Dr.WEB®

for Windows

User Manual

Version 5.0.1

Dr.Web® for Windows
User Manual
26.01.2009

Doctor Web, Ltd. 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, Ltd.

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

Doctor Web, Ltd. 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!

Contents

Introduction

Dr.Web® for Windows is a powerful anti-virus solution which regularly shows the best results during operation and in independent tests. The module architecture of the anti-virus 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 for Windows**, there are versions of the anti-virus for MS-DOS®, IBM® OS/2®, Novell® NetWare® and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

The program is distributed as two software packages:

- **Dr.Web for Windows** (Dr.Web for workstations)
- **Dr.Web for Windows Server** (Dr.Web for servers)

The User Manual describes both variants, if other is not specified, and a shortened name - **Dr.Web** - is used for them.

The **Dr.Web for Windows Server** components and configuration files are specially developed for efficient anti-virus protection of a file server considering its high loading, constant operation and undesirability of frequent user interference (by the server administrator).

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 Anti-virus for Windows 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 on the fly, and detects virus-like activity.

- **SpIDer Mail® for Windows** (**Mail Guard**) workstations 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. Providing **Dr.Web** application is licensed to work in the "Anti-virus + anti-spam" mode (with a suitable key file present), the **Mail Guard** uses Vade Retro spam filter to scan mail for spam messages. **SpIDer Mail** is not included into **Dr.Web for Windows Server**.

- **SpIDer Gate™** is an anti-virus HTTP-monitor. By default **SpIDer Gate** automatically checks incoming and outgoing HTTP-traffic and blocks all malware objects. This component is not included in **Dr.Web for Windows Server**.

- The **Parental Control** component is used to restrict access to both local and web resources. This component is not included in **Dr.Web for Windows Server**.

- **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**.

Dr.Web for workstations also includes the **Scheduler for Windows** 95/98/Me and the **Scanner for DOS** components.

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 F. 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 G.

What is This Manual About

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

You can find detailed description of all the GUI elements in the Help system of the anti-virus complex which can be accessed from any component.

This User Manual describes installation of **Dr.Web** 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 the anti-virus.

Document Conventions and Abbreviations

The following symbols and text conventions are used in this User Manual:

Symbol	Description
	Important note, instruction or warning about potential errors
Guard	The term in position of a definition
Cancel	Names of buttons, panes, menu items and other elements of the GUI
[F1]	Names of keyboard keys
C:\Windows\System	Names of files and folders

The following abbreviations are used in this User Manual:

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

System Requirements

Up to 55 MB on the hard drive is required to install **Dr.Web** depending on the set of components.

The **Scanner** (GUI-version and console version for Windows) and the **SpIDer Guard** components can run on computers operated by Windows 95/98/Me or Windows NT(SP6a)/2000(SP2)/XP/2003/Vista/2008.

SpIDer Guard can run under 32-bit systems only.

Operation under Windows 95 is possible only starting from Windows 95 OSR2 (v.4.00.950B). You may also 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.

SpIDer Mail can run on computers operated by Microsoft® Windows ® 95/98/Me or Microsoft® Windows® NT(SP6a)/2000(SP4)/XP/Vista.

SpIDer Gate and **Parental control** can run on computers operated by Microsoft® Windows® 2000/XP/Vista.

SpIDer Agent can run on computers operated by Microsoft® Windows® 2000/XP/2003/Vista/2008.

The **Scanner for DOS** operates under MS-DOS or in Windows command line mode.

Minimum system requirements are similar to those for the corresponding OS's. However, **SpIDer Guard** requires at least 32 MB of RAM for proper operation. Also, the PC must fully support i80386 processor command system.

You should install all critical updates recommended by the OS developer. If the OS is no longer supported by its manufacturer, then you should upgrade to a newer OS.

Before installing **Dr.Web**, you should uninstall all other anti-virus packages from the computer to avoid possible incompatibility with their resident components.

License Key File

User's rights to use **Dr.Web** software are regulated by a special file called the *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 Anti-virus for Windows).

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 and cannot be renewed.

The key file can be delivered as a **.key** file, an archive containing such file or a **.dwz** file used by the **Automatic Updating Module** to deliver packaged updates. A user can receive the key file in one of the following ways:

- 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.
- Via e-mail or by downloading it from the official registration page after providing the serial number supplied by the seller. Without a serial number the user can only receive a demo key file by filling out a form on the demo request page.
- The key file can be included in the distribution kit of the program.
- Via e-mail as an attachment with the .dwz extension. Double-click the attachment icon to install the key.
- Via a separate data carrier provided by the seller.
- Supplied as a zip archive containing a file with the .key extension. Extract the key file using the respective archiving tool (WinZip or Pkunzip) into the Dr.Web installation folder.

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.

If a key file is lost, you should register again. In this case, input the personal data specified during the first registration procedure. Only the e-mail address may differ. The key file will be sent to the specified e-mail address.

The number of requests for a key file receipt is limited. One user cannot register a serial number more than 25 times. If more requests are sent, the key file will not be delivered. To receive the key file, contact our Technical support service (describe your problem in detail, state your personal data input during the registration and the serial number) and the key file will be sent to your e-mail address.

If no valid key file is found (license or demo), the functionality of the program is blocked. Users of **Dr.Web** products for workstations (including **Dr.Web CC**) can use only the **Dr.Web Updater** which lets you register the software and receive a key file for it.

Beginning from version 4.33 the key files of **Dr.Web** for workstations and **Dr.Web** for servers differ. If you use the wrong key file, some components, such as **SpIDer Guard for Windows** will be disabled.

Installing Dr.Web Anti-virus for Windows

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 for Windows is not compatible with other anti-virus software, including previous versions of **Dr.Web Anti-virus**. Installing two anti-virus programs on one computer may lead to system crash and loss of important data.

The installation kit is supplied as a **Dr.Web for Windows** company disk or a single **.exe** file of around 55 MB.

To begin the installation of **Dr.Web for Windows** 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, a window with the **Autorun** menu of the disk will automatically open. Select **Browse CD** (or **Browse DVD**) and open the **Windows_Server** folder. If autorun is disabled, open this folder using the standard OS tools and run the executable file of the distribution kit

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**.

The installation procedure and the set of program components vary depending on the OS.

Installation of Dr.Web for Windows on computers running under Microsoft® Windows® 2000(SP4)/XP/2003/Vista/2008 is described in the following sections:

- Installing Dr.Web for Windows
- Updating Dr.Web for Windows
- Reinstalling and Removing Dr.Web for Windows

Installation of Dr.Web for Windows on computers running under Microsoft® Windows® 95/98/NT4(SP6a)/Me is described in the following sections:

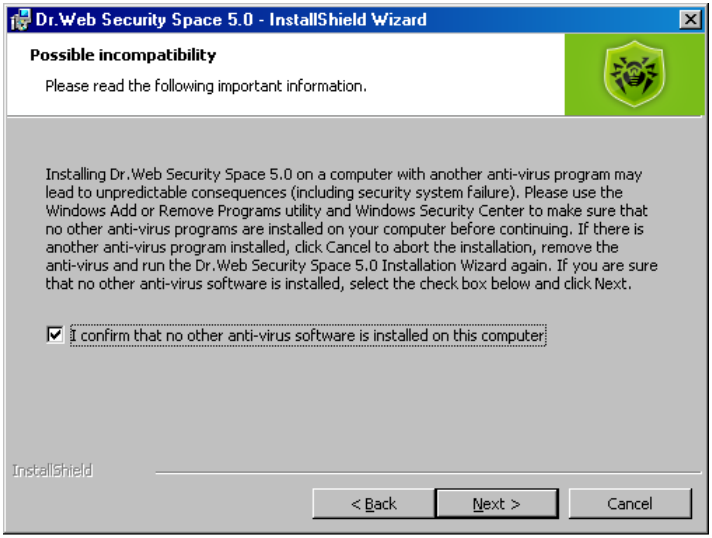
- Installing Dr.Web for Windows
- Reinstalling and Removing Dr.Web for Windows

Installation under Microsoft® Windows® 2000(SP4)/XP/2003/Vista/2008

Installing Dr.Web for Windows

Only a user with administrator privileges can install **Dr.Web for Windows**

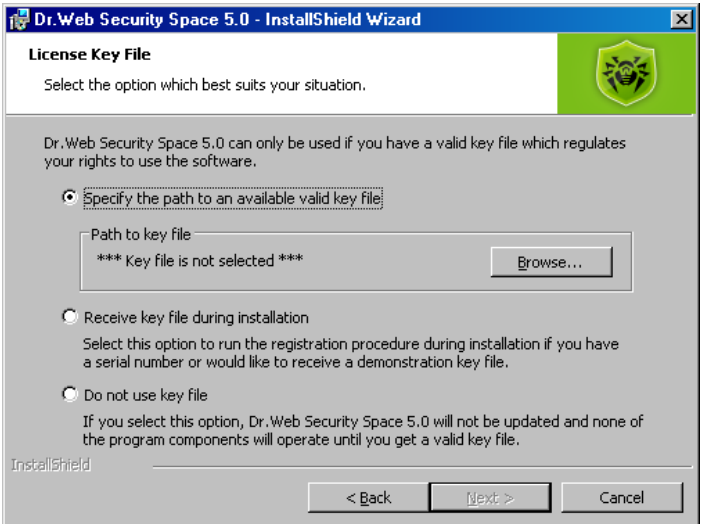
1. Select the language for the installation wizard (the choice will not affect the set of languages which will be available for the installed program complex).
2. In the next window you will be offered to read the License agreement. You should accept it and click **Next** in order to continue installation.
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**.



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**.

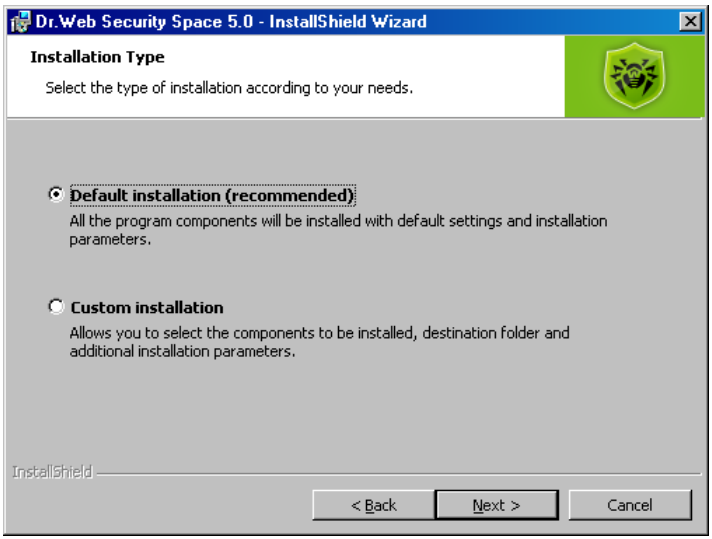


If no key file is available, but you have a serial number, select **Receive key file during installation**. Otherwise, select **Do not use key file** and click **Next**.

You should use key files of **Dr.Web** for workstations because they differ from key files of **Dr.Web** for workstations. The key file should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

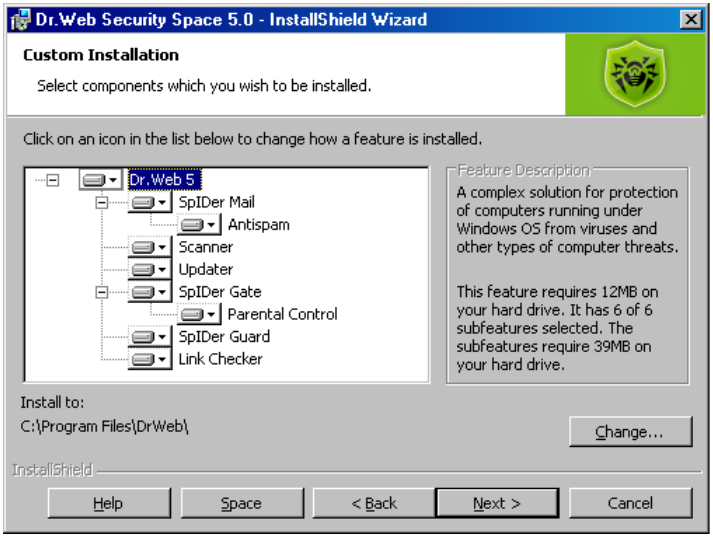
5. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components, both English and Russian GUI languages, and all secondary programs automatically up to step 10. **Custom Installation** is meant for experienced users. During custom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

additional installation parameters.



