Dr.WEB®

Anti-virus
for Windows servers

Defend what you create

Administrator Manual

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 6.0
Administrator Manual
30.11.2010

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

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

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

Doctor Web

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

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

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

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

Table of Contents

Introduction

Dr.Web® 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 Windows servers** is its significant feature. **Dr.Web** uses the anti-virus engine and virus databases which are common for all its components and different operating environments. At present, in addition to **Dr.Web Anti-virus for Windows servers**, there are versions of the anti-virus for IBM® OS/2®, Novell® NetWare®, Macintosh®, Microsoft Windows Mobile®, Andorid®, Symbian® and several Unix®-based systems (Linux®, FreeBSD®, Solaris®).

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

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

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

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

- **Dr.Web Scanner for Windows** (**Scanner**) is an anti-virus scanner with graphical interface. The program is run on user demand or according to schedule, and checks the computer for viruses. There is also a command line version (**Dr.Web Console scanner for Windows**).
- **SpIDer Guard® for Windows** (also called **Monitor** or **Guard**) is an anti-virus guard. The program resides in main memory, checks files and memory on the fly, and detects virus-like activity.
- **Dr.Web Automatic Updating Utility for Windows** (**Updater**) allows registered users to receive updates of the

virus database and other files of the program, as well as automatically install them.

- **SpIDer Agent** is a utility which lets you set up and manage components of **Dr.Web**.

To centralize the management of the anti-virus protection at an enterprise level, a special program – **Dr.Web Enterprise Suite** – is supplied. For more details on this program read Appendix E.

Internet service providers can organize anti-virus and anti-spam protection of their clients using **Dr.Web AV-Desk**. For more information on this software see Appendix F.

What is This Manual About

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

You can find detailed description of all the GUI elements in the Help system of **Dr.Web Anti-virus for Windows servers** which can be accessed from any component.

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

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

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

Document Conventions and Abbreviations

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

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

The following abbreviations are used in this User Manual:

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

System Requirements

Before installing **Dr.Web Anti-virus for Windows servers**, you should:

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

Specification	Requirement
OS	One of the following: • Microsoft® Windows® 2000 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 Web site. If necessary, the program will notify you about the components required and provide download links.
Hard disk space	Minimum 275 MB of disk space for a full installation, which includes: • Up to 80 MB of installation files • Up to 97 MB of temporary setup files that are removed automatically at completion of install
CPU	i686 compatible.
RAM	512 MB and more.
Other	Internet connection for updating of virus databases and **Dr.Web Anti-virus for Windows servers** components.

Licensing

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

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

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

Key File

The key file contains the following information:

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

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

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

Dr.Web Anti-virus for Windows 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 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 Windows servers** are licensed
- Integrity of the license key file is not violated

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

Get Key File

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

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

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

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

Renewing registration

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

To renew license key files

1. Open License Manager. To purchase a new license or renew an existing one, you can also use your personal web page on the **Doctor Web** web site. To visit your page, use **My Dr.Web** option in the **License Manager** or SpIDer Agent menu.

2. If current key file is invalid, **Dr.Web Anti-virus for Windows servers** automatically switches to using the new license.

How to Test Anti-virus

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

For this purpose, most of the anti-virus software vendors generally use a standard test.com program. This program was designed specially so that users could test reaction of newly-installed anti-virus tools to detection of viruses without compromising security of their computers. Although the test.com program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", **Dr.Web® Anti-virus 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 may create a new file with this line and save it with as test.com.

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

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

Installation procedure

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

There are two modes of the installation of anti-virus software:

