Dr.WEB®

Light

for Android

Defend what you create

User Manual

© Doctor Web, 2015. 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, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk and the Dr.WEB 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 Light for Android
Version 9.01.2
User Manual
24.12.2015

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 *Light* for Android** (hereinafter referred to as **Dr.Web *Light***). This anti-virus solution offers a reliable protection of the mobile devices working under the Android™ 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.

Dr.Web *Light* uses Origins Tracing™ for Android—the unique algorithm to detect malware designed specially for Android. This algorithm allows detecting the new virus families using the knowledge database on previous threats. Origins Tracing for Android can identify the recompiled viruses, e.g. Android.SMSSend, Android.MobileSpy, as well as the applications infected by Android.ADRD, Android.Geinimi, Android.DreamExploid. The names of the threats detected using Origins Tracing for Android are Android.VirusName.origin.

This manual is intended to help users of the devices running Android to install and adjust **Dr.Web *Light***. 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 *Light* 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)
- Detection of Windows autorun files
- Threats detection in the *.lnk files (defined by **Dr.Web** as Exploit.Cpllnk)
- Deletion of the infected objects or their isolation in quarantine

- Device unlocking if it is locked by ransomware
- **Dr.Web** virus databases updates via Internet
- Statistics of the detected threats and performed actions, application log

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

Dr.Web *Light* also supports working in Multi-Window mode that allows you to launch several applications in separate windows. This mode can be used only on Samsung Galaxy S III or higher version and Samsung Galaxy Note 2 or higher version.

System Requirements

To install and use **Dr.Web *Light***, ensure your mobile device works under the Android operating system of version 4.0/4.1/4.2/4.3/4.4/5.0/5.1.

The Internet connection is required for virus databases update procedure.

Please note that the correct operation of **Dr.Web *Light*** is not guaranteed on the devices with custom ROMs and on the "rooted" devices.

By default, the application is installed to the internal device memory. For correct operation of **Dr.Web *Light*** do not transfer the installed application to removable media.

Chapter 2. Installation

Dr.Web *Light* can be installed on the device directly from Google Play or by launching the installation file. You can also install the application using the synchronization with PC.

The application can be removed via Google Play or by means of the operating system of the device.

Install Application

You can install **Dr.Web *Light*** either via Google Play or launch the application installation file on the device or via synchronization with PC.

Install via Google Play

1. On your device, open Google Play, find **Dr.Web *Light*** in the list of applications and tap **Install**.

   If your device does not meet the system requirements, **Dr.Web *Light*** is not displayed in the list of Google Play.

2. Then the screen containing the information on device functions which the application needs to access will appear.
   - For application registration and license activation, Internet access and access to the list of Google accounts of the device are required.
   - 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.

For application installation without Google Play, you need to allow it on your device. To do this, select the **Unknown sources** check box on the **Settings** -> **Security** screen. The installation file of **Dr.Web *Light*** is available for download on the **Doctor Web** website.

Install via launching the installation file on the device

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**.

Install via device synchronization with PC using special synchronization software (e.g., HTC Sync™ etc.)

1. Synchronize your device with the PC.
2. Launch the installation manager included into the synchronization software package.
3. Specify the path to the file located on the computer, then follow the instructions of the installation wizard.
4. The application will be copied to the device where you can review the information on it and confirm the installation.
5. Close the installation wizard.

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

Update and Uninstall Application

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

Update or uninstall application via Google Play

1. Open Google Play and select **My Apps**.
2. Tap the sign of **Dr.Web *Light*** in the list of downloaded applications.

> If **Dr.Web *Light*** was installed without Google Play, it would not be shown in the **My Apps** section. In this case you can delete it by means of the operating system.

3. On the screen with the information on the application tap **Update** or **Uninstall**.

> The **Update** button is unavailable if a new version of the application has not been released yet.

4. Confirm the application update/removal.
   - In case you are updating the application, tap **Accept** to allow access to required device functions. The application will be installed automatically. Tap **Open** to start using the application.
   - In case you are uninstalling the application, tap **OK**. The application will be removed from the device.

