Dr.WEB®

Anti-virus
for Windows servers

Administrator Manual

Defend what you create

TRADEMARKS
Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER
In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web Anti-virus for Windows servers
Version 7.0
Administrator Manual
31.07.2012

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

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

Refer to the official web site for regional and international office information.

Doctor Web

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

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

1. Introduction

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

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

Dr.Web Anti-virus for servers can detect and remove undesirable programs (adware, dialers, jokes, riskware, and hacktools) from your computer. To detect undesirable programs and perform actions with the files contained in them, standard anti-virus components are used.

Dr.Web Anti-virus for servers includes the following components:

- **Dr.Web Scanner for Windows** (**Scanner**) is an anti-virus scanner with graphical interface. The program runs on user demand checks the computer for viruses. There is also a command line version (**Dr.Web Console Scanner for Windows**).
- **SpIDer Guard® for Windows** (also called **Monitor** or **Guard**) is an anti-virus guard. The program resides in the main memory, checks files and memory on the fly, and detects virus-like activity.
- **Dr.Web Updater** allows registered users to receive updates of the virus database and other program files as well as automatically install them.
- **SpIDer Agent** is a utility that lets you set up and manage **Dr. Web Anti-virus for servers** components.

1.1. About This Manual

This Administrator Manual describes installation and effective utilization of **Dr.Web Anti-virus for servers**.

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

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

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

Due to constant development, program interface of your installation can mismatch the images given in this document. You can always find the actual documentation at http://products.drweb.com.

1.2. Document Conventions

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

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

The following abbreviations are used in this Administrator Manual:

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

1.3. System Requirements

⚠ Before installing **Dr.Web Anti-virus for servers**:

- Install all critical updates recommended by the operating system developer.
- Uninstall all other anti-virus packages from the computer to avoid possible incompatibility with their resident components.

Specification	Requirement
OS	One of the following: • Microsoft® Windows® 2000 Server SP4 with Update Rollup 1 • Microsoft® Windows Server® 2003 SP1 • Microsoft® Windows Server® 2008 Both 32-bit and 64-bit versions of operating systems are supported. You may need to download and install certain system components from the official Microsoft website. If necessary, the program will notify you about the components required and provide download links.
Hard disk space	200 MB for **Dr.Web Anti-virus for servers** components. Files created during installation will require additional space.
CPU	i686 compatible
RAM	Minimum 512 MB of RAM.
Other	Internet connection for updating virus databases and **Dr.Web Anti-virus for servers** components.

1.4. Licensing

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

To use **Dr.Web Anti-virus for servers**, obtain and install a key file.

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

1.4.1. Key File

The key file contains the following information:

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

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

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

Dr.Web Anti-virus for servers uses *license key file*, which allows user to 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 the seller.

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

- License is not expired
- All anti-virus components required by **Dr.Web Anti-virus for servers** are licensed

- Integrity of the license key file has not been violated

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

1.4.2. Get Key File

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

To acquire key files via manual registration:

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

To receive a license key file, a product serial number is required.

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

Subsequent Registration

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

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

If no valid key file is found, the functionality of the program is blocked.

1.4.3. Renewing Registration

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

To renew license key files:

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

1.5. How to Test Anti-virus

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

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

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

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

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

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

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

1.6. Detection Methods

Dr.Web anti-virus solutions use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behaviour:

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

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

2. Installing Dr.Web Anti-virus for servers

Before installing the program, we strongly recommend to:

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

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

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

2.1. Installation Procedure

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

There are two installation modes of anti-virus software:

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

Background Installation

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

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

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

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

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

`/L`<*language_code*>

For example,

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

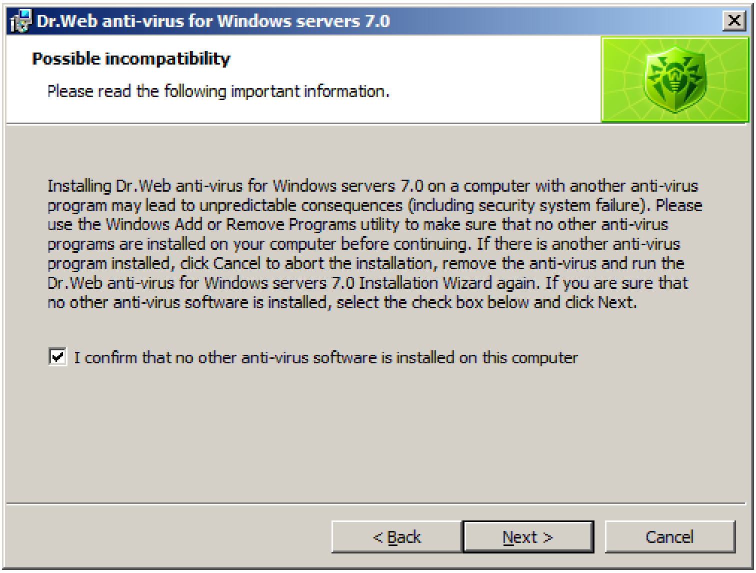
The list of languages:

Code	Language
1026	Bulgarian
2052	Chinese (Simplified)
1028	Chinese (Traditional)
1033	English
1061	Estonian
1036	French (France)
1031	German
1032	Greek
1038	Hungarian
1040	Italian
1041	Japanese
1062	Latvian
1063	Lithuanian
1045	Polish
2070	Portuguese
1049	Russian
1051	Slovak
1034	Spanish (Traditional Sort)
1055	Turkish
1058	Ukrainian

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

Installation in the usual mode

1. 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.
2. 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 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**.



Dr.Web anti-virus for Windows servers 7.0

Possible incompatibility

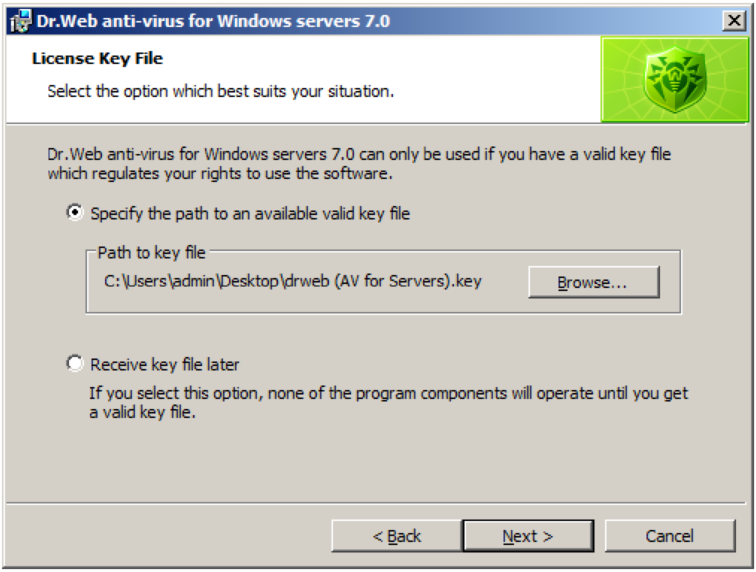
Please read the following important information.

