Dr.WEB® Security Space for BlackBerry

User 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 Security Space for BlackBerry
Version 10.01
User Manual
19.11.2015

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

Chapter 1. Introduction

Thank you for choosing **Dr.Web Security Space for BlackBerry** (hereinafter referred to as **Dr.Web**). This anti-virus solution offers a reliable protection of the mobile devices working under the BlackBerry™ operating system from various virus threats designed specifically for these devices.

The application 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 the devices running BlackBerry to install and adjust **Dr.Web**. It also describes all the basic functions of the application.

Document Conventions

The following conventions and symbols are used in this document:

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 webpages.
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.
⚠	A warning about potential errors or any other important comment.

Main Features

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

- Constant real-time protection of the file system (scanning of saved files, programs which are being installed etc.)
- Scanning of the whole file system of the device or files and folders selected by user
- Scanning of the archives
- Scanning of the files on SD card (or other external storage)
- Threats detection in the *.lnk files (defined by **Dr.Web** as Exploit.Cpllnk)
- Deletion of the infected objects or their isolation in quarantine
- **Dr.Web** virus databases updates via Internet
- Statistics of the detected threats and performed actions, application log
- Analyzing the security of the device and help in resolving the detected problems and vulnerabilities

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

System Requirements

To install and use **Dr.Web**, ensure your mobile device works under the BlackBerry operating system of version 10.3.2 and higher.

The Internet connection is required for virus databases update procedure.

Chapter 2. Licensing

To use **Dr.Web** for a long period of time, you need a license. A license allows to take advantage of all product features during the whole period and regulate the use rights for the purchased product.

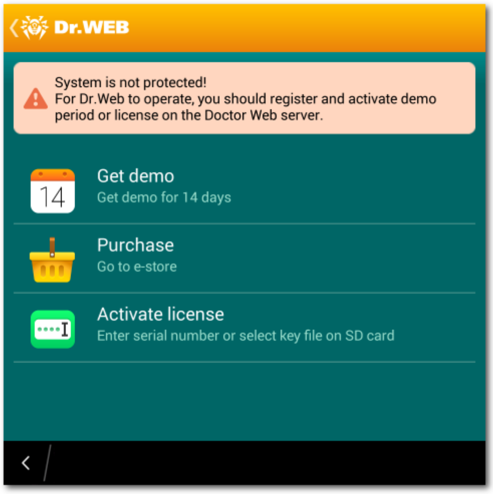
If you want to evaluate the product before purchasing it, you can activate a demo period. It provides you with full functionality of the main components, but the period of validity is considerably restricted.

If you have the license for the products **Dr.Web Security Space** or **Dr.Web Anti-virus** (full packaged product or digital license), you can use the existing license key file for operation of **Dr.Web**.

To activate a license or demo period or to purchase a license, use the corresponding screen (see Figure 1). This screen opens on the first launch of the application and in case valid license is missing.

To open the licensing screen, do the following:

1. Open the application menu on the main screen of the application (see Figure 2).
2. Tap the **Renew license** button.



System is not protected!
For Dr.Web to operate, you should register and activate demo period or license on the Doctor Web server.

Get demo
Get demo for 14 days

Purchase
Go to e-store

Activate license
Enter serial number or select key file on SD card

Figure 1. Licensing

License key file

The use rights for **Dr.Web** are specified in the *license key file*.

The license key file contains, among other, the following information:

- Licensed period for the product
- List of components the user is allowed to use
- Other limitations

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** stops detecting and neutralizing the malicious programs.

⚠ The license key file becomes invalid after editing. Do not save changes after opening the file in text editors to prevent the license from compromise.

Activate Demo Period

If you installed the application in purposes of evaluation, you can download the free license for 14 days.

To activate demo period:

1. Tap **Get demo** on the licensing screen (see Figure 1).
2. In the opened window, enter your email address.
3. Tap **Get demo**. Demo period will be activated.

