/TS – search for viruses in autorun files (in Autorun directory, system ini-files, Windows registry). It is used only in scanners for Windows.

/UPN – disable the output of names of file packers used for packing the scanned executable files to the log file.

/WA – do not terminate the program until any key is pressed, if viruses or suspicious objects are found (for console scanners only).

The modes specified by default (if no configuration file is available or used) are described in the table in Appendix_B._Adjustable parameters of Dr.Web components.

Certain parameters allow the "-" character to be used at the end. In such "negative" form the parameter means cancellation of the mode. Such option can be useful if this mode is enabled by default, or with the settings specified earlier in the configuration file. Here is the list of the command line parameters allowing "negative" form: **/ADW /AR /CU /DLS /FN /HCK /JOK /HA /IC /ML /MW /OK /PF /PR /RSK /SD /SO /SP/SS /TB /TM /TS /WA**

For **/CU**, **/IC** and **/SP** parameters the "negative" form cancels any actions specified in the description of these parameters. This means that infected and suspicious objects will be reported but no actions will be applied.

For **/INI** and **/RP** parameters the "negative" form is written as **/NI** and **/NR** accordingly.

For **/AL** and **/EX** the "negative" form is not allowed. However, specifying one of them cancels the other.

If several alternative parameters are found in the command line, the last of them takes effect.

Automatic Updating Module command line parameters

If the **Updater** is run by the **Scheduler** or in the command line mode, you can input the following command line parameters:

/DBG – detailed log.

The modes, specified by default (if no configuration file is available or used) are described in the table in Appendix_B._Adjustable parameters of Dr.Web components.

/DIR:<*directory***>** – change of the name of the folder where the updated files are placed; by default, the folder from which the **Updater** was launched is used.

/INI:<*path***>** – use alternative configuration file with specified name or path.

/GO – package operation mode, without dialogs.

/LNG:<*file_name***>** – language resources file name; if not specified, English is used.

/NI – do not use parameters specified in drweb32.ini configuration file.

/NR – do not create a log file.

/PASS:<*user password of http-server***>** – user password of the updating server.

/PPASS:<*proxy user password***>** – user password for the proxy server.

/PUSER:<*proxy user name***>** – user name for the proxy server.

/PURL:<*proxy address***>** – address of a proxy server.

/QU – to compulsory close the automatic utility after the updating is finished, regardless whether it was successful or not. The success of the updating can be checked via the drwebupw.exe return code (for example, from the bat-file by the errorlevel variable value: 0 – successful, other values – unsuccessful).

/REG – launch of the updating module for registration and receipt of a registration key file.

/RP<*file_name***>** or **/RP+<***file_name***>** – log to a file the name of which is specified in the switch. If no name is specified, log to a file with the default name. If the + character is present, the file is appended, if there is no character, a new one is created.

/SETTINGS - display the **Updater** settings.

/SO – enables sounds (only when errors occur).

/ST – run the automatic utility in invisible mode (stealth mode).

/UA – download all files specified in the updating list, regardless the used operating system and the installed components. The mode is designed for receipt of the full local copy of the **Dr.Web** server updating area; this mode cannot be used for updating the anti-virus installed on a computer.

/UPD – usual updating; it is used together with the /REG: switch - to run the updating session itself during the registration.

/UPM:<*proxy mode***>** – mode of using a proxy server, it can have the following values:

- **direct** – do not use proxy server
- **ieproxy** – use system settings
- **userproxy** – use settings specified by a user (in the **Update** pane of the **Dr.Web** toolbar or by the /PURL /PUSER /PPASS)

/URL:<*url of the updating server***>** – only UNC-paths are accepted.

/URM:<*mode***>** – to restart after the updating is finished. It can have the following values:

- **prompt** – prompt if a reboot is needed after the updating session is finished
- **noprompt** – if necessary, reboot without prompting
- **force** – reboot always (regardless whether it is required for the updating or not)
- **disable** – disable reboot

/USER:<*user name of http-server***>** – user name for the updating server.

/UVB – update the virus databases and drweb32.dll kernel only (disables **/UA**, if it is set).

/SO parameter allows the "-" character at the end. In such "negative" form the parameter means cancellation of the mode. This option can be useful if the mode is enabled with the settings specified earlier in the configuration file.

For **/INI** and **/RP** parameters the "negative" form is written as **/NI** and **/NR** accordingly.

If several alternative parameters are found in the command line, the last of them takes effect.

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. Adjustable Parameters of Dr.Web Components

Introduction

Adjustable parameters of the program components (except **SpIDer Guard**) are stored mainly in the program's configuration file (drweb32.ini resides in the installation folder). This is a text file and has separate sections for different components. Each parameter of any component is specified in the correspondent section as a string `parameter = value`.