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

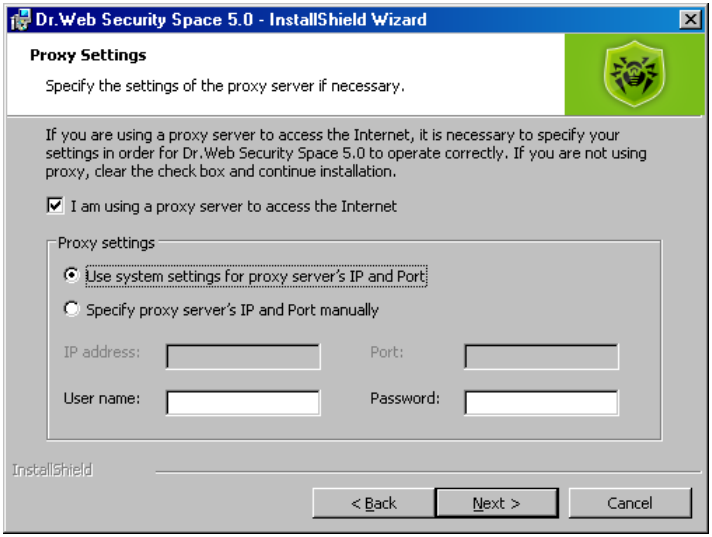
6. If you chose default installation type, go to step 10. In case of custom installation, a window for selecting the program components which you wish to install will open. In the hierarchical list select the check boxes against the components you wish to install and clear the check boxes you do not wish to install.



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

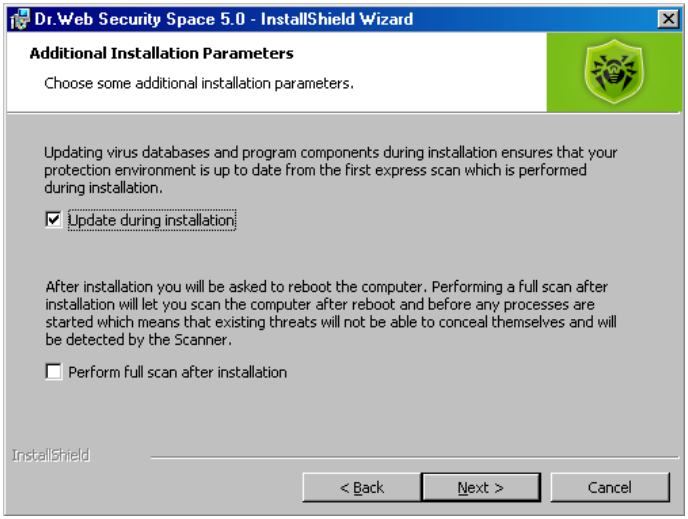
7. The window for selecting which shortcuts to **Dr.Web for Windows** should be created will open. Select the necessary options and click **Next**.

8. The window for adjusting proxy server settings will open. If you are using proxy to access the Internet, specify necessary information.



If you do not use a proxy server, clear the **I use a proxy server to access the Internet** check box and click **Next**.

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



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 a quick scan of the main memory, autorun files and offer to perform a detailed scan of the computer. 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 for Windows** it is necessary to disable changing of the **Dr.Web** interface in the Windows Blinds settings. To do this, add **drweb32.exe** to the list of excluded applications.

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

Updating Dr.Web for Windows

Updating installed components of **Dr.Web for Windows** version 5.0 is performed by the Updater (see Launching and Using the Automatic Updating Utility).

The installation wizard lets you change the set of program components and update **Dr.Web for Windows** up to the current version.

Copy the valid key file to any place other than the **Dr.Web** installation folder before updating to version 5.0.

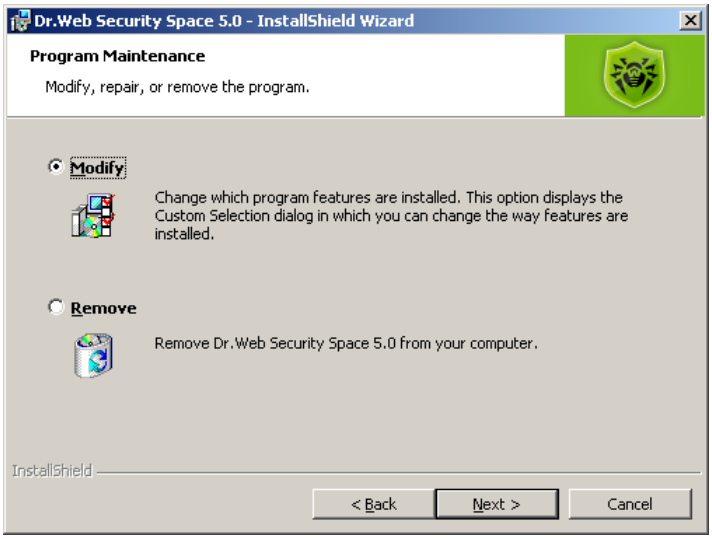
To update Dr.Web for Windows version 4.44 to version 5.0:

1. Run the installation wizard.
2. Follow the instructions described in the previous section.
3. At step 4 specify the path to the valid key file.
4. Continue following the instructions and end the installation.

Reinstalling and Removing Dr.Web for Windows

To modify, repair or remove an installed version of **Dr.Web for Windows**, start the installation wizard.

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



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 for Windows** 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.

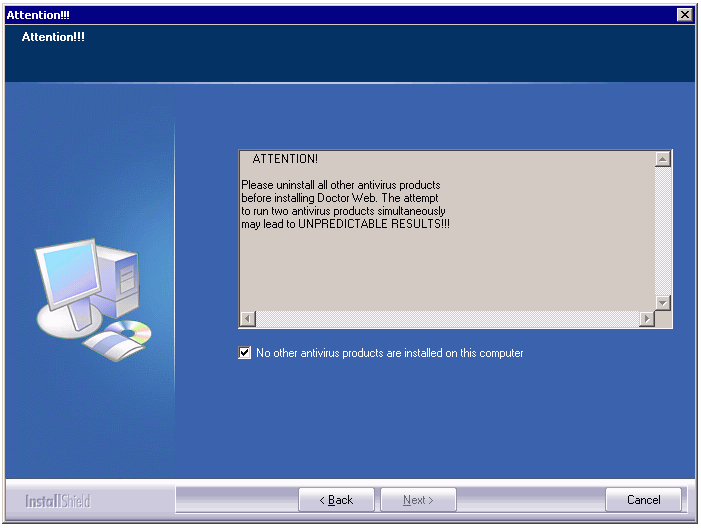
You can start the mofication, repair or removal procedure via the standard Windows utility - **Add/Remove Programs**.

Installation under Microsoft® Windows® 95/98/NT(SP6a)/Me

Installing Dr.Web for Windows

Only a user with administrator privileges can install **Dr.Web for Windows** on a computer running under Microsoft® Windows® NT

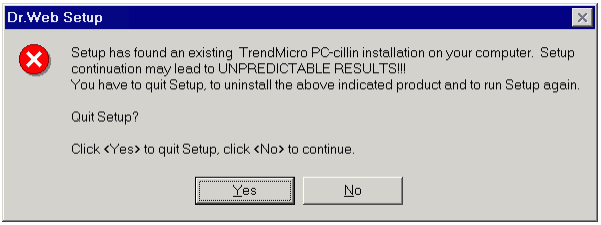
1. Select the language for the installation wizard (the choice will not affect the set of languages which will be available for the installed program complex).
   1. In the dialog window the installation wizard will inform on possible incompatibility of **Dr.Web** with other anti-viruses installed on 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 **No other antivirus products are installed on this computer** check box and click **Next**.
   2. The installation program checks your computer and if it detects known anti-viruses it generates an additional warning message. To cancel the installation click **Yes** (you can continue installation after the detected anti-virus is removed or deactivated). To continue the installation, click **No**.



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

You can continue installation with other anti-viruses installed on your computer if no active resident modules (guards/monitors) and mail traffic processing programs are present in the system.

3. 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.

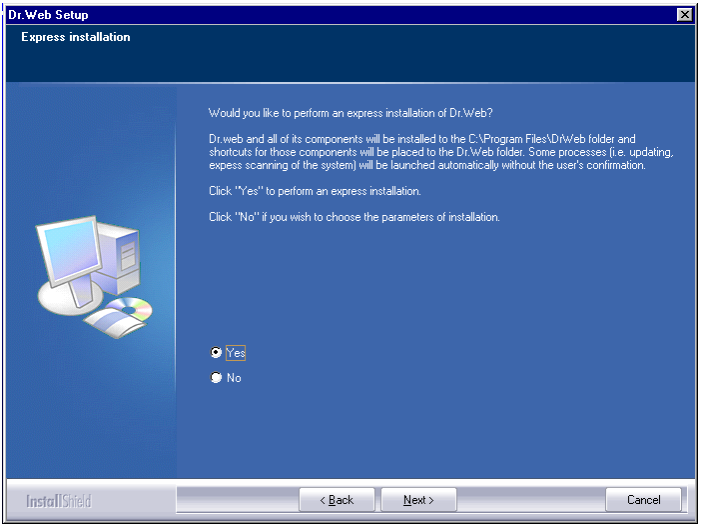


4. The installation program will bring up a warning window requesting a key file (license or demo) required for the program's operation. If a key file is present on your hard drive or on

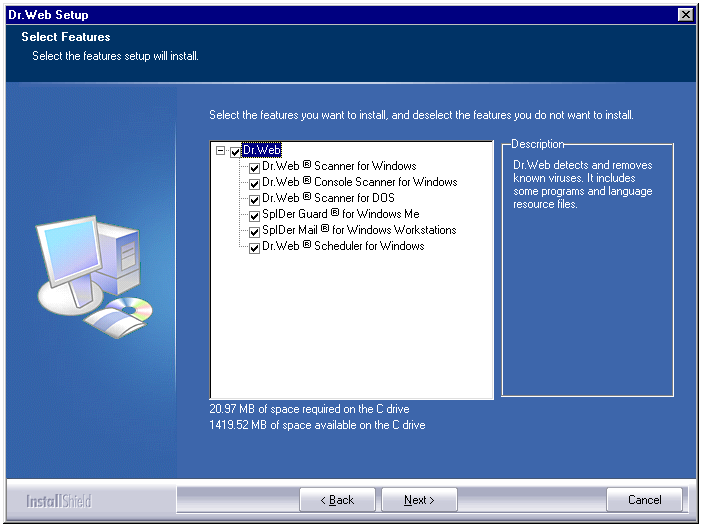
removable media, click **Browse**, select the key file and click **Next**.
If no key file is available then just click **Next**. A key file can be received later during the installation.

You should use key files of **Dr.Web** for workstations because they differ from key files of **Dr.Web** for servers. The key file should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

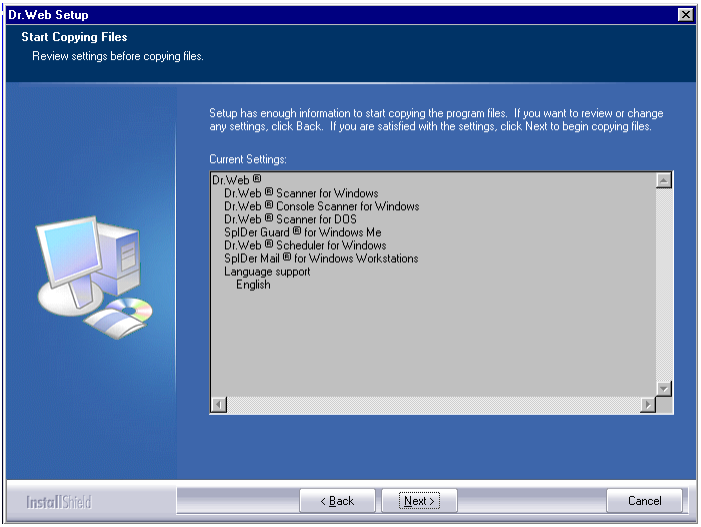
5. The program will offer to choose the type of installation in the **Express Installation** window.
   Express installation implies installation of all anti-virus components and assistance programs with all steps up to 11 carried out automatically. Some processes (i.e. updating, express scanning of the system) will be launched automatically without user's confirmation. Select **Yes** if you wish to perform the express installation, click Next and move on to step 11.
   Select **No** if you wish to choose the parameters of installation manually and then click **Next**.
6. If you have decided not to perform express installation you will be asked to choose the installation folder. Specify it and click **Next**.