Purchase License

To purchase a license:

1. Tap **Purchase** on the licensing screen (see Figure 1) or open the URL http://estore.drweb.com/mobile. **Doctor Web** web store will be opened.
2. Select the license period and the number of devices to protect.
3. Tap **Purchase**.

You will receive either the serial number or the license key file to the specified email. You can also choose to receive the serial number in an SMS to the mobile number entered on registration. To start using the purchased license you need either to register the serial number or copy the key file on the device.

Activate License

If you already have a license for **Dr.Web Security Space** or **Dr.Web Anti-virus** (full packaged product or digital license), you can register and use the existing license in the following ways.

Registering serial number

1. On the licensing screen (see Figure 1) tap **Activate license**.
2. Tap **Enter serial number**.
3. Enter the serial number.
4. If you're registering this serial number for the first time, you will be asked to enter your personal data. This information is necessary to receive the key file.
5. Tap **Get license**.

Copying key file on the device

1. Synchronize your device with PC and copy the key file to the **downloads** folder located in the internal device memory.
2. On the licensing screen (see Figure 1) select **Activate license**.
3. Tap **Download**. On the information window **Copy from file** tap **OK**.
4. The key file will be downloaded and installed. Review the license expiration date in the information window. Tap **OK**.

The key file for **Dr.Web Security Space** or **Dr.Web Anti-virus** program can be used with **Dr.Web** only if it supports DrWebGUI component.

To check whether such key file can be used:

1. Open the key file in a text editor (e.g., Notepad).
2. Check the list of values of the Applications parameter in the [Key] group: if DrWebGUI component is in the list, you can use the key file for operation of **Dr.Web**.

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

Get license key file by registering serial number on Doctor Web website

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 email address you specified in the registration form.

5. Extract the license key file on the computer that will be used for synchronization with your device and copying the key file.

Update License

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** supports hot license update without stopping or reinstalling the application.

Get information on license To get information on license, on the main screen (see Figure 2), open the application menu and tap **About**.

On the opened screen, you can review the following information on the licensing parameters:

- License owner name
- License activation and expiration dates

Configure notifications

You can enable/disable notifications about the upcoming license expiration using the **Notifications** option on the **License** section in **Dr.Web** settings (see Figure 3).

Update license

To update your license, you need either purchase or activate a new license.

You can also purchase a new license or renew your current license on your personal web page at **Doctor Web** official website. To go to this web page, select **About** in the application menu and tap **My Dr.Web** link.

Chapter 3. Installation and Removal

Dr.Web can be installed on the device directly from BlackBerry World or by launching the installation file.

The application can be removed via BlackBerry World or by means of the operating system of the device.

Install Application

You can install **Dr.Web** either via BlackBerry World or launch the application installation file on the device.

Installation via BlackBerry World

1. On your device, open BlackBerry World, find **Dr.Web** in the list of applications and tap **Download**.

> If your device does not meet the system requirements, **Dr.Web** is not displayed in the list of BlackBerry World.

2. Then the screen containing the information on device functions which the application needs to access will appear:
   - If you are installing **Dr.Web** free trial for 14 days, access to the in-app purchases function is required for further license purchase.
   - For operation of **SpIDer Guard** and **Dr.Web Scanner**, access to applications data and SD card (or other external storage) as well as reading/writing permissions are required.
   - For updating virus databases, access to Internet and device network settings is required.

   Tap **Accept**.
3. Tap **Open** to start using the application.

Installation via launching the installation file on the device

The installation file of **Dr.Web** is available for download on the **Doctor Web** website.

1. Copy the installation file to the device.
2. Use the file manager to find and launch the installation file.
3. In the opened window tap **Install**.
4. Then the screen containing the information on device functions which the application needs to access will appear. Review the information and tap **Install**.

Dr.Web was successfully installed on your device and is ready to use.