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

Installation in the background mode

To install **Dr.Web Anti-virus for Windows servers** in the background mode, in the command line enter the executable file name with necessary parameters (these parameters affects the logging and the 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 perform installation of **Dr.Web Anti-virus for Windows servers** with logging and reboot after installation, execute the following command:

```
C:\Documents and Settings\drweb-600-winsrv-x86
/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:

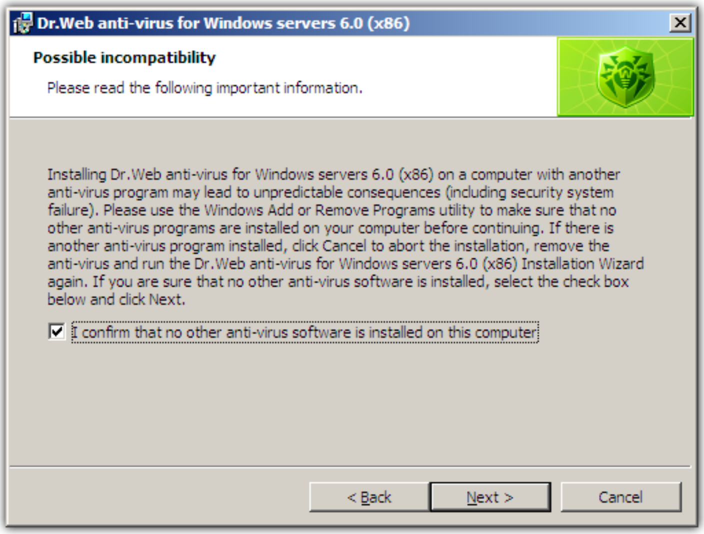
Code	Language
1026	Bulgarian
2052	Chinese (Simplified)
1028	Chinese (Traditional)
1033	English
1061	Estonian
1036	French (France)
1031	German
1032	Greek
1038	Hungarian
1040	Italian
1062	Latvian
1063	Lithuanian
1045	Polish
2070	Portuguese
1049	Russian

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

Regardless of your choice English language will be installed in addition.

Installation in the usual mode

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



Dr.Web anti-virus for Windows servers 6.0 (x86)

Possible incompatibility

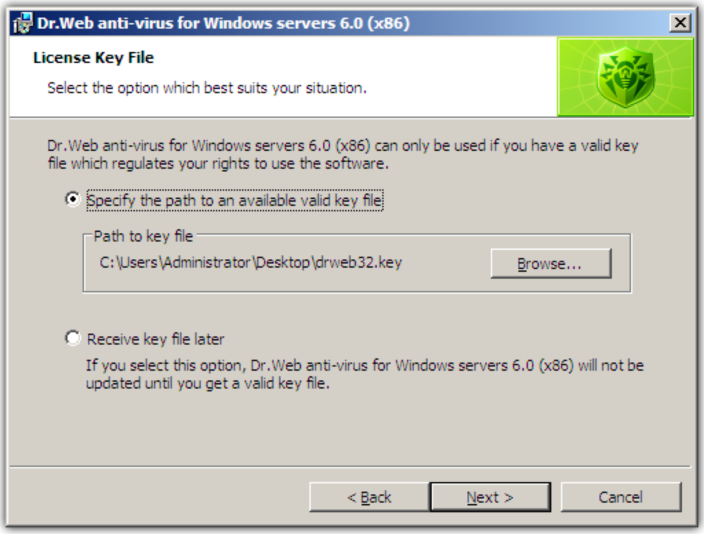
Please read the following important information.

Installing Dr.Web anti-virus for Windows servers 6.0 (x86) on a computer with another anti-virus program may lead to unpredictable consequences (including security system failure). Please use the Windows Add or Remove Programs utility 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 6.0 (x86) Installation Wizard again. If you are sure that no other anti-virus software is installed, select the check box below and click Next.

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

4. 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 6.0 (x86)

License Key File

Select the option which best suits your situation.

Dr.Web anti-virus for Windows servers 6.0 (x86) can only be used if you have a valid key file which regulates your rights to use the software.

● Specify the path to an available valid key file

Path to key file

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

○ Receive key file later

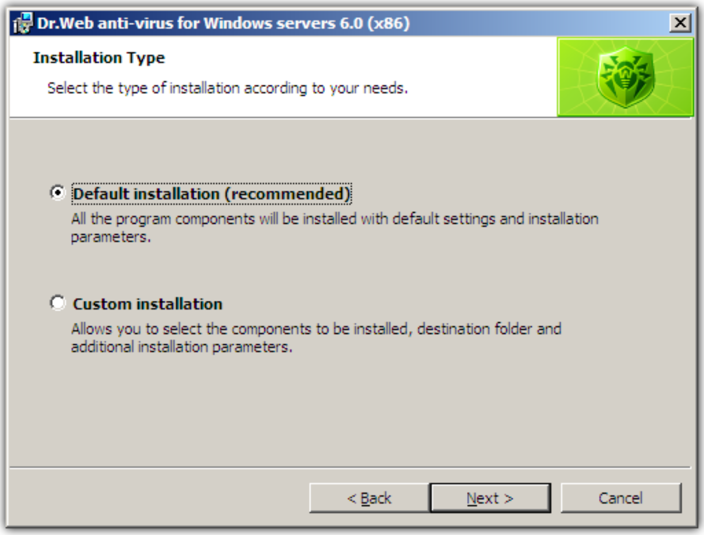
If you select this option, Dr.Web anti-virus for Windows servers 6.0 (x86) will not be updated until you get a valid key file.

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 Windows servers** key file. The key file should have the **.key** extension. If the key file is inside an archive, use an archiver to extract it.

5. The installation wizard will let you choose the type of installation. **Default Installation** implies installation of all components and all secondary programs automatically up to step 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.



Installation Type

Select the type of installation according to your needs.

● Default installation (recommended)

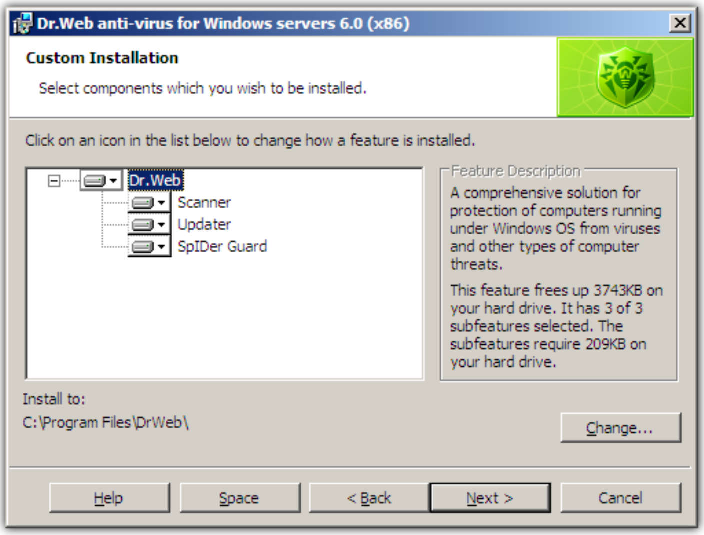
All the program components will be installed with default settings and installation parameters.

○ 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**.

6. 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 6.0 (x86)

Custom Installation

Select components which you wish to be installed.

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

- Dr.Web
  - Scanner
  - Updater
  - SpIDer Guard

Feature Description

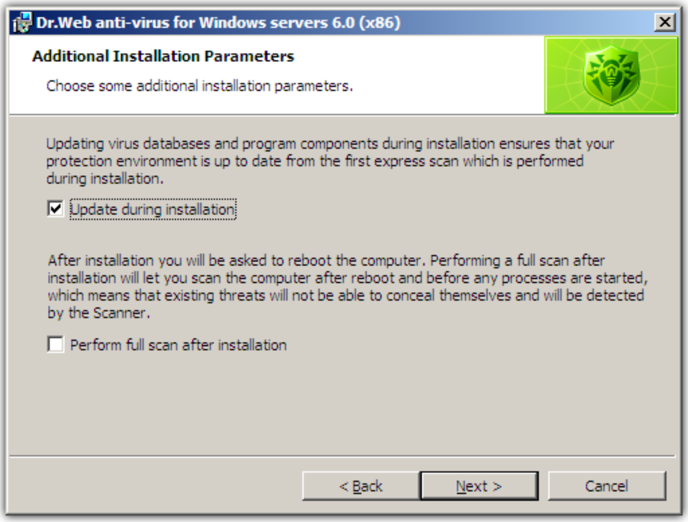
A comprehensive solution for protection of computers running under Windows OS from viruses and other types of computer threats.

This feature frees up 3743KB on your hard drive. It has 3 of 3 subfeatures selected. The subfeatures require 209KB on your hard drive.

Install to:
C:\Program Files\DrWeb\

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

7. The window for selecting which shortcuts to **Dr.Web Anti-virus for Windows servers** should be created will open. Select the necessary options and click **Next**.
8. The window for adjusting some additional parameters of installation will open. Select the **Update during installation** check box to download the latest virus databases during installation. Select the **Perform full scan after installation** check box to check the file system after your computer is rebooted at the end of the installation.



Dr.Web anti-virus for Windows servers 6.0 (x86)

Additional Installation Parameters

Choose some additional installation parameters.

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

☑ Update during installation

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

☐ Perform full scan after installation