7. The **Select Features** window will open allowing you to select the components which you wish to be installed.
   In the hierarchical list select the check boxes against the components you wish to install and clear the check boxes you do not wish to install. Click **Next** when you finish selecting the necessary components.
8. In the next dialog window you will be offered to select a directory in the **All Programs** submenu of the Windows **Start** menu where the icons of the installed components, help files, log files and the **unInstall Dr.Web** icon, which launches the removal procedure of **Dr.Web for Windows**, will be placed.By default, the installation program offers to create the **Dr.Web** folder. It is recommended to accept it and click **Next**.



9. The **Start Copying Files** window will open with an overview of the components which will be installed. See through the list of components which will be installed and click **Next** if it suits you.
10. The **Proxy Server Settings** window will open allowing you to specify your proxy settings.If you use a proxy server to access the Internet fill in the **Address**, **Name** and **Password** fields and click **Yes**. Otherwise, click **No**.



11. Next, if you have specified the location of your key file, a window requesting whether the virus databases should be updated will open. To learn more about the virus databases and their updating read Automatic Updating of the Virus Databases and other files of the program. To start the **Updater** and update the virus databases, click **Yes**.
    If the license key file is not available, the **Updater** will inform you about it and try to receive it via the Internet with the help of the user registration procedure.
12. Once a key file is received, click **Finish**. Virus databases will be immediately updated.
13. After installation is complete (registration and database update if necessary) the **Scanner** will perform a quick scan of the main memory, autorun files and offer to perform a detailed scan of the computer.

Scanner is not compatible with Windows Blinds (an application for adjusting Windows GUI). For correct operation of **Dr.Web for Windows** it is necessary to disable changing of the **Dr.Web** interface in the Windows Blinds settings. To do this, add **drweb32.exe** to the list of excluded applications.

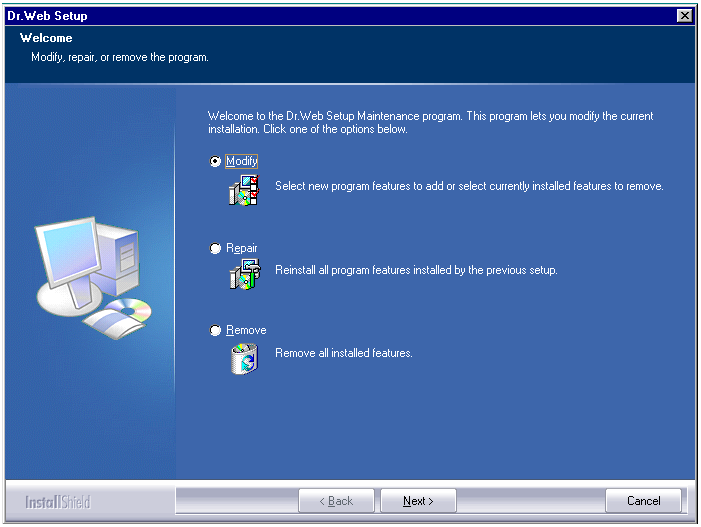
14. If **SpIDer Guard** or **SpIDer Mail** were installed, the program will ask for a computer reboot which is required to complete the installation.

By default, the installation program does not only install the **Scheduler for Windows**, but also creates a schedule for the automatic hourly updating of the program and a disabled task for anti-virus scanning. This component is not installed for Windows Vista.

Reinstalling and Removing Dr.Web

To modify, repair or remove an installed version of Dr.Web for Windows, start the installation wizard.

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



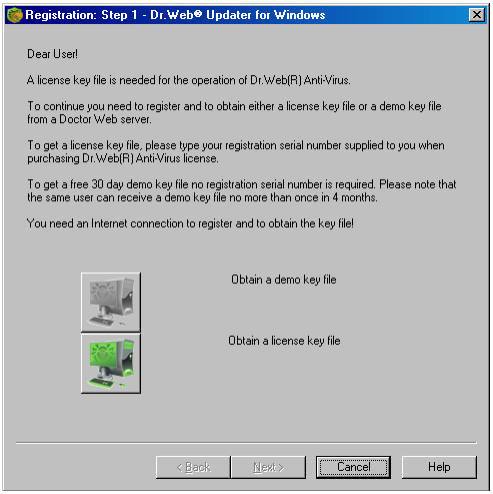
In this window:

- To change the set of installed components select **Modify** and click **Next**. The **Select Features** 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 for Windows** 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

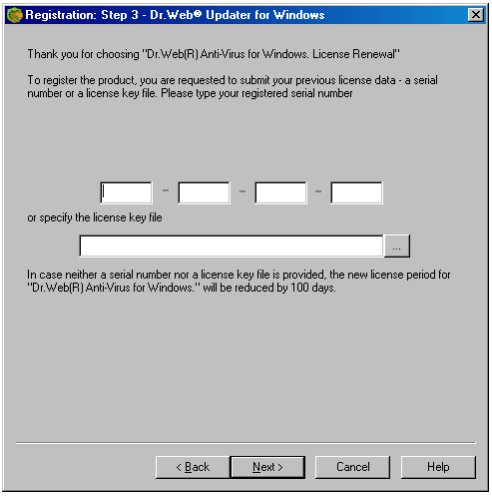
At the first step of the procedure you will be offered to choose what type of key file you would like to obtain - either license or demo.



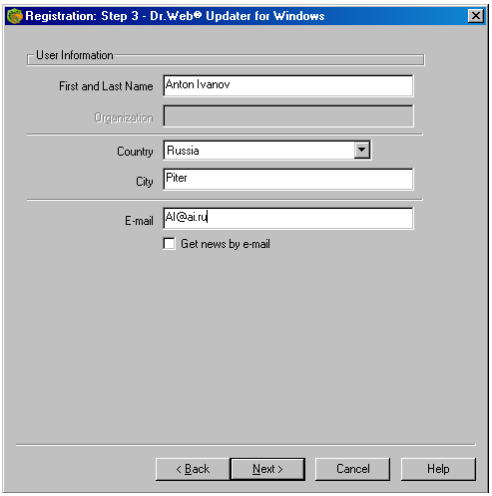
If you have a serial number, click the **Obtain a license key** file button.

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 or submit your previous license key file and click **Next**.



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

Structure and Functions of Installed Components

By default the installation program installs the following components of **Dr.Web Anti-virus** on the computer:

- When installing **Dr.Web** for workstations - the **Scanner for Windows** environment (GUI and console versions), **Scanner for DOS**, **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate, Parental control** and **SpIDer Agent.** On computers running under Microsoft® Windows® 95/98/Me also the **Scheduler** is installed.
- When installing **Dr.Web** for servers - the **Scanner for Windows** environment (GUI and console version), **SpIDer Guard** and **SpIDer Agent**.

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

SpIDer Gate, **Parental Control** and **SpIDer Agent** are not installed on computers running under Microsoft® Windows® 95/98/NT4(SP6a)/Me.

The components of **Dr.Web** 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.

Scanner for DOS can perform thorough disk scanning even if Windows is not installed or not working properly. When running the PC with a write-protected disk, it provides the highest level of virus detection in files.

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 only the opened files (by default - all opened files on removable media and files opened for writing on hard 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 a certain (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/SMTPI/MAP4/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 of 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.

To secure comprehensive anti-virus protection, we advise you to use the **Dr.Web** 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

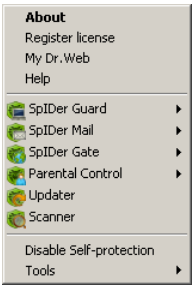
General Information

This component is not installed on computers running under Microsoft® Windows® 95/98/Me/.

After installing **Dr.Web Anti-virus** 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 Anti-virus**.



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

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

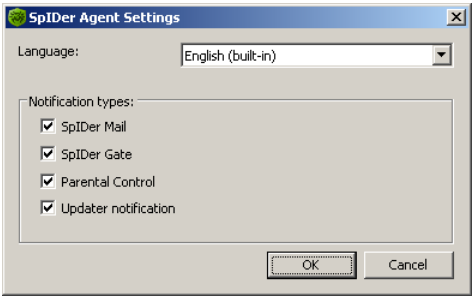
The **My Dr.Web** item opens your personal web page on the **Doctor Web, Ltd.** web site. This page gives information about your license (period of usage, serial number), allows to renew your license, contact Technical Support, etc.

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

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

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

The **Tools** item opens a submenu which allows access to the **License Manager** (see License Manager) and the settings of **SpIDer Agent** itself.

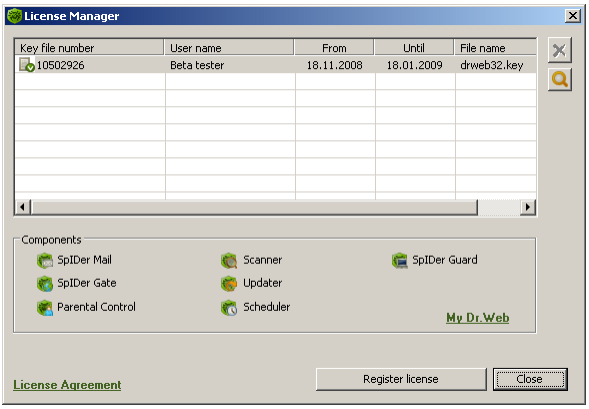


In this window you can specify the language of the **Dr.Web Anti-virus** GUI by selecting the necessary language in the **Select language** list.

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).

License Manager

License Manager shows information from the Dr.Web key files in an understandable form.



To add a key file to a list, click the button and select the file in a standard window.

To delete a key file from a list, select it and click the button.

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

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.

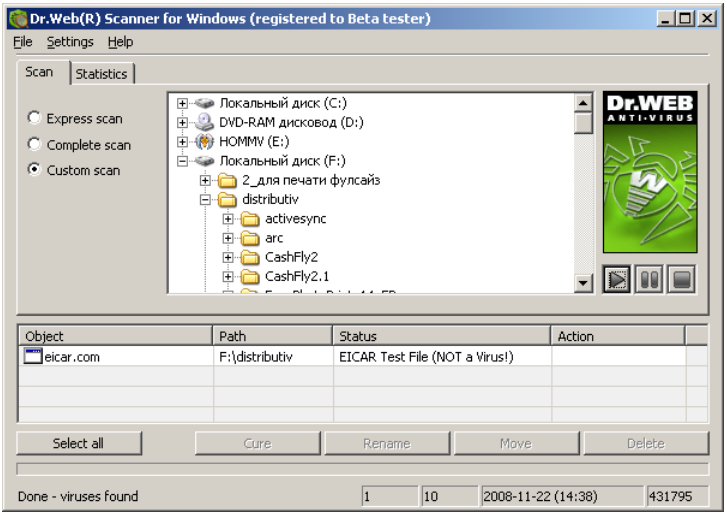
The **License Agreement** item open the file with the text of the License agreement.

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

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** for workstations 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). **Dr.Web** for servers applies automatic actions to avert a virus threat (for more information see Adjusting the Scanner Settings).



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 (read Scheduler for Windows).

If using Windows Vista, 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.