Installing Dr.Web anti-virus for Windows servers 7.0 on a computer with another anti-virus program may lead to unpredictable consequences (including security system failure). Please use the Windows Add or Remove Programs utility to make sure that no other anti-virus programs are installed on your computer before continuing. If there is another anti-virus program installed, click Cancel to abort the installation, remove the anti-virus and run the Dr.Web anti-virus for Windows servers 7.0 Installation Wizard again. If you are sure that no other anti-virus software is installed, select the check box below and click Next.

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

3. The installation program will bring up a warning window

requesting a key file 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**.



Dr.Web anti-virus for Windows servers 7.0

License Key File

Select the option which best suits your situation.

Dr.Web anti-virus for Windows servers 7.0 can only be used if you have a valid key file which regulates your rights to use the software.

● Specify the path to an available valid key file

Path to key file

C:\Users\admin\Desktop\drweb (AV for Servers).key

○ Receive key file later

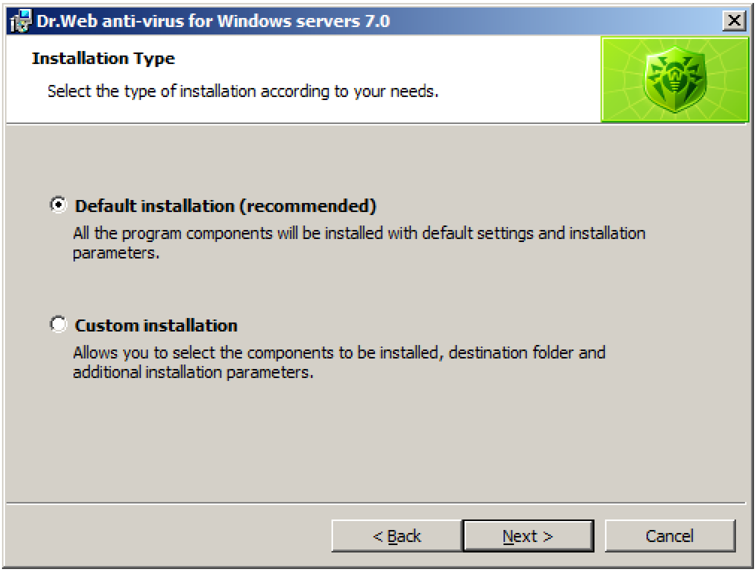
If you select this option, none of the program components will operate until you get a valid key file.

If no key file is available, select **Receive key file later**. If you select this option, none of the program components will operate until you get a valid key file.

Click **Next**.

Use only **Dr.Web Anti-virus for servers** key file. The key file should have the **.key** extension.

4. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components automatically up to step 9. **Custom Installation** is meant for experienced users. During custom installation you will be asked to select which components should be installed and adjust some additional installation parameters.



Dr.Web anti-virus for Windows servers 7.0

Installation Type

Select the type of installation according to your needs.

● **Default installation (recommended)**

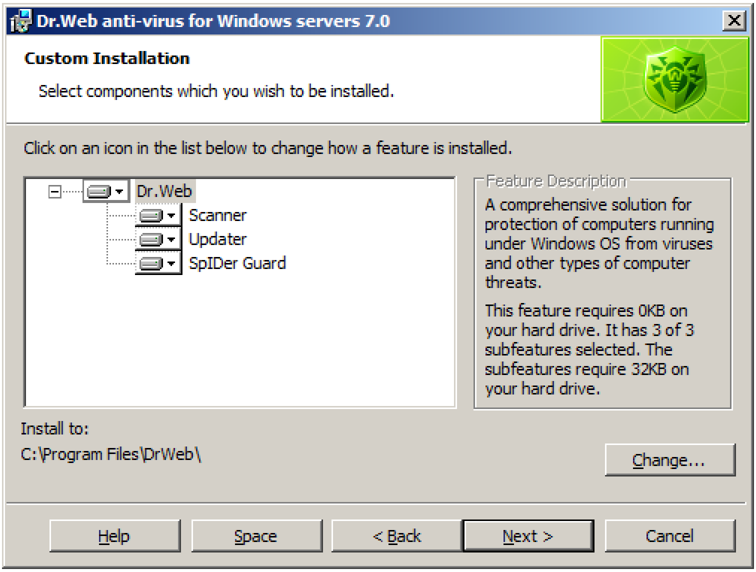
All the program components will be installed with default settings and installation parameters.

○ **Custom installation**

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

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

5. If you chose default installation type, go to step 9. In case of custom installation, a window for selecting the program components which you wish to install will open. In the hierarchical list select the components you wish to install. You can also change the installation folder if necessary.



Dr.Web anti-virus for Windows servers 7.0

Custom Installation

Select components which you wish to be installed.

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

- Dr.Web
  - Scanner
  - Updater
  - SpIDer Guard

Feature Description

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

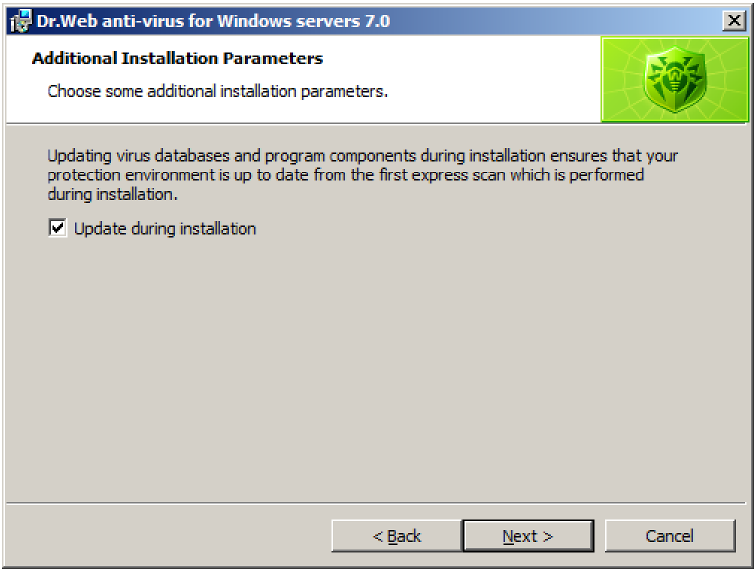
This feature requires 0KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 32KB on your hard drive.

Install to:

C:\Program Files\DrWeb\

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

6. The window for selecting which shortcuts to **Dr.Web Anti-virus for servers** should be created will open. Select the necessary options and click **Next**.
7. If you specified license key file in step 3, in the next window you can select the **Update during installation** check box to download the latest virus databases during installation.



