



Dr.WEB®

**Security Space
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 Security Space for Android
Version 10.01.2
User Manual
30.11.2015

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	6
Document Conventions	6
Main Features	6
System Requirements	7
Chapter 2. Licensing	8
Activate Demo Period	9
Purchase License	10
Activate License	11
Update License	12
Chapter 3. Installation and Removal	13
Install Application	13
Update and Uninstall Application	14
Chapter 4. Getting Started	16
Launch and Exit Application	16
Interface	16
Widgets	18
Notifications	18
My Dr.Web	20
Chapter 5. Application Functions	21
Anti-virus Protection	22
Constant Anti-virus Protection	22
On-Demand Scan	23
Threats Neutralization	25
Threats Detection in System Applications	26
Processing Device Lockers	27
Calls and SMS Filter	27
Filtering Mode	28
Black List	28
Filtering Profiles	29
View Blocked Calls and SMS	30
Update	31
Quarantine	32
Statistics	33



Dr.Web Anti-theft	34
Configure General Settings	35
Additional Functions	37
Buddies List	38
SMS Commands	38
Unlock Dr.Web Anti-theft	40
Restricting Internet Access	40
Dr.Web Firewall	42
Limit the Use of Mobile Internet	44
Processing Applications Traffic	45
Internet Traffic Statistics	47
Connection Rules	47
Current Internet Activity	48
Logging	49
Dr.Web Firewall Log	49
Application Logs	50
Security Troubleshooting	51
URL Shortening Service	53
Chapter 6. Operation in Central Protection Mode	54
Switching to Central Protection Mode	54
Application Filter	56
Switching to Standalone Mode	56
Chapter 7. Working with Dr.Web on Android TV	57
Appendices	58
Appendix A. Technical Support	58
Index	59



Chapter 1. Introduction

Thank you for choosing **Dr.Web Security Space for Android** (hereinafter referred to as **Dr.Web**). This anti-virus solution offers a reliable protection of the mobile devices working under the Android™ operating system as well as TV sets, media players and game consoles working under Android TV™ platform 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 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**. 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.
<u>Green and underlined</u>	Hyperlinks to topics and webpages.
<i>Italic</i>	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
	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)
- 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
- Filtering the unsolicited calls and SMS using the predefined and custom black and white lists settings
- **Dr.Web** virus databases updates via Internet
- Statistics of the detected threats and performed actions, application log
- Detecting the device location or locking its functions in case it has been lost or stolen
- Restricting access to the undesirable Internet resources when using Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser and Boat Browser Mini
- Scanning and shortening URLs
- Analyzing the security of the device and help in resolving the detected problems and vulnerabilities
- Controlling the Internet connections, protecting your device from unauthorized access and preventing leak of vital data through networks



Some of the listed functions are not available for the application installed on [Android TV](#) devices. For details see [Working with Dr.Web on Android TV](#) section.

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

Dr.Web 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**, 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. **Dr.Web** also operates on TV sets, media players and game consoles based on Android TV platform.

The Internet connection is required for virus databases update procedure. If you are using a tablet, for correct operation of calls and SMS filtering and **Dr.Web Anti-theft**, it is required to support the use of SIM cards.



Please note that the correct operation of **Dr.Web** is not guaranteed on the devices with custom ROMs and on the "rooted" devices. Technical support is not also provided for such devices.

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



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**.



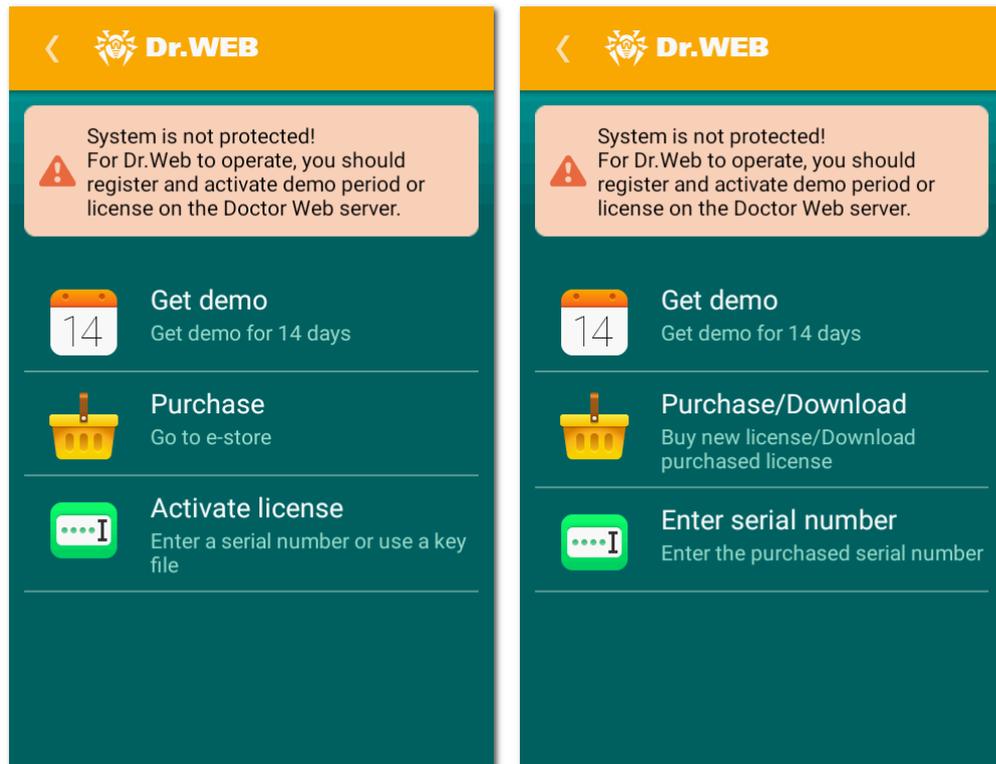
In case you purchase the application version with the unlimited license (**Dr.Web Security Space Life**) from Google Play, the license key file is received and registered automatically.