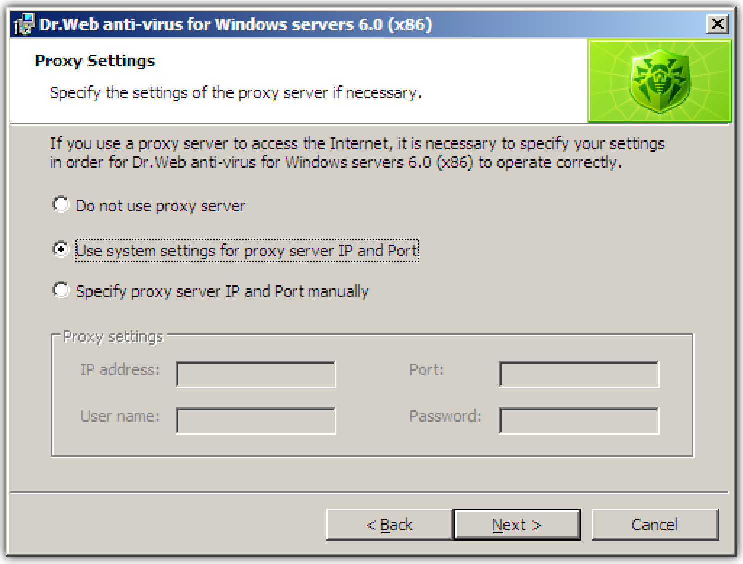
Click **Next**.

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

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

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

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



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 6.0 (x86) to operate correctly.

○ Do not use proxy server

● Use system settings for proxy server IP and Port

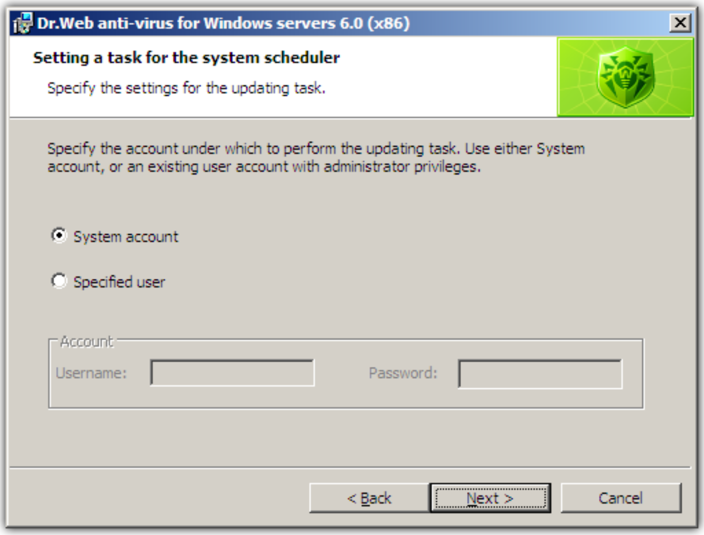
○ Specify proxy server IP and Port manually

Proxy settings

IP address: Port:

User name: Password:

10. Specify the account under which to perform the upgrading task.



Dr.Web anti-virus for Windows servers 6.0 (x86)

Setting a task for the system scheduler

Specify the settings for the updating task.

Specify the account under which to perform the updating task. Use either System account, or an existing user account with administrator privileges.

● System account

○ Specified user

Account

Username:

Password:

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

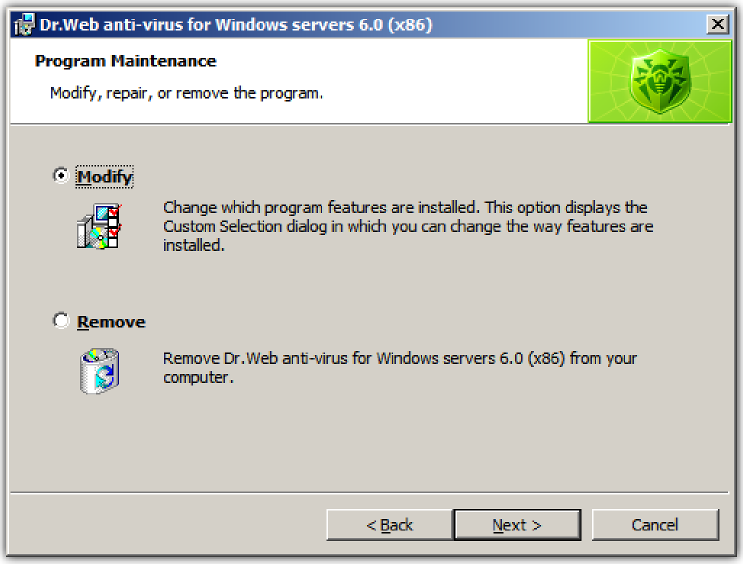
Scanner is not compatible with Windows Blinds (an application for adjusting Windows GUI). For correct operation of **Dr.Web Anti-virus for Windows servers** it is necessary to disable changing of the **Dr. Web** interface in the Windows Blinds settings. To do this, add drweb32w.exe to the list of excluded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

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

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

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

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



Dr.Web anti-virus for Windows servers 6.0 (x86)

Program Maintenance

Modify, repair, or remove the program.

● Modify

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

○ Remove

Remove Dr.Web anti-virus for Windows servers 6.0 (x86) from your computer.

In this window:

1. To change the set of installed components select **Modify** and click **Next**. The Custom Installation window will open. To remove all the components select **Remove**.
2. During removal of **Dr.Web Anti-virus for Windows servers** or changing the set of installed components it is necessary to disable **Self Protection**. To do this, enter the digits shown on the picture.

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**.

Getting Started

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

- the **Scanner for Windows** environment (GUI and console versions)
- **SpIDer Guard**
- **SpIDer Agent**

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

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

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

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

An advantage of the program is uninterrupted control of the virus situation during the whole PC runtime. Besides, some viruses can only be detected by the guard through their specific activity. This component is not included into **Dr.Web for Windows Server**.

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

- scan the PC's file system with the default (maximum) scanning detail settings;
- keep default settings of **SpIDer Guard**;
- perform a periodic complete scan of the PC, coordinated with the time of the virus database updates (at least once a week);
- immediately perform a complete scan in case **SpIDer Guard** was temporary disabled and the PC was connected to the Internet or files were downloaded from removable media.

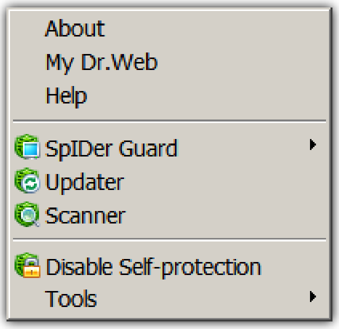
⚠ Anti-virus protection can only be effective if you update the virus databases and other files of the program regularly (preferably every hour). For more information read Automatic Updating of the Virus Databases and Other Files of the Program.

SpIDer Agent

After installing **Dr.Web Anti-virus for Windows servers** a **SpIDer Agent** icon is added to the taskbar notification area.

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

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



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

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

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

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

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

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

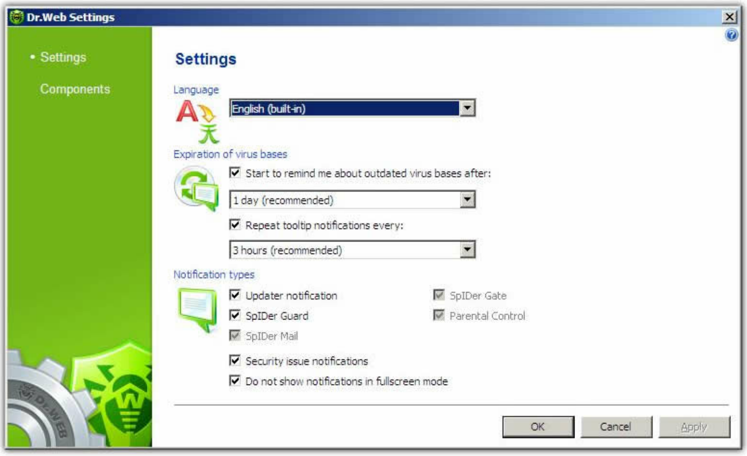
To disable self-protection:

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

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