Update and Uninstall Application

The application can be updated or uninstalled via BlackBerry World. You can also uninstall the application by means of the operating system connecting to Internet.

Uninstall application via BlackBerry World

1. Open BlackBerry World, go to the **My World** section and select **My Apps & Games** -> **Installed**.
2. In the list of installed applications tap and hold **Dr.Web** application sign.

3. Tap 🗑 in lower right hand corner of the screen.
4. In the opened window, tap **Delete** to remove the application from the device permanently or **Uninstall**, to have an opportunity to reinstall the application.

Uninstall application without connecting to Internet

1. On the main device screen, tap and hold the application sign until the signs start blinking.
2. Tap 🗑 on the application sign.

Update application via BlackBerry World

1. Open BlackBerry World, go to the **My World** section and select **My Apps & Games** -> **Updates**. If **Dr.Web** updates are available, the application will be displayed in this list.
2. Tap ↙ next to the application. Updates will be downloaded and installed on the device. If necessary, tap **Accept** to allow access to required device functions. Tap **Open** to start using the application.

Chapter 4. Getting Started

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

Launch and Exit Application

To launch the application

To launch **Dr.Web**, open the **All programs** screen and tap **Dr.Web** sign .

On the first launch of the application you will be asked to read and accept the License agreement, that is necessary to start using the application. In the same window, you may also agree to participate in the software quality improvement program by allowing to send impersonal data about the detected threats and visited websites to **Doctor Web** and Google servers. You can disable sending such statistical information at any time by clearing the **Send statistics** check box in the **General settings** section of the application parameters.

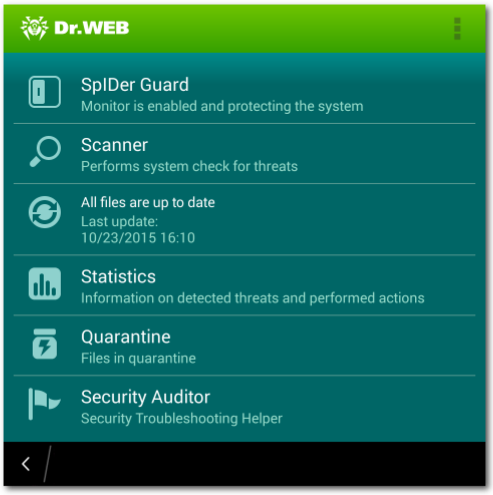
To exit the application

1. Swipe up from the bottom of the screen to minimize the application.
2. To exit the minimized application, tap ✕ in the lower right hand corner of the application frame.

Interface

On the application main screen (see Figure 2) the current protection status is displayed. It also provides access to the following application functions:

- **SpIDer Guard** – allows to enable/disable the constant anti-virus protection.
- **Scanner** – provides the on-demand scanning of the system (3 scan types are possible: full scan, express scan and custom scan).
- **Updating** – contains information on the date of the last update and launches the application update if required.
- **Statistics** – allows to review the statistics of the detected threats and performed actions.
- **Quarantine** – allows to view and process the objects in quarantine.
- **Security Auditor** – allows to perform the diagnostics of the system and helps to resolve the detected security problems and vulnerabilities.



Dr.WEB

SpIDer Guard
Monitor is enabled and protecting the system

Scanner
Performs system check for threats

All files are up to date
Last update:
10/23/2015 16:10

Statistics
Information on detected threats and performed actions

Quarantine
Files in quarantine

Security Auditor
Security Troubleshooting Helper

Figure 2. Main screen of the application

Accessing the application menu and navigating between screens

To open the application menu with additional options, tap the corresponding item in the upper right side of the screen. To return to the main screen, tap the application logo in the upper left side of the screen.

The application menu on the main screen allows you to open the application settings, the web help describing all its functions and settings, as well as open the application information screen.

The application information screen contains information on the application version, the license owner and its activation and expiration dates. It also contains links to **Doctor Web** official website and to the pages of the company in social networks: Twitter, Facebook, Instagram, and to its Youtube channel.

