



**Dr.WEB®**

**Anti-virus**  
for Symbian OS

**User Manual**

Defend what you create

**© 2003-2012 Doctor Web. All rights reserved.**

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

**TRADEMARKS**

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

**DISCLAIMER**

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

**Dr.Web for Symbian**

**Version 6.00.2**

**User Guide**

**06.04.2012**

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

Web site: [www.drweb.com](http://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

<b>Chapter 1. Introduction</b>	<b>6</b>
Document Conventions	7
Main Features	8
Distribution Kit	8
<b>Chapter 2. Licensing</b>	<b>9</b>
License Key File	9
Acquire License Key File	10
Use License Key File	12
Licence Update	12
<b>Chapter 3. Installation</b>	<b>13</b>
System Requirements	13
Install Application	13
Uninstall Application	15
<b>Chapter 4. Getting Started</b>	<b>16</b>
Launch and Exit the Application	16
Interface	17
Help System	18
<b>Chapter 5. Program Functions</b>	<b>19</b>
Constant Anti-Virus Protection	19
On-Demand Scanning	21
Malicious Objects Neutralization	24
Quarantine	25
Anti-Spam	26



<b>Black and White Lists</b>	<b>28</b>
<b>Update</b>	<b>29</b>
<b>Logging</b>	<b>30</b>
<b>Appendices</b>	<b>32</b>
<b>Appendix A. Contacting Support</b>	<b>32</b>
<b>Index</b>	<b>33</b>



## Chapter 1. Introduction

Thank you for purchasing **Dr.Web for Symbian**. This anti-virus solution offers reliable protection of mobile phones and communicators working under the Symbian Series 60 operating system from various virus threats designed specifically for mobile devices, and spam. The program employs the most advanced developments and technologies of **Doctor Web** aimed at detection and neutralization of malicious objects which may represent a threat to the device operation and information security.


This manual is intended to help users of mobile devices to install and adjust **Dr.Web for Symbian**. It also describes all the basic functions of the application.

The appendice contain information on the technical support.



## Document Conventions

The following conventions and symbols are used in this document:

Convention	Description
<b>Bold</b>	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.
<b>Green and bold</b>	Names of Dr.Web products and components.
<u>Green and underlined</u>	Hyperlinks to topics and web pages.
<i>Italic</i>	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.
	A warning about potential errors or any other important comment.



## Main Features

**Dr.Web for Symbian** is a reliable anti-virus solution for users of mobile devices working under the Symbian Series 60 operating system. The application protects devices from information security threats and spam by performing the following functions:

- Constant anti-virus protection of the device in the real-time mode
- Scanning of the whole file system of the device or files and folders selected by user
- Scanning of the files on removable memory cards
- Scanning of the archives and installation files (zip, cab, sis, jar, rar)
- Deletion of the infected objects or their isolation in quarantine
- SMS and calls filtering based on adjustable black and white lists
- Detailed reports on performed scans
- **Dr.Web virus databases** updates via Internet
- Access to context Help from any active application window

**Dr.Web for Symbian** has user-friendly interface and easy customizable settings which help you configure all program options to set up the appropriate protection level.

## Distribution Kit

**Dr.Web for Symbian** can be purchased either from the **Dr.Web** Web shop or from official distributors. For more information on purchasing, visit the **Doctor Web** official web site at <http://estore.drweb.com/>.

The distribution kit of **Dr.Web for Symbian** includes the **DrWebs60.sis** installation file and the **drweb-symbian-s60-en.pdf** file with this guide.



## Chapter 2. Licensing

The *key file* regulates the use rights for the purchased product.

### License Key File

A *key file* has the *.key* extension and contains, among other, the following information:

- Licensed period for the product
- Users number limitation for the license
- Other limitations

There are two types of key files:

- *License key file* is purchased with the **Dr.Web** software and allows purchasers to use the software and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. The file also contains information about the purchaser and seller.
- *Demo key file* is used for evaluation of **Dr.Web** products. It is distributed free of charge and provides full functionality of the software. However demo key files have limited validity period and cannot be renewed.