Uninstall application without connecting to Internet

1. Open the **Settings** -> **Applications** screen.
2. Tap the **Dr.Web *Light*** sign in the list of installed applications.
3. On the screen with the information on the application tap **Uninstall**. The application will be removed from the device.
4. Tap **OK** to return to the list of the installed applications.

Chapter 3. Getting Started

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

Launch and Exit Application

Launch the application

To launch **Dr.Web *Light***, open the **All programs** screen and tap **Dr.Web *Light*** 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. You will be notified in the same window about sending the statistics on the application operation and the detected threats to **Doctor Web** and Google servers. Sending the statistics can be disabled only when using the extended version of **Dr.Web**.

Exit the application

To exit **Dr.Web *Light***, press the **Home**  button.

You can use the **Dr.Web *Light*** sign  in the recently launched applications section to activate the application from the background operation.

When you first launch **Dr.Web *Light***, the application opens on its main screen. When you activate the application from the background operation, the application opens on the last active screen.

Interface

On the application main screen (see Figure 1) the current protection status is displayed. It also provides access to the following application functions:

- **Get full version now**—allows to learn about **Dr.Web Security Space** and download it from Google Play
- **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

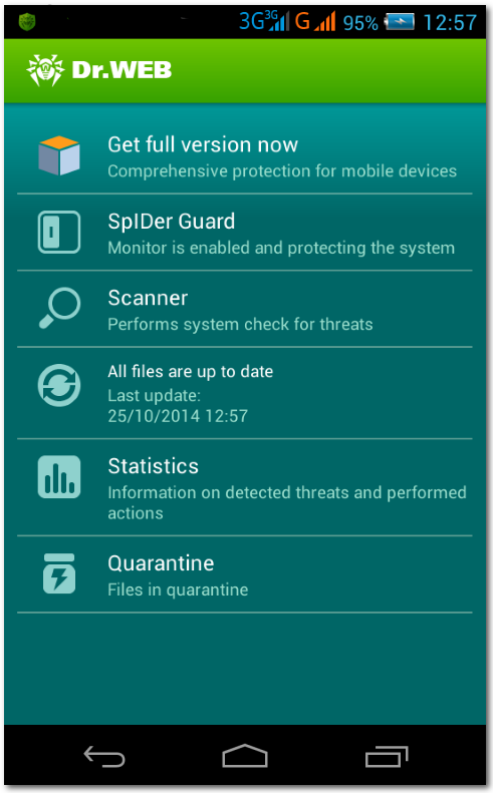


Figure 1. Main screen of the application

Access 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. 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.

Widgets

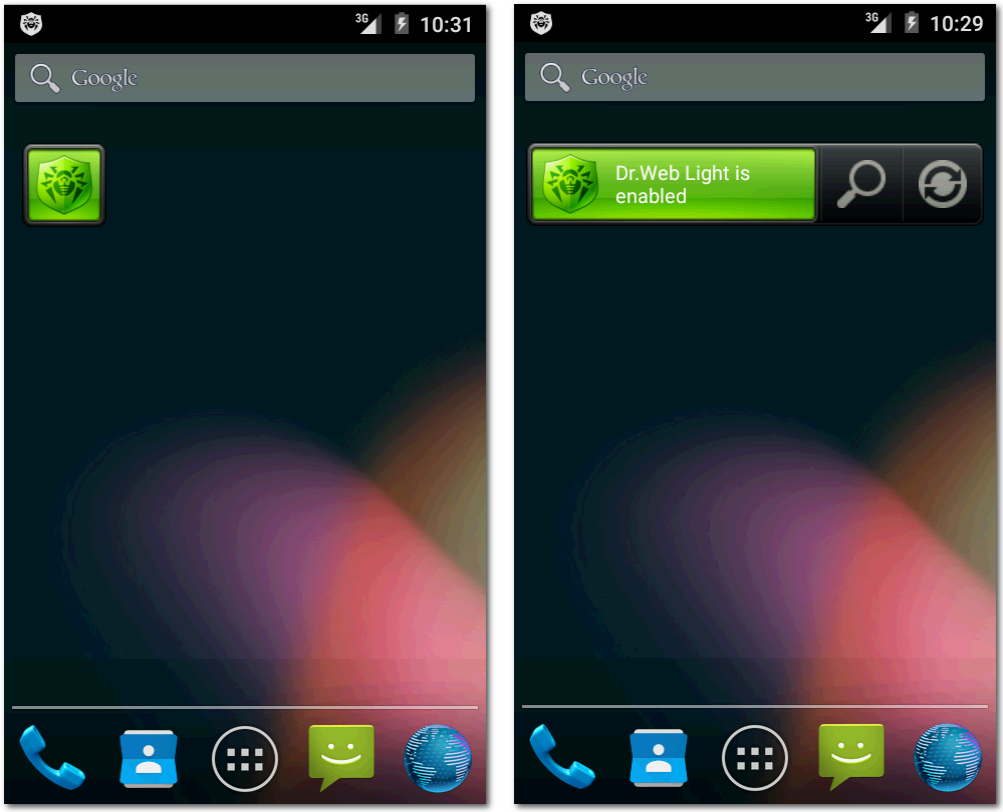
To make the work with **Dr.Web *Light*** easier and more convenient, you can add on your device **Home Screen** the special widgets which allow to manage the main application functions.