My Dr.Web

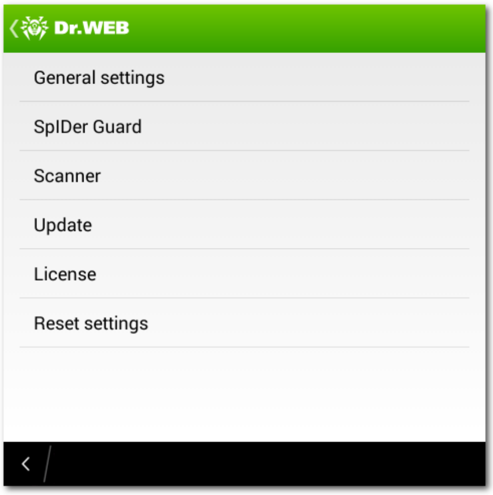
Online service **My Dr.Web** is your personal webpage of the official **Doctor Web** website. This page provides you with information on your license including usage period and serial number, allows to renew the license, review the information on the last update and the number of records in virus databases, contact technical support, etc.

To open this page, on the main screen (see Figure 2) open the application menu and tap **About**. Then tap **My Dr.Web** on the opened screen.

Chapter 5. Application Functions

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

To open the settings screen (see Figure 3), on the main screen open the application menu and select **Settings**.



Dr.WEB

General settings

SpIDer Guard

Scanner

Update

License

Reset settings

Figure 3. Application settings

Reset settings

You can reset the user settings of the application at any time and restore the standard settings. To do this:

1. Tap **Reset settings** on the settings screen (see Figure 3). On the opened screen, tap **Restore default settings** item.
2. Confirm the return to the default settings.

Constant Anti-Virus Protection

The constant system protection is carried out by a component **SpIDer Guard**. It resides in the internal device memory and checks all files as they are modified and saved.

Enable constant protection

On the first launch of the application, the constant protection is enabled automatically after you accept the License Agreement. To disable or re-enable it, tap the **SpIDer Guard** section of the main screen.

When **SpIDer Guard** is enabled, it begins protecting the file system of the device. It remains active even if you close the application.

If a security threat is detected, the list of detected threats will appear. This list can be closed only when you apply an action to every threat. On the lock screen notification on detected threats will appear. On tapping the notification, the threat list appears.

SpIDer Guard stops when the internal device memory is cleared. To restore constant anti-virus protection, reopen **Dr.Web**.

SpIDer Guard settings

To access the **Dr.Web** settings, open the application menu on the main screen and tap **Settings**. To configure **SpIDer Guard**, perform the following actions on the settings screen (see Figure 3):

- To enable check of files in archives, select the **Files in archives** check box on the **SpIDer Guard** section.

> ⚠ By default, the archives check is disabled. Enabling the check of archives can influence the system performance and increase the battery power consumption. Anyway, disabling the archives check do not decrease the protection level because **SpIDer Guard** checks installation *.apk and *.bar files regardless of the **Files in archives** parameter value.

- To enable/disable the detection of adware and riskware (including hacktools and jokes), tap **More options** on the **SpIDer Guard** section, then select/clear the **Adware** and **Riskware** check boxes.

Statistics

Dr.Web registers the events related to **SpIDer Guard** operation (enable/disable, internal device memory and installed applications check results, threats detection). The application actions are displayed on the **Actions** section of the **Statistics** screen.

On-Demand Scan

Dr.Web provides on-demand scanning of the file system. You can perform express or full check of the whole file system or scan the critical files and folders only. This function is performed by the **Dr.Web Scanner**.

