



**Dr.WEB®**

**Anti-virus**  
for Mac OS X

**User Manual**

Defend what you create

**© 2009 Doctor Web, Ltd.. 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, SpIDer Mail, SpIDer Guard, CureIt!, the Dr.WEB INSIDE logo 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 Mac OS**

**Version 5.00.0**

**User Manual**

**05.06.2009**

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>Document Conventions and Abbreviations</b>	<b>6</b>
<b>Chapter 1. Introduction</b>	<b>7</b>
What is Dr.Web for Mac OS	7
License Key File	9
<b>Chapter 2. Installation and Removal</b>	<b>10</b>
System Requirements	11
Installing Dr.Web for Mac OS	12
Removing Dr.Web for Mac OS	12
Receiving a key file	13
<b>Chapter 3. Basic Functions</b>	<b>14</b>
Starting and Quitting Dr.Web for Mac OS	14
Updating the Program	16
Constant Anti-virus Protection	17
Performing a System Scan On Demand	18
Getting Help	20
<b>Chapter 4. Advanced Usage</b>	<b>21</b>
Viewing the Results	21
Managing the Quarantine	22
Adjusting Schedules	23
Adjusting Automatic Actions	24
Excluding Files from Scanning	25
Adjusting Notifications	26
Using the License Manager	27



## **Appendices**

**28**


### **Appendix A. Technical Support**

**28**



# Document Conventions and Abbreviations

The following conventions and symbols are used in this manual:

Convention	Description
<b>Bold</b>	Names of buttons, 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.
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.

The following abbreviations are used in this manual:

- CPU - Central Processing Unit
- GUI - Graphical User Interface
- OS - operating system
- RAM - Random Access Memory



## Chapter 1. Introduction

Thank you for purchasing **Dr.Web for Mac OS**. It offers reliable protection from various types of computer threats using the most advanced virus detection and neutralization technologies.

This manual is intended to help users of computers running Mac OS install and use **Dr.Web for Mac OS**.

### What is Dr.Web for Mac OS

**Dr.Web for Mac OS** is an anti-virus solution designed to help users of computers running Mac OS protect their machines from viruses and other types of threats.

The core components of the program (*anti-virus engine* and *virus databases*) are not only extremely effective and resource-sparing, but also cross-platform, which allows specialists in **Doctor Web** to create outstanding anti-virus solutions for different operating systems. Components of **Dr.Web for Mac OS** are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.



**Dr.Web for Mac OS** consists of the following components each performing its own set of functions:

Component	Description
Scanner	This virus-detection component is used for: <ul style="list-style-type: none"><li>• Express, full and custom system scan on user demand or according to schedule</li><li>• Neutralization of detected threats (Cure, Delete, Quarantine - the necessary action is either selected by the user manually or an action specified in the settings is applied automatically for the corresponding type of threat)</li></ul>
SpIDer Guard	This is a resident anti-virus component which checks all files (which are being used) in real time.
Quarantine	This is a special folder which is used for isolation of infected files and other threats so that they cannot do harm to the system.
Automatic Updating Utility (Updater)	This component is used for updating virus databases and other program components on user demand or according to schedule.
License Manager	This component is used to simplify management of key files: it allows to receive demo and license key files, view information about them and renew your license.
Scheduler	This component is required to perform system scanning and program updates according to schedule. The Scheduler remains active even when you quit Dr.Web for Mac OS.

Flexible settings of **Dr.Web for Mac OS** allow to adjust sound notifications for various events, maximum size of the **Quarantine**, list of files and folders excluded from scanning, etc.



## License Key File

User's rights to use **Dr.Web for Mac OS** are regulated by a special file called the *key file*. The key file contains the following information:

- duration of the anti-virus license
- list of components a user is allowed to use
- other restrictions (e.g. the number of users allowed to use the plug-in)

The key file has the **.key** extension and it can be received at first launch of **Dr.Web for Mac OS** via the [License Manager component](#):

- For evaluation purposes you can use a demo key file. The demo key file provides full functionality of the main anti-virus components, but has a limited term of usage.
- To get a license key file, you will need the product's serial number. You can purchase any **Dr.Web** anti-virus product or the serial number for it via our [partners](#) or the [online store](#).