Dr.Web anti-virus for Windows servers 7.0

Additional Installation Parameters

Choose some additional installation parameters.

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

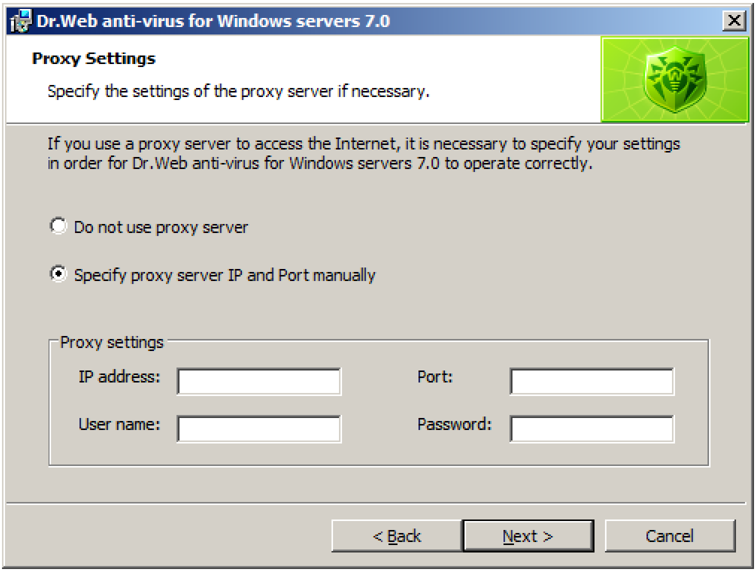
☑ Update during installation

Click **Next**.

8. The window for adjusting proxy server settings will open.

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

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



Dr.Web anti-virus for Windows servers 7.0

Proxy Settings

Specify the settings of the proxy server if necessary.

If you use a proxy server to access the Internet, it is necessary to specify your settings in order for Dr.Web anti-virus for Windows servers 7.0 to operate correctly.

○ Do not use proxy server

● Specify proxy server IP and Port manually

Proxy settings

IP address:

Port:

User name:

Password:

9. A window informing that the program is ready to be installed will open. Click **Install** to start the installation process or **Back** to change any of the installation parameters.
10. If you specified license key file and selected the **Update during installation** check box in step 7, virus databases and components of **Dr.Web Anti-virus for servers** will be updated automatically.
11. After installation is complete the **Scanner** will perform express scan. Avert any detected threats and close the **Scanner** after the scanning process.
12. The program will ask for a computer reboot which is required to complete the installation.

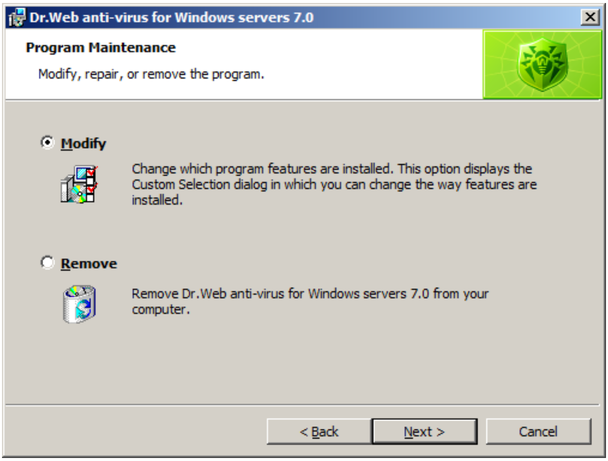
2.2. Reinstalling and Removing Dr.Web Anti-virus for servers

To modify, repair, or remove an installed version of **Dr.Web Anti-virus for servers**, start the installation wizard.

In the opened window:

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

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



Program Maintenance

Modify, repair, or remove the program.

● Modify

Change which program features are installed. This option displays the Custom Selection dialog in which you can change the way features are installed.

○ Remove

Remove Dr.Web anti-virus for Windows servers 7.0 from your computer.

3. Getting Started

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

- **Scanner** (GUI and console versions)
- **SpIDer Guard**
- **Automatic Updating Utility**
- **SpIDer Agent**

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

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

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

An advantage of the program is that it provides you with uninterrupted control of the virus situation during the entire time a PC is running. In addition, some viruses can only be detected by the guard through their specific activity.

Ensuring Protection Against Virus Threats

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

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

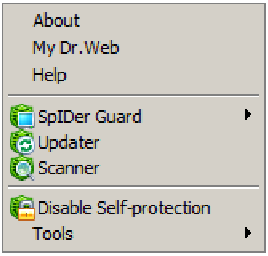
Anti-virus protection can only be effective if you update the virus databases and other program files regularly (preferably every hour). For more information, read Automatic Updating.

3.1. SpIDer Agent

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

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

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



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

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

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

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

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

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

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

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

To disable self-protection:

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

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

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

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

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

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

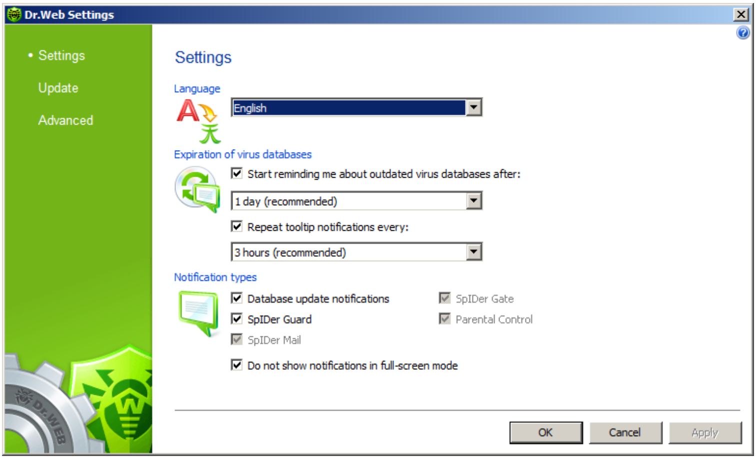
The **Administrative/User mode** item allows you to switch between full-function **Administrative mode** and restricted **User mode**. In **User mode**, access to settings of components is forbidden, as well as disabling of all components and self-protection. **License Manager** and **Anti-virus Network**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

This item displays when you do not have administrative privileges. For instance, when User Account Control of Windows Server 2008 operating system is enabled. Otherwise, the item is hidden and **Dr.Web Anti-virus for servers** operates in full-function mode all the time.