The values of parameters can be changed in one of the following ways:

- via the interface of the corresponding program (**Scanner**, **SpIDer Mail**). The most important of such settings are described above (read Adjusting the Scanner Settings, Adjusting Certain Program Settings);
- by setting command line parameters when calling programs from the command line or according to schedule (for the **Scanner** of different versions). Read Appendix A for more details on this option;
- by editing the configuration file via any text editor.

Only experienced users should edit the configuration file. Using this option without clear understanding of the anti-virus structure may degrade the reliability of the anti-virus protection or even result in failure of some programs.

Before editing the configuration file, you should deactivate **SpIDer Mail** as it is described in corresponding sections.

The parameters of the Windows versions of the Scanner, SpIDer Guard, Scheduler and Updater

The following data for every parameter is displayed in columns of Table 3:

- parameter name
- name of components using the parameter
- parameter name in the configuration file
- parameter values
- command line keys

The parameter name is either printed in conformity with the interface (printed in bold), or as a conventional name, if no parameter in the interface corresponds to it (printed in light type).

In the Table "Scanner" is used for both versions o the **Scanner** ("Scanner-GUI" and "Console scanner").

If a correspondent parameter of the configuration file is missing for some mode, the values of parameters are specified in brackets and relate to the interface dialog element or to the specified command line switch.

The default values for the **Scanner**, **Scheduler** and **Updater** are printed in bold; for all components – in bold italic.

The command line switches corresponding to the given parameter are described shortly, without the majority of modifiers. Detailed information on switches is given in Appendix A.

Parameter	Components	Configur. file parameter	Values	Keys
Scan mode	Scanner	ScanFiles	All ByType ByMasks	/AL /EX
Express scan of the system	Scanner			/FAST

Parameter	**Components**	**Configur. file parameter**	**Values**	**Keys**
Full scan of the system	Scanner			/FULL
Priority of the scanning process, from 1 to 50	Scanner			/SCP
Heuristic analysis	Scanner	HeuristicAnalysis	Yes / No	/HA
Scan memory	Scanner	TestMemory	Yes / No	/TM
Scan autorun files	Scanner	TestStartup	Yes / No	/TS
Scan boot sectors	Scanner	TestBootSectors	Yes / No	/TB
Scan subfolders	Scanner	ScanSubDirectories	Yes / No	/SD
Prompt on multiple floppies	Scanner	PromptFloppy	Yes / No	/PF
Archives	Scanner	CheckArchives	Yes / No	/AR
Mail files	Scanner	CheckEMailFiles	Yes / No	/ML
Max size of unpacked archive to check, KB	Console Scanner	MaxFileSizeToExtract	(empty)	
Max compression ratio for archive	Console Scanne	MaxCompressionRatio	(empty)	
Threshold for MaxCompression Ratio, KB	Console scanner	CompressionCheckThreshold	(empty)	

Parameter	**Components**	**Configur. file parameter**	**Values**	**Keys**
List of extensions	Scanner	FilesTypes	(see below the Table)	
List of masks	Scanner	UserMasks	(see below the Table)	
Locations of excluded folders	Scanner	ExcludePaths	(empty)	
Excluded files	Scanner	ExcludeFiles	(empty)	
Scan hard drives (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanHDD	Yes / No	
Scan floppies (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanFDD	Yes / No	
Scan compact disks (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanCD	Yes / No	

Parameter	Components	Configur. file parameter	Values	Keys
Scan network disks (if scanned with the * command line parameter and when the Select drives button is pressed)	Scanner	ScanNet	Yes / No	
Prompt on action	Scanner	PromptOnAction	Yes / No	/PR
Rename extension	Scanner	RenameFilesTo	#??	
Move path	Scanner	MoveFilesTo	infected.!!!	
Location of virus databases	Scanner	VirusBase	*.vdb	
Path to the folder with temporary files of the component	Scanner	TempPath	%TMP%, %TEMP%, install directory	
Actions with all types of malicious programs	Scanner		Report	/MW
Infected objects	Scanner	InfectedFiles	Report Cure Delete Rename Move Lock (guard) Shutdown (guard)	/CU

Parameter	Components	Configur. file parameter	Values	Keys
Incurable objects	Scanner	IncurableFiles	Report Delete Rename Move Lock (guard) Shutdown (guard)	/IC
Suspicious objects	Scanner	SuspiciousFiles	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/SP
Infected archives	Scanner	ActionInfectedArchive	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/AR
Infected mail files	Scanner	ActionInfectedMail	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/ML