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

- License is not expired
- The license applies to all components of the product
- Integrity of the license key file is not violated

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



The license key file is secured with digital signature. Do not edit or otherwise modify the file to prevent the license from compromise!

## Acquire License Key File

You can receive a license key file in one of the following ways:

- By e-mail in an archived attachment
- Download it on your device from the **Doctor Web** server via Internet using the License manager
- With the application distribution kit
- On separate media

### To acquire a key file by e-mail

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Enter the serial number which is typed on the registration card.
3. Fill in the registration form.
4. The license key file is archived and sent to the e-mail address you specified in the registration form.
5. Extract the license key file to the computer that will be used for synchronization of your device and **copying** the key file via Nokia PC Suite/Nokia Ovi Suite.

To receive a trial license key file by e-mail, fill in the registration form at <http://download.drweb.com/demoreq/>.



## To download a key file on the device

---



The key file download procedure requires a working connection to the Internet via HTTP. To open the connection, use the built-in GPRS module of your device.

---

If you are using WAP, please contact your mobile operator to inquire about existing connection and download files limitations.

---

1. In the warning window with notification about absence of a valid license key file or in the main window of the programselect **Options** -> **Get key** to launch the License manager.
2. In the **Options** list select the type of the key file that you want to download.

You can download the license or demo key file.

- If you have a serial number, select **Get license key**.
  - If you installed the program in purposes of evaluation, select **Get demo key** and proceed to step 4.
3. Enter the serial number and select **Next**.
  4. Enter your personal data and select **Next**. This information is necessary to receive the key file.
  5. The key file will be downloaded and installed. Select the Internet access point if required. The key file downloading procedure log is displayed on the screen:
    - If the license key is downloaded successfully, select **Finish** to return to the main window of the program.
    - If an error occurred, the error details are displayed.

In this case the key file will be automatically installed and ready to use.

For more information on licensing and types of license key files, visit the **Doctor Web** official web site at <http://www.drweb.com>.



## Use License Key File

If you have obtained the key file by e-mail or it was included into the distribution kit, you should copy it to the special folder on the device to start using it. You can use the Nokia PC Suite/Nokia Ovi Suite software.

### To start using the key file of the device with Dr.Web for Symbian:

1. In the warning window with notification about absence of a valid license key file or in the main window of the program select **Options** -> **Get license**.
2. Select **Copy from file** in the **Options** list.
3. Synchronize your device with the computer where the key file resides and then launch the Nokia PC Suite/Nokia Ovi Suite File Manager.
4. Copy the key file from the computer to the **C:\Data\DrWeb\** folder located on your mobile device using Nokia Phone Browser.
5. Select **Done** on the device.

The key file will be installed and ready to use.

## Licence Update

When license expires, you may need to update the license. The new license then should be registered with the product or the expired license should be renewed if it is supported for your key file. **Dr.Web for Symbian** supports hot license update without stopping or reinstalling the program.

### To update license

Use the key file [acquisition procedure](#). **Dr.Web for Symbian** automatically switches to the new license.



## Chapter 3. Installation

**Dr.Web for Symbian** can be installed on the mobile device either using the Nokia PC Suite/Nokia Ovi Suite software or manually.

### System Requirements

To install and use **Dr.Web for Symbian**, ensure your mobile device works under one of the following operating systems:

- Symbian 9, Series60 3rd Edition, Series60 5th Edition, Symbian<sup>3</sup>, Symbian Belle.



**Dr.Web for Symbian** can be installed only on Nokia devices.

---

The Internet connection is also required for virus databases update procedure.


### Install Application

**Dr.Web for Symbian** can be installed on your mobile device by synchronisation with the PC using the Nokia PC Suite/Nokia Ovi Suite software or by launching the installation file directly on the mobile device.

#### Install application via Nokia PC Suite/Nokia Ovi Suite

1. To install **Dr.Web for Symbian** via Nokia PC Suite/Nokia Ovi Suite synchronize your device with computer and launch Nokia PC Suite/Nokia Ovi Suite Application Installer.
2. Specify the path to the installation file **DrWebs60.sis** located on the computer. In the bottom of the Installer window the information about the selected application is displayed. Click



the Installation button  to send the file and start installation of the program on your device.