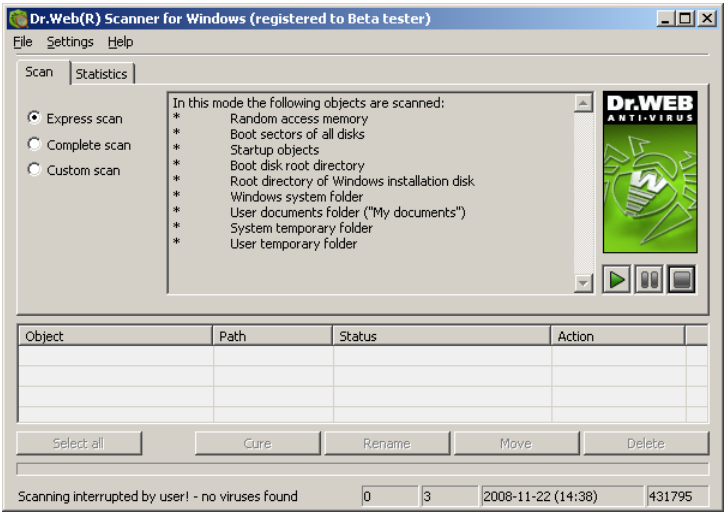
To launch the Scanner do one of the following:

- Click the **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).
- 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.



By default, immediately after the **Scanner** is launched it scans the main memory and Windows autorun files. Other objects of the file system are scanned on user demand.

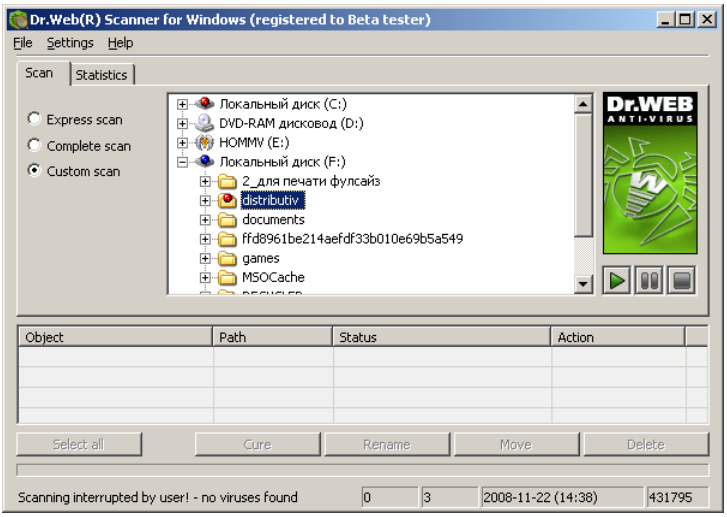
There are 3 scanning modes: **Express scan**, **Complete scan** and **Custom scan**. Depending on the selected mode, either a list of objects which will be scanned or a file system tree is displayed at the center of the window.

If **Express scan** mode is selected, 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, 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 whole disk **C:** and the folder on the disk **F:** are selected for scanning.



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, Clik 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** for workstations 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.

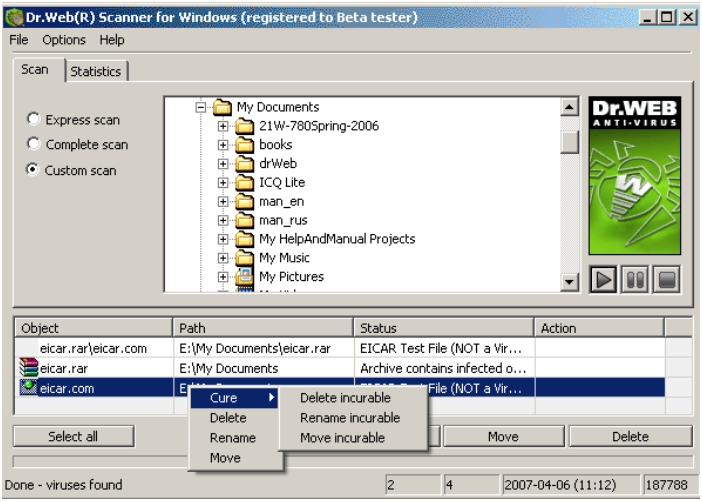
To apply actions to detected objects:

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 and move the cursor to next position.
- [CTRL+A] - to select all objects.
- the asterisk button [*] on numeric keyboard - to invert selection.

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.

Suspicious objects are moved to the **Quarantine** 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, if using Windows 95/98/Me, the log file resides in the program's installation folder and for Windows NT/2000/XP/2003/Vista/2008 - 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.

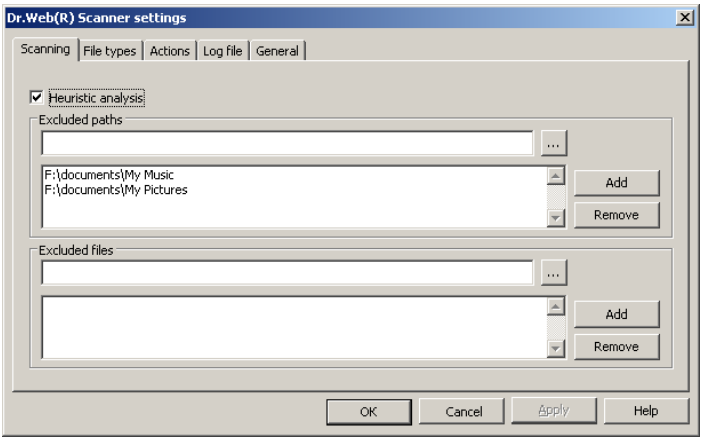
Adjusting the Scanner Settings

If using Windows Vista, 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. Select the **Options** item in the menu located at the top of the main window and then choose **Change settings** in the opened submenu. This will open the **Scanner settings** window which contains several tabs.



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.

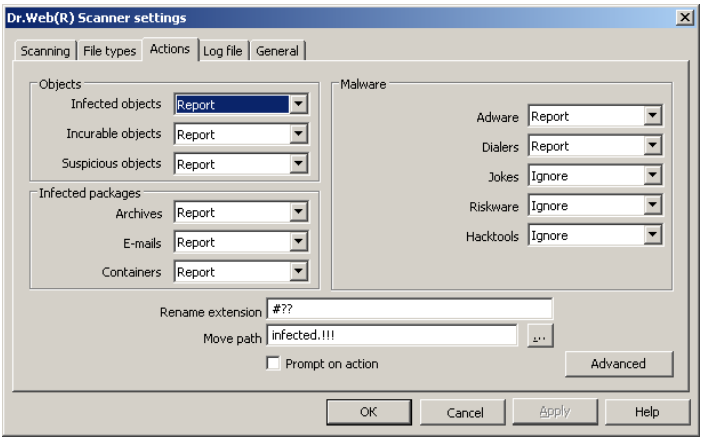
The most frequent changes in default settings are described below.

The default settings of **Dr.Web** for workstations 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.

Dr.Web for servers automatically performs actions to avert a virus threat by default.

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

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



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

The **Cure** action is the best for automatic mode. This action is set in **Dr.Web** for servers by default.

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. This action is set by default in **Dr.Web** for servers by default.

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).

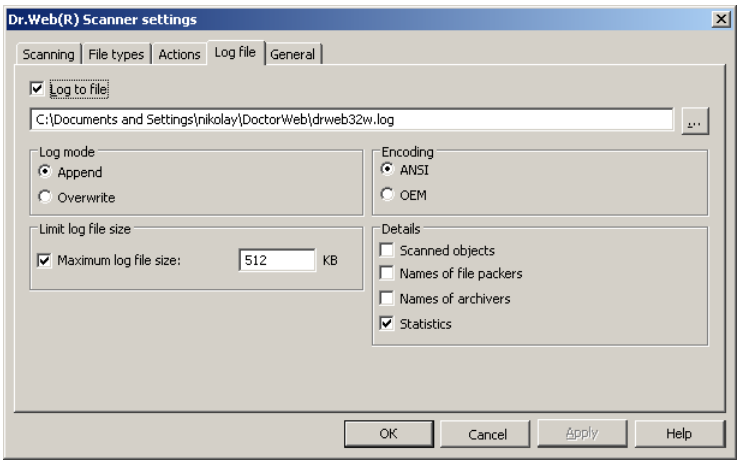
In **Dr.Web** for workstations it is recommended to keep the default **Report** action. In **Dr.Web** for servers it is recommended to keep the default **Move to** action.

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. In **Dr.Web** for workstations the **Report** action is specified by default. In **Dr.Web** for servers, the **Move to** 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.

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



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

Dr.Web Scanner for DOS is activated in a similar way but with the **drweb386** command. All the filenames and paths should be specified in a format supported by the OS (for example, only short filenames are allowed). This component is not included in **Dr.Web** for servers.

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 B.

/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 C for more details).

SpIDer Guard for Windows

General Information

Depending on the OS, one of the two versions of **SpIDer Guard** is installed:

- **SpIDer Guard for Windows 95/98/Me** (hereinafter referred to as **SpIDer Guard Me**).
- **SpIDer Guard for Windows NT/2000/XP/Vista/2008** (hereinafter referred to as **SpIDer Guard XP**).

By default, **SpIDer Guard** is loaded automatically at every Windows startup. Active **SpIDer Guard Me** cannot be unloaded during the current Windows session (for information on how to unload **SpIDer Guard XP** read Loading_and_Unloading_SpIDer_Guard). 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 (reed SpIDer_Agent). If **SpIDer Guard Me** is used, you should disable the automatic loading of **SpIDer Guard** (read Loading_and Unloading SpIDer Guard) and then restart Windows.

In Microsoft® Windows® NT/2000/XP/2003/Vista®/2008 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 and informs the user about it.

By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web** for workstations acts like the **Scanner** only informing

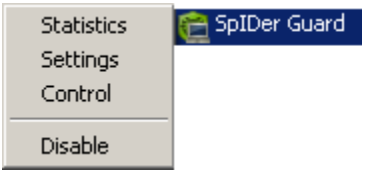
the user and offering to decide what action to apply. In **Dr.Web** for servers, if a suspicious or infected object is detected, an automatic action is taken to avert virus threat by default.

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.

In Microsoft® Windows® Vista® 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. A similar context menu for **SpIDer Guard Me** appears above the icon of the guard itself, which is located in the Windows notification area.



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 's parameters (for more details read Main Parameters of SpIDer Guard

).

In Microsoft® Windows® Vista® access to the **SpIDer Guard** settings and Control panel is possible only for the user with administrator rights.

The **Control** item (for **SpIDer Guard XP** only) allows to open the Control panel window of **SpIDer Guard** (for users with administrator rights only).

The **Disable** item (for **SpIDer Guard XP** only) allows to temporary disable most functions of the program (for users with administrator rights only).

When installing **SpIDer Guard XP**, one more element called **Dr.Web Anti-virus** is added to Windows Control Panel. It comprises the settings specific for the program under Microsoft® Windows®. These settings can only be modified by a user with administrator privileges (e.g. he can enable displaying the **SpIDer Guard** icon in the taskbar notification area).

When you hover the mouse cursor over the icon, a pop-up window with **SpIDer Guard** statistics, the date of the last update and the number of virus records in the database appears. Also, pop-up notifications on various events may sometimes appear above the icon. You can set up these notifications in the **Reminders** tab.

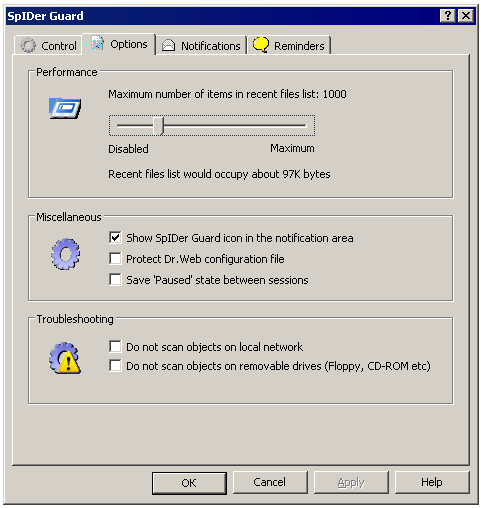
The administrator of the PC operated by Windows NT/2000/XP/2003/Vista can allow the **SpIDer Guard** icon to be shown.

To show the SpIDer Guard icon in the taskbar notification area:

1. Open the **SpIDer Guard** Control panel window:
   - Double-click the **Dr.Web Anti-virus** item in the Windows Control Panel (the **Control Panel** item in the Windows **Start** menu).