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

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



Settings

Language

English (built-in)

Expiration of virus bases

☑ Start to remind me about outdated virus bases after:

1 day (recommended)

☑ Repeat tooltip notifications every:

3 hours (recommended)

Notification types

☑ Updater notification

☑ SpIDer Guard

☑ SpIDer Mail

☑ SpIDer Gate

☑ Parental Control

☑ Security issue notifications

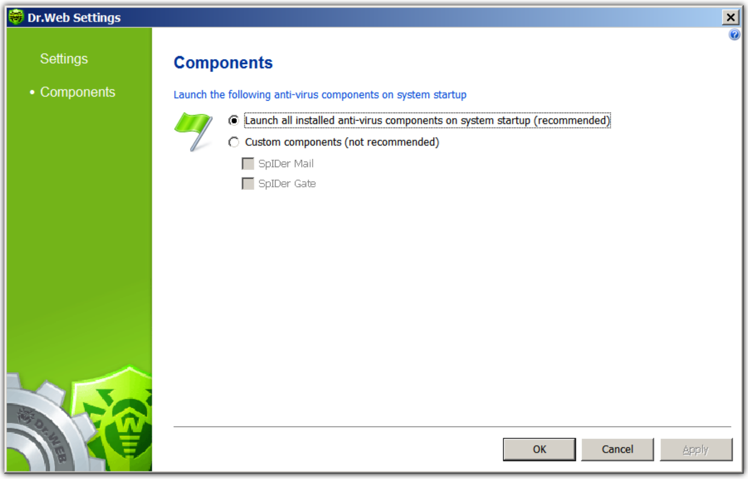
☑ Do not show notifications in fullscreen mode

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

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

On the **Components** page you can choose one of the following:

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


Dr.Web Settings

Components

Launch the following anti-virus components on system startup

● Launch all installed anti-virus components on system startup (recommended)

○ Custom components (not recommended)

□ SpIDer Mail

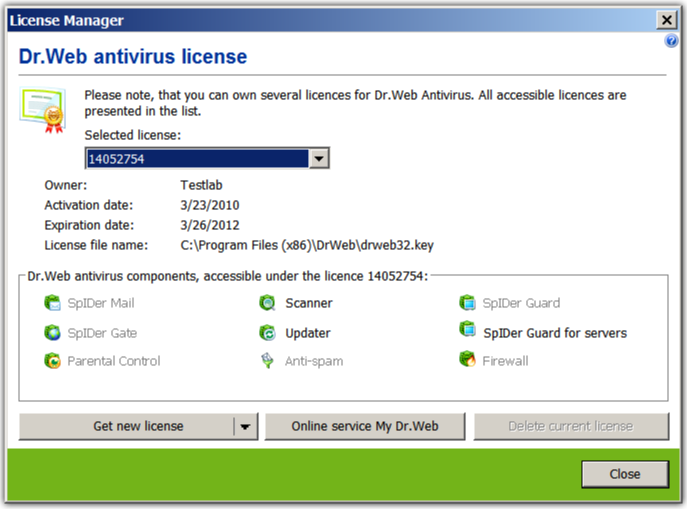
□ SpIDer Gate

- **Scheduler.** This command displays the standard Windows Scheduler task which determines the **Dr.Web® Anti-virus for Windows servers** updating schedule.
- **Quarantine** (see Quarantine);
- to report generation.

Before contacting **Doctor Web technical support**, generate the report on your OS and **Dr.Web** operation. For parameters adjustment, in the opened window click **Special parameters report forming**. The report will be stored as an archive in the DoctorWeb subfolder of the %USERPROFILE% directory.

License Manager

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



License Manager

Dr.Web antivirus license

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

Selected license: 14052754

Owner: Testlab
Activation date: 3/23/2010
Expiration date: 3/26/2012
License file name: C:\Program Files (x86)\DrWeb\drweb32.key

Dr.Web antivirus components, accessible under the licence 14052754:

Selected **Dr.Web Anti-virus for Windows 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 **Doctor Web** web site. This page gives information about your license (period of usage, serial number), allows to renew your license, contact Technical Support, etc.

To add a key file

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

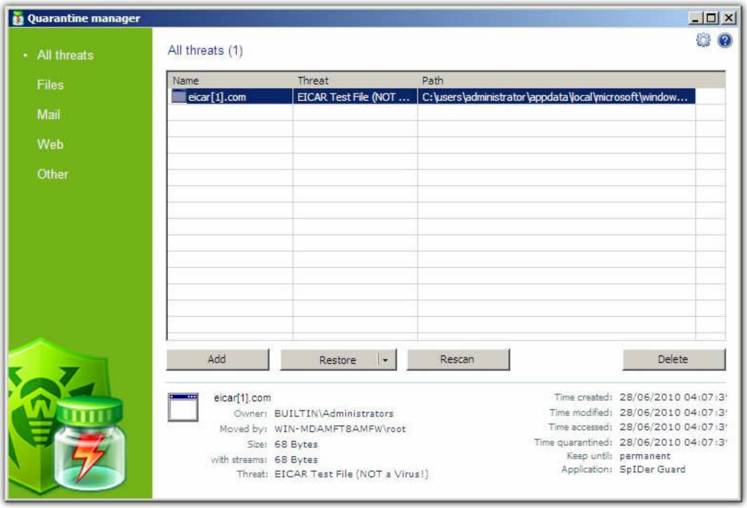
3. **Dr.Web Anti-virus for Windows servers** will automatically start to use a key file.

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

Quarantine

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

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



Name	Threat	Path
eicar[1].com	EICAR Test File (NOT ...	C:\users\administrator\appdata\local\microsoft\window...

eicar[1].com
Owner: BUILTIN\Administrators
Moved by: WIN-MDAMFT8AMFW\root
Size: 68 Bytes
with streams: 68 Bytes
Threat: EICAR Test File (NOT a Virus!)

Time created: 28/06/2010 04:07:3
Time modified: 28/06/2010 04:07:3
Time accessed: 28/06/2010 04:07:3
Time quarantined: 28/06/2010 04:07:3
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 Windows 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.
- **Remove** – delete the file from the quarantine and from the system.

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

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

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

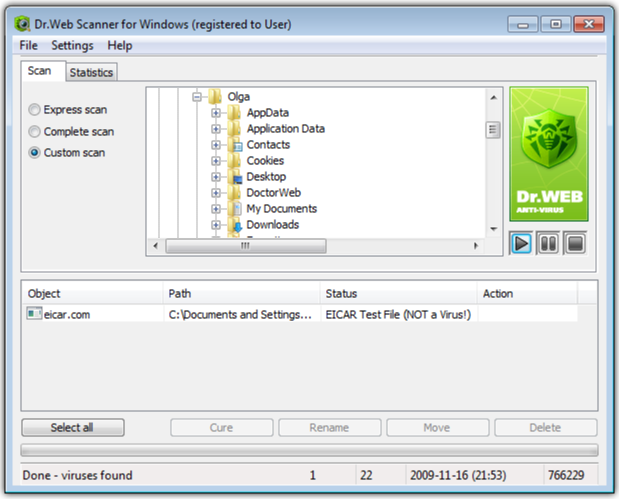
- In the **Set quarantine size** section you can configure the amount of disk space for **Quarantine** folder.
- In the **View** section, you can set the **Show backup files** flag to display backup copies of **Quarantine** files in the object's table.

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

Using Dr.Web Scanner for Windows

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

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



○ Express scan
○ Complete scan
● Custom scan

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

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

Launching Scanner. General Information.

If your system hasn't been scanned for 7 days, a corresponding notification appears (see SpIDer Agent).

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

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

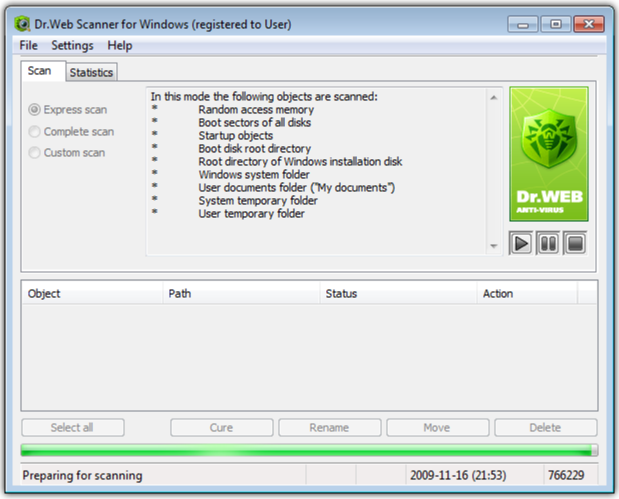
To launch the Scanner do one of the following:

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

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

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

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



● Express scan
○ Complete scan
○ Custom scan