When [central protection mode](#) is activated, the license is automatically downloaded from the central protection server.

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

Open the licensing screen

1. Open the application menu on the main screen of the application (see [Figure 2](#)) or, if the application operates on [Android TV](#) device, select the **About** section on the main screen.
2. Tap the **Renew license** button.



Figures 1a and 1b. 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.

Demo period activation procedure depends on the **Dr.Web** installation type.



If the application was installed from Google Play

1. Tap **Get demo** on the licensing screen (see [Figure 1b](#)). Demo period will be activated automatically for the email address of your Google account shown in the **Get demo** section. If you have several Google accounts, the first of them will be selected for activating.
2. If you do not have a Google account, the window for entering an email address will appear. Enter your email address and tap **Get demo**. Demo period will be activated.

If the application was installed from the Doctor Web website

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

Purchase License

License purchasing procedure depends on the **Dr.Web** installation type.



License purchasing is unavailable from the application installed on [Android TV](#) devices. You can purchase a license directly in Google Play or [Doctor Web web store](#).

If the application was installed from Google Play

1. On the licensing screen (see [Figure 1b](#)), select **Purchase/Download**.
2. If you do not have a Google account, the window for entering an email address will appear. This address will be used for license registration. This will allow you to download the purchased key file to use with **Dr.Web** in case you re-install the application or install it on another device. Enter your email address and tap **Get license**.
3. On the **Purchase license** screen, select one of the license types:
 - **1 year license, 2 year license or 1 year license without technical support**. If you select one of these license types, the standard application purchase window will appear. After completing the payment, the corresponding license will be activated automatically. Once the download completes, the information on the license and its validity period will be displayed on the screen. If the download did not start because of a technical issue, please contact the **Doctor Web** technical support.
 - **Unlimited license**. If you select the license without any time limits, you'll be brought to the **Dr.Web Security Space Life** product [purchase and installation](#) in Google Play. If you used **Dr.Web**, you'll be asked to delete it. Tap **OK** to confirm the removal. If you want to save application settings in order to use them with **Dr.Web Security Space Life**, [export](#) the current configuration to file before deleting the application.



If you have **Dr.Web Anti-theft** enabled on your device, clear the **Dr.Web Security Space** check box on the **Location and Security** tab of the **Select device administrator** section in the device settings before uninstalling **Dr.Web** (the names of settings can be different depending on the device model and operating system version). Your device will be locked by **Dr.Web Anti-theft**. Enter the password set for **Dr.Web Anti-theft** to continue the application removal.

The license file will be downloaded and installed automatically during the installation of **Dr.Web Security Space Life**.

If the application was installed from the Doctor Web website

1. Tap **Purchase** on the licensing screen (see [Figure 1a](#)) 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, depending on the **Dr.Web** installation type.

If the application was installed from Google Play

- If you already activated a license or demo period, on the licensing screen (see Figure 1b), tap **Purchase/Download**. Enter the email address that you have previously used to register the license if necessary. The license registered on the specified email address will be restored automatically from the server.
- If you have a serial number, you can register it:
 1. On the licensing screen (see [Figure 1b](#)), tap **Enter serial number**.



The serial number received to activate the demonstration period of **Dr.Web** product for workstations cannot be used with **Dr.Web** version installed from Google Play. You need to activate the demo period for the corresponding **Dr.Web** product on PC at first, so that you will get the license key file, then you can [copy](#) it to the device. The instructions on using the received license key file on devices will be sent to you by email during the demonstration period activation.

2. Enter the serial number and tap **Get license**.

If the application was installed from the Doctor Web website

The activation methods listed below are available.

Register serial number

1. On the licensing screen (see [Figure 1a](#)) 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**.

Copy key file on the device

1. Synchronize your device with PC and copy the key file to the **Android/data/com.drweb/files** folder located in the internal device memory.
2. On the licensing screen (see [Figure 1a](#)) 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

- **On Android.** On the main screen (see [Figure 2](#)), open the application menu and tap **About**.
- **On Android TV.** On the main screen (see [Figure 20](#)), select the **About** section.

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 6](#)).

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 purchased and 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** 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** in the list of applications and tap **Install** or **Purchase** (if you want to install **Dr.Web Security Space Life** version with unlimited license).



If your device does not meet the [system requirements](#), **Dr.Web** is not displayed in the list of Google Play.

2. If you have selected **Dr.Web Security Space Life** version, to continue the installation, you need to complete payment.
3. 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 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 calls and SMS filtering, access to calls and SMS receiving/sending function, permissions for reading contact list, calls and messages logs and changing signals (to turn off sound if the call is blocked) are required.
 - For **Dr.Web Anti-theft** operation, permissions for sending SMS (to send **Dr.Web Anti-theft** messages about changing SIM card and replies to received commands), getting device coordinates, GPS and Wi-Fi managing and deleting all personal information from the device (in case a corresponding command is received) are required.
 - For **Cloud Checker** URL filter operation, access to browsing history and bookmarks of the supported browsers is required.
 - For using floating window with the information on current traffic, permission to display interface elements on the top of other windows is required.
 - For updating virus databases, access to Internet and device network settings is required.