- Select **Control** in the context menu of the **SpIDer Guard XP** icon.

2. Select the **Options** tab.

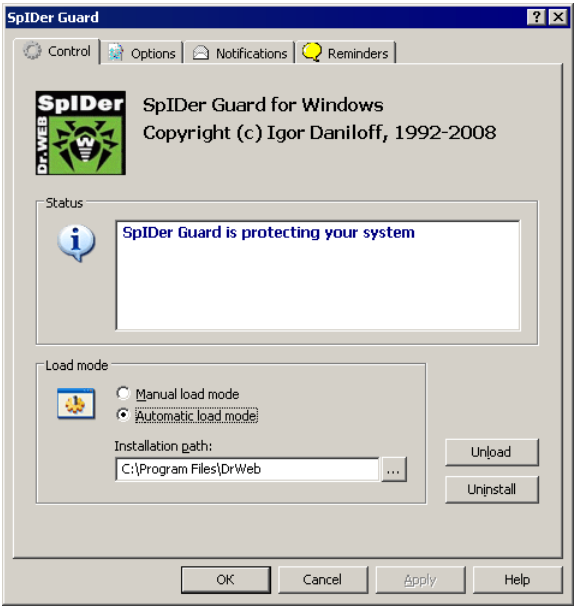


3. To enable the **SpIDer Guard** icon select the **Show the SpIDer Guard's icon in the notification area** check box; to disable the **SpIDer Guard** icon, clear this check box.
4. Click **OK** to apply changes and close the **SpIDer Guard** Control panel window.

Loading and Unloading SpIDer Guard

To disable automatic loading of SpIDer Guard XP:

1. Open the **SpIDer Guard** control panel:
   - Double-click the **Dr.Web Anti-virus** item in the Windows Control Panel (the **Control Panel** item in the Windows **Start** menu).
   - Select **Control** in the menu of the **SpIDer Guard** item.
2. Select the **Control** tab in the **SpIDer Guard** control panel.



3. Select the **Manual load mode** radio button in the **Load mode** group box.
4. Click **OK** to apply changes and close the **SpIDer Guard** Control panel window.

At the next Windows startup **SpIDer Guard** will not be loaded automatically.

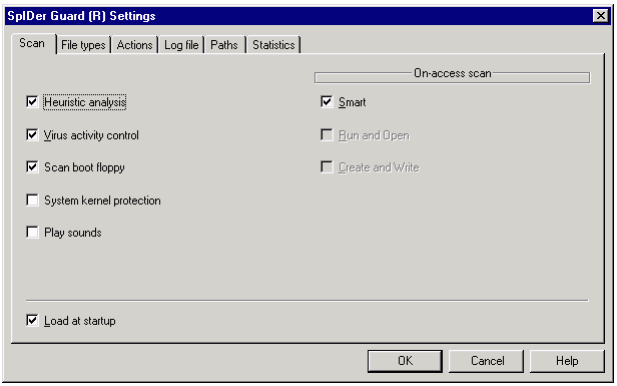
To load SpIDer Guard XP manually:

- Click the **Load** button in the window described above. Being run manually, **SpIDer Guard XP** can be terminated by pressing the **Unload** button.

SpIDer Guard Me is always set for automatic load mode, but this mode can also be disabled.

To disable automatic loading of SpIDer Guard Me:

1. Select the **Settings** item in the context menu of the **SpIDer Guard Me** icon in the taskbar notification area. The **SpIDer Guard Settings** window will open.
2. Select the **Scan** tab.



3. Clear the **Load at startup** check box.
4. Click **OK** to apply changes and close the **SpIDer Guard** Control panel window.

At the next Windows startup **SpIDer Guard** will not be loaded automatically.

To load SpIDer Guard Me manually:

- Select the **All Programs** item in the Windows **Start** menu, then select **Dr.Web** -> **SpIDer Guard**. When **SpIDer Guard** is loaded, it automatically applies the automatic load mode.

Main Parameters of the SpIDer Guard

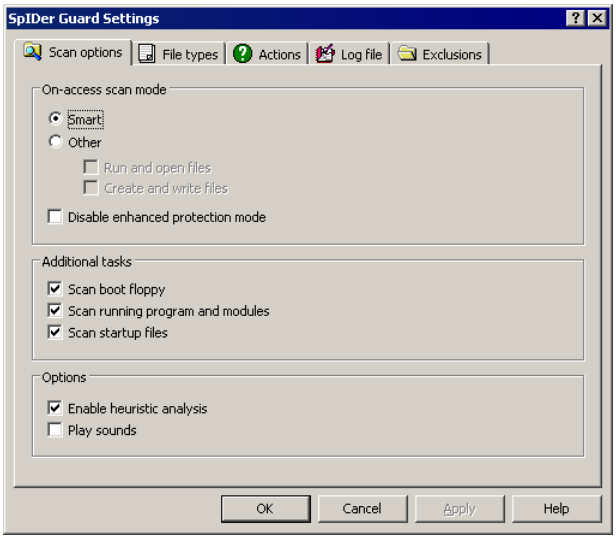
The main adjustable parameters of both versions of **SpIDer Guard** are in the **Settings** panel of **SpIDer Guard Me** and **SpIDer Guard XP**. To receive help on parameters specified in a tab, select that tab and click **Help**. For more detailed information on each element of the GUI right click that element.

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.

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

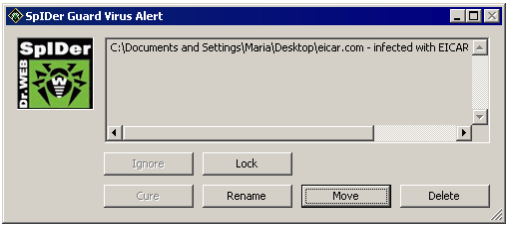
By default, in the enhanced protection mode **SpIDer Guard XP** in the first place checks all files which have been selected in the program's settings; all other opened files are put on the queue (i.e. files opened for reading in the **Smart** and **Create and Write** modes). As soon as computer resources are free, the guard will check these files. By default, the enhanced protection mode is disabled. To enable this mode clear the **Disable enhanced protection mode** check box in the **Scan options** pane of the **SpIDer Guard XP Settings** window.



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

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

In **Dr.Web** for workstations for supposedly curable viruses, incurable viruses and suspicious objects, the program's action to inform a user what action should be taken is specified by default. **SpIDer Guard** blocks the detected object and generates a message box asking what actions should be taken further.



By default, **SpIDer Guard** in **Dr.Web** for servers automatically undertakes actions to avert the detected threats (for more details read below).

If an object containing joke programs, riskware or hacktools is detected, the **Ignore** action is applied to it by default.

When adware or dialers are detected, the guard's default reaction is different: for servers – **Move to**, for workstations – **Report**.

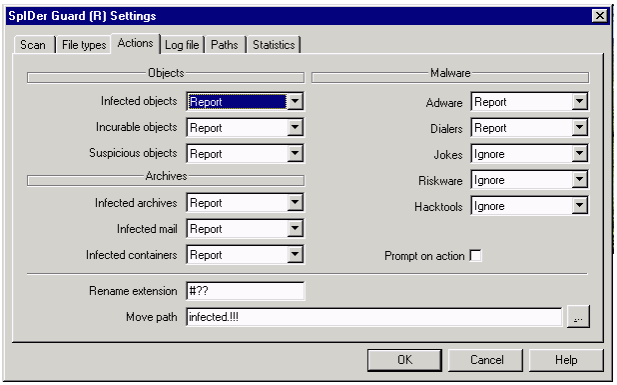
Available actions depend on the type of the detected object. The **Cure** , **Rename**, **Move** and **Delete** actions are similar to those of the **Scanner**.

When the **Lock** button is pressed, the infected file is marked by Windows as inaccessible.

You can modify the **SpIDer Guard** settings to enable it to automatically react to infected objects without requesting a user.

To change the default actions in SpIDer Guard Me:

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

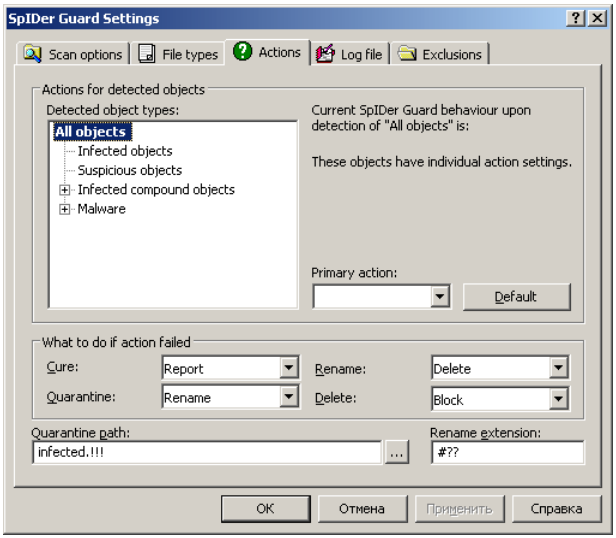


2. In the **Infected objects** drop-down list choose the program's action upon detection of an infected object (**Cure** action is recommended).
3. In the **Incurable objects** drop-down list choose the program's action upon detection of an incurable object (**Move to** action is recommended). Other actions with moved files are described in Actions Upon Detection of a Virus.
4. In the **Suspicious objects** drop-down list choose the program' s action upon detection of a suspicious object. (**Ignore** or **Move** actions are recommended).
5. The same procedure is used when setting the program's actions upon detection of objects containing adware, dialers, jokes, riskware and hacktools.

6. Click **OK** to apply changes and close the **SpIDer Guard** Settings window.

To change the default actions in SpIDer Guard XP:

1. Select the **Actions** tab in the **SpIDer Guard Settings** window.



2. In the hierarchy list in the left part of the window select **Infected objects**. In the upper right part of the window the program's action upon detection of an object infected with a known virus will be displayed. The action specified by the current settings and the alternative action to be taken if the primary action fails should be specified. The adjustments of the primary action settings are described below; the settings for alternative actions are described in step 5.
3. To enable the default actions taken upon detection of a given type of objects click the **Default** button. In the version of the program for workstations all infected, suspicious objects and malware (except jokes, riskware and hacktools which are ignored) are reported by default. In the version of the program for servers infected objects are cured; jokes, riskware and hacktools are ignored; adware, dialers, suspicious objects and objects in archives are moved to quarantine.

4. In the **Primary action** drop-down list select the initial program' s action upon detection of an infected object. Click the **Change** button to instruct the program to use the action specified by you.
5. In the **What to do if action failed** section the settings of alternative actions to be undertaken if the first action fails reside. These settings are specified for each of the following possible variants: curing, moving to the quarantine, deletion and renaming. In every drop-down list you can choose the action to be taken, if the primary action fails.
6. The program's actions upon detection of suspicious objects, infected file archives, mail archives and containers, as well as objects containing adware, dialers, joke programs, riskware and hacktools are set in a similar way.
7. If necessary, specify the name and the path to the folder for moved files in the **Quarantine path** field.
8. If necessary, specify the mask for renaming the file extension if **Rename** is applied.
9. Click **OK** to apply changes and close the **SpIDer Guard** Settings window.

In the **Log file** tab you can specify parameters of the log file (similar to the **Scanner**).

SpIDer Mail for Windows Workstations

This component is not supplied in **Dr.Web for Windows Server**.

General Information

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.

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 Vade Retro spam filter 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).

Checking e-mails for spam is possible only if the **Dr.Web** application is licensed (a key file is present) to work in the "Anti-virus + anti-spam" mode.

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.

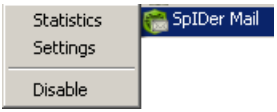
SpIDer Guard and the **Scanner** can also detect viruses in mailboxes of several formats, but **SpIDer Mail** has several advantages:

- 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.

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). A similar context menu for **SpIDer Mail** installed on a computer running under Microsoft® Windows® 95/98/Me appears above the icon of the guard itself, which is located in the Windows notification area.



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

When using Windows Vista a 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 it was described above (read Adjusting SpIDer Mail. Setting the Launch Mode).

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).