```
In this mode the following objects are scanned:
*         Random access memory
*         Boot sectors of all disks
*         Startup objects
*         Boot disk root directory
*         Root directory of Windows installation disk
*         Windows system folder
*         User documents folder ("My documents")
*         System temporary folder
*         User temporary folder
```

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

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

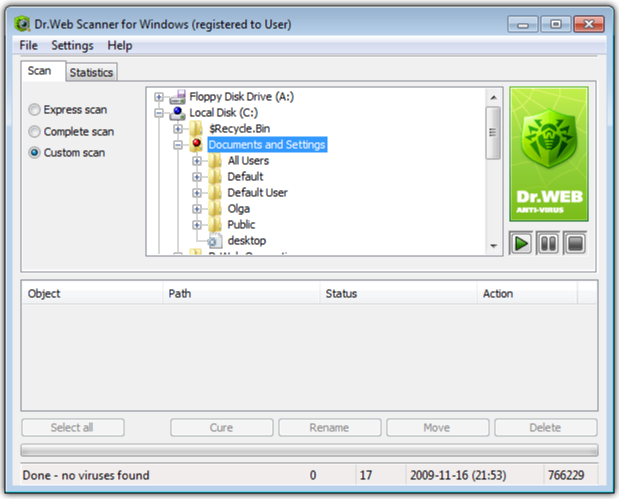
There are 3 scanning modes: **Express scan**, **Complete scan** and **Custom scan**. Depending on the selected mode, either a list of objects which will be scanned or a file system tree is displayed at the center of the window.

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

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

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

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



Dr.Web Scanner for Windows (registered to User)

○ Express scan
○ Complete scan
● Custom scan

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

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

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

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

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

If express or complete scanning mode is set, **Scanner** will define, whether the HOSTS-file (the text file which contains a database of domain names and is used at their translation in network addresses) has been changed. The HOSTS-file can be changed by malicious software (for example, on purpose to redirect the user on a certain web site). In case the HOSTS-file has been changed, **Scanner** will suggest to restore its initial condition. It will allow to eliminate unapproved change of the file by malicious software.

Actions Upon Detection of a Virus

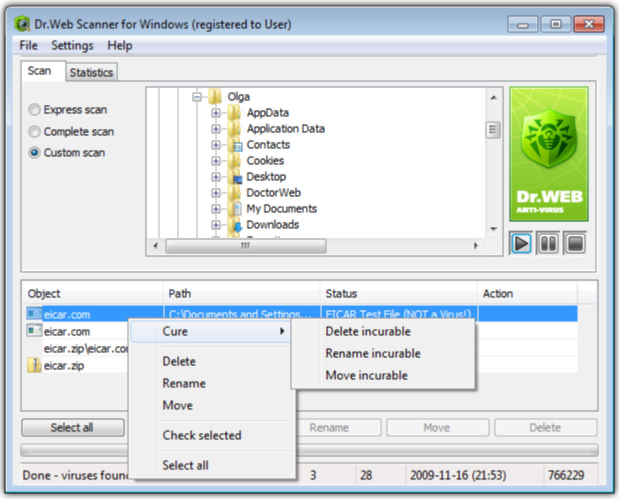
By default, if a known virus or a suspicious object is detected, **Scanner** informs you about it in the report field located at the bottom of the **Scan** tab. Infected processed in computer memory are terminated automatically. Trojan programs are deleted upon detection.

To apply actions to detected objects:

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

> You can specify an action either for all objects or for specific objects in the report list. To select all objects click the **Select All** button. To select objects in the report list the following keys and combinations of keys are additionally used:
>
> - [Insert] - to select an object.
> - [CTRL+A] - to select all objects.
> - the asterisk button [*] on numeric keyboard - to select or deselect all.

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



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

Done - viruses foun 3 28 2009-11-16 (21:53) 766229

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

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

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

The **Delete** action means that the infected object is deleted.

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

For suspicious objects curing is impossible.

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

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

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

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

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

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

Adjusting Scanner Settings

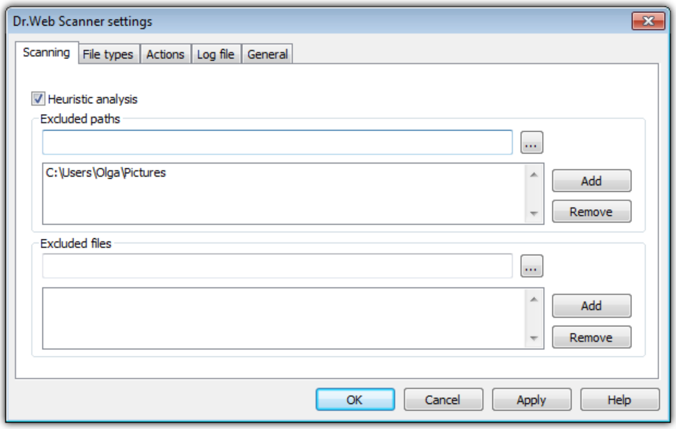
It is recommended for **Scanner** to be run by a user with administrator privileges because files to which unprivileged users have no access (including system folders) are not scanned.

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

To modify the Scanner settings:

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

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



☑ Heuristic analysis

Excluded paths

C:\Users\Olga\Pictures

Excluded files

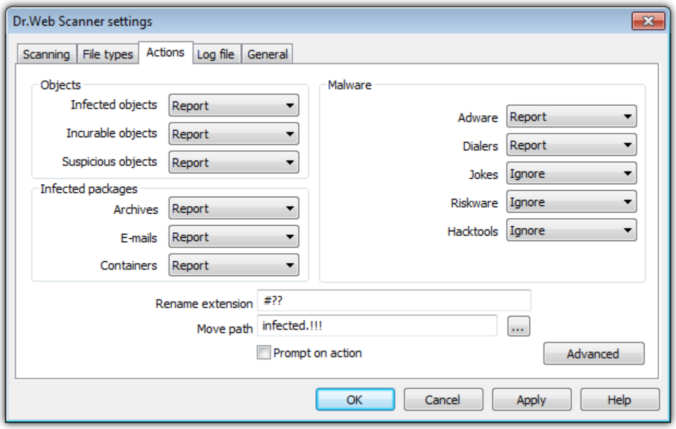
2. Make the necessary changes and click **Apply** when switching to another pane.
3. For more detailed information on the settings specified in each tab use the **Help** button. Also, for the majority of settings specified in the panes, a context help feature is available which is activated by right-clicking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

The most frequent changes in default settings are described below.

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

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

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



Objects
Infected objects: Report
Incurable objects: Report
Suspicious objects: Report

Infected packages
Archives: Report
E-mails: Report
Containers: Report

Malware
Adware: Report
Dialers: Report
Jokes: Ignore
Riskware: Ignore
Hacktools: Ignore

Rename extension: #??
Move path: infected.!!!
□ Prompt on action

2. In the **Infected objects** drop-down list, select the program’s action upon detection of an infected object.
3. Select the program’s action upon detection of an incurable object in the **Incurable objects** drop-down list. The range of actions is the same as those described above but the **Cure** action is not available.
4. In the **Suspicious objects** drop-down list select the program’s action upon detection of a suspicious object (fully similar to the previous paragraph).

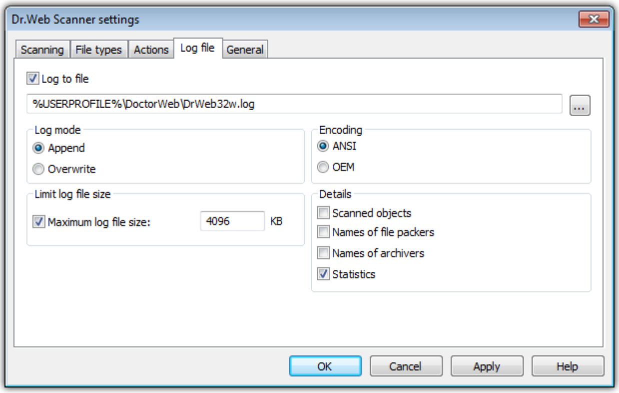
It is recommended to keep the default **Report** action.

5. Similar actions should be specified for detection of objects

containing Adware, Dialers, Jokes, Riskware and Hacktools.

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

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



☑ Log to file

%USERPROFILE%\DoctorWeb\DrWeb32w.log

Log mode
● Append
○ Overwrite

Encoding
● ANSI
○ OEM

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

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

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

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

Command Line Scanning Mode

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

The launching command syntax is as follows:

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

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

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

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

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

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

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

/cu – cure infected objects.

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

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

/go – no prompts on actions should be generated.

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

DrWebWcl Console Scanner can be used with the same parameters. To do this, type the **drwebwcl** command name instead of **drweb32w**.

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

DWScancl Console Scanner

Dr.Web Anti-virus for Windows servers also includes **DWScancl Console Scanner**. In contrast to **DrWebWcl Console Scanner**, **DWScancl Console Scanner** is designed for multiprocessors and provides advanced settings (larger amout of switches).

⚠ **DWScancl Console Scanner** moves suspicious files not to the infected.!!! folder, but to **Quarantine**.

The launching command syntax is as follows:

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

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

All switches are listed in Appendix A.

SpIDer Guard for Windows

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

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

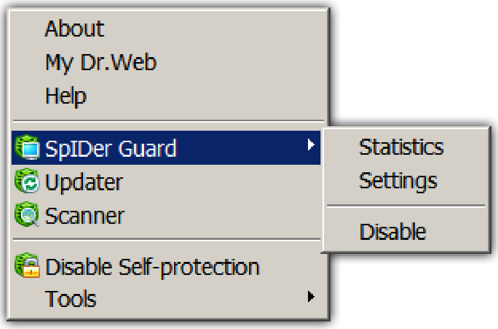
By default, upon detection of infected objects **SpIDer Guard** supplied with **Dr.Web Anti-virus for Windows servers** acts according to actions set on Actions tab.

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.