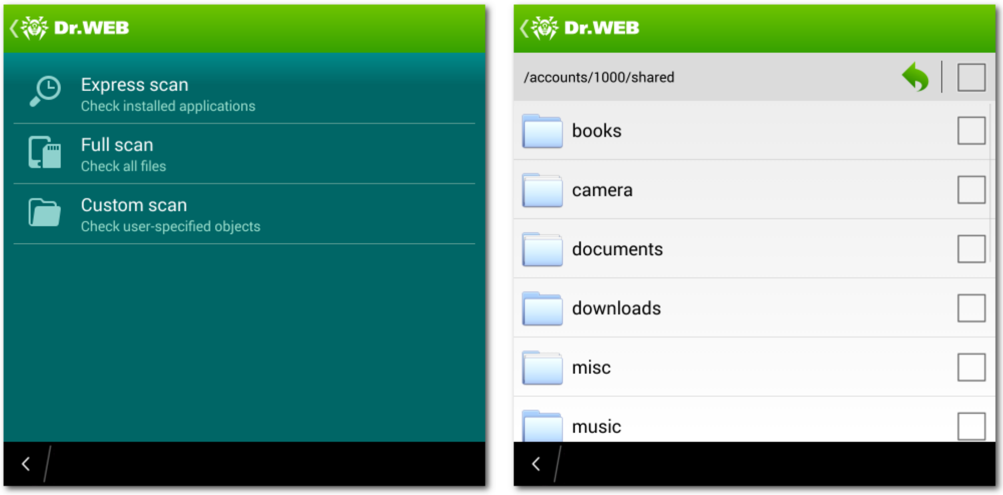
It is recommended to periodically scan the system in case **SpIDer Guard** had not been active for some time. Usually, the express scan is sufficient for this purpose.

Scanning

To scan the system, on the main screen tap **Scanner** and on the opened screen (see Figure 4) do one of the following actions:

- To launch only the installed applications check, tap **Express scan**.
- To scan all the files, tap **Full scan**.
- To scan only critical files and folders, tap **Custom scan**, select the objects in the hierarchical list (see Figure 5) and then tap **Scan**. While selecting the objects to scan, you can use the options located to the right above the list to select all objects and to go up one folder.

After the scanning completes, you can review the list of detected threats and choose an action for each malicious object.



Figures 4 and 5. Dr.Web Scanner and custom scan screens

Sending suspicious files to Doctor Web anti-virus laboratory

You can submit suspicious ZIP archives (including *.jar, *.apk and *.bar), presumably containing viruses, or a clean ZIP archive that has been identified as so-called "false positive" to **Doctor Web** anti-virus laboratory:

1. Tap and hold the file in the hierarchical list (see Figure 5), then tap **Send to Laboratory**.
2. In the next screen, enter your email address in order to receive the results of the file analysis.
3. Select a category for your request:
   - **Suspicious file**, if you think that the file represents a threat.
   - **False detection** or **False detection by Origins Tracing**, if you think that the file was identified as threat by mistake.

   To make a selection between two categories of false positive, use the name of the threat that the file presumably contains: select the **False detection by Origins Tracing** category, if the name contains the ".origin" postfix and the **False detection** one in other cases.
4. Tap **Submit**.

Only the ZIP archives of not more than 10 MB can be submitted to **Doctor Web** anti-virus laboratory.

Dr.Web Scanner settings

To access **Dr.Web Scanner** settings, on the main screen open the application menu, tap **Settings**. The following settings are available:

- To enable check of files in archives, select the **Files in archives** check box on the **Scanner** section.

By default, the archives check is disabled. Enabling the check of archives may influence the system performance and increase the battery power consumption. Anyway, disabling the archives check does not decrease the protection level because **SpIDer Guard** checks all *.apk and *.bar files regardless of the **Files in archives** parameter value.

- To enable/disable the detection of adware and riskware (including hacktools and jokes), on the **Scanner** section, tap **More options**, then select/clear the **Adware** and **Riskware** check boxes.

Statistics

Dr.Web registers the events related to **Dr.Web Scanner** operation (check type and results, threats detection). The application actions are displayed on the **Actions** section of the **Statistics** screen.