Tap **Accept**.



4. 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** 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 was successfully installed on your device and is ready to use. For further operation of the application you need to activate a [license](#) or [demo period](#) (except **Dr.Web Security Space Life**).

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.



In case **Dr.Web Anti-theft** is enabled on your device, you need to clear the **Dr.Web Security Space** check box on the **Location and Security** tab of the **Select device administrator** section in device settings before uninstalling the application (the names of settings can be different depending on the device model and the operating system version).

Update or uninstall application via Google Play

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



If **Dr.Web** 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** 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.



Quarantine and saved application log are not deleted by default. You can delete them manually from the `Android/data/com.drweb/files` folder in the internal device memory.

Check the availability of the new version of application

If you downloaded and installed **Dr.Web** from **Doctor Web** website, you can enable check for the new version availability every time the virus databases are updated. To do this, select the **New version of app** check box in the application [update](#) settings section. When a new version of the application becomes available, you will get a standard notification to download and install it.



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

Launch the application

- **On Android.** Open the **All programs** screen and tap **Dr.Web** sign .
- **On Android TV.** Go to the **Apps** section and select **Dr.Web** in the list of available applications.

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](#).



If **Dr.Web** was installed via the *.apk file provided by the [anti-virus network administrator](#) of your company, you will not need to read and accept the License agreement.

Exit the application

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

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

When you first launch **Dr.Web**, 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 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
- **Calls and SMS filtering**—allows to specify the filtering mode and review the lists of blocked calls and messages



If you are using a device without SIM cards support, the calls and SMS filtering and **Dr.Web Anti-theft** are not available, so the corresponding sections are absent on the main application screen. On [Android TV](#) devices, **Dr.Web Firewall** is also unavailable.

- **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
- **Anti-theft**—allows to configure **Dr.Web Anti-theft**
- **Cloud Checker**—allows to configure the URL-filter to restrict user access to the Internet resources
- **Firewall**—allows to configure control of the Internet connections and data transfer over the network
- **Security Auditor**—allows to perform the diagnostics of the system and helps to resolve the detected security problems and vulnerabilities

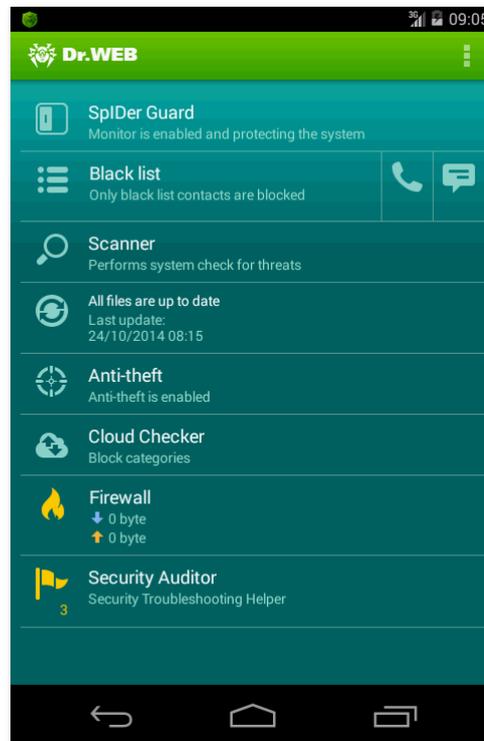


Figure 2. Main screen of the application

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, to access [quarantine](#) and application [statistics](#), 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, your [personal web page](#) there and to the pages of the company in social networks: Twitter, Facebook, Instagram, and to its Youtube channel. If **Dr.Web** is operating in central protection mode and is used to connect to **Dr.Web AV-Desk** anti-virus service, the screen also contains the subscription expiration date or the date when the service was blocked for the device (station).



On [Android TV](#) devices, the application menu is unavailable. You can find information on the application version, the license owner and its activation and expiration dates in the **About** section on the main application screen.



Widgets

To make the work with **Dr.Web** 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** widgets in the list:
 - **Dr.Web 1×1 (small)**—displays the current protection status and allows to enable/disable **SpIDer Guard** (see [Figure 3](#))
 - **Dr.Web 4×1 (medium)**—displays the current protection status, the selected filtering profile, the number of blocked calls and messages and allows to enable/disable **SpIDer Guard**, open **Dr.Web Scanner** screen (see [Figure 4](#))



Figures 3 and 4. Dr.Web widgets

Notifications

Dr.Web features a special pane in the notifications area on the device screen providing a quick access to the main application functions (see [Figure 5](#)). You can enable/disable this type of notifications using



the **Notifications pane** option on the **General settings** section (see [Figure 6](#)).



Notification pane is unavailable on [Android TV](#) devices.