Managing the Guard

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



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

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

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

Main Parameters of the SpIDer Guard

The main adjustable parameters of **SpIDer Guard** are in the **Settings** panel. To receive help on parameters specified 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.

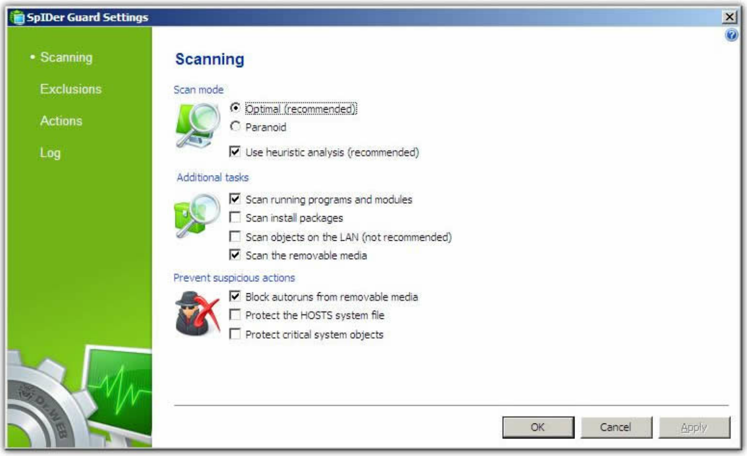
Scanning Page

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).

⚠ If any problems occur during installation of important Microsoft updates, clear the **Protect critical system objects** checkbox.



SpIDer Guard Settings

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 the removable media

Prevent suspicious actions

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

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

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

Exclusions 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 the **Browse** button to the right and select the object in a standard file browsing window.

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

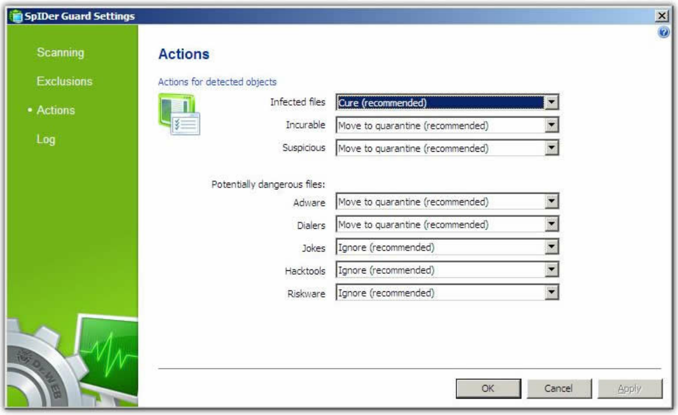
Actions Page

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**.

To change the default actions in SpIDer Guard:

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



Actions

Actions for detected objects

Infected files: Cure (recommended)
Incurable: Move to quarantine (recommended)
Suspicious: Move to quarantine (recommended)

Potentially dangerous files:
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. Other actions with moved files are described in Actions Upon Detection of a Virus chapter.

4. In the **Suspicious objects** drop-down list choose the program's action upon detection of a suspicious object. **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.

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

During **Dr.Web Anti-virus for Windows servers** installation a task to update the virus databases and other files of the package is automatically created in the system scheduler (the Scheduled Tasks directory). To view the parameters of this task, select **Scheduler** in the **Tools** submenu of **SpIDer Agent** context menu, that will open Task Scheduler.

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

Automatic Updating

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

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

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

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

General Information

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

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

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

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

Thus, the structure of the virus databases will be as follows:

- the main virus database – drwebase.vdb
- extensions of the main virus database – drw50000.vdb, drw50001.vdb, drw50002.vdb, drw50003.vdb and drw50004.vdb
- weekly add-ons – drw50005.vdb, drw50006.vdb etc.
- hot add-on – drwtoday.vdb
- accumulative add-on – drwdaily.vdb
- additional databases of malicious programs – drwnasty.vdb and drwrisky.vdb
- cumulative add-ons to malicious programs database –

dwn50001.vdb, dwn50002.vdb etc. and dwr50001.vdb, dwr50002.vdb etc.

- hot add-ons of the additional databases of malicious programs – dwntoday.vdb and dwrtoday.vdb

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

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

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

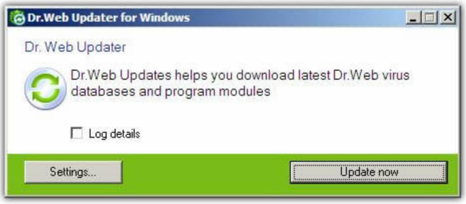
Launching and Using the Automatic Updating Utility

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

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

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

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

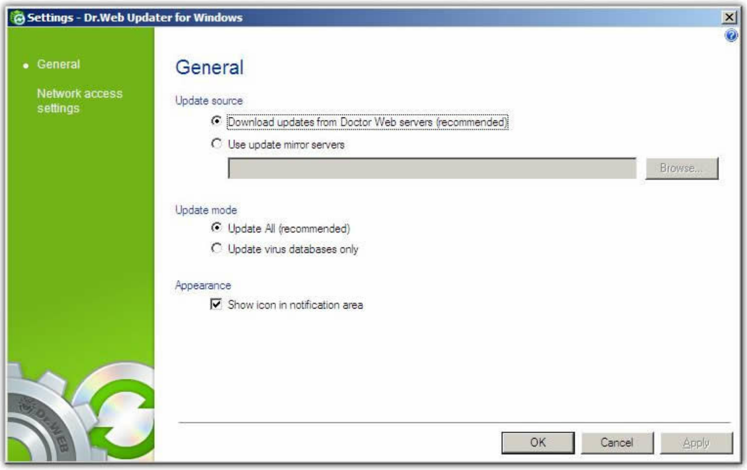


Dr.Web Updates helps you download latest Dr.Web virus databases and program modules

□ Log details

Settings

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



Settings - Dr.Web Updater for Windows

General

Update source

● Download updates from Doctor Web servers (recommended)

○ Use update mirror servers

Update mode

● Update All (recommended)

○ Update virus databases only

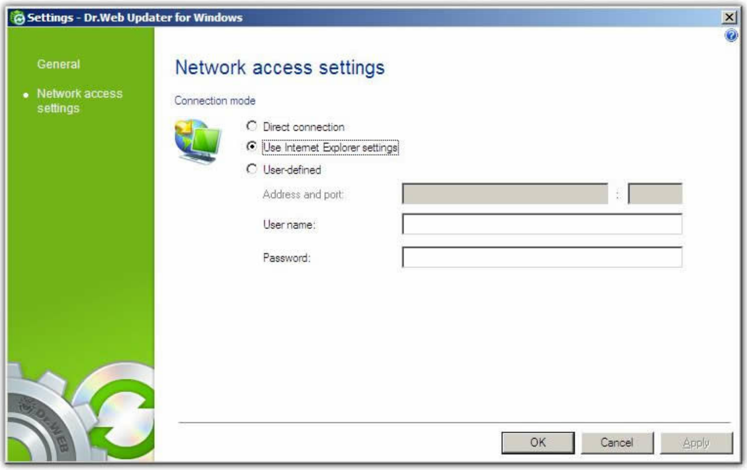
Appearance

☑ Show icon in notification area

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

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

In the **Network access settings** page you can set up network access.



Settings - Dr.Web Updater for Windows

Network access settings

Connection mode

○ Direct connection
● Use Internet Explorer settings
○ User-defined

Address and port: :

User name:

Password:

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

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

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

Launching Update

When launching update, the program checks the presence of the license key file in the installation folder. If no key file is found, the updating is impossible.

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

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

After the key file is successfully checked, the updating is performed.

The program automatically downloads all updated files, according to your version of **Dr.Web Anti-virus for Windows servers**, and, if your subscription terms allow, the new program version (if it is released).

The **Scanner** can use the updated databases after the next restart. **SpIDer Guard** periodically checks the state of the databases and starts to use updated databases automatically.

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

Appendices

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

Introduction

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

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

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

The Scanner command line parameters

/? – display short help on the program and launch scanning.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

/ML – scan files of e-mail format (UUENCODE, XXENCODE, BINHEX and MIME). As it is specified (**/ML**) the switch instructs to inform a user if an infected or suspicious object is detected in a mail archive. If the switch is supplemented with the D, M or R modifier, other actions are taken: **/MLD** - delete; **/MLM** – move (by default, to the infected.!!! directory); **/MLR** – rename (by default, the first symbol of extension is replaced by the # character). The switch may end with the N modifier. In this case the "Mail archive" message will not be displayed.

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

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

/NR – do not create a log file.

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

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

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

/PR – prompt for confirmation before action.

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

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

/SCP:<*n*> – sets the priority of the scanning process, where <n> is a number ranging from 1 to 50.

/SD – scan subdirectories.

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

/SO – enables sounds.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The DWScancl Console Scanner parameters

/AR – test archive files.

/AC – test containers.

/AFS – use forward slash to separate pathes in archive.

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

/ARL:<*level*> – maximum archive level.

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

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

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

/BI – show virus bases info.

/DR – recursive scan directory.

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