Parameter	**Components**	**Configur. file parameter**	**Values**	**Keys**
Adware programs	Scanner	ActionAdware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/ADW
Dialer programs	Scanner	ActionDialers	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/DLS
Joke programs	Scanner	ActionJokes	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/JOK
Riskware	Scanner	ActionRiskware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/RSK

Parameter	Components	Configur. file parameter	Values	Keys
Hacktools	Scanner	ActionHacktools	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/HCK
Permit archives deletion without a prompt	Scanner	EnableDeleteArchiveAction	Yes / No	
Log to file	Scanner, Updating module	LogToFile	Yes / No	/RP /NR
Write log file	Scheduler		(On / Off)	
Log file name	Scanner	LogFileName	drweb32w.log spider.log spidernt.log	/RP
Log file name	Updating module		drwebupw.log	/RP
Log file name	Scheduler		drwebscd.log	
Log mode	Scanner, Updating module	OverwriteLog	Yes / No	/RP
Log encoding	Scanner, Updating module	LogFormat	ANSI OEM	
Scanned objects in log file	Scanner	LogScanned	Yes / No	/OK
Names of file packers in log file	Scanner	LogPacked	Yes / No	

Parameter	**Components**	**Configur. file parameter**	**Values**	**Keys**
Names of archivers in report	Scanner	LogArchived	Yes / No	
Statistics in log file	Scanner	LogStatistics	Yes / No	
Maximum log file size	Scanner, Updating module	LimitLog	Yes / No	
Log size limit, KB	Scanner, Updating module	MaxLogSize	512 8192	
Close the window after sessions	Scanner, Updating module		Yes / No	/QU
Wait for a key to be pressed as soon as scanning is complete (in case a virus is detected)	Console scanner	WaitAfterScan	(On / Off)	/WA
Operate in packet mode	Scanner, Updating module		(On / Off)	/GO
Prohibit interruption by a user	Scanner		(On / Off)	/NS
Scan once a day	Scanner		(On / Off)	/DA
Scan the explicitly selected objects only	Scanner-GUI		(On / Off)	/SHELL
Do not open windows (stealth mode)	Scanner-GUI		(On / Off)	/ST

Parameter	Components	Configur. file parameter	Values	Keys
Use alternative configuration file. Do not use any configuration file	Scanner, Updating module		(On / Off)	/INI /NI
Use own swap file	Scanner	UseDiskForSwap	Yes / No	
Display progress bar	Scanner	ShowProgressBar	Yes / No	
Sounds	Scanner, Updating module	PlaySounds	Yes / No	/SO
Alert (sound)	Scanner	AlertWav	alert.wav	
Cured (sound)	Scanner	CuredWav	cured.wav	
Deleted (sound)	Scanner	DeletedWav	deleted.wav	
Renamed (sound)	Scanner	RenamedWav	renamed.wav	
Moved (sound)	Scanner	MovedWav	moved.wav	
Finish (sound)	Scanner	FinishWav	finish.wav	
Error (sound)	Scanner, Updating module	ErrorWav	error.wav	
Autosave settings	Scanner	AutoSaveSettings	Yes / No	/SS
Show icon in tray	Scheduler		(On / Off)	
Use registry settings	Scanner-GUI		(On / Off)	
Scan priority	Scanner	ScanPriority	25 50	

Parameter	Components	Configur. file parameter	Values	Keys
Language	Scanner, Updating module	LngFileName	ru-drweb.dwl	/LNG
Proxy mode	Scanner-GUI (the updating module settings)	UpdateProxyMode	direct ieproxy userproxy	/UPM
Update the virus databases and drweb32.dll kernel only	Updating module	UpdateVirusBasesOnly	Yes / No	/UVB
Download all files from the update list	Updating module	UpdateAllFiles	Yes / No	/UA
Reboot mode at updating	Updating module	UpdateRebootMode	prompt noprompt force disable	/URM
Log details	Updating module		(On / Off)	/DBG

By default, the list of file extensions (the **FilesTypes** parameter value) contains the following extensions: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

By default, the list of selected masks (the **UserMasks** parameter value of the configuration file) contains the values formed by adding the asterisk ***** symbol and a full stop before an extension from the list of file extensions (for example, ***.exe**).

Parameters of SpIDer Mail

Parameters of **SpIDer Mail** are described in the table below. The layout of this table is similar to that of the table above. In the list of admissible parameter values, the default values for **SpIDer Mail** are given in italics.