The key file is delivered as a file with the **.key** extension or as a ZIP archive containing such file.

The parameters of the key file which specify the user's rights are set in accordance with the License agreement. The file also contains information on the user and seller of the anti-virus.



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.

---

When the license key file expires, to continue using **Dr.Web for Mac OS** you have to get a new key file and replace the old one with it (see [Using the License Manager](#)).



## Chapter 2. Installation and Removal

The **Dr.Web for Mac OS** software is distributed as a single disk image file (Dr.Web for Mac OS.dmg). The file can be found on the **Dr. Web for Mac OS** CD/DVD disc or downloaded from the Internet (<http://www.drweb.com>).

---



**Dr.Web for Mac OS** 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. If you already have an earlier version of **Dr.Web for Mac OS** or other anti-virus software installed, it is necessary to uninstall it using the installation file or standard tools of the OS (see [Removing Dr.Web for Mac OS](#)).

---



## System Requirements

This section provides system requirements for installation and proper operation of **Dr.Web for Mac OS** on your computer.

### Hardware requirements

Specification	Requirement
CPU	Any Intel processor
RAM	64 MB
Disk space	20 MB (more may be required depending on the amount and size of objects in the Quarantine)
Monitor	VGA-compatible monitor

### OS and software requirements

Specification	Requirement
OS	Mac OS X v.10.4 or later
Internet	Internet connection for updates



## Installing Dr.Web for Mac OS

### To install Dr.Web for Mac OS:

1. Mount Dr.Web for Mac OS.dmg and start the installation.
2. The welcome window of the **Dr.Web for Mac OS** installer will open. Follow the steps and instructions of the installer.
3. Specify the name and password of any administrator account on your computer. Installation will be performed automatically.

## Removing Dr.Web for Mac OS

### To uninstall Dr.Web for Mac OS:

1. Mount Dr.Web for Mac OS.dmg.
2. Select **Dr.Web Uninstaller**.
3. Specify the name and password of an administrator account on your computer. **Dr.Web for Mac OS** will be removed automatically.



## Receiving a key file

After installation a window for registration of **Dr.Web for Mac OS** will open. Registration is required to verify that you are a legitimate user of the anti-virus. Select the necessary option and click **Continue**.

Option	Description
Receive license key file	You will need to specify the serial number which is included with the program
Receive demo key file	No serial number is needed because the demo key file is used for evaluation purposes and has a short term of usage
Specify path to an available valid key file	Select this option if you already have a valid key file present on the computer

If you select one of the first two options, you will be asked to specify your personal information (name, e-mail address, country and city of residence). This information is used only by **Doctor Web** to generate the key file and is not passed on to anyone else. The key file which you will receive will contain this information for identification purposes.



## Chapter 3. Basic Functions

This chapter contains information on the main functions of **Dr.Web for Mac OS**.

### Starting and Quitting Dr.Web for Mac OS

**To start Dr.Web for Mac OS do one of the following:**

- Open the **Application** folder via the Finder and double-click **Dr. Web for Mac OS.app**
- Bring up the agent's menu (click the Dr.Web icon in the menu bar) and select **Open Dr.Web**.

The main window of **Dr.Web for Mac OS** consists of five sections. These sections are used to control and access various components of the anti-virus:

- **SpIDer Guard** - this section lets you enable/disable the resident anti-virus component of **Dr.Web for Mac OS**.  
See [Constant Anti-virus Protection](#).
- **Scanner** - this section lets you access the main on-demand anti-virus scanning component.  
See [Performing a System Scan](#).
- **Quarantine** - this lets you access and control the contents of the **Quarantine**.  
See [Managing the Quarantine](#).



- **Results** - this section lets you access and view statistics of the program's operation with a summary of detected threats and apply necessary actions.

See [Viewing the Results](#).

- **Update** - this section contains information about the last update and lets you start the **Updater**.