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

/FR:<*regexpr*> – scan files matched expression.

/FM:<*masks*> – scan files matched 'masks'.

/H or **/?** – show this message.

/HA – use heuristic analysis.

/KEY:<*keyfile*> – use `keyfile' as activation key.

/LN – resolve shell links.

/LS – use LocalSystem account rights.

/MA – test e-mail like files.

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

/NB – don't backup curing/deleting files.

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

/NT – test NTFS streams.

/OK – show OK for clean files.

/P:<*prio*> – test priority: O,L,N,H,M.

/PAL:<*level*> – maximum pack level (1000).

/RA:<*file.log*> – add report into file.log.

/RP:<*file.log*> – write report into file.log.

/RPC:<*secs*> – Dr.Web SE connection timeout.

/RPCD – use dynamic RPC identification.

/RPCE – use dynamic RPC endpoint.

/RPCE:<*name*> – use specified RPC endpoint.

/RPCH:<*name*> – use specified host name for remote call.

/RPCP:<*name*> – use specified RPC protocol (lpc,np,tcp).

/QL – list quarantined files on all disks.

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

/QR[:[d][:p]] – delete quarantined files on drive 'd' (letter) older than 'p' days (number).

/QNA – double quote file names always.

/REP – go follow reparse points.

/SCC – show content of compaund objects.

/SCN – show container name.

/SPN – show packer name.

/SLS – show log on screen.

/SPS – show progress on screen.

/SST – show file scan time.

/TB – test boot sectors.

/TM – test processes in memory.

/TS – test system startup processes.

/TR – test system restore points directories.

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

/WCL – drwebwcl compatible output.

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

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

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

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

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

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

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

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

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

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

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

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

actions: Cure, Delete, Quarantine, Ignore, Report

Automatic Updating Module command line parameters

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

/DBG – detailed log.

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

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

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

/GO – package operation mode, without dialogs.

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

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

/NR – do not create a log file.

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

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

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

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

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

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

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

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

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

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

/UPD – usual updating.

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

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

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

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

- **prompt** – prompt if a reboot is needed after the updating session is finished
- **noprompt** – if necessary, reboot without prompting

- **force** – reboot always (regardless whether it is required for the updating or not)
- **disable** – disable reboot

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

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

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

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

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

Return codes

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

Return code value	Event
0	OK, no virus found
1	known virus detected
2	modification of known virus detected
4	suspicious object found
8	known virus detected in file archive, mail archive or container
16	modification of known virus detected in file archive, mail archive or container

Return code value	Event
32	suspicious file found in file archive, mail archive or container
64	at least one infected object successfully cured
128	at least one infected or suspicious file deleted/renamed/moved

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

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

Appendix B. Adjustable Parameters of Dr.Web Components

Introduction

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

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

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

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

The parameters of the Windows versions of the Scanner and Updater

The following data for every parameter is displayed in columns of the table:

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

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

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

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

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

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

Parameter	Components	Configur. file parameter	Values	Keys
Priority of the scanning process, from 1 to 50	Scanner			/SCP
Heuristic analysis	Scanner	HeuristicAnalysis	Yes / No	/HA
Scan memory	Scanner	TestMemory	Yes / No	/TM
Scan autorun files	Scanner	TestStartup	Yes / No	/TS
Scan boot sectors	Scanner	TestBootSectors	Yes / No	/TB
Scan subfolders	Scanner	ScanSub Directories	Yes / No	/SD
Prompt on multiple floppies	Scanner	PromptFloppy	Yes / No	/PF
Archives	Scanner	CheckArchives	Yes / No	/AR
Mail files	Scanner	CheckEMailFiles	Yes / No	/ML
Max size of unpacked archive to check, KB	Console Scanner	MaxFileSizeTo Extract	(empty)	
Max compression ratio for archive	Console Scanner	MaxCompression Ratio	(empty)	
Threshold for MaxCompressionRatio, KB	Console scanner	Compression CheckThreshold	(empty)	
List of extensions	Scanner	FilesTypes	(see below the Table)	

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

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

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

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

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

Parameter	Components	Configur. file parameter	Values	Keys
Names of archivers in report	Scanner	LogArchived	Yes / No	
Statistics in log file	Scanner	LogStatistics	Yes / No	
Maximum log file size	Scanner, Updating module	LimitLog	Yes / No	
Log size limit, KB	Scanner, Updating module	MaxLogSize	512 8192	
Close the window after sessions	Scanner, Updating module		Yes / No	/QU
Wait for a key to be pressed as soon as scanning is complete (in case a virus is detected)	Console scanner	WaitAfterScan	(On / Off)	/WA
Operate in packet mode	Scanner, Updating module		(On / Off)	/GO
Prohibit interruption by a user	Scanner		(On / Off)	/NS
Scan once a day	Scanner		(On / Off)	/DA
Scan the explicitly selected objects only	Scanner-GUI		(On / Off)	/SHELL

Parameter	Components	Configur. file parameter	Values	Keys
Do not open windows (stealth mode)	Scanner-GUI		(On / Off)	/ST
Use alternative configuration file. Do not use any configuration file	Scanner, Updating module		(On / Off)	/INI /NI
Use own swap file	Scanner	UseDiskForSwap	Yes / No	
Display progress bar	Scanner	ShowProgress Bar	Yes / No	
Sounds	Scanner, Updating module	PlaySounds	Yes / No	/SO
Alert (sound)	Scanner	AlertWav	alert.wav	
Cured (sound)	Scanner	CuredWav	cured. wav	