3.2. General Settings

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

Settings Page



Settings

Language

English

Expiration of virus databases

☑ Start reminding me about outdated virus databases after:

1 day (recommended)

☑ Repeat tooltip notifications every:

3 hours (recommended)

Notification types

☑ Database update notifications

☑ SpIDer Guard

☑ SpIDer Mail

☑ SpIDer Gate

☑ Parental Control

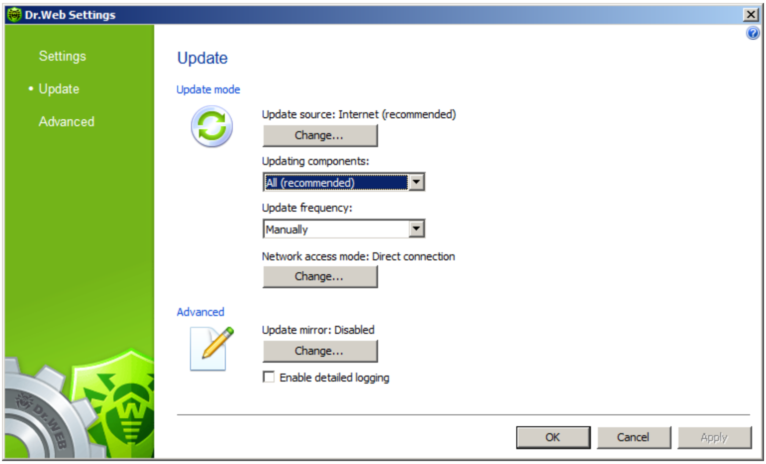
☑ Do not show notifications in full-screen mode

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

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

Update Page

On this page you can configure **Dr.Web Anti-virus for servers** update parameters such as components that should be updated, an updating source, update period, and update mirror.



Update source: Internet (recommended)

Updating components: All (recommended)

Update frequency: Manually

Network access mode: Direct connection

Update mirror: Disabled

☐ Enable detailed logging

Update source

To select an update source, click **Change**. In the opened window select one of the following update sources:

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

Update mirror

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

Network access mode

On this page you can also configure network access. To do this, in the **Network access mode** click **Change** and then select one of the following modes:

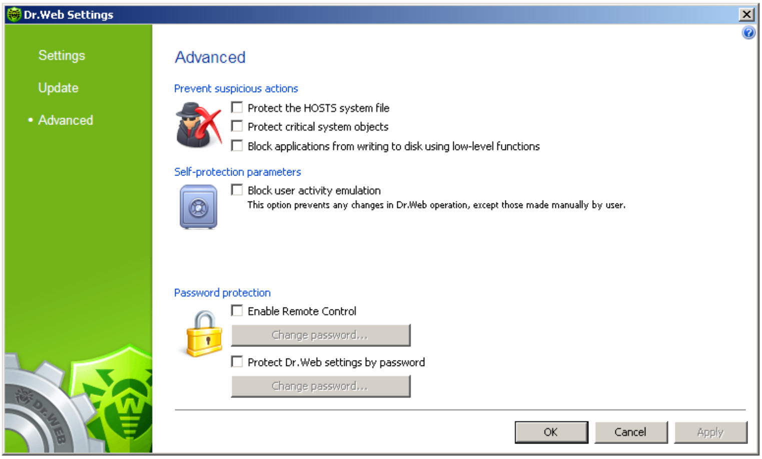
- If you do not use proxy server for Internet connections, select **Direct connection**.
- If you want to specify proxy server settings manually, select **User-defined** and enter connection parameters.

Also you can set the **Enable detailed logging** flag to increase change log detail level. All changes are logged into dwupdater.log, that is located in %allusersprofile%\Application Data\Doctor Web\Logs\ folder (in Windows Server 2008, %allusersprofile%\Doctor Web\Logs\).

Advanced Page

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

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



Advanced

Prevent suspicious actions

☐ Protect the HOSTS system file

☐ Protect critical system objects

☐ Block applications from writing to disk using low-level functions

Self-protection parameters

☐ Block user activity emulation

This option prevents any changes in Dr.Web operation, except those made manually by user.

Password protection

☐ Enable Remote Control

☐ Protect Dr.Web settings by password

Password protection

Here you can configure the following options:

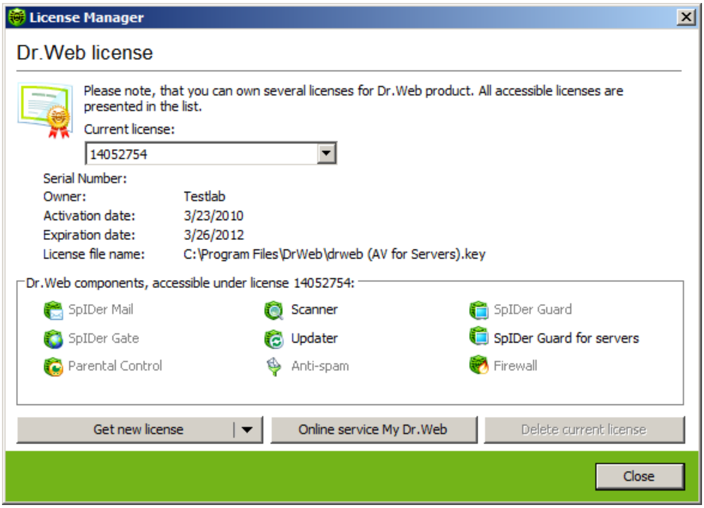
- Allow remote access to **Dr.Web Anti-virus for servers** on your computer and set a password that will be required to connect to your anti-virus from other computers.
- Protect **Dr.Web Anti-virus for servers** settings on your computer with a password. Set a password that will be required to access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

3.3. License Manager

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

The **License Manager** item is available in the menu when operation in Administrative mode only.

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



License Manager

Dr.Web license

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

Current license: 14052754

Serial Number:
Owner: Testlab
Activation date: 3/23/2010
Expiration date: 3/26/2012
License file name: C:\Program Files\DrWeb\drweb (AV for Servers).key

Dr.Web components, accessible under license 14052754:

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

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

To add a key file

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

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

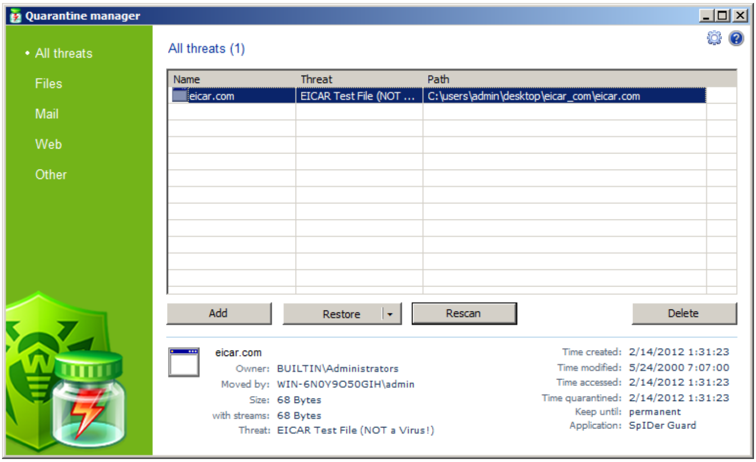
⚠ By default, the license key file should be located in the **Dr.Web Anti-virus for servers** installation folder. **Dr.Web Anti-virus for servers** verifies the file regularly. Do not edit or otherwise modify the file to prevent the license from compromise.