See [Updating the Program](#).

**To quit Dr.Web for Mac OS do one of the following:**

- Click the **Quit Dr.Web for Mac OS** item in the application menu (the menu bar is at the top of the main desktop).
- Press COMMAND+Q on the keyboard when **Dr.Web for Mac OS** is active.



When you quit **Dr.Web for Mac OS**, the **SpIDer Guard** and **Scheduler** components remain active. The former is a resident anti-virus monitor which checks all files in real time when they are used, and the latter starts the scanning and updating processes according to schedule (see [Adjusting Schedules](#)).

---



## Updating the Program

New types of computer threats with new concealment features are being constantly developed by malefactors all over the world. Updating the components and virus databases of **Dr.Web for Mac OS** ensures that your protection is always up to date and ready for those new threat types. Updating is performed by a special component called the **Updater**.

You can periodically start the **Updater** manually (see below) or configure the **Scheduler** to update program components and virus databases according to a specified schedule (see [Adjusting Schedules](#)).

### To start the Updater manually:

- Click the **Update** button in the **Updater** section of the **Dr.Web for Mac OS** main window.
- Bring up the agent's menu (click the Dr.Web icon in the menu bar) and select **Update**.



## Constant Anti-virus Protection

Constant anti-virus protection is carried out via **SpIDer Guard** - the resident component which checks all files accessed by the user or other programs in the system in real time. By default, it is enabled as soon as you install **Dr.Web for Mac OS**. Whenever a threat is detected, **SpIDer Guard** generates a warning window and applies an action specified in the [Actions tab of the preferences](#).

### To enable/disable SpIDer Guard:

- Click the **Enable/Disable** button in the **SpIDer Guard** section of the main window.
- Bring up the agent's menu (click the Dr.Web icon in the menu bar) and select the corresponding item.



Only users with administrator privileges can disable **SpIDer Guard**.

---

You can exclude certain files and folders from scanning by **SpIDer Guard** and set up the maximum time for scanning one file in the [Exclusions tab of the preferences](#).



## Performing a System Scan On Demand

On-demand scanning is performed by the **Scanner**. It checks objects in the file system on user demand or according to schedule in order to detect various threats which are present in the system but are not active. It is necessary to periodically perform a system scan via the **Scanner** section of the **Dr.Web for Mac OS** GUI.

You can start the scanning process manually (see below) or configure the **Scheduler** to scan the system according to a specified schedule (see [Adjusting Schedules](#)).

### To perform a system scan manually:

1. Open the **Scanner** section.
2. Select a scan mode (see the panel with the file system tree for more information):
  - **Express scan** - quickly check only the most vulnerable parts of the system.
  - **Full scan** - perform a full scan of the entire file system.
  - **Custom scan** - manually specify files and folders which you wish to check.

These three are the default scan modes (also called "scan sets" because they contain information about the set of objects to be scanned). Trying to change the Full and Express sets will switch you to the Custom set. If you click the plus "+" symbol under the list of scan sets, a new one will be created which you can use for scans later. You can create as many additional scan sets as you wish and delete those which you do not need by clicking the minus "-" symbol.

3. Click the button with an icon of a gear to select how to apply actions for detected threats. When automatic actions are enabled, the **Scanner** applies actions specified in the [Scanner settings](#) to all detected objects automatically.
4. Click the **Start** button in the bottom right part of the **Scanner** section.



When you start the scanning process, the main window switches to the **Results** section (see [Viewing the Results](#)) and virus databases begin loading. The **Scanner** shows the name of each file which is currently being scanned and generates a list of detected threats.

The **Scanner** requires administrator privileges to check critical areas of the HDD. Click the lock at the bottom of the **Scanner** section to grant the **Scanner** administrator privileges for every scanning process started by you.



## Getting Help

To get help about the program you can use **Dr.Web Help** which can be accessed via the Apple Help viewer.

### To access Dr.Web Help:

- Click **Help** in the menu bar and then select the **Dr.Web Help** item or search for keywords using the text box.

If you cannot find an answer or solution to your problem, you should [contact technical support](#) for assistance.