Widgets are unavailable on Android TV devices.

Add a widget

1. Open the list of available widgets using the standard widget adding feature of your device.
2. Select one of **Dr.Web *Light*** widgets in the list:
   - **Dr.Web 1×1 (small)**—displays the current protection status and allows to enable/disable **SpIDer Guard** (see Figure 2)
   - **Dr.Web 4×1 (medium)**—displays the current protection status and allows to enable/disable **SpIDer Guard**, open **Dr.Web Scanner** screen and start the virus databases update (see

Figure 3)



Figures 2 and 3. Dr.Web widgets

Notifications

Dr.Web *Light* features a special pane in the notifications area on the device screen providing a quick access to the main application functions (see Figure 4). You can enable/disable this type of notifications using the **Notifications pane** option on the **General settings** section (see Figure 5).

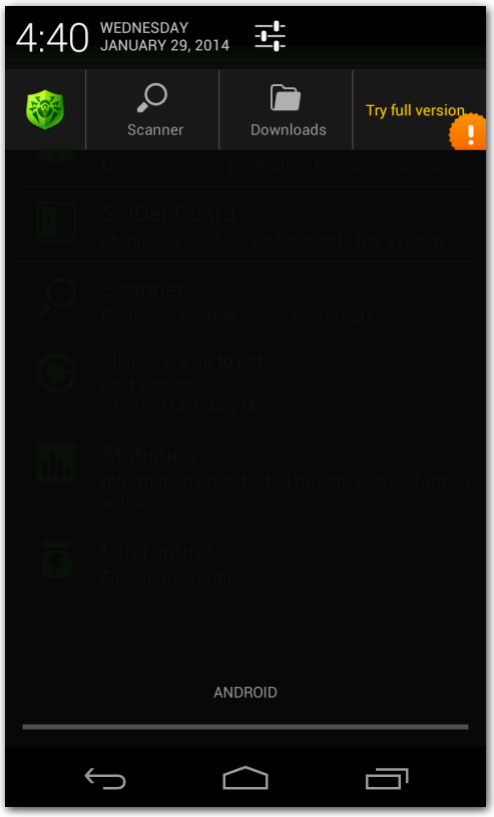


Figure 4. Notifications pane

Using the pane, you can perform the following actions:

- Open the application main screen. To do this, tap the **Dr.Web** icon.
- Launch express, full or custom scan by tapping **Scanner** and then selecting the scan type.
- Launch the downloads scan by tapping **Downloads** and then selecting objects to scan in the **Downloads** folder.
- Review the information on **Dr.Web Security Space** and download it for free trial use during 14 days.

In case threats are detected, the icons in the notifications pane change to indicate it:

- —if the threats are detected by **Dr.Web Scanner**
- —if the threats are detected by **SpIDer Guard**

On Android 5.0 and higher, if a threat is detected, notification pane will be opened until you apply some action to the threat.