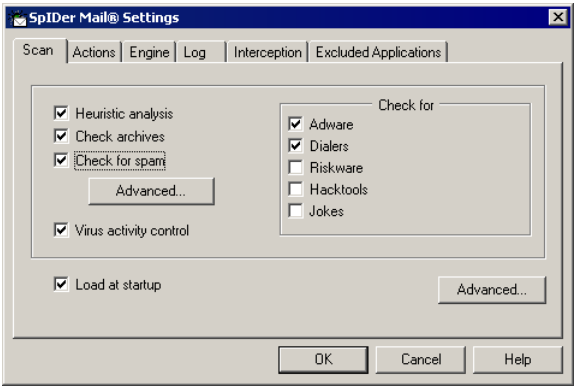
When adjusting is finished, click **OK**.

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

By default **SpIDer Mail** does not scan incoming messages for spam. To enable the spam filter, select the **Check for the spam** check box on the **Scan** pane.

Configuration of the spam filter is possible only if the **Dr.Web** application is licensed (a key file is present) to work in the "Anti-virus + anti-spam" mode.

Settings of the spam filter can be set in the **SpIDer Mail** **Spam Settings** window.



To open this window click the **Advanced** button in the **Scan** pane. It is located below the **Check for spam** field.

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 Vade Retro spam filter's 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. This rule is created only for Windows 2000/XP/2003.

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 prefix to Subject field** 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 Chinese/Japanese/Korean 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.

By default, **SpIDer Mail** detects both the messages with infected

objects and the messages containing other types of unsolicited programs:

- adware
- dialers

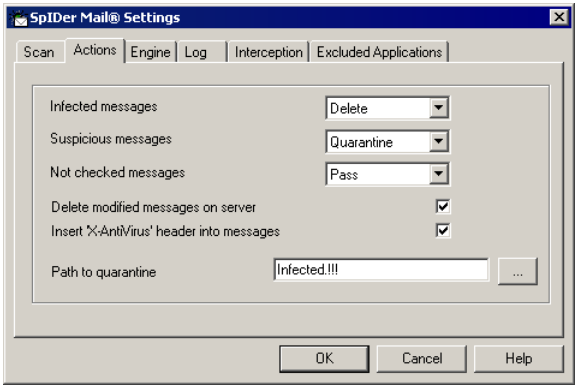
SpIDer Mail can also detect the following types of unsolicited programs:

- riskware
- hacktools
- joke programs

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.

Actions of the **SpIDer Mail** component upon detection of unsolicited programs are similar to those for infected messages. Read more below.

The settings of the program's actions upon detection of virus objects in the incoming mail are adjusted via the **Actions** pane.



For infected messages (those containing viruses known to the program) the **Delete** action is specified by default, i.e. rejection to receive a message (as a rule, such messages are deleted at POP3/IMAP4 server). Experienced users can select the **Quarantine** action in the **Infected messages** drop-down list. In this case, the messages will be moved to a special folder (the Quarantine) for subsequent analysis.

If a user is sure that suspicious messages received by him do not contain viruses, he can select the **Pass** action in the **Suspicious messages** drop-down list.

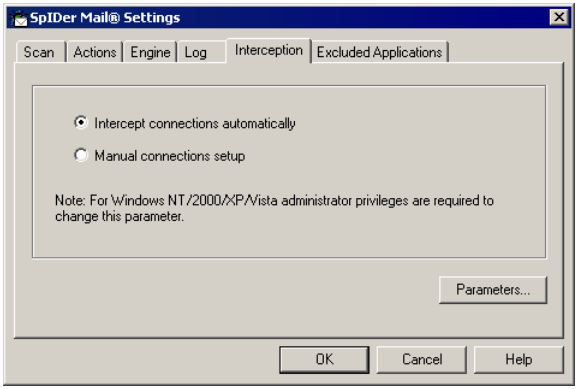
Protection against suspicious messages can be disabled if a PC is additionally protected by a constantly loaded **SpIDer Guard** component.

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.

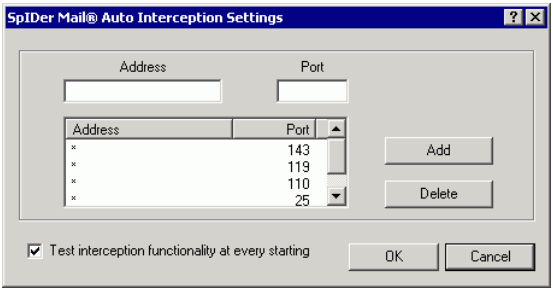
Experienced users can disable the mode when the deleted or moved messages are immediately deleted from the POP3/IMAP4 server, and delete such messages manually or using more advanced settings of the mail program. For this, clear the **Delete modified messages on server** check box.

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.



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.



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.

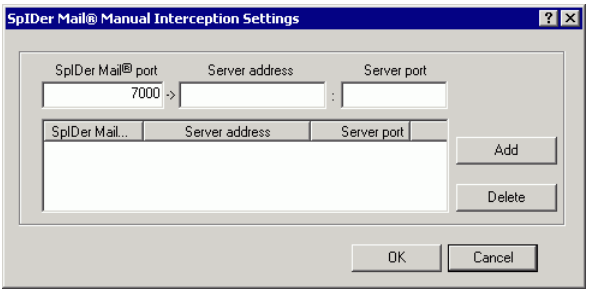
To add a server or a group of servers to the list, specify its address (IP address or domain name) in the **Address** field and the called port number into the **Port** field and click **Add**.

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.



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 Dr.Web

General Information

This component is not installed on computers running under Microsoft® Windows® 95/98/Me.

This component is not included into **Dr.Web for Windows Server**.

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.

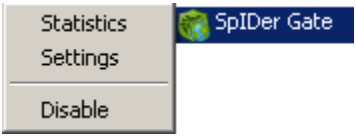
You can adjust the SpIDer Gate Settings to completely disable monitoring of incoming or outgoing traffic, compose a list of applications whose HTTP-traffic should always be checked or exclude certain applications from being monitored.

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 change the automatic launch mode by clearing the corresponding check box.

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 Mail** performance within the current session.

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

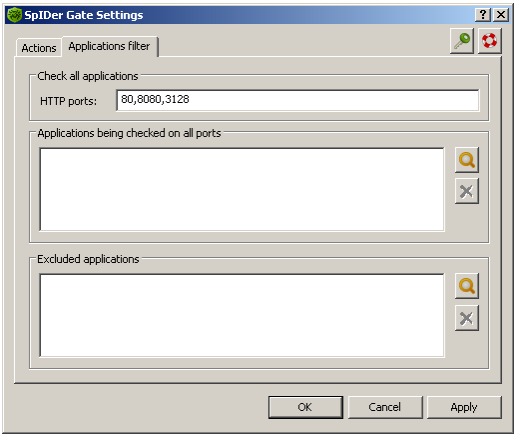
SpIDer Gate Settings

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

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 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.

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.

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 button and select the application in a standard window.

To delete an application from a list, select it and click the button.

Parental Control

Parental Control Component

This component is not installed on computers running under Microsoft® Windows® 95/98/Me.

This component is not included into **Dr.Web for Windows Server**.

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.

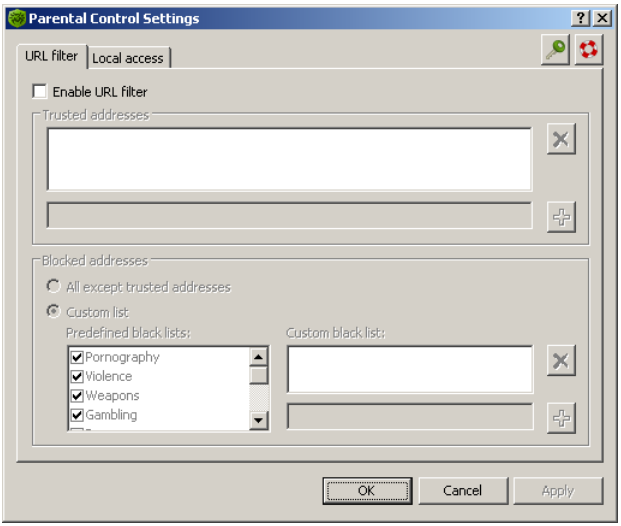
Parental Control Settings

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 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.



To completely restrict access to the Internet, select the **Restrict** local access check box in the **Local Access** tab.

To restrict access to web resources:

1. Select the **Enable URL filter** check box to enable the web resources access control.
2. Add the domain names which you trust to the **Trusted URLs list.**
3. Select a group(s) of addresses access to which should be restricted in the **Blocked URLs** group box.
4. To restrict access to all web resources except those in the **Trusted URLs** list, select **All except trusted URLs**. To enable filtering of web addresses according to categories and/or a user-compiled list, select **Custom URLs**.
5. Select the types of blocked web sites in the **Categories** list.

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 button to the right (the button with the "plus" symbol). 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 the  button.

Scheduler for Windows

This component is installed if using Microsoft® Windows® 95/98/Me. To manage automatic launching of tasks it is recommended to use Task Scheduler (the standard Windows scheduler) in which tasks for scanning the PC and updating the anti-virus complex are automatically created during the installation of **Dr.Web Anti-virus for Windows**.

By default, the managing utility to automatically launch tasks – the **Scheduler for Windows** – is included into **Dr.Web** for workstations. This is an additional program. Its functions can be performed by other schedulers suitable for you. However, this program is designed to administer the scanning process and updating of the anti-virus program and provides additional functionalities to a user.

When the program is installed, it generates a green round icon resembling a dial-plate in the notification area.

Main tools for setting and managing the **Scheduler for Windows** reside in the context menu of this icon.

If the **Open** menu item is selected, the **Scheduler** main window will open (read below).

The **Language** item allows to select one of the languages of the program's interface.

The **Options** item duplicates the same menu item of the main window and allows to execute the following actions:

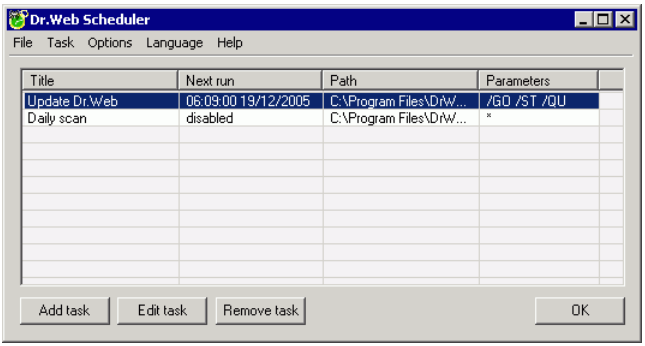
- cancel (restore) the program's autorun
- hide (show) the **Scheduler** icon in the task bar
- disable (enable) log writing

By default, **Scheduler for Windows** constantly resides in the memory and is active. If you wish to unload it from the memory, select the **Unload** menu item.

To run the Scheduler manually:

1. In the Windows **Start** menu select the **All Programs** item.
2. In the opened submenu select **Dr.Web**.
3. In the opened submenu, select **Scheduler**.

The main window contains functions of the program's administration. To open the main window, double click the program's icon in the notification area or select the **Open** item in the context menu.



To unload the program from the memory select the **Unload** item in the **File** menu.

To cancel (restore) automatic program load clear (select) the **Load at startup** item in the **Options** menu.

To hide (show) the **Scheduler** icon in the task bar clear (select) the **Show icon in tray** check box in the **Options** menu.

To disable (enable) log writing clear (select) the **Write log file** check

box in the **Options** menu.

The main tools for managing the tasks list are located in the **Task** menu item. They are fully duplicated by the context menu of the tasks list and the buttons at the bottom of the window.

By default, the program is installed with the list of two tasks:

- To hourly receive updates from the Internet, marked as "critical" (read below).
- To scan hard drives with the default parameters every day at 3 o ’clock.

The second task has the "disabled" status which actually prohibits it.