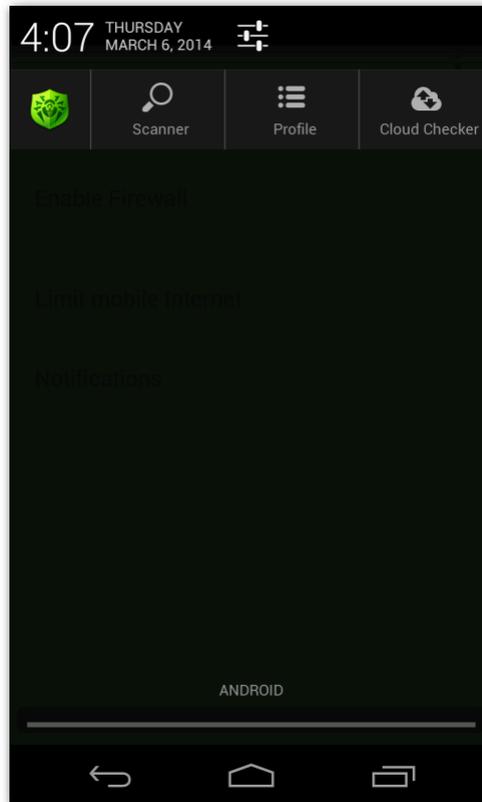


Figure 5. Notifications pane

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.
- Select the calls and SMS filtering profile by tapping **Profile**.
- Open the URL filter configuration screen by tapping **Cloud Checker**.



If your device does not support the use of SIM cards, the notifications pane contains the **Downloads** option allowing to launch the downloads scan instead of the **Profile** one.

If **Dr.Web** operates in [central protection mode](#) and you do not have permissions to change calls and SMS filter and/or **Cloud Checker** settings, **Profile** and/or **Cloud Checker** options will be unavailable in the notifications pane.



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.

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 of setting up the anti-virus check, SMS and calls filtering, the operation of **Dr.Web Anti-theft** and URL filter for configuring protection of your device.



Application settings are unavailable on [Android TV](#) devices.

To open the settings screen (see [Figure 6](#)), on the main screen open the application menu and select **Settings**.

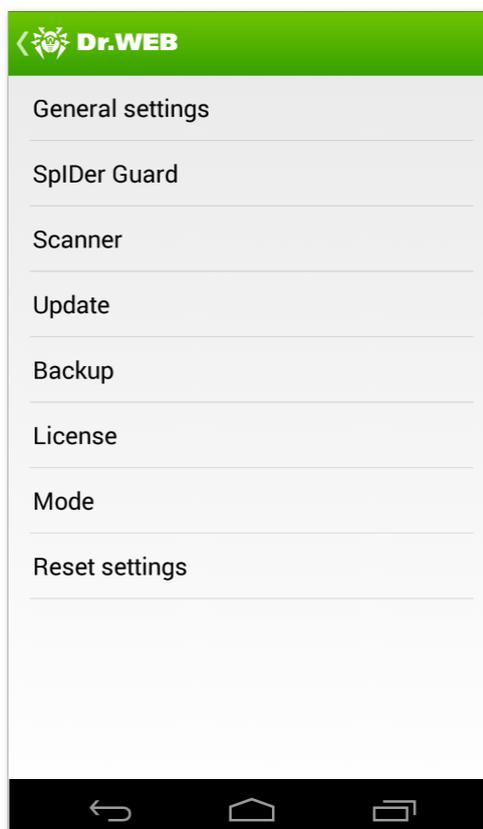


Figure 6. Application settings



If [Dr.Web Anti-theft](#) is enabled, you will need to enter **Dr.Web Anti-theft** password before changing certain application settings (**Reset settings**, **Backup** and **Mode**).

Reset settings

You can reset the user settings of the application, including calls and SMS filter, **Dr.Web Anti-theft**, **Dr.Web Firewall** and **Cloud Checker** settings, at any time and restore the standard settings.

1. Tap **Reset settings** on the settings screen (see [Figure 6](#)). On the opened screen, tap **Restore default settings** item.
2. Confirm the return to the default settings.



Import and export settings

You can also save all current application settings to the file in the internal device memory. You will be able to re-use them in future (for example, in case you re-install **Dr.Web** or use it on another device) by downloading from the file.

- To save the current configuration, on the settings screen (see [Figure 6](#)) tap **Backup** and then tap **Export settings**. In the opened window enter the password to set up for protection of the settings file, then tap **OK**. All settings are saved in the **Android/data/com.drweb/files/DrWebPro.bkp** file in the internal device memory.
- To load the saved settings from the file, on the settings screen (see [Figure 6](#)) tap **Backup** and then tap **Import settings**. Confirm the settings and parameters loading from the file and enter the password of file. All current application settings will be replaced by the settings from the file.

Anti-virus Protection

The main function implemented in **Dr.Web** is the ability to constantly scan the file system in [real-time mode](#). **Dr.Web** also performs system [on-demand scans](#). On security threats detection, **Dr.Web** performs [actions](#) selected by the user.

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.



In the [central protection mode](#) some features and settings of **SpIDer Guard** may be modified and blocked for compliance with the company security policy or according to the list of purchased services.

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**.

SpIDer Guard settings

To access **SpIDer Guard** settings, open the application settings screen (see [Figure 6](#)).

- 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 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 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.



In the **central protection mode** some features and settings of **Dr.Web Scanner** may be modified and blocked for compliance with the company security policy or according to the list of purchased services. Scanning may be performed in accordance with the schedule specified on the central protection server.