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

3.4. Quarantine Manager

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

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



All threats (1)

Name	Threat	Path
eicar.com	EICAR Test File (NOT ...	C:\users\admin\desktop\eicar_com\eicar.com

eicar.com

Owner: BUILTIN\Administrators
Moved by: WIN-6N0Y9O50GIH\admin
Size: 68 Bytes
with streams: 68 Bytes
Threat: EICAR Test File (NOT a Virus!)

Time created: 2/14/2012 1:31:23
Time modified: 5/24/2000 7:07:00
Time accessed: 2/14/2012 1:31:23
Time quarantined: 2/14/2012 1:31:23
Keep until: permanent
Application: SpIDer Guard

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

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

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

To configure table view:

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

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

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

Use the following buttons to manage the quarantine:

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

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

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

- **Rescan** – scan the file one more time. If during rescan file is detected as clean, **Quarantine Manager** will suggest to restore it.
- **Remove** – delete the file from the quarantine and from the system

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

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

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

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

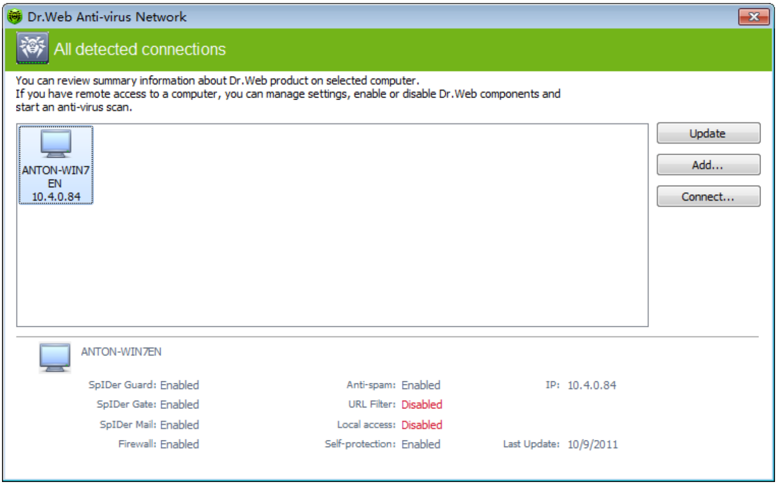
To configure **Quarantine** parameters, click the **Settings** ⚙ button in the **Quarantine** window. The **Quarantine** properties window will be opened. In this window you can change the following parameters:

- In the **Set quarantine size** section you can configure the amount of disk space for **Quarantine** folder
- In the **View** section, you can set the **Show backup files** checkbox to display backup copies of **Quarantine** files in the object table

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

3.5. Anti-virus Network

This section allows managing **Dr.Web Anti-virus for servers** on other computers of your network. To access **Dr.Web Anti-virus for servers** remote control, in the context menu of the **SpIDer Agent** icon in the taskbar notification area, select **Tools**, and then select **Anti-virus Network** item.



All detected connections

You can review summary information about Dr.Web product on selected computer.
If you have remote access to a computer, you can manage settings, enable or disable Dr.Web components and start an anti-virus scan.

ANTON-WIN7EN
10.4.0.84

ANTON-WIN7EN

SpIDer Guard:	Enabled	Anti-spam:	Enabled	IP:	10.4.0.84
SpIDer Gate:	Enabled	URL Filter:	Disabled		
SpIDer Mail:	Enabled	Local access:	Disabled		
Firewall:	Enabled	Self-protection:	Enabled	Last Update:	10/9/2011

To access remote anti-virus, select a computer in the list and click **Connect**. Enter password specified in settings of the remote anti-virus. An icon for the remote **SpIDer Agent** appears in the Windows notification area. The user of the remote anti-virus will be notified about remote connection. The following items to configure and manage remote **Dr.Web Anti-virus for servers** are available (set of components depends on which **Dr.Web product** is installed):

- **About**
- **Register license**
- **My Dr.Web**
- **Help**
- **SpIDer Guard**
- **SpIDer Mail**
- **SpIDer Gate**
- **Parental Control**

- **Firewall**
- **Tools**
- Update
- **Enable/Disable Self-protection**

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

- License Manager
- General Settings of **Dr.Web** operation
- Report generation wizard.

You can manage settings, enable or disable components, and look through statistics.

Anti-virus Network, **Quarantine Manager** and **Scanner** are not available. **Firewall** settings and statistics are not available as well, but you can enable or disable **Firewall** (if you accessed **Dr.Web Anti-virus** or **Dr.Web Security Space**). Also you can select the **Disconnect** item to terminate remote connection.

If required computer is not on the list, you can try to add it manually. For this, click **Add** button and enter IP-address.

You can establish only one connection with remote **Dr.Web product**. If one connection is already established, the **Connect** button is disabled.

Computers are listed in **Anti-virus Network** if **Dr.Web** products installed on these computers allow remote connection. You can allow connection to your **Dr.Web Anti-virus for servers** on the **Advanced** tab in General settings.

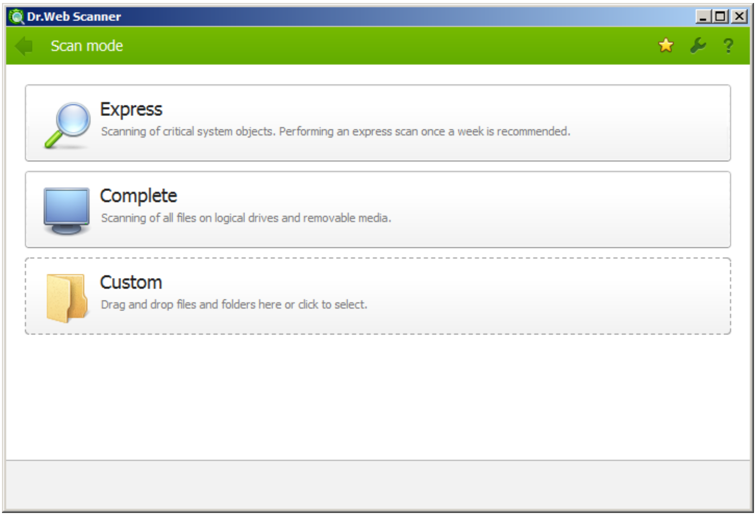
The **Anti-virus Network** item is available in the menu when operation in Administrative mode only.

4. Dr.Web Scanner

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

By default, **Dr.Web Scanner** uses all detection methods to detect viruses and other malicious software. Information on all infected or suspicious objects displays in the table where you can manually select a necessary action.

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



Express

Scanning of critical system objects. Performing an express scan once a week is recommended.

Complete

Scanning of all files on logical drives and removable media.

Custom

Drag and drop files and folders here or click to select.