Chapter 4. Application Functions

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

To open the settings screen (see Figure 5), on the main screen open the application menu and select **Settings**.

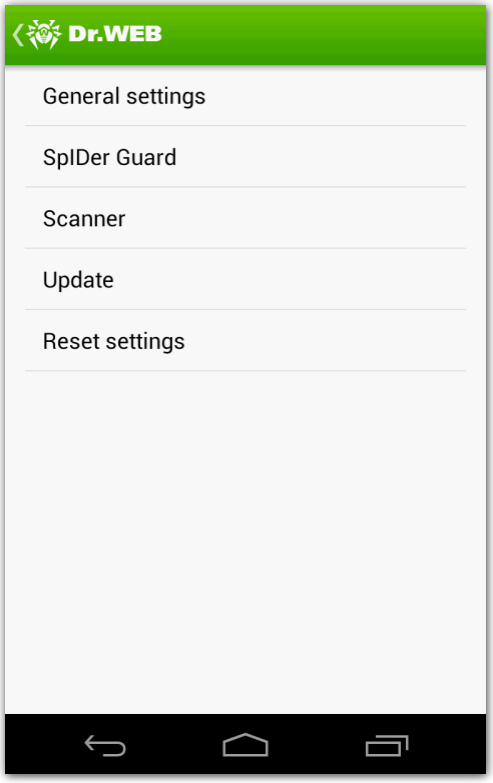


Figure 5. Application settings

Reset settings

You can reset the user settings of the application at any time and restore the standard settings.

1. Tap **Reset settings** on the settings screen (see Figure 5). 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 checks all files in the device memory 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 alerting sign  (on Android 5.0 and higher— ) appears in the status bar on the screen as well as a popup window notifying about the threats detection. From the notifications pane, you can open the full list of malicious objects in order to select actions to neutralize them.

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

SpIDer Guard settings

To access **SpIDer Guard** settings, open the application settings screen (see Figure 5).

- 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 files regardless of the **Files in archives** parameter value.

- To enable check of the files on the SD card (or other external storage) on each mounting, select the **SD card mounting** check box on the **SpIDer Guard** section.
- To enable/disable 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.
- To enable device memory check for Windows auto run files, select the **Autorun files** check box on the **General settings** section. This option configures the on-demand scans as well.
- To show the sign  (on Android 5.0 and higher— ) in the status bar on **SpIDer Guard** activity, select the **Ongoing notifications** check box on the **General settings** section.

Statistics

Dr.Web *Light* registers the events related to **SpIDer Guard** operation (enable/disable, 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 *Light* 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.