Perform scanning

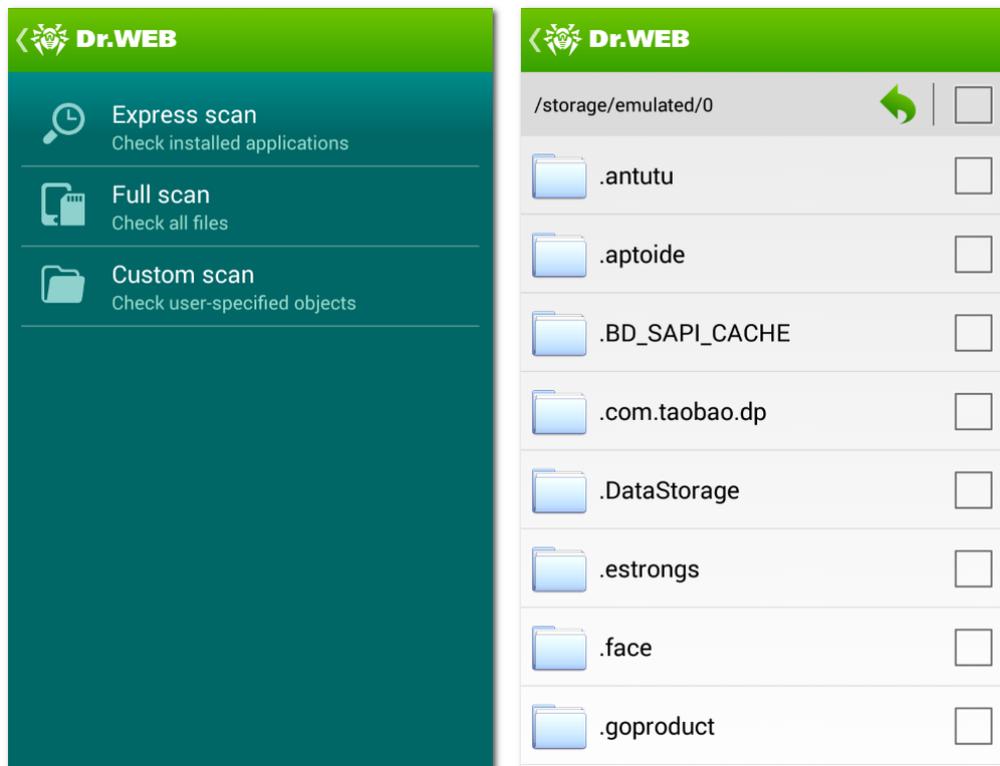
To scan the system, on the main screen tap **Scanner** and on the opened screen (see [Figure 7](#)) do one of the following actions:

- 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 8) 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 7 and 8. 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 7](#)), 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 6](#)).

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

- To show the paths to the scanned files for each processor core separately when using the multi-core devices, on the **Scanner** section, select the **Progress by cores** check box. During the scanning, all processor cores are enabled, but paths to the files are shown for a maximum of four cores.
- 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.
- 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 real-time scan as well.

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

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 6](#)).

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** 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 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 6).

Processing Device Lockers

Dr.Web 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 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** 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** 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.

Calls and SMS Filter

Dr.Web filters the incoming phone calls and SMS. It allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.



For devices operating under Android 4.4 and higher, SMS filtering is implemented via Google Hangouts application. Thus, SMS cannot be blocked if:

- Google Hangouts is currently open on the device screen
- Other messaging application (not Google Hangouts) is used on the device

Moreover, correct SMS filtering via Google Hangouts is not guaranteed for every device.

Calls and SMS filtering may not work properly on the devices with two SIM cards.

The [filtering mode](#) is specified by user. The application provides you with the predefined profiles, which determine the filters. You can also [create](#) user profiles with separate filtering settings.



In the [central protection mode](#) some filter features and settings may be modified and blocked for compliance with the company security policy or according to the list of purchased services.

To [view](#) blocked calls and messages, tap the corresponding [sign](#) on the main application screen.

Filtering Mode

You can chose one of the followings messages and calls filter types:

- **Accept all**—filtering is disabled and all the incoming calls and SMS are accepted
- **Reject all**—all the incoming calls and SMS are blocked
- **Phone book**—calls and SMS only from the phone book contacts are accepted
- **Black list**—calls and SMS from the numbers included into the [black list](#) are blocked

Alternatively, you can use the custom filter. **Dr.Web** allows to create any number of user [profiles](#), each of them having a specified list of contacts and a defined action (accept/reject) for the calls and SMS from these contacts.



If a user profile is selected, the contacts from the black list are blocked in addition to the ones from the profile list.

Black List

You can add the contact, from which you would like to block calls and SMS, into the black list. Calls and messages from the black listed numbers are blocked in case the **Black list** filtering mode or any user profile is selected.

Calls and SMS from numbers added to the black list can be accepted if:

- These numbers are included in the user [profile](#) list and the **Allow only contacts from the list** action is selected for them
- The **Accept all** mode is enabled

Create black list

1. To create the black list, on the main screen of the application tap the filtering section and then select **Configure** on the opened menu.
2. Tap the **Black list** tab.



3. Tap **Add** to add numbers to the black list. You can select numbers by the following ways:
 - Select numbers from the contact list
 - Select numbers from the call and SMS logs
 - Enter numbers and information on them manually

To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the black list you can select them by one or multiple at one time.

To add the selected numbers to the list, tap **Add**.

4. For each contact added to the black list, one of the following actions can be selected:
 - **Block calls and SMS**—to block all incoming calls and messages from the contact.
 - **Block only calls**—to block only calls from the contact. Messages from him will be accepted.
 - **Block only SMS**—to block only messages from the contact. Calls from him will be accepted.By default, the **Block calls and SMS** action is selected for each new contact. You can change it if necessary.
5. To edit the information on the contact from the black list, tap and hold it, then swipe it in the list and tap **Edit**. Modify the information entered in the **Name** and **Number** fields. Tap **Save**.



Information on the contact added to the black list from the phone book and also on the private numbers cannot be modified.