Threats Neutralization

Viewing the list of detected threats

In case threats were detected, the list of detected threats will appear. This list can be closed only when you apply an action to every threat. On the lock screen notification on detected threats will appear. On tapping the notification, the threat list appears.

For each threat in the list, the following information is displayed:

- Name of the threat
- Path to the file containing the threat

The type of threat detected as "not a virus" is displayed in brackets: adware, riskware, joke or hacktool program.

Performing actions over the threats

Tap the threat in the list to see the available actions and to apply one of them to the selected threat. **Dr.Web** allows to choose one of the following actions for detected threats:

- **Delete** – the threat is completely removed from the internal device memory.
- **Move to quarantine** – the threat is moved to a special folder where it is isolated from the rest of the system.

If a threat is detected in an installed application, it cannot be moved to quarantine. In this case the **Move to quarantine** action is missing in the list of actions.

- **Ignore** – the threat is temporarily ignored and no action is applied to it.
- **Report false positive** – you can send the threat to **Doctor Web** anti-virus laboratory to report that it is not harmful and was identified by the anti-virus as dangerous by mistake. Enter your email in order to receive the results of the file analysis. Tap **Submit**.

The **Report false positive** action is available only for the threat modifications with ".origin" postfix detected in the device system area.

You can set up sound notifications on threats detection, deletion or moving to quarantine. To do this, on the main screen open the application menu and tap **Settings**, then select the **Sounds** check box on the **General settings** section of the settings screen (see Figure 3).

Update

Dr.Web uses **Dr.Web** virus databases to detect threats. These databases contain details and signatures for all viruses and malicious programs for devices running Android known at the moment of the application release. However modern computer viruses are characterized by the evolvement and modification; also new viruses sometimes emerge. Therefore, to mitigate the risk of infection, **Doctor Web** provides you with periodical updates to virus databases via Internet.

On the main screen of the application the date of the last update is displayed on the section **Updating**.

Start update

1. To update virus databases tap the update section on the main screen.
2. Updating procedure will launch automatically.

It is recommended to update the virus databases on application installation to let **Dr.Web** use the most recent information about known threats. As soon as experts of the **Doctor Web** anti-virus laboratory discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour.

Configure updates

By default, the updates are automatically downloaded four times a day. On the **Updating** section of the settings screen (see Figure 3), you can enable/disable the use of mobile networks to download updates. Select the **Do not use mobile networks to download updates** check box to disable the use of the mobile networks to download the updates. If no Wi-Fi networks is available, you will be offered to use 3G or GPRS. Changing this setting does not affect the use of mobile networks by other application and device functions.

Updates are downloaded via Internet. You may be additionally charged by your mobile operator for the data transfer. For detailed information, contact your mobile operator.

Quarantine

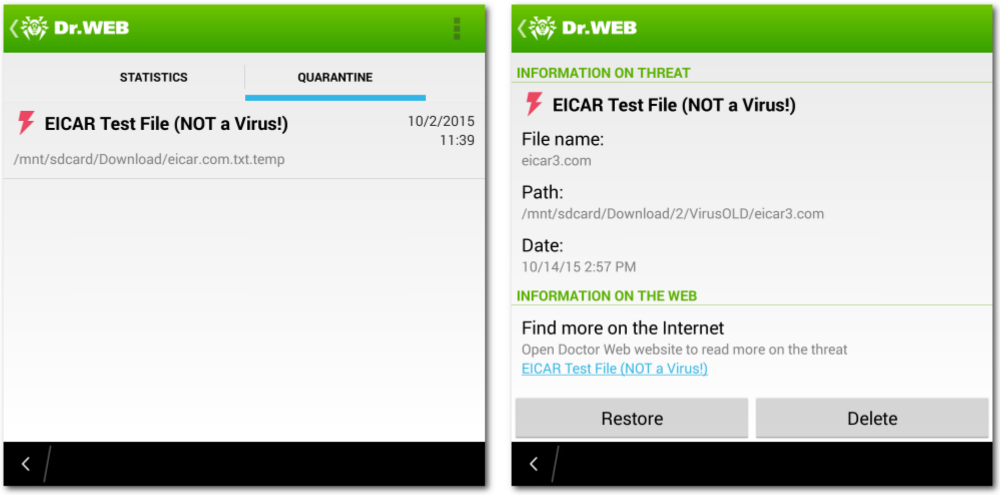
Dr.Web allows you to move the detected threats to quarantine, where they are isolated from the rest of file system and therefore cannot damage the system.