3. On the device screen a window with a suggestion to install the application will open. Select **Yes**. Then a window with information on the application (program version, supplier, certificate) will open. Select **Continue**.
4. A window with a suggestion to select the application language will open. You can select English or Russian. Select **Continue**.
5. On the page **Install where?** select the device memory or the memory card for installation of the program.
6. The installation of **Dr.Web for Symbian** on the device starts.
7. On completion of installation click **Done** in the Application Installer window.

### Install application without Nokia PC Suite/Nokia Ovi Suite

1. To install **Dr.Web for Symbian** without Nokia PC Suite/Nokia Ovi Suite, copy the installation file of the program (**DrWebs60.sis**) on the device using the memory card or by connecting the device to the computer.
2. Select in the **Menu** of your device **Tools** -> **Applications Manager**. In the list of applications select **Dr.Web**.
3. Before installation select **Options** -> **Show details** to review the information on the program, its supplier and security certificate. Then select **Options** -> **Install**.
4. Follow the [instructions](#) on installation of the program via Nokia PC Suite/Nokia Ovi Suite starting by step 4.

**Dr.Web for Symbian** is now installed on your device. For further operation of the application you need to [obtain the key file](#).



## Uninstall Application

**Dr.Web for Symbian** can be completely removed from your device.

### To remove the application

1. In the **Menu** of your device select **Tools** -> **Applications Manager**.
2. Select **Dr.Web** in the list of installed applications and then select **Options** -> **Uninstall**.
3. Confirm the removal of the selected application. The application will be removed from the device.



## Chapter 4. Getting Started

This section describes the interface of **Dr.Web for Symbian** and provides step-by-step procedures for launching or exiting the application and accessing Online Help.

### Launch and Exit the Application

#### To launch the application

To launch **Dr.Web for Symbian** in the **Main menu** of your device select **Dr.Web** in the list of settings and installed applications. The main window of the program will open.

#### To exit the application

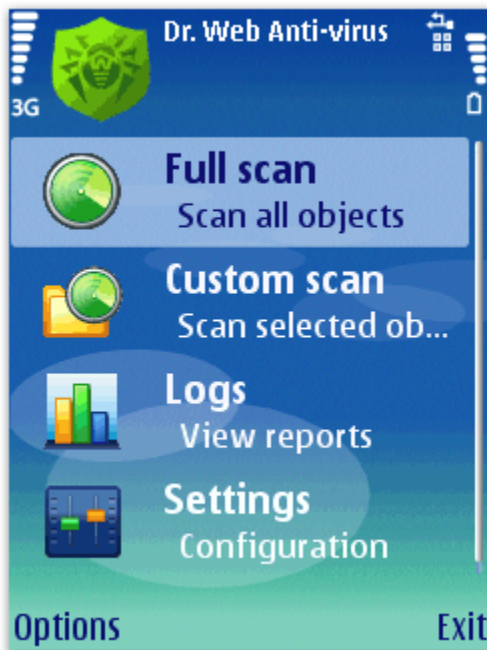
To exit **Dr.Web for Symbian** in the main window of the program (see [Interface](#)) select **Exit**.



## Interface

The main window of **Dr.Web for Symbian** consists of four buttons, which provide access to all the main functions of the application (see [Figure 1](#)):

- **Full scan** – launches the scanning of the whole file system
- **Custom scan** – allows to select the files and folders for scanning
- **View logs** – opens the program logs and the list of quarantine
- **Settings** – opens the list of application settings



**Figure 1. The main window.**



Besides, the main window contains the following option buttons:

- **Exit** – closes the application
- **Options** – opens the list of additional options of application

The program icon at the top part of the main window may provide the following information:

Icon	Comment
	The license key file is missing. For operation of <b>Dr.Web for Symbian</b> you need to <a href="#">acquire the license key file</a> .
	The program virus bases are out of date. You need to <a href="#">update the virus bases</a> .

## Help System

You can access the context help system implemented in **Dr.Web for Symbian** from any active window of the application.