6. To delete a number from the list, tap and hold or swipe it, then tap **Delete**.
7. You can also create a list of keywords to block the SMS containing these words. To do this, in the adding contacts menu select the **Keyword** option. On the **Block SMS by keywords** screen enter the keyword and tap **Add**.

Clear black list

To delete all contacts from the black list, open the application menu and select **Clear the list**.

Filtering Profiles

Dr.Web allows to create user profiles for the calls and SMS filtering.

Create a new profile

1. In the list of available filtering modes, tap **Configure**.
2. On the **Profiles** tab, tap **Add profile**.
3. Enter the profile name.
4. Specify an action for all incoming calls and messages from the profile list numbers. You can select one of the following actions:
 - **Allow only contacts from the list**—to accept the calls and SMS only from the contacts included into the current profile list. Calls and SMS from the numbers included in this list will be accepted even if these numbers are added to the [black list](#).
 - **Block contacts from the list**—to block calls and SMS from the contacts of current profile.
5. Tap **Add contact** to add contacts into the list. You can select numbers by the following ways:
 - Select numbers from the contact list
 - Select numbers from the calls and SMS logs
 - Enter numbers and information on them manually



To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the list you can select them by one or several at one time.

To add the selected numbers to the list, tap **Add**. The number on contacts in the profile list is displayed in parentheses to the right of the profile name.



The list of contacts of the user profile cannot be empty.

6. To edit the information on the contact in the list, tap and hold or swipe it, then tap **Edit**. Modify the information entered in the **Name** and **Number** fields. Tap **Save**.
-



Information on the contact added to the black list from the phone book and also on the private numbers cannot be modified.

7. To delete a contact from the profile list, tap and hold it, then swipe it to make appear a menu, where tap **Delete**.
-



Contacts deleted from the user profile are not deleted from the phone book.

Edit a profile

1. In the list of available filtering modes, tap **Configure**.
2. Do one of the following:
 - Tap the profile you need to edit
 - Tap and hold the profile, then swipe it to the left or to the right and tap **Edit**
3. In the opened window, make the desired changes.
4. Tap **Save**.

Delete a profile

1. In the list of available filtering modes, tap **Configure**.
2. Tap and hold the profile, then swipe it to the left or to the right and tap **Delete**.

View Blocked Calls and SMS

The filtering section on the main screen of the application contains the information on the number of blocked calls and SMS. To review the lists of the blocked calls and messages, tap the corresponding icon:

- —to open the list of the blocked calls
- —to open the list of the blocked messages

To the right on the header of each list the number of not viewed calls/messages is displayed in parentheses. For each call/SMS in th list the following information is displayed:

- Date and time of the call/SMS
- Number and name of the call/SMS sender



To display on your device **Home Screen** the information about the presence of blocked calls and SMS, add **Dr.Web 4×1 (medium) widget**.

Actions for the blocked calls and messages

1. You can call the number of the blocked call. To do this, tap a call in the list. The screen with an entered number will open. To make a call, tap **Call**.
2. By tapping an SMS in the list you can review the message text and details and also select an action to perform on it:
 - **Restore**—to restore the SMS in the incoming messages list



Restore item is unavailable on Android 4.4 and later.

- **Delete**—to delete the SMS

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**.



In the **central protection mode** the option of manual start of update is blocked, updates are downloaded automatically from the central protection server. If on the central protection server the mobile mode is enabled, the manual start of update will be available while the connection with the central protection server is closed.

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 6](#)), 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.

In the [central protection mode](#) update settings can be modified and blocked for compliance with the company security policy or according to the list of purchased services.

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 9](#)).
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 9. 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 10](#)):

- **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 10. 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 sending to **Doctor Web** technical support 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.

Dr.Web Anti-theft

Dr.Web Anti-theft allows to detect the device location or lock its functions in case it has been lost or stolen.



In the [central protection mode](#) some features and settings of **Dr.Web Anti-theft** may be modified and blocked for compliance with the company security policy or according to the list of purchased services.

You can manage **Dr.Web Anti-theft** using special [SMS commands](#). To access the **Dr.Web Anti-theft** configuration parameters, you need to enter a special [password](#) set during the [initial configuration](#). Be careful to remember this password as it is used to manage all the functions of **Dr.Web Anti-theft** and also to unlock your device in case it is locked. If you forgot your password set for **Dr.Web Anti-theft**, you can use the special [service](#) to reset the password and to unlock your device.

Dr.Web Anti-theft also allows to create a [Buddies list](#) (up to 5 phone numbers) to send SMS commands to your device even if you forgot your password for **Dr.Web Anti-theft**.



Dr.Web Anti-theft may not work properly on the devices with two SIM cards.

If **Dr.Web Anti-theft** is enabled, you will need to enter **Dr.Web Anti-theft** password before changing certain [application settings](#) (**Reset settings**, **Backup** and **Mode**).

Configure General Settings

On the first start of **Dr.Web Anti-theft**, a wizard window opens to help you set the main functions of the component.

- Tap **Continue** to set up the main functions of **Dr.Web Anti-theft**.
- Tap **Cancel** if you want to configure **Dr.Web Anti-theft** later.

Configure general settings of Dr.Web Anti-theft using the Wizard

1. On the first step of setting up **Dr.Web Anti-theft** enter a password. Your password should contain at least 4 characters. You will need to enter this password to manage all functions of **Dr.Web Anti-theft**. You can make the characters visible when entering the password by tapping  to the right of the password field. To hide the entered password, tap . Tap **Continue**.
2. Confirm the entered password. Tap **OK**.
3. Configure the [Buddies list](#). Tap **Continue**.