Parameter	**Configuration file parameter**	**Value**	**Key**
Use alternative configuration file		(On / Off)	-ini: file_name
Use alternative user key file		(On / Off)	-key: file_name
Language	LngFileName	ru-drweb.dwl	-lng: file_name
Heuristic analysis	HeuristicAnalysis	Yes / No	
Check archive files	CheckArchives	Yes / No	
Virus activity control	VirusActivityControl	Yes / No	
Message scan timeout, s	ScanTimeout	250	
Max file size to extract, KB	MaxFileSizeToExtract	30720	
Max compression ratio	MaxCompressionRatio	Infinite	
Max archive level	MaxArchiveLevel	64	
Show virus alerts for outgoing mail	ShowAlerts	Yes / No	
Infected messages	ActionInfected	Delete Move	
Suspicious messages	ActionSuspicious	Delete Move Skip	
Not checked messages	ActionNotChecked	Delete Move Skip	

Parameter	**Configuration file parameter**	**Value**	**Key**
Delete modified messages on the server	DeleteMessagesOnServer	Yes / No	
Insert 'X-AntiVirus' header into messages	InsertXAntiVirus	Yes / No	•
Path to quarantine	PathForMovedFiles	infected.!!!	
Path to Dr.Web engine	EnginePath	(empty)	
Path to Dr.Web virus database	VirusBasesPath	(empty)	
Flag file to detection update	UpdateFlag	drwtoday.vdb	
Period to check flag file, s	UpdatePeriod	300	
Maximum load engines	MaximumLoadEngines	10	
Preload engines	PreloadEngines	1	
Unused engine unload timeout, s	UnusedEngineUnloadTimeout	420	
Enable logging	EnableLog	Yes / No	
Enable logging scan info	EnableLogScanInfo	Yes / No	
Log to file	LogFileName	spiderml.log	
Maximum log file size, KB	MaximumLogSize	500	
Enable icon animation	EnableIconAnimation	Yes / No	
Enable tray icon	HideIcon	Yes / No	
Show notifications	NoBalloons	Yes / No	

Parameter	**Configuration file parameter**	**Value**	**Key**
Intercept connections automatically or Manual connections setup radio buttons	HookModeAuto	Yes / No	
Test interception functionality on every starting (aut. mode)	HookCheck	Yes / No	
Address-Port (the first element of the list, aut.mode)	Hook1	*:143 address:port	
Address-Port (continuation of the list, aut.mode)	Hook2 Hook3 …	address:port address:port …	
SpIDerMail port-Server address – Server port (manual mode, first element of the list)	HookManual1	7000 -> address POP3/SMTP/ IMAP4/ NNTP: port	
SpIDerMail port-Server Address - Server Port (manual mode, continuation of the list)	HookManual2 HookManual3 …	7001 -> address POP3/SMTP/ IMAP4/ NNTP: port 7002 -> address POP3/SMTP/ IMAP4/ NNTP: port …	
Enable the Disable menu item	AllowDisable	Yes / No	

Parameter	Configuration file parameter	Value	Key
Enable the Exit menu item	AllowExit	Yes / No	
Enable the Settings menu item	AllowSettings	Yes / No	
Enable the Reinitialize menu item	AllowReinitialize	Yes / No	
Max simultaneously processed queries at one local port (manual mode)	MaximumChildConnections	20	
A string added to message	Xbanner	(empty)	
Path to temporary files directory of the component	TempPath	%TMP%, %TEMP%, install directory	
Reinitialize			-reinit
Disable			-disable
Enable			-enable
Update			-update
Exit			-exit

Appendix C. Malicious Programs and Methods of Neutralizing Them

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

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

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

Classification of malicious programs and other computer threats.

Computer viruses

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

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

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

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

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

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

Polymorphic viruses also encrypt 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 e-mail) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user's action or in an automatic mode, choosing which computers to attack.

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

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

Trojan horses (Trojans)

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

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

Rootkits

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

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

Hacktools

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

Spyware

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

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

Adware

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

Joke programs

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

Dialers

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

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

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

Below is a list of various hacker attacks and internet fraud:

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

Actions applied to malicious programs

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

Cure – an action applied to viruses, worms and trojans. It implies deletion of malicious code from infected files or deletion of a malicious program's functional copies as well as the recovery of affected objects (i.e. return of the object's structure and operability to the state which was before the infection) if it is possible. Not all malicious programs can be cured. However, products of **Doctor Web, Ltd.** are based on more effective curing and file recovery algorithms compared to other anti-virus manufacturers.

Move to quarantine – an action when the malicious object is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the virus laboratory of **Doctor Web, Ltd.** for analysis.

Delete – the most effective action for neutralizing computer threats. It can be applied to any type of malicious objects. Note, that deletion will sometimes be applied to certain files for which curing was selected. This will happen if the file contains only malicious code and no useful information. E.g. curing of a computer worm implies deletion of all its functional copies.