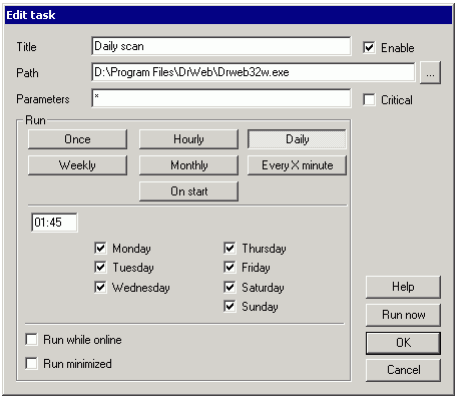
To enable a task, open it for editing as described below.

To view a task and edit it, if necessary:

1. Do one of the following:

- double click a task
- select a task in the list and choose the **Edit task** item in the context menu or in the **Task** menu
- select a task in the list and click the **Edit task** button at the bottom of the main window

A window for editing the task will open.



2. If the task is disabled you can enable it. To do this, select the **Enable** check box. The parameters of the task will be enabled for editing.

   If you do not want a task to be performed, nor you want to remove it (e.g. if you plan to enable it later), you can disable the earlier active task by clearing the **Enable** check box.

3. If necessary, edit the launch schedule (when pressing different buttons in the **Run** section, the window outlook will somewhat change).
4. If you wish the task to be performed only when a connection to the Internet is established, select the **Run while online** check box.
5. If you wish the skipped task to be performed as soon as possible, select the **Critical** check box.
6. If you wish the application to be performed in minimized mode when run by the **Scheduler** task, select the **Run minimized** check box.
7. Click **OK** to apply any changes.

To run the task immediately click the **Run now** button.

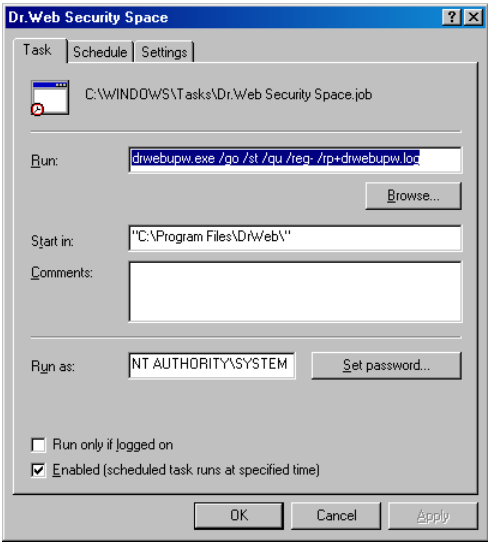
Experienced users can also edit the parameters and the path of the launched task.

To add a new task, select the **Add task** item in the context menu or in

the **Task** menu or click the **Add task** button in the bottom of the main window. A window for inputting parameters of the new task, similar to the one described above, will open. Further actions are the same as for editing the task.

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

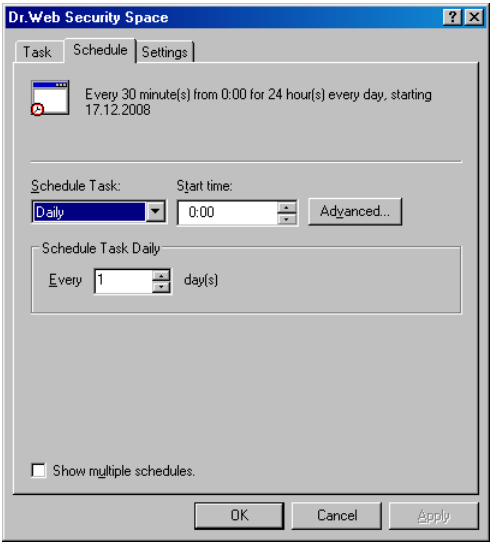
If **Dr.Web** is installed on computers operated by Microsoft® Windows ® NT(SP6a)/2000(SP4)/XP/2003/Vista/2008, a task to update the virus databases and other files of the package is automatically created in the system scheduler (the Scheduled Tasks directory). To view the parameters of this task, select the **Accessories** item in the **All Programs** submenu of the Windows **Start** menu, then select **System Tools**, then select **Scheduled Tasks**. A directory with the same name will open. Double click the **Automatic update of DrWeb** icon in this directory. A window for setting up a task will open.



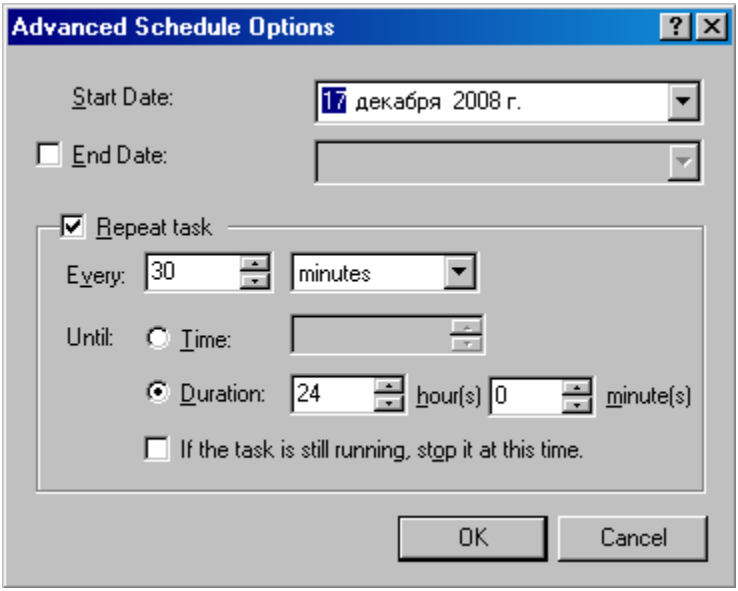
In the **Task** tab the full name of the executable file and the command line parameters of the task are specified. The **Enabled** check box instructs to perform the task (if the check box is cleared the task is saved to the folder, but is not performed).

In the **Schedule** tab the schedule according to which a task will be

run automatically is made.



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



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 of the Virus Databases and Other Files of the Program

General Information

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.

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** and **drw50001.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 **02**, i.e. the first add-on of the database in the anti-virus version 5.0 is called **drw50002.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**. When such a file is received, the previous file is deleted. When next weekly add-on is installed, all the virus records from the last file of the hot add-on are included into it, the hot add-on file is downloaded with zero number of the virus records.
- 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** and

drw50001.vdb

- weekly add-ons - **drw50002.vdb**, **drw50003.vdb** etc.
- hot add-on - **drwtoday.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.

In Windows NT/2000/XP/Vista a 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 Scheduler for Windows);
- 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 (read SpIDer Guard for Windows);

- by clicking the **Update** item of the **File** menu in the main window of the scanner (read Using Dr.Web Scanner for Windows);

When launching the **Updater**, 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 automatic 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 the anti-virus from.

After the key file is successfully checked, the updating is performed. The program automatically downloads all updated files, according to your version of the anti-virus, and, if your subscription terms allow, the new program version (if it is released).

A PC reboot may be required when updating of executable files and libraries is done. A correspondent message box is generated to a user about it. If the **Updater** is updated itself, one more reboot may be necessary during the update.

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 B).

Appendices

Appendix A. List of Differences Between Dr.Web for Windows and Dr.Web for Windows Server

Components and installation

The following components are not included into **Dr.Web for Windows Server**:

- **Scanner for DOS**
- **SpIDer Mail**
- **Scheduler for Windows**

The installation program of **Dr.Web for Windows Server** in the custom installation mode implying selection of components does not offer to install these components.

Default settings

The differences in the default settings of the two versions of the anti-virus are determined by the modes the programs are to be used for: the version for servers should operate in automatic mode with the recurring control of log files; the version for workstations is operated by a user. In the table below all default settings different for the two versions are summarized.

Parameter	Dr.Web for Windows	Dr.Web for Windows Server
Scanner: actions with infected files InfectedFiles	Inform Report	Cure Cure
Scanner: actions with suspicious files SuspiciousFiles	Inform Report	Move Move

Parameter	Dr.Web for Windows	Dr.Web for Windows Server
Scanner: actions with incurable files IncurableFiles	Inform Report	Move Move
Guard: actions with infected files InfectedFiles	Inform Report	Cure Cure
Guard: actions with suspicious files SuspiciousFiles	Inform Report	Move Move
Guard: actions with incurable files IncurableFiles	Inform Report	Move Move
Scanner and guard: actions with infected archives ActionInfectedArchive	Inform Report	Move Move
Scanner and guard: actions with infected mail files ActionInfectedMail	Inform Report	Move Move
Scanner and guard: actions with infected containers ActionInfectedContainer	Inform Report	Move Move
Scanner and guard: log the list of scanned (not infected) objects to a file LogScanned	No Yes	Yes No
Log file size, KB MaxLogSize	512	8192

The first column lists the name of the parameter of a component and the name of the parameter of the configuration file, the second column contains the default parameter value, if using the anti-virus for workstations (the verbal description and the parameter value in the configuration file), the third column contains the same information for the anti-virus for servers.

Appendix B. 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.)
/FN – to load Russian letters to the video display decoder (for **Dr.Web for DOS** only).

/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 C. 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 C. 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.

/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 C. Adjustable Parameters of Dr.Web Components

Introduction

Adjustable parameters of the program components 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 Guard**, **SpIDer Mail**). The most important of such settings are described above (read Adjusting_ the_ Scanner Settings, Main_ Parameters_ of_ the_ SpIDer_ Guard, 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 B 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 Guard** and **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).

The following components names are used in the Table:

- "SpIDer" – both versions of **SpIDer Guard** ("SpIDer-XP" and "SpIDer-Me")
- "Scanner" – 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 **SpIDer Guard** - in italic; for all components – in bold italic.

Default values for **SpIDer Guard** and **Scanner**, included into **Dr.Web for Windows Server**, in cases when they differ from the default values of the anti-virus for workstations, are underlined.

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 B.

Parameter	Components	Configur. file parameter	Values	Keys
"On-access" scan	SpIDer	GuardMode	Smart RunAndOpen CreateAndWrite the last two modes	
Scan mode	Scanner, SpIDer	ScanFiles	All ByType ByMasks	/AL /EX
Express scan of the system	Scanner			/FAST
Full scan of the system	Scanner			/FULL
Priority of the scanning process, from 1 to 50	Scanner			/SCP
Heuristic analysis	Scanner, SpIDer	HeuristicAnalysis	Yes / No	/HA
Virus activity control	SpIDer-Me	VirusActivityControl	Yes / No	
Scan boot floppy	SpIDer	ScanBootOnShutDown	Yes / No	
System kernel protection	SpIDer-Me	DisableIDTHook	Yes / No	
Disable network scan	SpIDer-Me	DisableNetworkScan	Yes / No	
Do not scan objects on local network	SpIDer-XP		(On / Off)	
Do not scan objects on removable drives	SpIDer-XP		(On / Off)	

Parameter	Components	Configur. file parameter	Values	Keys
Scan memory	Scanner, SpIDer-Me	TestMemory	Yes / No	/TM
Scan autorun files	Scanner, SpIDer	TestStartup	Yes / No	/TS
Scan boot sectors	Scanner, SpIDer-Me	TestBootSectors	Yes / No	/TB
Scan subfolders	Scanner	ScanSubDirectories	Yes / No	/SD
Prompt on multiple floppies	Scanner	PromptFloppy	Yes / No	/PF
Archives	Scanner, SpIDer	CheckArchives	Yes / No	/AR
Packed executable files	SpIDer	CheckPackedFiles	Yes / No	
Mail files	Scanner, SpIDer	CheckEMailFiles	Yes / No	/ML
Max size of unpacked archive to check, KB	SpIDer-XP, Console Scanner	MaxFileSizeToExtract	(empty)	
Max compression ratio for archive	SpIDer-XP, Console Scanne	MaxCompressionRatio	(empty)	
Threshold for MaxCompressionRatio, KB	SpIDer-XP, Console scanner	CompressionCheckThreshold	(empty)	
List of extensions	Scanner, SpIDer	FilesTypes	(see below the Table)	
List of masks	Scanner, SpIDer	UserMasks	(see below the Table)	

Parameter	Components	Configur. file parameter	Values	Keys
Locations of excluded folders	Scanner, SpIDer	ExcludePaths	(empty)	
Excluded files	Scanner, SpIDer-Me	ExcludeFiles	(empty)	
Allow wildcards	SpIDer-XP	AllowWildcards	Yes / No	
Allow relative file names	SpIDer-XP	AllowRelativeFileNames	Yes / No	
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	
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, SpIDer-Me	PromptOnAction	Yes / No	/PR