On Android 4.4 and higher, it is necessary to add to the [Buddies list](#) at least one phone number.

4. If you do not have a Google account, you will be asked to enter an email address to register **Dr.Web Anti-theft** on the **Doctor Web** server. It is required for sending you the special code to unlock your device or set a new password in case you forget the password set for **Dr.Web Anti-theft**. Provide an existing email address and tap **Continue**.



A working Internet connection is required for registering the email address on the server.

5. Enter the text which will be displayed on the screen of the locked device. Tap **Continue**.
6. This completes the general configuration of **Dr.Web Anti-theft**. You will be then asked to register the email address of your Google account (or the one specified on the previous step) on the **Doctor Web** server. Tap **Finish** to start the registration procedure.
 - If the registration completes successfully, the Wizard window closes and the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)) opens.
 - If an error occurs during the registration, its description is displayed on the screen and **Dr.Web Anti-theft** is not activated on your device.

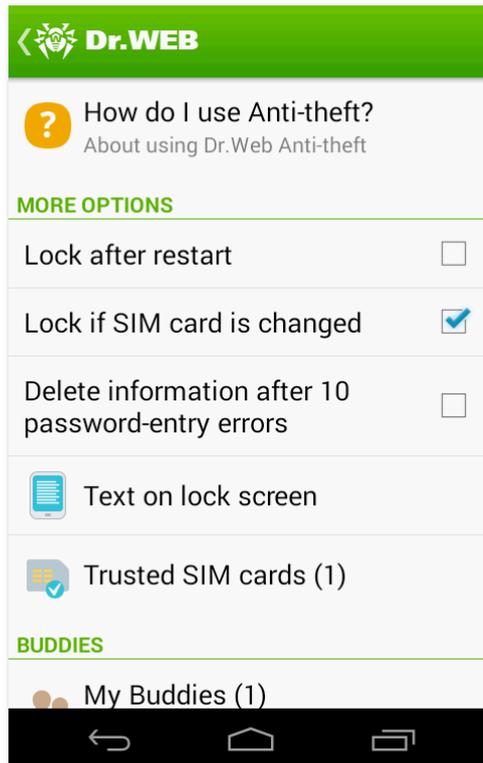


Figure 11. Dr.Web Anti-theft settings



Before opening the settings screen of **Dr.Web Anti-theft**, you will see a prompt to grant **Dr.Web** the device administrator privileges, that you need to accept for correct operation of **Dr.Web Anti-theft**.

Get help

To open the help on **Dr.Web Anti-theft**, on the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)), tap **How do I use Anti-theft?**

Change password

To change the password set for **Dr.Web Anti-theft**, on the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)) screen perform the following actions:

1. On the **Password and administration** section tap **Change password**.
2. Enter your current password. Tap **OK**.
3. Enter a new password. Tap **Continue**.
4. Confirm your new password. Tap **OK**.

Register new email address

To change the email address registered for **Dr.Web Anti-theft** on the **Doctor Web** server, on the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)) perform the following actions:

1. On the **Password and administration** section tap **Change email address**.
2. Enter the email address to register on the **Doctor Web** server. Tap **OK**.
3. A confirmation of the email address change will be sent to the previous email address.



Disable Dr.Web Anti-theft

To disable **Dr.Web Anti-theft** on your device, on the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)) perform the following actions:

1. On the **Change email address** section tap **Disable Dr.Web Anti-theft**.
2. Enter the password set for **Dr.Web Anti-theft** and tap **Disable Dr.Web Anti-theft**.



Disabling **Dr.Web Anti-theft** significantly decreases the protection level of your device.

Additional Functions

To configure **Dr.Web Anti-theft**, on the main application screen tap **Anti-theft**. To access the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)), enter the password set for the **Dr.Web Anti-theft** on its first start. If you forgot your password, send SMS with the **#RESETPASSWORD#** command to your device from the number included into the Buddies list or use a special [service](#).

Additional settings

You can access additional settings on the **More options** section of **Dr.Web Anti-theft** settings screen (see [Figure 11](#)).

- To lock your device after it is restarted, enable the **Lock after restart** option.
- To lock your device in case the SIM card is changed, enable the **Lock if SIM card is changed** option.
- To completely delete all your personal data from the SD card after 10 errors in entering password, enable the **Delete information after 10 password-entry errors** option.
- To specify the text which is displayed on the screen of the locked device, tap **Text on lock screen**, enter the text (e.g., you can add your contact information to return you the lost device), then tap **Save**.
- To review and edit the list of trusted SIM cards, tap **Trusted SIM cards**.

Trusted SIM cards

You can add the SIM cards that you use with your mobile device in a special trusted SIM cards list of **Dr.Web Anti-theft**. When you change one trusted SIM card to another one from the list, your device won't be locked by **Dr.Web Anti-theft**. The trusted SIM cards can be added at the device reboot or when opening **Dr.Web**. You can also add the no SIM mode to the trusted list.



The no SIM mode is active either when the SIM card is missing physically or in case the installed applications have no access to the information about the SIM cards on the device. As a result, you can get an erroneous message about the SIM card missing, but if you make the no SIM mode trusted, all **Dr.Web Anti-theft** functions will be fully available.

To view or edit the list of trusted SIM cards, tap **Trusted SIM cards** in the [additional settings](#) of **Dr.Web Anti-theft**:

1. By default, the added SIM cards are named SIM1, SIM2, etc. To rename a SIM card, tap it in the list (or press and hold it, then tap **Edit** in the menu). In the SIM card information window, enter the new name into the **Name** field and tap **Save**.
2. To delete a SIM card from the trusted list, press and hold it, then tap **Delete** in the menu.