4.1. Scanning Your System

Dr.Web Scanner is installed as a usual Windows application and can be launched by the user or automatically (see Automatic Launch of Scanning).

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

To launch Scanner:

Do one of the following:

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

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

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

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

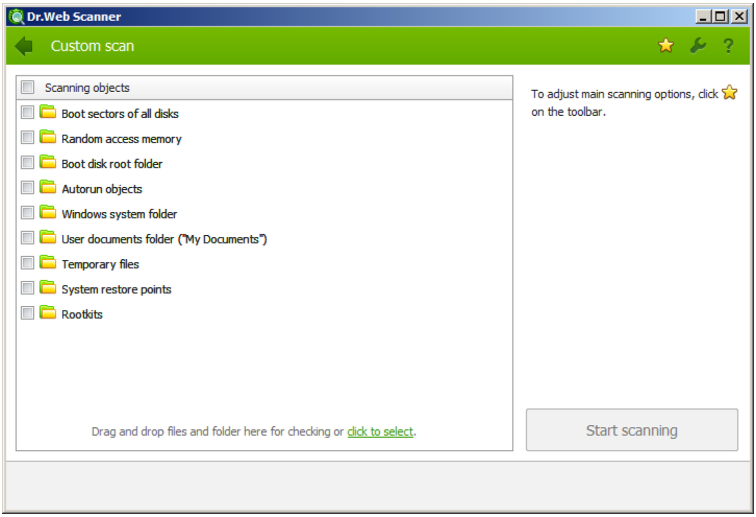
- Random access memory
- Boot sectors of all disks
- Autorun objects
- Boot disk root directory
- Windows installation disk root directory
- Windows system folder

- User documents folder ("My documents")
- System temporary folder
- User temporary folder

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

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

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



□ Scanning objects
□ Boot sectors of all disks
□ Random access memory
□ Boot disk root folder
□ Autorun objects
□ Windows system folder
□ User documents folder ("My Documents")
□ Temporary files
□ System restore points
□ Rootkits

Drag and drop files and folder here for checking or click to select.

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

When scanning starts, **Pause** and **Stop** buttons become available. You can do the following:

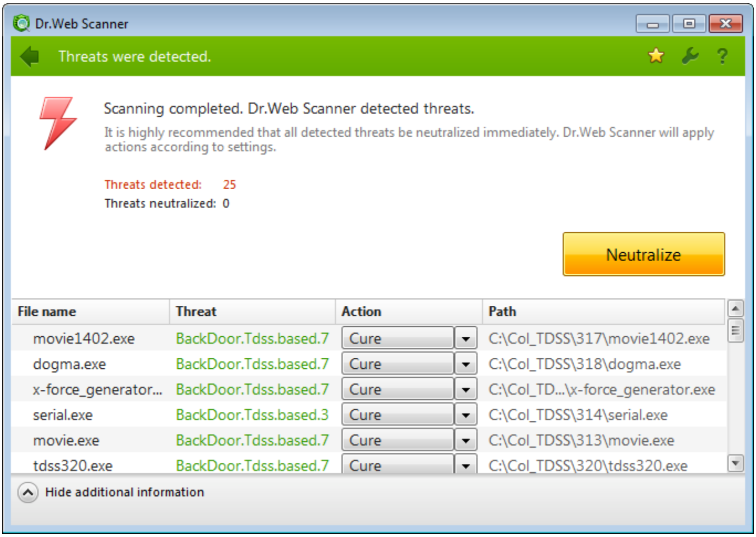
- to pause scanning, click **Pause** button. To resume scanning after pause, click **Resume** button;
- to stop scanning, click **Stop** button.

The **Pause** button is not available at scanning processes and RAM.

4.2. Neutralizing Detected Threats

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

Threats to your security can be neutralized either by restoring the original state of each infected objects (*curing*), or, when curing is impossible, by removing the infected object completely from your operating system (*deleting*).



Scanning completed. Dr.Web Scanner detected threats.

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

Threats detected: 25
Threats neutralized: 0

File name	Threat	Action	Path
movie1402.exe	BackDoor.Tdss.based.7	Cure	C:\Col_TDSS\317\movie1402.exe
dogma.exe	BackDoor.Tdss.based.7	Cure	C:\Col_TDSS\318\dogma.exe
x-force_generator...	BackDoor.Tdss.based.7	Cure	C:\Col_TD...\x-force_generator.exe
serial.exe	BackDoor.Tdss.based.3	Cure	C:\Col_TDSS\314\serial.exe
movie.exe	BackDoor.Tdss.based.7	Cure	C:\Col_TDSS\313\movie.exe
tdss320.exe	BackDoor.Tdss.based.7	Cure	C:\Col_TDSS\320\tdss320.exe

To select an action:

1. Where necessary, select a custom action from the drop-down list in the **Action** field. By default, **Scanner** selects a recommended action for the type of detected threat.

2. Click **Neutralize**. **Scanner** applies all selected actions to the detected threats.

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

There are some limitations:

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

The detailed report on the program's operation is saved in dwscanner. log file that resides in the %USERPROFILE%\Doctor Web folder.

4.3. Scanner Settings

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

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

To configure Scanner:

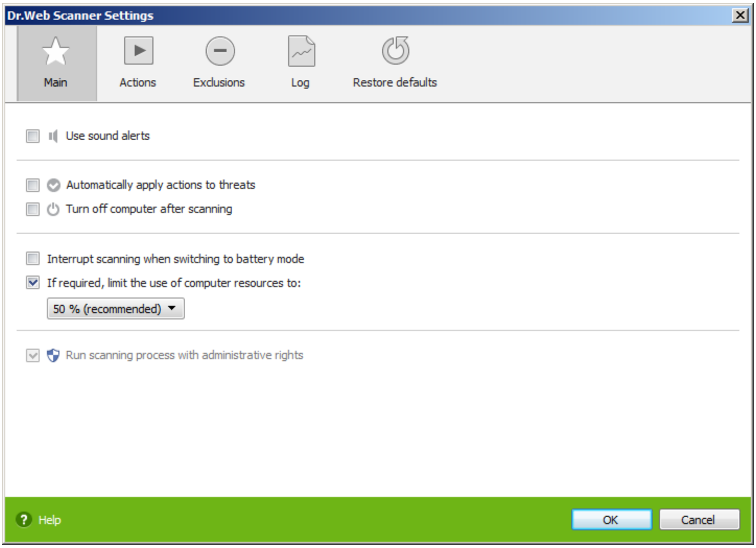
1. To open **Scanner** settings, click the **Settings** icon on the toolbar. This opens the **Dr.Web Scanner settings** window which contains several tabs.
2. Make the necessary changes.
3. For more detailed information on the settings specified in each tab use the **Help** button.
4. When editing is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