Deleted (sound)	Scanner	DeletedWav	deleted. wav	
Renamed (sound)	Scanner	RenamedWav	renamed. wav	
Moved (sound)	Scanner	MovedWav	moved. wav	
Finish (sound)	Scanner	FinishWav	finish.wav	
Error (sound)	Scanner, Updating module	ErrorWav	error.wav	
Autosave settings	Scanner	AutoSave Settings	Yes / No	/SS
Use registry settings	Scanner-GUI		(On / Off)	

Parameter	Components	Configur. file parameter	Values	Keys
Scan priority	Scanner	ScanPriority	25 50	
Language	Scanner, Updating module	LngFileName	ru-drweb. dwl	/LNG
Proxy mode	Scanner-GUI (the updating module settings)	UpdateProxy Mode	direct ieproxy userproxy	/UPM
Update the virus databases and drweb32.dll kernel only	Updating module	UpdateVirus BasesOnly	Yes / No	/UVB
Download all files from the update list	Updating module	UpdateAllFiles	Yes / No	/UA
Reboot mode at updating	Updating module	UpdateReboot Mode	prompt noprompt force disable	/URM
Log details	Updating module		(On / Off)	/DBG

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

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

Appendix C. Malicious Programs and Methods of Neutralizing Them

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

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

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

Classification of malicious programs and other computer threats.

Computer viruses

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

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

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

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

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

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

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

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

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

Computer worms

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

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

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

Trojan horses (Trojans)

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

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

Rootkits

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

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

Hacktools

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

Spyware

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

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

Adware

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

Joke programs

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

Dialers

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

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

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

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

- **Brute force attack** – performed by a special Trojan horse program, which uses its inbuilt password dictionary or generates random symbol strings in order to figure out the network access password by trial-and-error.
- **DoS-attack** (denial of service) or **DDoS-attack** (distributed denial of service) – a type of network attack, which verges on terrorism. It is carried out via a huge number of service requests sent to a server. When a certain number of requests is received (depending on the server’s hardware capabilities) the server becomes unable to cope with them and a denial of service occurs. DDoS-attacks are carried out from many different IP-addresses at the same time, unlike DoS-attacks, when requests are sent from one IP-address.
- **Mail bombs** – a simple network attack, when a big e-mail (or thousands of small ones) is sent to a computer or a company’s mail server, which leads to a system breakdown. There is a special method of protection against such attacks used in the Dr.Web products for mail servers.
- **Sniffing** – a type of network attack also called “passive tapping of network”. 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 malicious programs

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

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

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

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

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

Appendix D. Naming of Viruses

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

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

Prefixes

Affected operating systems

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

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

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

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

Macrovirus prefixes

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

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

Development languages

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

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

The following prefix also refers to development language:

- Java - viruses designed for the Java virtual machine

Script-viruses

Prefixes of viruses written in different scrip languages:

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

Trojan horses

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

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

Tools for network attacks

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

Malicious programs

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

Miscellaneous

- Exploit - a tool exploiting known vulnerabilities of an 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 E. Corporate network protection by Dr.Web® Enterprise Suite

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

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

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

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

Dr.Web ES allows the following:

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

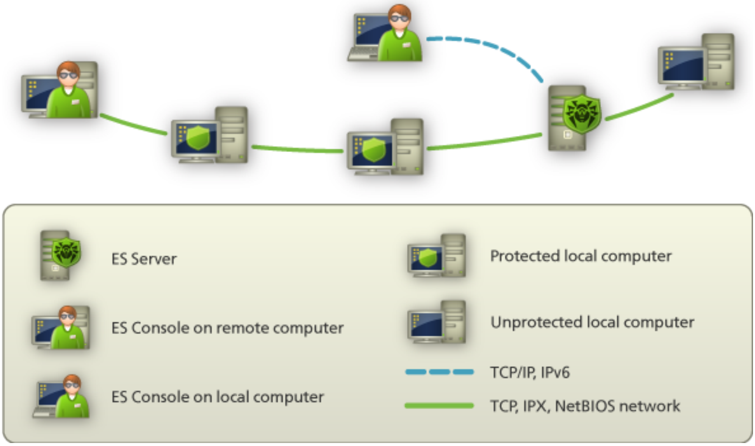
Dr.Web ES allows both to leave a user with the right to modify the settings and to administrate the anti-virus package of his computer, and to flexibly restrict modifications, or even forbid them at all.

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

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

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

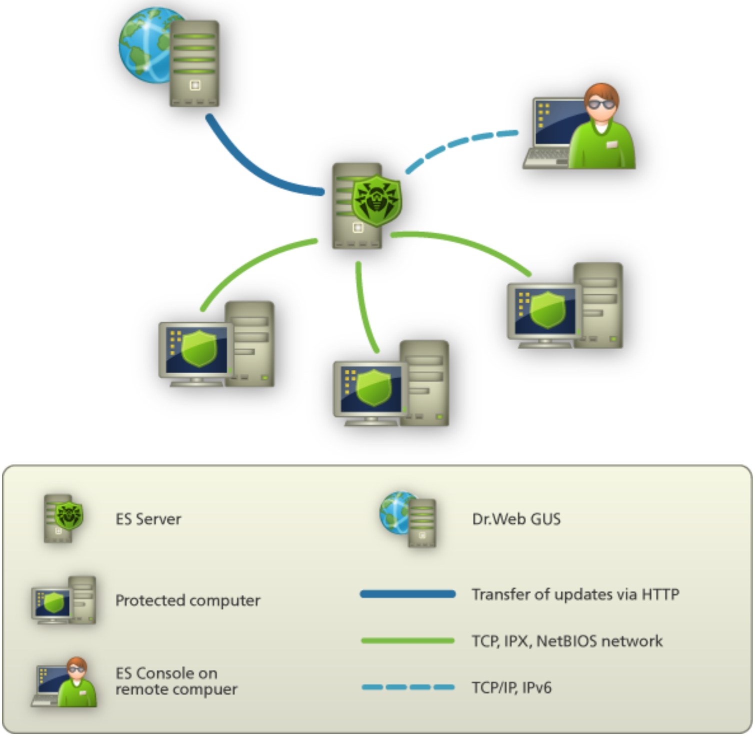
The illustration below describes the general scheme of the fragment of the local network where the protecting anti-virus network is organized.


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

Physical structure of the anti-virus network

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

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



Logical structure of the anti-virus network

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

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

updating is performed

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Dr.Web AV-Desk allows the following:

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

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

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

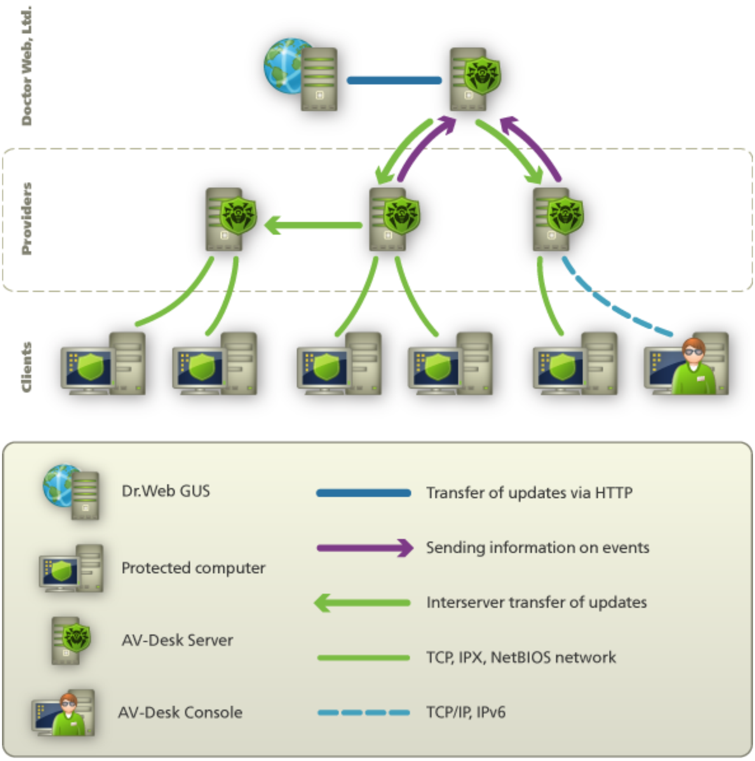
  - view general information about the **AV-Desk** server;

  - read the documentation;

  - view the repository.

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

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


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

Physical structure of the anti-virus network

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

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

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

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

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

Appendix G. 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/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in **Dr.Web** knowledge database at http://wiki.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