## Chapter 4. Advanced Usage

This chapter contains information on performing more advanced tasks with **Dr.Web for Mac OS** and adjusting its settings.

### Viewing the Results

When the scanning process starts, the main window switches to the **Results** section. At the top of the tab is the **Statistics** group box with the summary of the scanning process (during the scanning process, in the right part of the group box, the **Scanner** shows the name of each file which is currently being scanned).

In the middle of the **Results** section is a table with the list of all detected objects which may present a threat:

- The **File** column contains the path and file name.
- The **Details** column contains information about the threat (e.g. name or type of the object).
- The **Action** column contains information about the action applied to the detected object. If it is empty, then no action was applied yet (see below for more information).
- The **Date** column contains the date when the threat was detected.
- The **Detected by** column specifies whether the threat was detected by the **SpIDer Guard** or the **Scanner** component.

#### To apply an action to object(s) in the list:

1. Select an object (hold the SHIFT key to select multiple objects).
2. Do one of the following:
  - Click the **Neutralize** button at the bottom to apply the action [specified in the Actions tab](#) for the corresponding type of threat.
  - Click the arrow on the **Neutralize** button and choose the necessary action.



- Control-click the selected object(s) and choose an action from the contextual menu.

## Managing the Quarantine

The **Quarantine** is a special folder where you can move detected objects to isolate them from the rest of the system in case you need the object and it cannot be cured (as curing algorithms are being constantly improved with the virus databases, it may become possible to cure it after one of the updates).

You can view and manage the contents of the **Quarantine** via the **Dr. Web for Mac OS** GUI: the **Quarantine** section of the main window. In the middle of the section is a table with the list of objects in the **Quarantine**:

- The **File** column contains the path and file name.
- The **Details** column contains information about the threat (e.g. name or type of the threat).
- The **Date and Time** column contains the date and time when the object was moved to the **Quarantine**.
- The **Type** column specifies whether the object is stored in the system or user **Quarantine** (there is one common system **Quarantine** and separate ones for each user).

### To apply an action to object(s) in the Quarantine:

1. Select an object (hold the SHIFT key to select multiple objects).
2. Click the necessary button below the table:
  - **Delete** - completely remove the file from the file system.
  - **Cure** - attempt to cure the file.
  - **Recover File** - move the file back to the place in the file system where it was moved from.

You can specify a quarantine period for objects before they are deleted and set the maximum size for the **Quarantine** in the **Dr. Web for Mac OS** preferences.



### To adjust the settings of the Quarantine:

- Click the **Preferences** item in the application menu and select **Quarantine** in the left part of the window.

## Adjusting Schedules

The **Scheduler** component can be used to set up schedules for automatic scanning and updating. It is adjusted in the **Scanner** and **Update** sections of the **Dr.Web for Mac OS** preferences.

### To set up a scanning schedule:

1. Click the **Preferences** item in the application menu, select **Scanner** and open the **Scheduler** tab.
2. Select the check box at the top and specify the time and interval between scanning sessions in days.
3. Select the scan mode:
  - **Express** - quickly check only the most vulnerable parts of the system.
  - **Full** - perform a full scan of the entire file system.
  - **Custom** - manually specify files and folders which you wish to check in the list.

### To set up an update schedule:

1. Click the **Preferences** item in the application menu and select **Update** in the left part of the window.
2. Select one of the options:
  - **Update automatically** - default interval recommended by Dr.Web.
  - **Update every** - specify an interval for updating.
  - **Do not update** - do not perform automatic updates (remember to update manually).



## Adjusting Automatic Actions

**Dr.Web for Mac OS** can apply actions to detected threats automatically choosing the actions according to the types of threats. Different automatic actions can be set up for the **Scanner** and **SpIDer Guard**.

### To adjust actions for the Scanner:

- Click the **Preferences** item in the application menu, select **Scanner** and open the **Actions** tab.

### To adjust actions for SpIDer Guard:

- Click the **Preferences** item in the application menu, select **SpIDer Guard** and open the **Actions** tab.