### To access the help system

To obtain help on the active window of the program select **Options -> Help**.



## Chapter 5. Program Functions

This section describes main features of **Dr.Web for Symbian** and provides step-by-step procedures for configuring protection of your device against viruses and spam.

### Constant Anti-Virus Protection

The main function implemented in **Dr.Web for Symbian** is the ability to constantly scan the file system in real-time mode. This function is provided carried out by a component called *file monitor*. It resides in the memory of the device and checks all files as they are created or modified, thus it protects the system against malicious objects.

The monitor can be enabled in the **Settings** -> **Monitor** section. To enable/disable the monitor, select the corresponding value for the **Constant protection** option. Activated, the monitor begins protecting the file system of the device. It remains active even if you close the application.

On security threats detection, a message with information on them is displayed on the device screen. You can open the list of detected threats and choose the actions to apply to neutralize them.

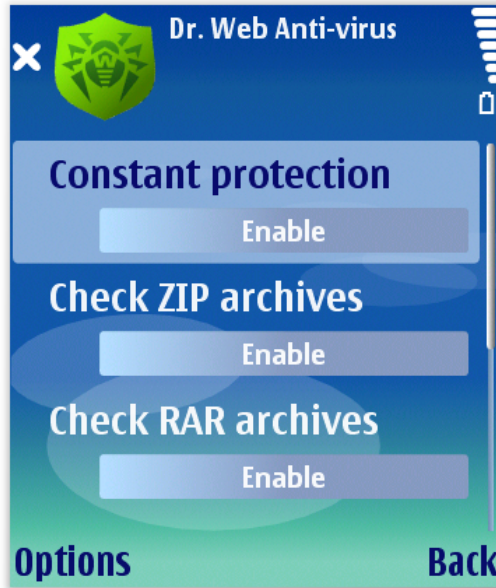
#### To configure monitor

To configure the monitor, select **Settings** -> **Monitor** (see [Figure 2](#)). You can configure the following parameters:

- Enable/disable automatic launch of the file monitor and **Anti-spam** on device reboot and application update by selecting the corresponding value for the **Automatic startup** option.
- Enable/disable scanning of the ZIP, CAB, SIS and RAR archives by selecting the **Enable/Disable** value for the corresponding options.



- Enable/disable monitor debug logging. The debug log is used to send to **Doctor Web** Technical Support in case you experience problems with the application.



**Figure 2. Monitor settings**

**Dr.Web for Symbian** allows you to view the statistics of the monitor operation and monitor log, which contain information on all events connected with monitor operation (i.e. monitor starts and stops, detection of malicious objects, inability to check a certain file, etc.).

### **To view monitor statistics**

To open the monitor statistics, in the main window of the program select **Options** -> **Monitor statistics**. The statistics includes the following information:

- Total number of objects checked by the monitor
- Number of detected threats
- Number of neutralized threats



- Number of check errors
- Information on the virus databases (the date of the last update and the number of virus records)

Select **OK** to close the statistics window.

### To view monitor log

To open the monitor log, select **Logs** and then open the **Monitor** tab.

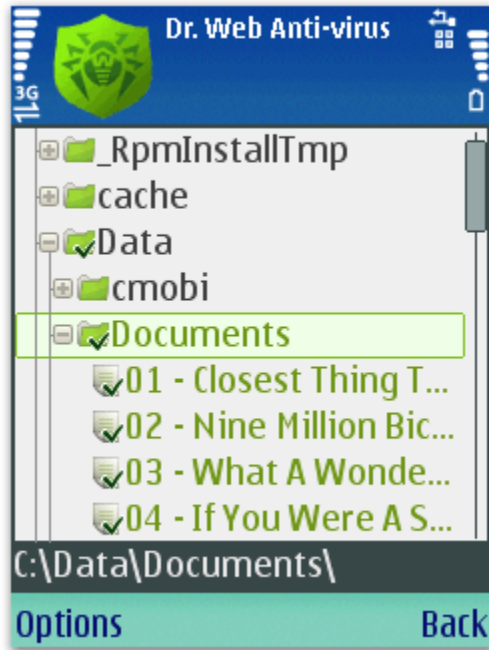
## On-Demand Scanning

**Dr.Web for Symbian** performs the scanning of the whole file system of the mobile device or only of the critical files and folders selected by user. This function is carried out by a component called *scanner*.