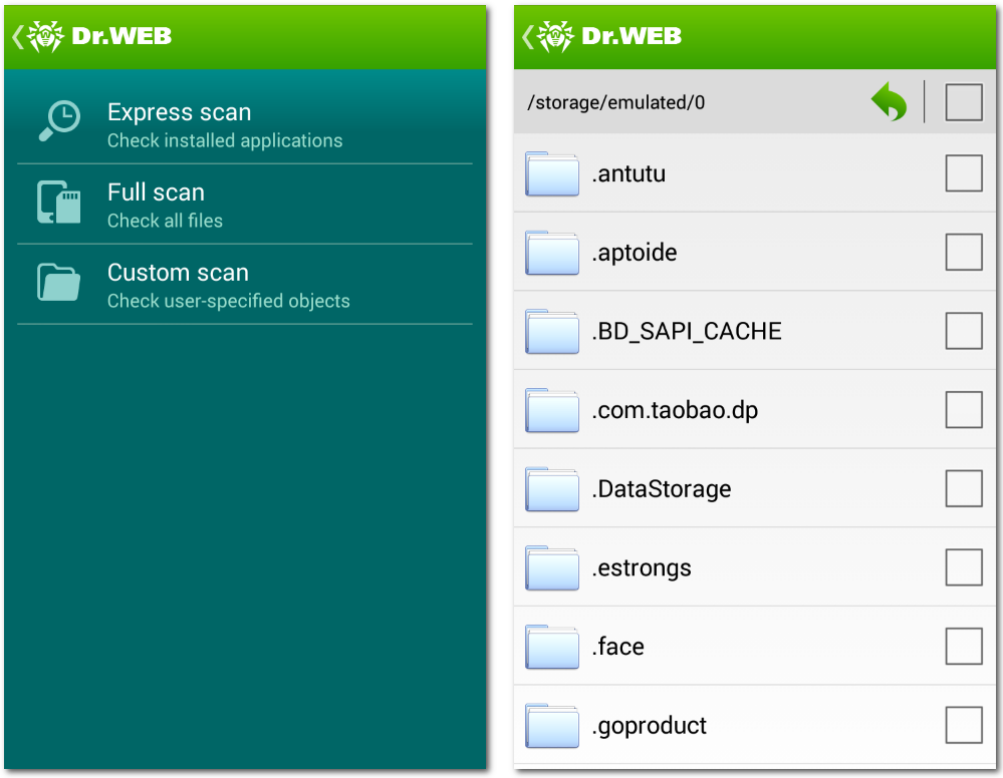
Perform scanning

To scan the system, on the main screen tap **Scanner** and on the opened screen (see Figure 6) 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 7) 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 6 and 7. Dr.Web Scanner and custom scan screens

Send suspicious files to Doctor Web anti-virus laboratory

You can submit suspicious ZIP archives (including *.jar, *.apk), 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 6), 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, open the application settings screen (see Figure 5).

- 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 **Dr.Web Scanner** checks all *.apk files regardless of the **Files in archives** parameter value.

- To enable/disable 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 *Light* 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

View the list of detected threats

In case threats were detected by **SpIDer Guard**, the sign  (on Android 5.0 and higher— ) appears in the status bar on the screen. A tooltip notifying about the threats detection is also displayed on the screen. From the notifications pane, you can open the full list of malicious objects in order to select actions to neutralize them.

On Android 5.0 and higher, if a threat is detected, notification pane will be displayed on the top of all applications until you apply some action to the threat or until you swipe over the threat notification. Moreover, on Android 5.0 and higher, the threat notification will appear on the lock screen from which you can go to the threat list.

When scanning your device by **Dr.Web Scanner**, the list of the detected threats opens automatically after the scan is completed. The list of threats can be closed only when you apply an action to every threat.

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.

Perform actions over the threats

Tap the threat in the list and select one of the following actions:

- **Delete**—the threat is completely removed from the 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 5).

Threats Detection in System Applications

The applications installed in the system area in some cases can perform functions that are typical for malware, so during the scanning by **Dr.Web *Light*** such applications are detected as security threats. If these applications were installed by the device manufacturer, the standard threats neutralization actions are not applicable to them, but you can use the following guidelines:

If the system applications detected as threats were not installed by the device manufacturer, the standard threats neutralization actions can be applied to them only in the full version of anti-virus in case your device is rooted.

- Stop the application from the device settings (open the **Settings** -> **Applications** screen and tap the application detected as threat, then on the screen with information on this application, tap **Stop**)

This action needs to be redone every time the device is restarted.

- Disable the application from the device settings (open the **Settings** -> **Applications** screen and tap the application detected as threat, then on the screen with information on this application, tap **Disable**)
- If a custom operating system (ROM) is installed on the device, you can restore the official software of your device manufacturer by yourself or in a service center
- If you are using official software of the device manufacturer, try to contact the vendor for more information on this application
- If your device is rooted, you can try to delete this application using special tools and utilities

To disable the notifications about threats detection in known system applications, select the **System applications** check box on **General settings** -> **More options** section of the settings screen (see Figure 5).

Processing Device Lockers

Dr.Web *Light* protects the mobile devices against ransomware programs targeting Android users that expanded markedly. These programs pose severe danger to Android smart phones and tablets. They can encrypt the files on external storage, lock the device screen and display a ransom demand for the decryption of the files and unlock the device.

Photos, videos and documents located on external storage can be compromised by such malicious programs. In addition, they steal and transmit to the intruders' servers various information about the infected device (including, for example, its IMEI), information from the infected device's phone book (contact names, phone numbers and email addresses). Ransomware programs **SpIDer Guard** incoming and outgoing communications and can bar those communications if desired. All the information collected, including phone call data, is also transmitted to the control server.