Look through the different types of threats and select necessary actions for them.



The default automatic actions are considered optimal and it is not recommended to change them unless it is necessary and you know what you are doing.

---



By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrator rights from changing these settings. To unlock them, click the lock at the bottom of the settings window when **SpIDer Guard** settings are selected.

---



## Excluding Files from Scanning

You can make up a list of files and folders which should be excluded from scanning. Exclusions can be adjusted for both the **Scanner** and **SpIDer Guard**.

### To adjust exclusions for the Scanner:

- Click the **Preferences** item in the application menu, select **Scanner** and open the **Exclusions** tab.

### To adjust actions for SpIDer Guard:

- Click the **Preferences** item in the application menu, select **SpIDer Guard** and open the **Exclusions** tab.

The **Quarantine** folder is in the list by default because it is used to isolate detected threats and, as access to it is blocked, there is no use scanning it.

You can add a certain file or folder to the list by clicking the **Choose** button. Select **Do not check archives** if you wish to exclude all archive types from scanning.

For **SpIDer Guard** you can also specify a time limit for scanning one file so that your resident monitor does not "hang up" on a corrupted file.



Default settings in the **Exclusions** tab are considered optimal and it is not recommended to change them unless it is necessary and you know what you are doing.

---



By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrator rights from changing these settings. To unlock them, click the lock at the bottom of the settings window when **SpIDer Guard** settings are selected.

---



## Adjusting Notifications

**Dr.Web for Mac OS** can notify the user about various events which may occur during operation. There are two types of notifications:

- On-screen messages displayed by **SpIDer Guard**.
- Sound alerts which are used both by the **Scanner** and **SpIDer Guard**.

### To adjust sound alerts for the Scanner:

- Click the **Preferences** item in the application menu, select **Scanner** and open the **Sounds** tab.

### To adjust message notifications and sound alerts for SpIDer Guard:

- Click the **Preferences** item in the application menu, select **SpIDer Guard** and open the **Notifications** tab.

You can enable/disable on-screen notification messages via the **Display notifications** check box. Select **Remember position** if you want the program to display notifications at the position on the screen where you moved it to. Use the slider to set the duration for a message to remain on the screen.

You can enable/disable sound alerts via the **Use sound alerts** check box at the top of the tab. Selecting the check box below lets you specify a time interval during the day for which sound alerts will be enabled.

In the list of events, select the check boxes against events which should be accompanied by a sound alert. Select the event itself to choose a sound for it: either pick one of the available sounds in the **Sound** box or click **Choose** to add a custom sound.



By default, all **SpIDer Guard** settings are locked in order to prevent anyone without administrator rights from changing these settings. To unlock them, click the lock at the bottom of the settings window when **SpIDer Guard** settings are selected.

## Using the License Manager

The **License Manager** is a component used to simplify the management of your key files (see [License Key File](#)). You usually receive the key file after installation because it is required for operation of **Dr.Web for Mac OS**. If you did not receive a key file or it has expired, you can use the **License Manager** to get a new one.

### To open the License Manager:

- Click the **License Manager** item in the application menu.

In the **License Manager** window you can view information about the status of your current key file and renew it by clicking the **Get a new key** button at the bottom (see [Receiving a key file](#)).



# Appendices

## Appendix A. Technical Support

The **Dr.Web** technical support web page is located at

<http://support.drweb.com/>

If you experience problems during installation or operation of the company's products please do the following before contacting the technical support department:

- Read the latest versions of product documentation available at <http://solutions.drweb.com/>
- Read the **FAQ** section at <http://support.drweb.com/faq/>
- Visit the **Dr.Web** users forum at <http://forum.drweb.com/>

If the problems cannot be solved then you can contact the technical support department in one of the following ways:

- Fill out a special web-form at <http://support.drweb.com/new/>
- Write an e-mail message to [support@drweb.com](mailto:support@drweb.com)
- Telephone the technical support department in Moscow:  
+7 (495) 789-45-87

You can find the nearest office of **Doctor Web** and contact information at <http://company.drweb.com/contact/>