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

Appendix D. Naming of Viruses

Specialists of the **Dr.Web Virus Laboratory** give names to all collected samples of computer threats. These names are formed according to certain principles and reflect a threat's design, classes of vulnerable objects, distribution environment (OS and applications) and some other features. Knowing these principles may be useful for understanding software and organizational vulnerabilities of the protected system. In certain cases this classification is conventional, as some viruses can possess several features at the same time. Besides, it should not be considered exhaustive, as new types of viruses constantly appear and the classification is made more precise. The full and constantly updated version of this classification is available at the Dr.Web web site.

The full name of a virus consists of several elements, separated with full stops. Some elements at the beginning of the full name (prefixes) and at the end of it (suffixes) are standard for the accepted classification. Below is a list of all prefixes and suffixes used in **Dr.Web** divided into groups.

Prefixes

Affected operating systems

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

- Win - 16-bit Windows 3.1 programs
- Win95 - 32-bit Windows 95/98/Me programs
- WinNT - 32-bit Windows NT/2000/XP/Vista programs
- Win32 - 32-bit Windows 95/98/Me and NT/2000/XP/Vista programs
- Win32.NET - programs in Microsoft .NET Framework operating system
- OS2 - OS/2 programs

- Unix - programs in various Unix-based systems
- Linux - Linux programs
- FreeBSD - FreeBSD programs
- SunOS - SunOS (Solaris) programs
- Symbian - Symbian OS (mobile OS) programs

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

Macrovirus prefixes

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

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

Development languages

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

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

The following prefix also refers to development language:

- Java - viruses designed for the Java virtual machine

Script-viruses

Prefixes of viruses written in different scrip languages:

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

Trojan horses

- Trojan - a general name for different Trojan horses (Trojans). In many cases the prefixes of this group are used with the Trojan prefix.
- PWS - password stealing Trojan
- Backdoor - Trojan with RAT-function (Remote Administration Tool - a utility for remote administration)
- IRC - Trojan which uses Internet Relay Chat channels
- DownLoader - Trojan which secretly downloads different malicious programs from the Internet
- MulDrop - Trojan which secretly downloads different viruses contained in its body
- Proxy - Trojan which allows a third party user to work anonymously in the Internet via the infected computer
- StartPage (synonym: Seeker) - Trojan which makes unauthorized replacement of the browser’s home page address (start page)
- Click - Trojan which redirects a user’s browser to a certain web site (or sites)
- KeyLogger - a spyware Trojan which logs key strokes; it may send collected data to a malefactor
- AVKill - terminates or deletes anti-virus programs, firewalls, etc.
- KillFiles, KillDisk, DiskEraser - deletes certain files (all files on drives, files in certain directories, files by certain mask, etc.)
- DelWin - deletes files vital for the operation of Windows OS
- FormatC - formats drive C

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

Tools for network attacks

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

Malicious programs

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

Miscellaneous

- Exploit - a tool exploiting known vulnerabilities of an OS or application to implant malicious code or perform unauthorized actions.
- Generic - this prefix is used after another prefix describing the environment or the development method to name a typical representative of this type of viruses. Such virus does not possess any characteristic features (such as text strings, special effects, etc.) which could be used to assign it some specific name.
- Silly - this prefix was used to name simple featureless viruses the with different modifiers in the past.

Suffixes

Suffixes are used to name some specific virus objects:

- Origin - this suffix is added to names of objects detected using the *Origins Tracing* algorithm.
- generator - an object which is not a virus, but a virus generator.
- based - a virus which is developed with the help of the specified generator or a modified virus. In both cases the names of this type are generic and can define hundreds and sometimes even thousands of viruses.
- dropper - an object which is not a virus, but an installer of the given virus.

Appendix E. Corporate network protection by Dr.Web® Enterprise Suite

Dr.Web provides reliable, flexible and easy customized protection against viruses and other unsolicited programs.

The versions of the program designed for Windows, as well as versions for other platforms, provide reliable computer protection in a company. Still, the functioning of computers within a corporate network has certain problems for the anti-virus protection:

- usually, the software is installed onto computers by a company network administrator. The installation of anti-virus programs, their timely updating is an additional work for the administrator and requires physical access to computers
- any changes made in the settings of the anti-virus by an inexperienced user (including its disabling because of the seeming inconveniences) generate "holes" in protection – the viruses begin to penetrate inside the corporate network and their disinfection becomes a much more complicated task
- the anti-virus protection can be fully efficient if its operation is analyzed by qualified specialists which includes analysis of protocols, files moved to the quarantine, etc. This work may be difficult in conditions, when this data is kept in dozens or hundreds computers

To solve these problems, **Dr.Web Enterprise Suite** (**Dr.Web ES**) was developed.