Dr.Web *Light* detects and removes ransomware programs whenever they try to penetrate a protected device. However, they are characterized by the high-speed evolvement and modification. So, especially if **Dr.Web** virus databases have not been updated for some time and do not contain information on new examples, the device lockers can be installed on the device.

If your mobile device is locked by a ransomware program and **SpIDer Guard** is enabled on it, you can unlock your device by performing the following actions:

1. In 5 seconds, plug and unplug a charger.
2. In the next 10 seconds, plug earphones.
3. In the next 5 seconds, unplug earphones.
4. In the next 10 seconds, shake your device briskly.
5. **Dr.Web *Light*** ends all active processes on the device, including the one of the application locker, and then activates a vibration signal (on the devices which have this feature). Then **Dr.Web *Light*** screen will open.

Please note that ending active processes can result in losing data of other applications that were active when the device was locked.

6. After the device is unlocked, it is recommended to update **Dr.Web** virus databases and perform an express scan of the system, or to delete the malicious application from your device.

Update

Dr.Web *Light* 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 *Light*** 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 5), 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 *Light* 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 8).
3. Tapping the threat in the list brings you to the window with the following information on the threat:
   - 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

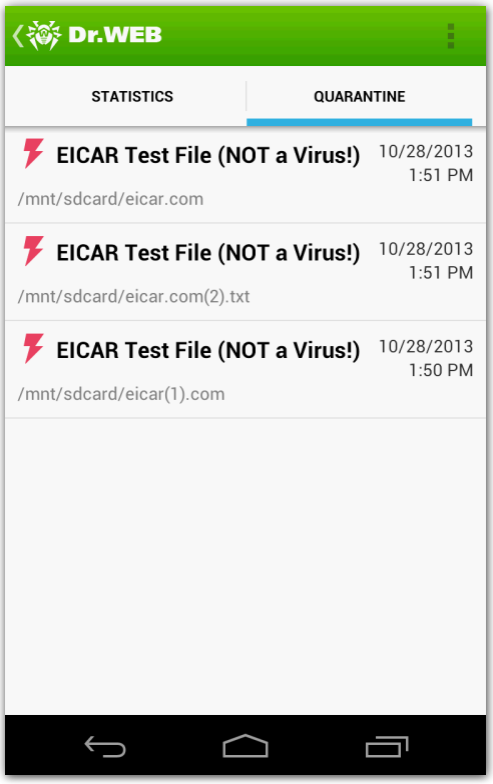


Figure 8. Quarantine

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 *Light* 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 9):

- **Total**—contains the information on the total number of scanned files, detected and neutralized threats.
- **Actions**—contains the information on **Dr.Web Scanner** check results, **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.

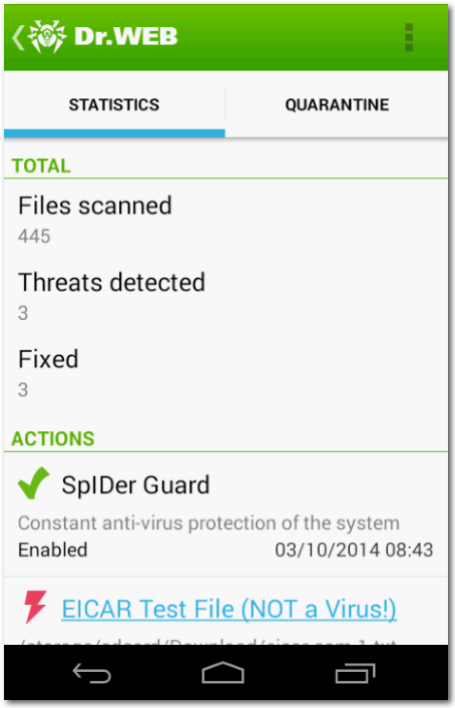


Figure 9. Statistics

Clear statistics

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

Save event log

You can save application event log for further analysis in case you experience troubles while using the application.

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 **Android/data/com.drweb/files** folder in the internal device memory.

Index

Index

© Doctor Web, 2015