Manage files in quarantine

1. To review the list of the threats moved to quarantine, open the application menu on the main screen and then tap **Quarantine**.
2. The list of all threats in quarantine will open (see Figure 6).
3. Tapping the threat in the list brings you to the window with the following information on the threat (see Figure 7):
    - File name
    - Path to the file
    - Date of moving to quarantine

    You can also open the link on the **Information on the web** section to read the detailed information on the threat on **Doctor Web** official web-site.
4. For each threat in the list one of the following action can be performed:

- **Restore** – to return the file back to the folder where it was moved from (use this action only if you are sure that the file is safe).
- **Delete** – to completely remove the file from the device.



EICAR Test File (NOT a Virus!) 10/2/2015 11:39
/mnt/sdcard/Download/eicar.com.txt.temp

INFORMATION ON THREAT

EICAR Test File (NOT a Virus!)

File name:
eicar3.com

Path:
/mnt/sdcard/Download/2/VirusOLD/eicar3.com

Date:
10/14/15 2:57 PM

INFORMATION ON THE WEB

Find more on the Internet
Open Doctor Web website to read more on the threat
EICAR Test File (NOT a Virus!)

Figures 6 and 7. Quarantine

Quarantine size

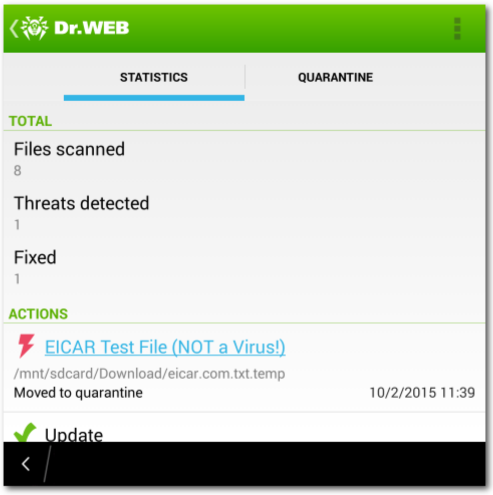
You can review the information on the internal device memory free space and space occupied by quarantine. To do this, open the application menu on the **Quarantine** tab and select **Quarantine size**.

Statistics

Dr.Web compiles the statistics of detected threats and application actions. To view the statistics, on the main screen open the application menu and then tap **Statistics**.

The **Statistics** tab contains two following information sections (see Figure 8):

- **Total** section contains the information on the total number of scanned files, detected and neutralized threats.
- **Actions** section contains the information on **Dr.Web Scanner** start/stop, **SpIDer Guard** enable/disable, detected threats and performed actions of the application. Tap the threat name to open its description on the **Doctor Web** website.



TOTAL

Files scanned
8

Threats detected
1

Fixed
1

ACTIONS

EICAR Test File (NOT a Virus!)
/mnt/sdcard/Download/eicar.com.txt.temp
Moved to quarantine 10/2/2015 11:39

Update

Figure 8. Statistics

Clear statistics

To clear all the statistics, open the application menu and tap **Actions**.

Event log

Dr.Web logs the events related to its operation in a special file that can be saved in the internal device memory for further analysis in case you experience troubles while using **Dr.Web**.