Dr.Web ES allows the following:

- centralized (without unnecessary access of the personnel) installation of anti-virus packages on the protected computers
- centralized setting of parameters of the anti-virus packages
- centralized updating of the virus databases and programs on protected computers
- to monitor the virus events, as well as the state of the anti-virus packages and the OS on all protected computers

Dr.Web ES allows both to leave a user with the right to modify the settings and to administrate the anti-virus package of his computer, and to flexibly restrict modifications, or even forbid them at all.

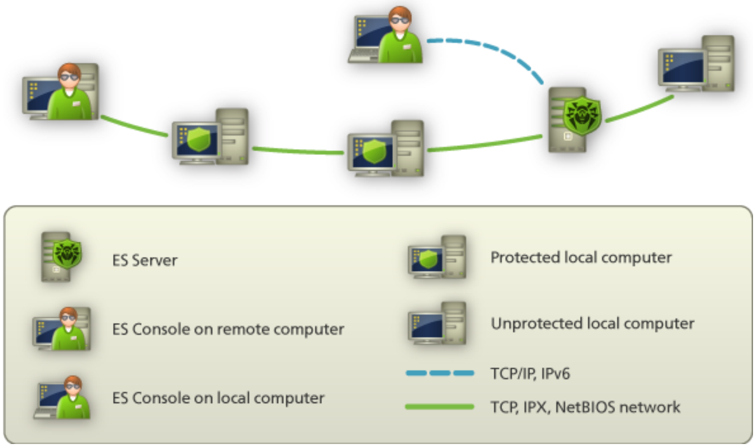
Dr.Web ES has a "client-server" architecture. Its components are installed on computers of the local network and exchange information using network protocols (more detailed description of interaction of the program‘s components is given below). The computers on which the interacting components of **Dr.Web ES** are installed are caledl the anti-virus network. The anti-virus network includes the following components:

- **Anti-virus agent**. This component is installed on a protected computer; it installs updates and manages the anti-virus package as instructed by the anti-virus server (read below). The agent also sends information on the virus events and other necessary information about the protected computer to the anti-virus server
- **Anti-virus server**. This component is installed on one of the computers of the local network. The anti-virus server stores distribution kits of anti-virus packages for different OS’s of protected computers, the updates of the virus databases, of the anti-virus packages and anti-virus agents, users’ keys and settings of packages of the protected computers and sends them by requests of agents to corresponding computers. The anti-virus server keeps one log of events of the whole anti-virus network and separate logs for each protected computer
- **Anti-virus console**. This component is used for remote administration of the anti-virus network by editing the settings of the anti-virus server and settings of protected computers stored on the anti-virus server

---

The **Anti-virus Console** can be installed on computers outside the local network; it only requires a TCP/IP connection between the console and the anti-virus server.

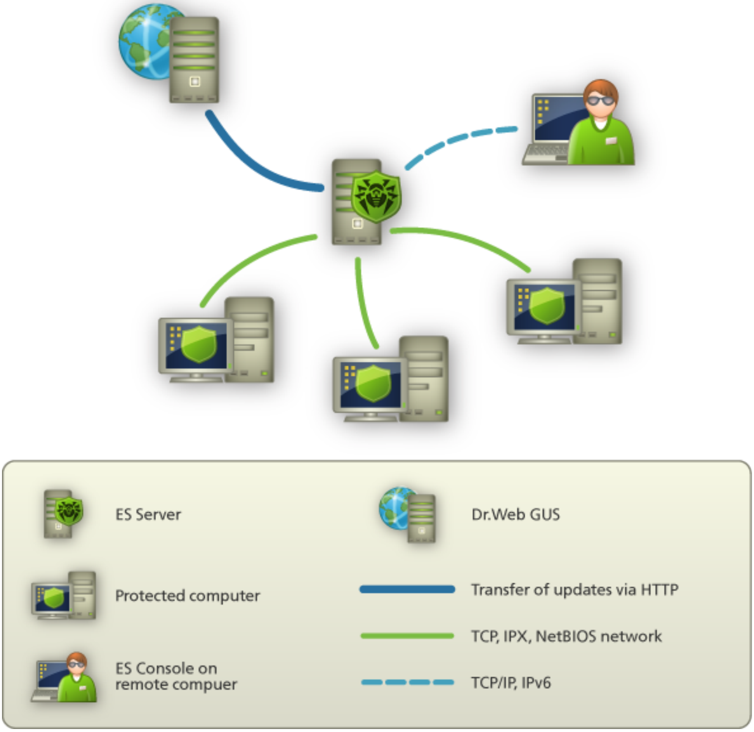
The illustration below describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.