### Scanning

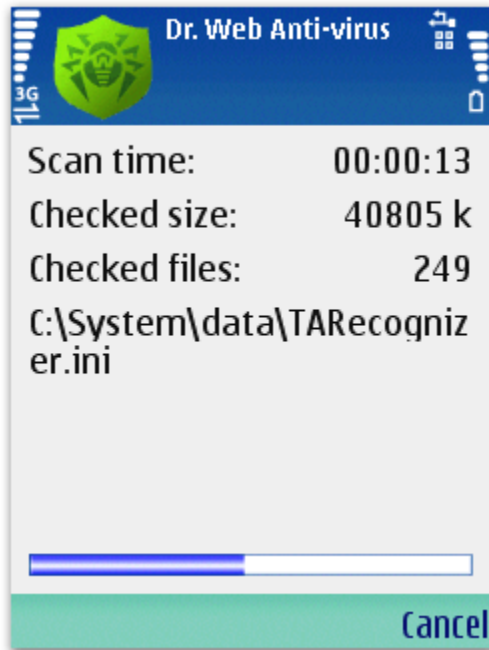
To scan the file system, in the main window of the program (see [Figure 1](#)) choose the scanning mode:

- To launch the scanning of all the files located on your device (according to the [scanning settings](#)), select **Full scan**.
- To scan only critical files and/or folders, select **Custom scan**. Select the objects in the hierarchical list (see [Figure 3](#)) and then select **Options** -> **Scan**



**Figure 3. Custom scan. Select objects.**

While performing the anti-virus check, the information on the total time of scanning, the number and the total size of scanned objects as well as the name of the currently scanned file are displayed, provided that the corresponding [display settings](#) had been made (see [Figure 4](#)).



**Figure 4. Scan window.**

After the scanning completes, you can review the list of detected malicious objects and choose an action for each detected malicious object (see [Malicious Objects Neutralization](#)).

### Scanning settings

To configure the scanning, select **Settings** in the main window of the program and then select **Scanner** section. You can specify the following options:

- **Log file read errors** – enables/disables logging the errors of reading the files.
- **Log scan time** – enables/disables logging the time of scan start and stop.



- **Scan ROM drive** – enables/disables scanning of the device firmware.
- **Scan SD-Card** – enables/disables scanning of the files and folders located on the removable memory cards.

On the **Interface** section you can specify the type of information displayed during scanning. By setting the correspondent value of the **Scanned file details** option you can set up the program to show/hide the name of the currently scanned file and the total size of checked files while scanning.



Selecting the value **show** for the **Scanned file details** option decreases the scanning rate.

---

To save the settings of current section and to return to the list of sections select **Back**.

To save the settings of all sections and to return to the main window select **Back** in the window of the settings sections list.

**Dr.Web for Symbian** logs events relating to the operation of the scanner that performs anti-virus checks (scanner starts and stops, detection of malicious objects, inability to check a certain file, etc).

### To view the scanner log

In the main window of the program select **View logs** and open the **Scanner** tab.

## Malicious Objects Neutralization

On completion of the complete or custom scan **Dr.Web for Symbian** allows to choose one of the following actions in the **Options** list for detected malicious object:

- **Delete** – the object is completely removed from the memory of the device.
- **Quarantine** – the object is moved to a special folder where it is isolated from the rest of the file system.



- **Ignore** – the object will be temporarily ignored. Next time you scan the system, the application detects the threat again.



Leave the detected objects in the file system only if you are absolutely sure they do not present a threat.

---

## Quarantine

**Dr.Web for Symbian** allows you to move the infected files to quarantine folder where they are isolated from the rest of file system.