Main Page

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

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

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



□ Use sound alerts

□ Automatically apply actions to threats

□ Turn off computer after scanning

□ Interrupt scanning when switching to battery mode

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

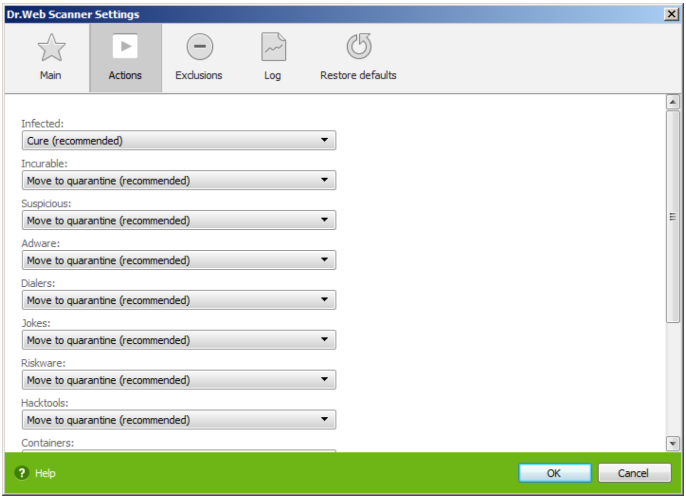
50 % (recommended)

☑ Run scanning process with administrative rights

Actions Page

To set reaction on threat detection:

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



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

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

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

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

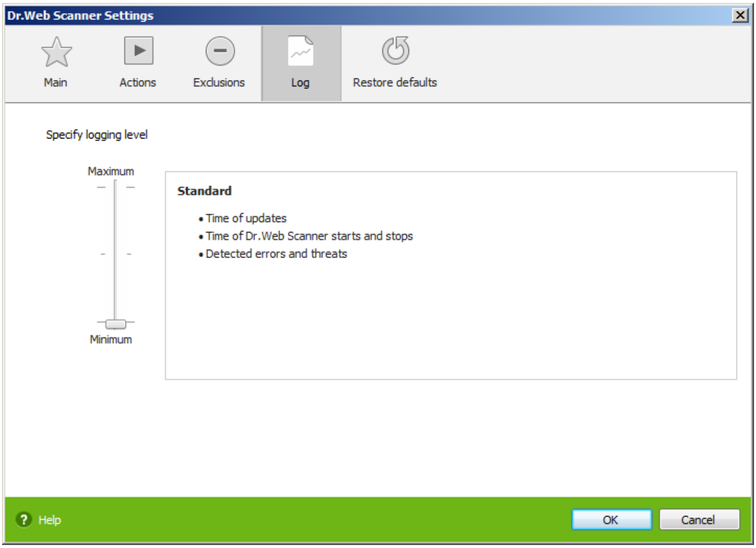
4. In the **Suspicious objects** drop-down list select the program's action upon detection of a suspicious object (fully similar to the previous paragraph).
5. Similar actions should be specified for detection of objects containing Adware, Dialers, Jokes, Riskware and Hacktools.
6. The same way the automatic actions of the program upon

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

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

Log Page

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



Specify logging level

Maximum

Minimum

Standard

- Time of updates
- Time of Dr.Web Scanner starts and stops
- Detected errors and threats

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

4.4. Scanning in Command Line Mode

You can run **Scanner** in the command line mode, then you can specify settings of the current scanning session and list objects for scanning as additional parameters. This mode provides automatic activation of **Scanner** according to schedule.

To run scanning from command line:

Enter a command in the following format:

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

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

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

- **/FAST** perform an express scan of the system (for more information on the express scan mode see Scan Modes).
- **/FULL** perform a full scan of all hard drives and removable data carriers (including boot sectors).
- **/LITE** perform a basic scan of random access memory, boot sectors of all disks and startup objects.

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

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

4.5. Console Scanner

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

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

To run Console Scanner:

Enter the following command:

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

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

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

Return codes:

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

4.6 Automatic Launch of Scanning

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

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

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

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

You can also create your own anti-virus scanning tasks. Please refer to the Help system and Windows documentation for more details on the system scheduler operation.

5. SpIDer Guard

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

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

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

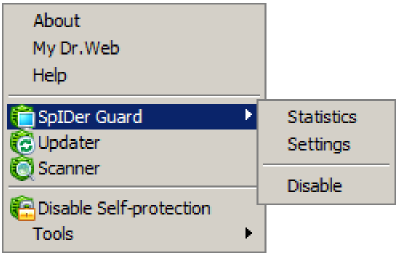
By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web Anti-virus for servers** acts according to actions set on the Actions tab.

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

Incompatibility between **Dr.Web Anti-virus for servers** and **MS Exchange Server** is possible. If any problems occur, add MS Exchange Server databases and transaction log in the list of **SpIDer Guard** exceptions.

5.1. Managing SpIDer Guard

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



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

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

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

5.2. SpIDer Guard Settings

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

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

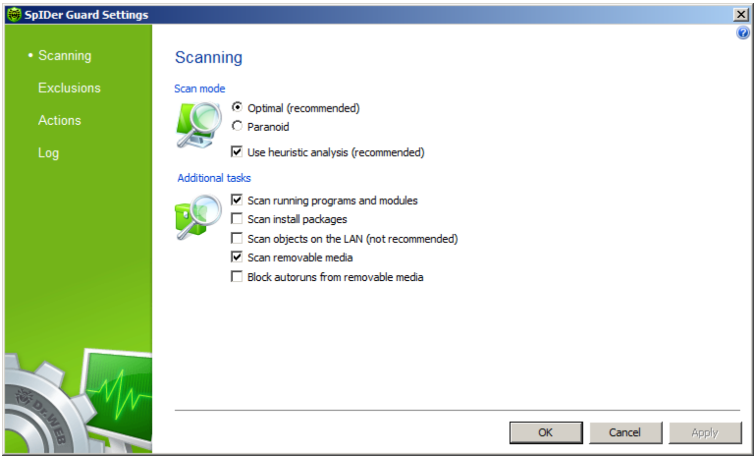
Some of the most frequently changed settings of the program are described below.

Scanning Page

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

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

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



Scanning

Scan mode

● Optimal (recommended)

○ Paranoid

☑ Use heuristic analysis (recommended)

Additional tasks

☑ Scan running programs and modules

☐ Scan install packages

☐ Scan objects on the LAN (not recommended)

☑ Scan removable media

☐ Block autoruns from removable media

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

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

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

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

These parameters are applied in any scan mode.

Also you can select **Block autoruns from removable media** check-box to disable autoplay option for portable data storages such as CD/DVD, flash memory etc. This option helps to protect you computer from viruses transmitted via removable media.