ES Server
ES Console on remote computer
ES Console on local computer
Protected local computer
Unprotected local computer
TCP/IP, IPv6
TCP, IPX, NetBIOS network

Physical structure of the anti-virus network

The flow of commands, data and statistical information in the anti-virus network obligatory goes trough the anti-virus server. The anti-virus console also exchanges the data with the server only; the changes in configuration of a workstation and the transfer of commands to the anti-virus agent are made by the server on the basis of the console commands.

Thus, the logical structure of the fragment of the anti-virus network looks as in the illustration below.


ES Server
Dr.Web GUS
Protected computer
Transfer of updates via HTTP
TCP, IPX, NetBIOS network
ES Console on remote compuer
TCP/IP, IPv6

Logical structure of the anti-virus network

The following requests are sent from the server to workstations and back (thin firm line in the illustration) using one of the supported network protocols (TCP, IPX or NetBIOS):

- requests of an agent for the centralized schedule’s receipt and the centralized schedule of the given workstation
- the settings of the agent and the anti-virus package
- requests for the scheduled tasks to be performed (scanning, updating of the virus database, etc.)
- modules of the anti-virus packages – when the agent receives a task to install them
- updates of the software and the virus databases – when the updating is performed

- messages of the agent on the configuration of a workstation
- statistics on the agent’s operation and the anti-virus packages to be included into centralized log
- messages on virus events and other events which should be logged

The volume of traffic between the workstations and the server, depending on the settings of workstations and their quantity, can be rather substantial, that is why **Dr.Web ES** provides the traffic compression option.

The traffic between the server and a workstation can be encrypted. This allows to avoid leakage of data transferred via the described channel, as well as to avoid the replacement of the SW downloaded onto the workstations.

Thus, **Dr.Web ES** provides:

- easy centralized installation of the anti-virus SW on protected computers, and in most cases (for computers operated by Windows 2000/XP/Vista) the installation can be done without physical access to a computer
- centralized set up of the anti-virus SW and update with minimum man-hour spent
- control of the state of the anti-virus protection
- centralized launch or termination of tasks of the anti-virus SW on computers (if necessary)
- collection and analysis of information on virus events in all protected computers
- the option to give some users right to set up the anti-virus SW (if necessary)
- management of the anti-virus network and receipt of information about it by the administrator of the anti-virus protection both from workstations of the corporate network and remotely, from the Internet

In large corporate networks with hundreds or thousands computers it is advisable to create the **Dr.Web ES** anti-virus network with several servers. The hierarchy connection between the servers allows to simplify the updating of the virus databases and the SW of the workstations and the receipt of the information on the virus events from them. The administrator can analyze the logs of the network, both of separate servers and the summary log of the whole anti-virus network.

Dr.Web ES in corporate networks increases reliability of the anti-virus protection and cuts costs for its administration comparing to installation of personal anti-virus programs on protected computers.

Dr.Web Enterprise Suite has several advantages in comparison to other similar products:

- high reliability and security of applied solutions
- easy administration
- multiplatform structure of all components
- excellent scalability

We recommend to purchase and install **Dr.Web ES** if:

- your corporate network has significant size (several dozens of computers or more)
- your network is small, but due to some reasons (determined by the specific SW, equipment or professional skill of the personnel) you already apply the policy of strict administration of installation and set up of a software

For computers not included into the corporate network use personal anti-viruses – **Dr.Web for Windows** and the **Dr.Web** versions for other platforms.

Appendix F. Dr.Web® AV-Desk for Internet services providers

Dr.Web AV-Desk allows to simplify maintenance of anti-virus protection of a large number of users. **Dr.Web AV-Desk** is designed for companies specialized in providing various Internet services (Internet providers (ISP), application services providers (ASP), online banking vendors, etc.).

AV-Desk allows to install **Dr.Web** anti-virus packages for Windows on the workstations of the company's clients, manage their operation, updating, follow up and promptly solve problems, which occur on clients' computers, without the necessity to physically access the workstation or provide support and instructions to the user.

Creating such anti-virus network solves a number of problems, which both corporate clients and individual users often have to face:

- in companies, the software is usually installed onto computers by a company network administrator. The installation of anti-virus programs, their timely updating is an additional work for the administrator and requires physical access to computers;
- at home, users do not always follow up virus events on their computers or may even not install any anti-virus at all;
- semiskilled users can make changes in the settings of the anti-virus (including its disabling because of the seeming inconveniences), which incurs "holes" in protection and thus substantially degrade the level of security;
- anti-virus protection can be fully efficient if its operation is analyzed by qualified specialists, which includes analysis of protocols, files moved to the quarantine, etc. In companies, this work is hampered by the fact that such data is stored in dozens or hundreds computers. At home, operation of the anti-virus once installed is rarely analyzed.