### To manage files in Quarantine

1. To display the list of quarantined objects, in the main window select **Options** -> **Quarantine**.
2. The list of quarantined objects opens (see [Figure 5](#)).
3. Select one or several files in the list.
4. Choose one of the following actions in the **Options** list to the apply to the selected files:
  - **Restore** – returns the files back to the folder where they were moved from (use this action only if you are sure that the object is safe).
  - **Delete** – completely removes the files from the device.

To view the detailed information on the object from the list, select it and then select **Options** -> **Details** .



Figure 5. Quarantine.

## Anti-Spam

**Anti-spam** filters the calls and SMS messages allowing to block in automatic or manual mode the undesired messages and calls, such as advertisements or messages and calls from unknown numbers. The filtering is based on the [black and white lists](#).



## To configure Anti-spam

To configure the operation of Anti-spam, select **Anti-spam** section in the list of application settings. Open the **Options** tab and specify the following options:

- **Automatic startup** – allows to enable/disable automatic launch of **Anti-spam** (SMS and calls filtering) and file monitor on device reboot and application update.



For correct operation of **Anti-spam** it is recommended to set up the **Enable** value for this option.

---

- **Address book is** – the **White list** value means that the contacts from the address book are considered as included into the white list, the **Not in lists** value cancels the adding the contacts to the lists.
- **SMS filtering** – allows to enable/disable message filtering.
- **Contact not in lists** – allows to specify the program's actions for SMS received from unknown numbers and numbers not included to black and white lists. You can select one of the following values:
  - **Prompt about incoming** – in case this value is selected, the program prompts the user about rejecting/receiving the message. Depending on the selected action, it will be proposed to the user to add the sender's number to the white or black list respectively.
  - **By white list** – means that only the messages from the white list contacts will be passed and all the rest will be blocked.
  - **By black list** – means that all the messages except those from the black list contacts will be passed.
- **Calls filtering** – allows to enable/disable calls filtering.



- **Calls filter type** – allows to specify the type of calls filter:
  - **By white list** – means that only the calls from the white list contacts will be passed and all the rest will be blocked.
  - **By black list** – means that the calls from all numbers except those of black list contacts will be passed.
- **Reject calls** – allows to specify the calls rejection with/without answer. Rejecting a call without answer means that the call will be blocked. If a call is rejected with answer, it is accepted and then finished immediately.
- **Unknown call number** – allows to pass/reject calls from unknown numbers.

To save the settings of current section and to return to the list of sections select **Back**.

**Dr.Web for Symbian** registers all the events concerning messages filtering and **Anti-spam** operation (component's starts and stops, information on filtered messages and calls, etc).

#### **To view the Anti-spam log**

In the main window of the program select **Logs** and open the **SMS** tab.

## **Black and White Lists**

To create and edit the black and white lists use the corresponding tabs of the **Settings** -> **Anti-spam** section.

#### **To add a contact to the list**

1. Open the tab of the list you want to add a new contact to on the **Anti-spam** section.
2. Select **Options** -> **Add**, then select on of the following options:
  - **Number** – in this case you can enter manually the information on the contact you want to add to the list: in the **Number or Name** field enter the phone number or the mnemonic name of the contact.



- **Contact** – in this case you can choose the contact from the address book, for example, if the contact has several phone numbers and you want to add them all into the list.
- **Group** – in this case you can select a group from the address book of your mobile.

In the **Description** field you can enter any additional information and comments for the contact.

3. Select **Save**. The contact will be added to the selected list.



Black list has a higher priority level, thus, if a number is added to both black and white lists, the messages from this number will be blocked.

---

### To edit the information on a contact/group in the list

1. Select a contact/group in the list and then select **Options** -> **Edit**.
2. Modify the information entered to the fields.
3. Select **Save**.

### To remove a contact/group from the list

- Select a contact/group in the list and then select **Options** -> **Remove**.

## Update

**Dr.Web for Symbian** uses **Dr.Web virus databases** to detect malicious software. These databases contain details and signatures for all viruses and malicious programs for mobile devices known at the moment of the application release. However modern computer viruses are characterized by the evolvment and modification; also new viruses sometimes emerge. Therefore, to mitigate the risk of infection during the licensed period, Doctor Web provides you with periodical updates to virus databases and application components. The updater component of **Dr.Web for Symbian** helps you download the updates via Internet and automatically installs them.