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

Exclusions Page

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

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

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

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

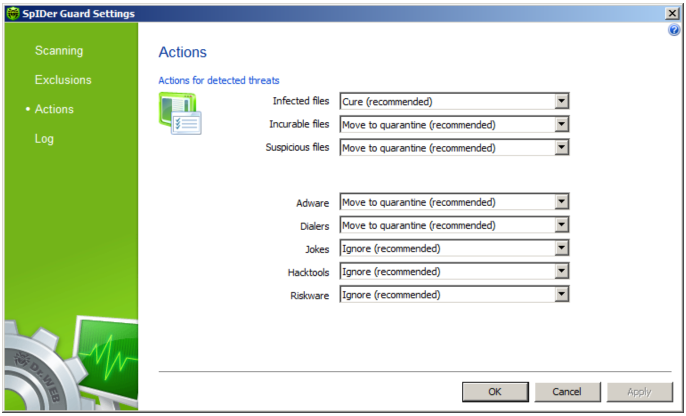
Actions Page

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

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

To change the default actions in SpIDer Guard:

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



SpIDer Guard Settings

Actions

Actions for detected threats

Infected files: Cure (recommended)

Incurable files: Move to quarantine (recommended)

Suspicious files: Move to quarantine (recommended)

Adware: Move to quarantine (recommended)

Dialers: Move to quarantine (recommended)

Jokes: Ignore (recommended)

Hacktools: Ignore (recommended)

Riskware: Ignore (recommended)

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

Log Page

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

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

  It is recommended to use this mode when determining objects that **SpIDer Guard** checks most often.
- **Debugging** – in this mode, **SpIDer Guard** logs all details on its activity. This may result in considerable log growth.

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

6. Automatic Updating

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

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

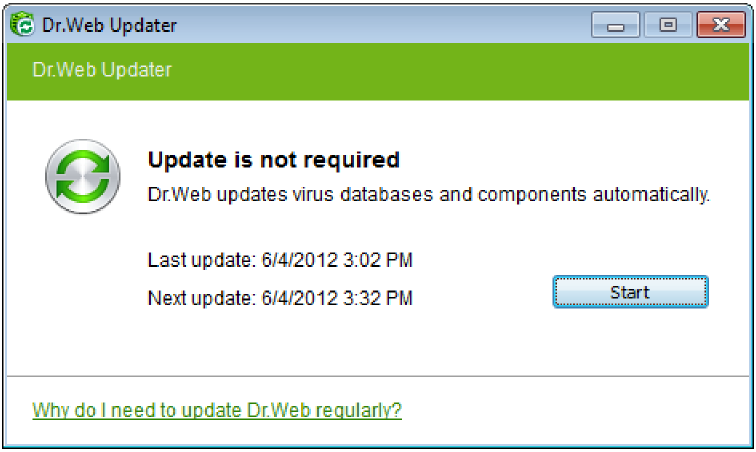
11.1. Running Updates

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

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

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

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



Update is not required

Dr.Web updates virus databases and components automatically.

Last update: 6/4/2012 3:02 PM

Next update: 6/4/2012 3:32 PM

Update Procedure

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

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

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

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

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

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

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

Appendices

Appendix A. Command Line Parameters

Additional command line parameters (switches) are used to set parameters for programs which can be launched by opening an executable file. This relates to **Scanner**, **Console Scanner** and to **Dr.Web Updater**. 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.

Scanner and Console Scanner Parameters

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

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

/AC – check installation packages. Option is enabled by default.

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

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

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

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

/ART:<*size*> – minimum size of file inside archive beginning from which compression ratio check will be performed (*unlimited*, KB).

/ARX:<*size*> – maximum size of objects in archives that should be checked (*unlimited*, KB).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/P:*<prio>* – test priority:

0 – the lowest,
L – low,
N – general. Priority by default,
H – the highest,
M – maximal.

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

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

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

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

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

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

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

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

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

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

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

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

/QNA – double quote file names always.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/AC- option is clearly disabled,
/AC, **/AC+** option is clearly enabled.

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

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

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

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

Example of using command line parameters with **Console Scanner**:

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

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

Dr.Web Updater Command Parameters

Common options:

Parameter	Description
-h [--help]	Show this message.
-v [--verbosity] arg	Log level. Can be one of following: error, info, debug.
-d [--data-dir] arg	Directory where repository and settings are located.
--log-dir arg	Directory for storing log file.

Parameter	Description
--log-file arg (=dwupdater.log)	Log file name.
-r [--repo-dir] arg	Repository directory, (<data_dir>/repo by default).
-t [--trace]	Enable backtrace.
-c [--command] arg (=update)	Command to execute: getversions, getcomponents, getrevisions, init, update, uninstall, exec and keyupdate.
-z [--zone] arg	List of zones that should be used instead of specified in configuration file.

init command parameters:

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

update command parameters:

Parameter	Description
-p [--product] arg	Product name. If specified, only this product will be updated. If nothing is specified, all products will be updated. If components are specified, only these components will be updated.
-n [--component] arg	Components that should be updated to specified version. *<Name>* , *<target revision>*.
-x [--selfrestart] arg (=yes)	Reboot after updating of **Dr.Web Updater**. Default value is `yes`. If value is set to `no`, reboot required notification will appear
--geo-update	Attempt to get list of IP-addresses from update.drweb.com before updating.
--type arg (=normal)	One of the following: • reset-all – reset revision to 0 for all components • reset-failed – reset revision to 0 for failed components • normal-failed – try to update all components including failed from current revision to newest or specified • update-revision – try to update all components of current revision to newest if exists • normal – update all components
-g [--proxy] arg	Proxy-server for updating. *<Address>*:*<port>*
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
--param arg	Pass additional parameters to the script. *<Name>*: *<value>* .
-l [--progress-to-console]	Print information about downloading and script execution to console.

exec command parameters:

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

getcomponents command parameters:

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

getrevisions command parameters:

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

uninstall command parameters:

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

keyupdate command parameters:

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

download command parameters:

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

Appendix B. Computer Threats and Neutralization Methods

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

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

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

Classification of Computer Threats

Computer viruses

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

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

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

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

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

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

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

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

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

Computer worms

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

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

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

Trojan horses (Trojans)

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

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

Rootkits

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

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

Hacktools

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

Spyware

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

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

Adware

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

Joke programs

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

Dialers

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

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

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

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

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

Actions Applied to Threats

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

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

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

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

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

Appendix C. Naming of Viruses

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

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

Prefixes

Affected operating systems

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

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

- FreeBSD – FreeBSD programs
- SunOS – SunOS (Solaris) programs
- Symbian – Symbian OS (mobile OS) programs

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

Macrovirus prefixes

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

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

Development languages

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

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

The following prefix also refers to development language:

- Java – viruses designed for the Java virtual machine

Script-viruses

Prefixes of viruses written in different scrip languages:

- VBS – Visual Basic Script

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

Trojan horses

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

Tools for network attacks

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

Malicious programs

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

Miscellaneous

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

Suffixes

Suffixes are used to name some specific virus objects:

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

Appendix D. Technical Support

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

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

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

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

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