Parameter	Components	Configur. file parameter	Values	Keys
Rename extension	Scanner, SpIDer	RenameFilesTo	#??	
Move path	Scanner, SpIDer	MoveFilesTo	infected.!!!	
Location of virus databases	Scanner, SpIDer	VirusBase	*.vdb	
Flag-file for virus database reloading	SpIDer	UpdateFlags	drwtoday.vdb	
Generate a popup message	SpIDer-XP	Acknowledge	Yes / No	
Path to the folder with temporary files of the component	Scanner, SpIDer	TempPath	%TMP%, %TEMP%, install directory	
Enable switching off the Guard	SpIDer	EnableSwitch	Yes / No	
Guard load mode	SpIDer-XP		Manual mode Automatic mode	
Save "Paused" state between sessions	SpIDer-XP		(On / Off)	
Protect Dr.Web configuration file	SpIDer-XP		(On / Off)	
Disable enhanced protection mode	SpIDer-XP	DisableEnhancedProtection	Yes / No	
Scanned files list size	SpIDer-XP		100	
Actions with all types of malicious programs	Scanner		Report	/MW

Parameter	Components	Configur. file parameter	Values	Keys
Infected objects	Scanner, SpIDer	InfectedFiles	Report Cure Delete Rename Move Lock (guard) Shutdown (guard)	/CU
Incurable objects	Scanner, SpIDer	IncurableFiles	Report Delete Rename Move Lock (guard) Shutdown (guard)	/IC
Suspicious objects	Scanner, SpIDer	SuspiciousFiles	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/SP
Infected archives	Scanner, SpIDer	ActionInfectedArchive	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/AR

Parameter	Components	Configur. file parameter	Values	Keys
Infected mail files	Scanner, SpIDer	ActionInfectedMail	Report Delete Rename Move Lock (guard) Ignore (guard) Shutdown (guard)	/ML
Adware programs	Scanner, SpIDer	ActionAdware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/ADW
Dialer programs	Scanner, SpIDer	ActionDialers	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/DLS
Joke programs	Scanner, SpIDer	ActionJokes	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/JOK

Parameter	Components	Configur. file parameter	Values	Keys
Riskware	Scanner, SpIDer	ActionRiskware	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/RSK
Hacktools	Scanner, SpIDer	ActionHacktools	Report Delete Rename Move Ignore Lock (guard) Shutdown (guard)	/HCK
What to do if renaming failed	SpIDer-XP	ActionIfRenameFailed	Report Delete Rename Move Lock Shutdown	
What to do if moving failed	SpIDer-XP	ActionIfMoveFailed	Report Delete Rename Move Lock Shutdown	
What to do if deletion failed	SpIDer-XP	ActionIfDeleteFailed	Report Delete Rename Move Lock Shutdown	

Parameter	Components	Configur. file parameter	Values	Keys
What to do if reporting failed	SpIDer-XP	ActionIfReportFailed	Report Delete Rename Move Lock Shutdown	
Permit archives deletion without a prompt	Scanner, SpIDer	EnableDeleteArchiveAction	Yes / No	
Infected object found (send notifications)	SpIDer-XP		(On / Off)	
Incurable object found (send notifications)	SpIDer-XP		(On / Off)	
Suspicious object found (send notifications)	SpIDer-XP		(On / Off)	
Send E-mail notification on virus events	SpIDer-XP		(On / Off)	
Send message notification on virus events	SpIDer-XP		(On / Off)	
Log to file	Scanner, SpIDer, Updating module	LogToFile	Yes / No	/RP /NR
Write log file	Scheduler		(On / Off)	
Log file name	Scanner SpIDer-Me SpIDer-XP	LogFileName	drweb32w.log spider.log spidernt.log	/RP

Parameter	Components	Configur. file parameter	Values	Keys
Log file name	Updating module		drwebupw.log	/RP
Log file name	Scheduler		drwebscd.log	
Log mode	Scanner, SpIDer, Updating module	OverwriteLog	Yes / No	/RP
Log encoding	Scanner, SpIDer, Updating module	LogFormat	ANSI OEM	
Scanned objects in log file	Scanner, SpIDer	LogScanned	Yes / No	/OK
Names of file packers in log file	Scanner, SpIDer	LogPacked	Yes / No	
Names of archivers in report	Scanner, SpIDer	LogArchived	Yes / No	
Statistics in log file	Scanner, SpIDer	LogStatistics	Yes / No	
Maximum log file size	Scanner, SpIDer, Updating module	LimitLog	Yes / No	
Log size limit, KB	Scanner, SpIDer, Updating module	MaxLogSize	512 8192	
Close the window after sessions	Scanner, Updating module		Yes / No	/QU

Parameter	Components	Configur. file parameter	Values	Keys
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
Use alternative configuration file. Do not use any configuration file	Scanner, Updating module		(On / Off)	/INI /NI
Use own swap file	Scanner, SpIDer	UseDiskForSwap	Yes / No	
Display progress bar	Scanner	ShowProgressBar	Yes / No	
Sounds	Scanner, SpIDer, Updating module	PlaySounds	Yes / No	/SO
Alert (sound)	Scanner	AlertWav	alert.wav	
Cured (sound)	Scanner	CuredWav	cured.wav	
Deleted (sound)	Scanner	DeletedWav	deleted.wav	

Parameter	Components	Configur. file parameter	Values	Keys
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
Disable changes in settings without reboot	SpIDer-Me	DisableHotReconfigure	Yes / No	
Show SpIDer Guard icon in system tray	SpIDer-XP		(On / Off)	
Show icon in tray	Scheduler		(On / Off)	
Use registry settings	Scanner-GUI		(On / Off)	
Scan priority	Scanner	ScanPriority	25 50	
Language	Scanner, SpIDer, 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

Parameter	Components	Configur. file parameter	Values	Keys
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 for Windows workstations

Parameters of **SpIDer Mail for Windows workstations** 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

Parameter	Configuration file parameter	Value	Key
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	
Delete modified messages on the server	DeleteMessagesOnServer	Yes / No	
Insert 'X-AntiVirus' header into messages	InsertXAntiVirus	Yes / No	•

Parameter	Configuration file parameter	Value	Key
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	
Intercept connections automatically or Manual connections setup radio buttons	HookModeAuto	Yes / No	

Parameter	Configuration file parameter	Value	Key
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	
Enable the Exit menu item	AllowExit	Yes / No	
Enable the Settings menu item	AllowSettings	Yes / No	

Parameter	Configuration file parameter	Value	Key
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 D. 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 he 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 E. 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 support 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 F. Corporate network protection by Dr.Web® Enterprise Suite

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

The versions of the program designed for workstations and for Windows servers, 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 (workstations and servers of the local network)
- 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.

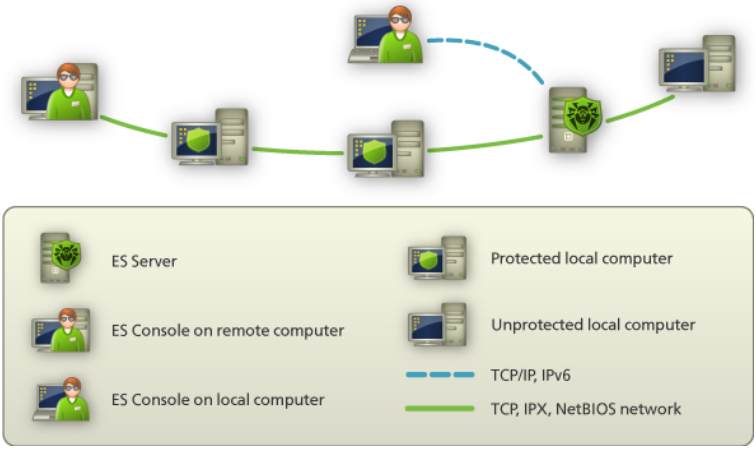
Dr.Web ES has a "client-server" architecture. Its components are

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.

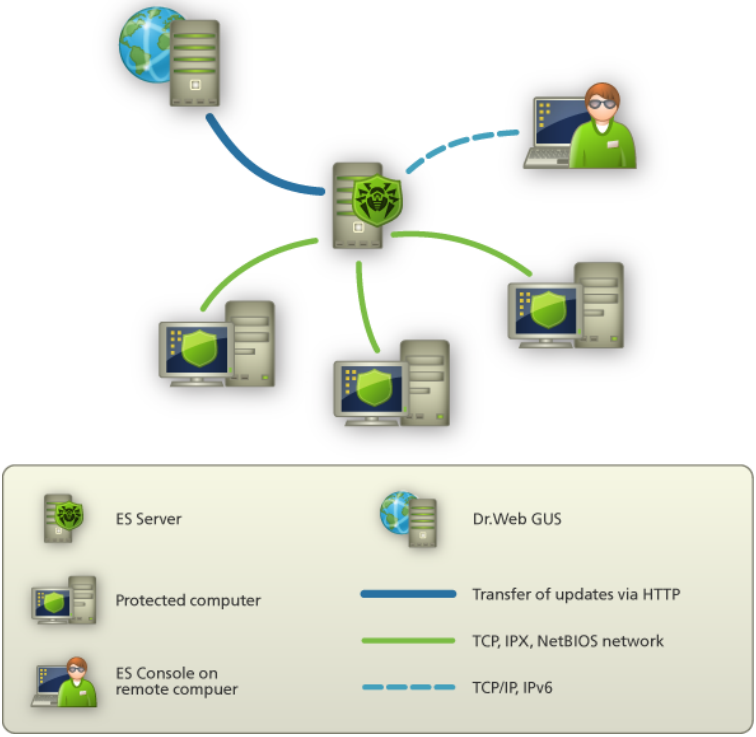
The illustration below describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.



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.



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 G. 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:

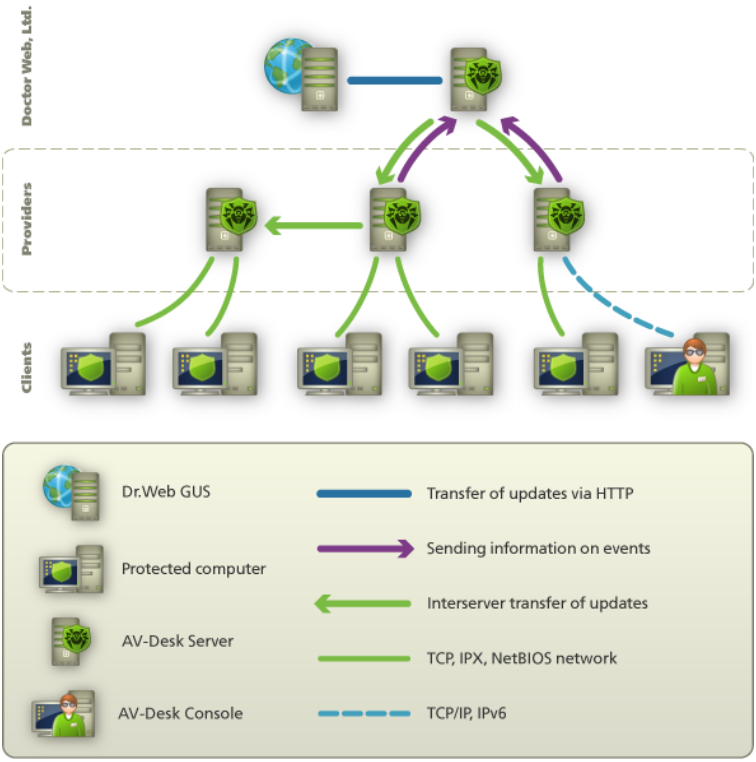
- simple installation of software components and prompt arrangement of anti-virus protection,
- creation of distribution files with unique identifiers and their transfer to the users for installation,
- centralized setup of anti-virus packages on protected computers,

- 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.
- **Anti-virus console** is used for the remote administration of the anti-virus network by means of editing the settings of the anti-virus server and protected computers stored on the anti-virus server and protected computers.
- **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.



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