Dr.Web AV-Desk was developed to solve these problems. It provides a reliable, flexible and easy customized anti-virus protection for workstations, saves administrators' time and efforts and relieves users of the necessity to worry about anti-virus protection, while maintaining a high level of security.

Dr.Web AV-Desk allows the following:

- simple installation of software components and prompt arrangement of anti-virus protection,
- creation of distribution files with unique identifiers and their transfer to the users for installation,
- centralized setup of anti-virus packages on protected computers,
- centralized virus databases and program files updates on protected computers,
- monitoring of virus events and the state of anti-virus packages and OS's on all protected computers.

Dr.Web AV-Desk has a "client-server" architecture. An anti-virus network arranged with **AV-Desk** includes the following components:

- **Anti-virus server** stores distribution kits of anti-virus packages for different OS's of protected computers, updates of virus databases, anti-virus packages and anti-virus agents, user keys and package settings of protected computers. The anti-virus server sends necessary information to the correspondent computers on Agents' requests and keeps a general log of events of the whole anti-virus network.
- **Web console** allows to create and edit user accounts, and generate individual **AV-Desk** agent distribution files for each user. The web console can be used on any computer connected to the Internet.
- In-built web server is automatically installed with the **Anti-virus server**. It is a certain extension of a standard web page of the server and allows to:

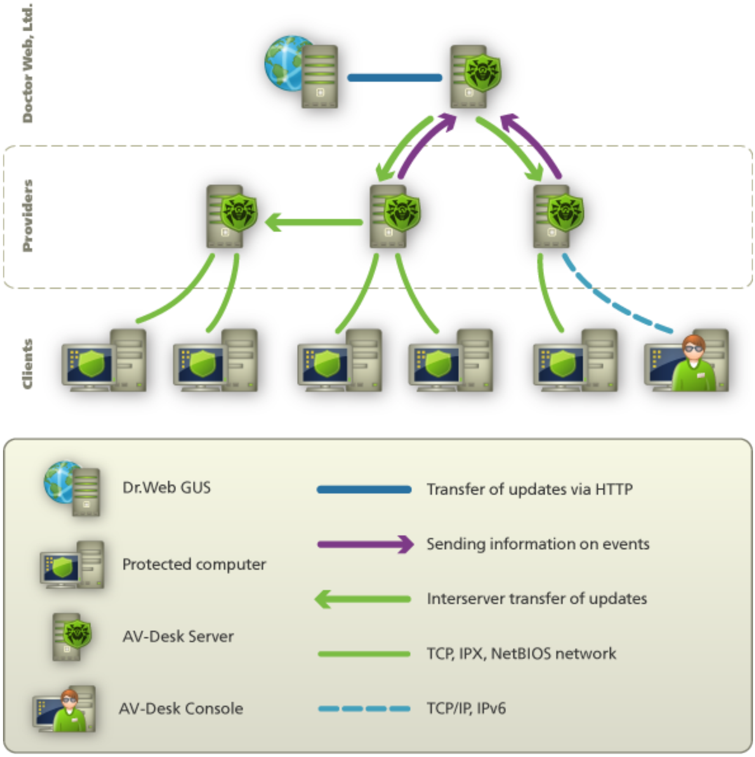
  - view general information about the **AV-Desk** server;

  - read the documentation;

  - view the repository.

- **Anti-virus AV-Desk agent** is installed on protected computers. It installs, updates and controls the anti-virus package as instructed by the anti-virus server. The **AV-Desk agent** reports virus events and other necessary information about the protected computer to the anti-virus server.

The following illustration describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.


Doctor Web, Ltd.
Providers
Clients
Dr.Web GUS
Protected computer
AV-Desk Server
AV-Desk Console
Transfer of updates via HTTP
Sending information on events
Interserver transfer of updates
TCP, IPX, NetBIOS network
TCP/IP, IPv6

Physical structure of the anti-virus network

The flow of commands, data and statistical information in the anti-virus network obligatory goes trough the anti-virus server. The anti-virus console also exchanges the data with the server only; the changes in configuration of a workstation and the transfer of commands to the anti-virus agent are made by the server on the basis of the console commands.

In large networks with hundreds or thousands computers it is advisable to create the **Dr.Web AV-Desk** anti-virus network with several servers. The hierarchy connection between the servers allows to simplify the updating of the virus databases and the SW of the workstations and the receipt of the information on the virus events from them. The administrator can analyze the logs of the network, both of separate servers and the summary log of the whole anti-virus network.

In large networks, **Dr.Web AV-Desk** increases reliability of anti-virus protection and cuts costs for its administration compared personal anti-virus programs.

Dr.Web AV-Desk has several advantages in comparison to other similar products:

- high reliability and security of applied solutions
- easy administration
- multiplatform structure of all components
- excellent scalability