The update procedure requires a working connection to the Internet via HTTP. To open the connection, use the built-in GPRS module of your device.

If you are using WAP, please contact your mobile operator to inquire about existing connection and download files limitations.

### To update the virus databases

1. In the main window of the program select **Options** -> **Update**.
2. In the updater window select **Options** -> **Update**.
3. After updates are downloaded and installed select **Back** to return to the main window.

You can check the program version and the version and creation date of the virus databases in the **Dr.Web for Symbian** information window.

### To open application information

In the main window of application select **Options** -> **About**.

## Logging

All events related to the operation of **Dr.Web for Symbian** and all main components configurations are registered on the special files located on the mobile device in the C:\Data\DrWeb directory (see [Table 1](#)). You can access to this directory via Nokia PC Suite/Nokia Ovi Suite application.

**Table 1. Dr.Web for Symbian configuration and log files.**

File name	Comment
DrWeb.dat	Anti-spam configuration file
DrWebScanner.dat	Scanner configuration file



File name	Comment
DrwScannerLog.txt	Scanner log file
DrWebMonLog.txt	Monitor log file
DrwServerLog.txt	Anti-spam log file
DrwGetKeyLog.txt	Key file downloading procedure log
DrwUpdaterLog.txt	Updater log file

You can save the scanner and anti-spam configurations on the computer, for example, with the view to use them after reinstalling the application.

The log files can be also saved and reviewed on the computer. In case you experience troubles while using **Dr.Web for Symbian** you can send the log files to the [Doctor Web technical support](#).



The DrwGetKeyLog.txt and DrwUpdaterLog.txt log files can be saved only for sending to the technical support as they are coded in special technical format.

---



# Appendices

## Appendix A. Contacting Support

Support is available to customers who have purchased a commercial version of **Doctor Web** products. Visit **Doctor Web Technical Support** web site 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 the 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-form in the corresponding section of the support site at <http://support.drweb.com/>.

For regional office information, see the **Doctor Web** official web site at <http://company.drweb.com/contacts/moscow>.



# Index

## A

- about 29
- access to help 18
- anti-spam
  - black and white lists 28
  - log 26
  - settings 26
- anti-spam log 26
- anti-virus check 19, 21
- appendices
  - technical support 32

## B

- black list 28

## C

- check
  - custom 21
  - for spam 26
  - full 21
- configuration
  - anti-spam 26
  - monitor 19
  - scanner 21
- constant protection 19

## D

- demo key file 9
- distribution kit 8
- document conventions 7

- Dr.Web for Symbian 6
  - anti-spam 26
  - distribution kit 8
  - functions 19
  - getting started 16
  - help 18
  - install 13
  - interface 17
  - istall 13
  - launch 16
  - licensing 9
  - logging 30
  - main features 8
  - quarantine 25
  - requirements 13
  - uninstall 13, 15
  - update 29

## E

- exit application 16

## G

- getting help 18

## H

- help system 18

## I

- install 13
- interface 17
- introduction 6



# Index

## K

- key file
  - acquisition 10
  - get 10
  - renewal 12
  - update 12
  - use 12
  - validity 9

## L

- launch application 16
- license
  - acquisition 10
  - renewal 12
  - update 12
  - use 12
  - validity 9
- license key file 9
  - acquisition 10
  - renewal 12
  - update 12
  - use 12
- licensing 9
- logging 30
  - anti-spam 26
  - monitor 19
  - scanner 21

## M

- main features 8
- monitor 19
  - logging 19
  - settings 19
- monitor log 19

## N

- neutralization of malicious objects 24

## P

- program functions 19

## Q

- quarantine 24, 25

## R

- removal 13
- renew license 12
- requirements 13

## S

- scanner log 21
- scanning
  - logging 21
  - settings 21
- start to use 16
- system requirements 13



# Index

## T

technical support 32

## U

uninstall 13, 15

update

    license 12

    virus databases 29

## V

virus check 19, 21

virus databases

    update 29

virus neutralization 24

## W

white list 28