To save the event log:

1. Open the application menu on the **Statistics** tab and then tap **Save log**.
2. The log will be saved in DrWeb_Log.txt file located in the **downloads** folder in the internal device memory.

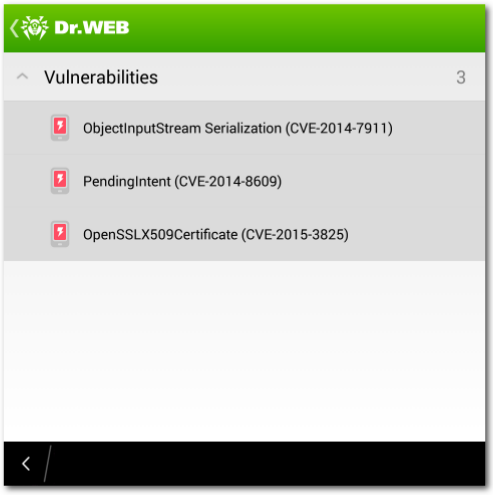
Security Troubleshooting

Dr.Web performs diagnostics of the security of your device and helps resolving the detected problems and vulnerabilities using a special component - **Security Auditor**. This component is enabled automatically when the application is launched for the first time and after registering the license. The number of the detected problems is displayed on the **Security Auditor** section of the main application screen.

If no problems or vulnerabilities are detected by **Security Auditor** in the operation system of your device, the corresponding section is not displayed on the main application screen.

Resolving security problems

To review the list of the detected problems and vulnerabilities (see Figure 9), tap the **Security Auditor** section on the main application screen.



ObjectInputStream Serialization (CVE-2014-7911)
PendingIntent (CVE-2014-8609)
OpenSSLX509Certificate (CVE-2015-3825)

Figure 9. List of security problems detected on the device

To view the detailed information on any detected problem and to resolve it, open one of the categories and tap a problem in the list.

Hidden device administrators

Applications that are activated as device administrators but not shown on the list of administrators on the corresponding section of the device settings cannot be deleted by means of the operation system. Most likely, such applications are dangerous.

If you don't know why such application is not displayed in the list of device administrators, it is recommended to delete it from the device. To delete the application, tap **Delete** on the screen with the detailed information on the problem related to this application.

Vulnerabilities

Dr.Web detects such vulnerabilities as Master Key (#8219321), Extra Field (#9695860), Name Length Field (#9950697), Fake ID (#13678484), ObjectInputStream Serialization (CVE-2014-7911), PendingIntent (CVE-2014-8609), Android Installer Hijacking, OpenSSLX509Certificate (CVE-2015-3825), Stagefright in the device system. They allow adding malicious code to some applications, that may result in acquisition of dangerous functions by these applications and damage the device. **Dr.Web** also detects the Heartbleed vulnerability, that can be used by fraudsters to access the user confidential information.

If one or more of these vulnerabilities are detected on your device, check for operation system updates on the official website of your device manufacturer. Newer versions may have these vulnerabilities fixed. If there are no updates yet, it is recommended to install applications only from trusted sources.

Applications exploiting Fake ID vulnerability

If applications exploiting Fake ID vulnerability have been detected on the device, they will be displayed in the separate **Security Auditor** category. These applications can be malicious, therefore it is recommended to delete them. To delete the application, tap **Delete** on the screen with the detailed information on the problem related to this application, or use standard OS tools.

Appendicies

This section contains additional information on working with **Dr.Web**:

Appendix A. Technical Support

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

- Download and review the latest manuals and guides at http://download.drweb.com/doc/.
- Read the frequently asked questions at http://support.drweb.com/show_faq/.
- Browse the **Dr.Web** official forum at http://forum.drweb.com/.
- Request assistance or read the frequently asked questions on your personal My Dr.Web webpage.

If you have not found solution for the problem, you can fill 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 website at http://company.drweb.com/contacts/moscow.

Index

Index