The SIM card that is currently in use on your device cannot be deleted from the list.

Buddies List

Dr.Web Anti-theft allows to add up to 5 phone numbers to the Buddies list. You can specify sending SMS commands without entering password for these numbers. You can also send an SMS command to disable **Dr.Web Anti-theft** and reset its password from these numbers.



On Android 4.4 and higher, it is necessary to add to the Buddies list at least one phone number.

Create Buddies list

1. On the **Dr.Web Anti-theft** settings screen (see [Figure 11](#)), tap **My Buddies** on the **Buddies** section.
2. Tap **Add** to add numbers to the Buddies list. You can select numbers by the following ways:
 - Select numbers from the contact list
 - Select numbers from the call and SMS logs
 - Enter numbers and information on them manually

To search contacts in the phone book as well as in the call and SMS logs, you can use the search option available on pressing the **Search** button. When selecting numbers to add to the Buddies list, you can select them by one or multiple at one time.

To add the selected numbers to the list, tap **Add**.

3. To edit the information on the contact from the Buddies list, tap it in the list and then modify the information entered in the **Name** and **Number** fields. Tap **Save**.
4. To delete a number from the Buddies list, tap and hold it, then tap **Save**.



On Android 4.4, all phone numbers can be deleted from the Buddies list, but the empty list cannot be saved.

5. To notify your Buddies about changing the SIM card in your device, enable the **Inform your Buddies about a SIM card change** option.
6. To allow sending SMS commands from the Buddies numbers without entering the **Dr.Web Anti-theft** password, enable the **Allow SMS commands without a password** option.



Even if the **Allow SMS commands without a password** option is disabled, your Buddies can send you the **#RESETPASSWORD#** command without password. This command is used to unlock the device and to reset the password for **Dr.Web Anti-theft**.

On Android 4.4 and higher, the **Allow SMS commands without a password** option cannot be disabled.

SMS Commands

You can manage **Dr.Web Anti-theft** by sending special SMS commands, which allow getting information on your device location or lock its functions and delete your personal data.



SMS commands table

You can use the following SMS commands to manage **Dr.Web Anti-theft**:

Command	Action
#LOCK#Password#	Lock the device.
#SIGNAL#Password#	Lock the device and enable a sound alert which remains active even after restarting the device.
#LOCATE#Password#	Get the GPS coordinates of the device in an SMS. This SMS contains a link indicating the device location on the map. After you tap the link, the device location is indicated by a special Doctor Web service called Dr.Web Anti-theft Locator . It opens a map in the Internet browser window and locates the device on it. The exactitude of the device coordinates depends on GPS receiver availability, Wi-Fi networks and GSM transmitting stations visibility. Thus, depending on the available data, the received coordinates may be exact (displaying a position on the map) or approximate (displaying a circle of a certain radius). You can select a map service from the list at the top of the map page.
#UNLOCK#Password#	Unlock the device without resetting the Dr.Web Anti-theft password.
#WIPE#Password#	Restore the factory settings of the device and delete all the information from the internal device memory. This action will be also performed in case of 10 error when entering the password and the Delete information after 10 password-entry errors option is enabled in the Dr.Web Anti-theft settings .
#RESETPASSWORD#	Unlock the device and reset the Dr.Web Anti-theft password. This command can be sent only from the number included into the Buddies list .



SMS commands are not case sensitive. For example, to lock the device, you can send the **#LOCK#Password#** command written as **#Lock#Password#**, **#lock#Password#**, **#lOck#Password#**, etc.

To get more precise results after sending the **#LOCATE#** command, enable the use of the mobile networks for geolocation in the device parameters.

Send SMS command via Dr.Web Anti-theft interface

You can send SMS commands directly from **Dr.Web Anti-theft** interface to the devices on which **Dr.Web Anti-theft** resides.

1. On the **Anti-theft** settings screen (see [Figure 11](#)), tap **Send SMS command** on the **Buddies** section.
2. Enter the phone number to send the SMS command to.
3. Select a command from the list:
 - **Lock phone**—corresponds to the **#LOCK#** command
 - **Lock phone and enable sound alert**—corresponds to the **#SIGNAL#** command
 - **Detect phone location**—corresponds to the **#LOCATE#** command
 - **Unlock phone**—corresponds to the **#UNLOCK#** command
 - **Delete all data**—corresponds to the **#WIPE#** command
 - **Reset password**—corresponds to the **#RESETPASSWORD#** command
4. Enter the password set for **Dr.Web Anti-theft** on the command recipient device. If you are in the Buddies list of the command recipient, you do not need to enter the password.
5. Tap **Submit**.



Unlock Dr.Web Anti-theft

If you forgot your password set for **Dr.Web Anti-theft** and your device is locked, perform the following actions:

1. Open the page <https://antitheft.drweb.com/>.
 2. Enter the code displayed on the screen of the locked device and the email you used to register **Dr.Web Anti-theft** on the **Doctor Web** server into the corresponding fields (see [Figure 12](#)).
 3. Tap **Get code**. A special code to unlock the device and disable **Dr.Web Anti-theft** will be sent to the specified email address.
 4. Enter this code in the **Enter Anti-theft password** field on the screen of the locked device.
- The device will be unlocked, **Dr.Web Anti-theft** will be disabled. To start using **Dr.Web Anti-theft** again, you need to re-enable and reconfigure it.

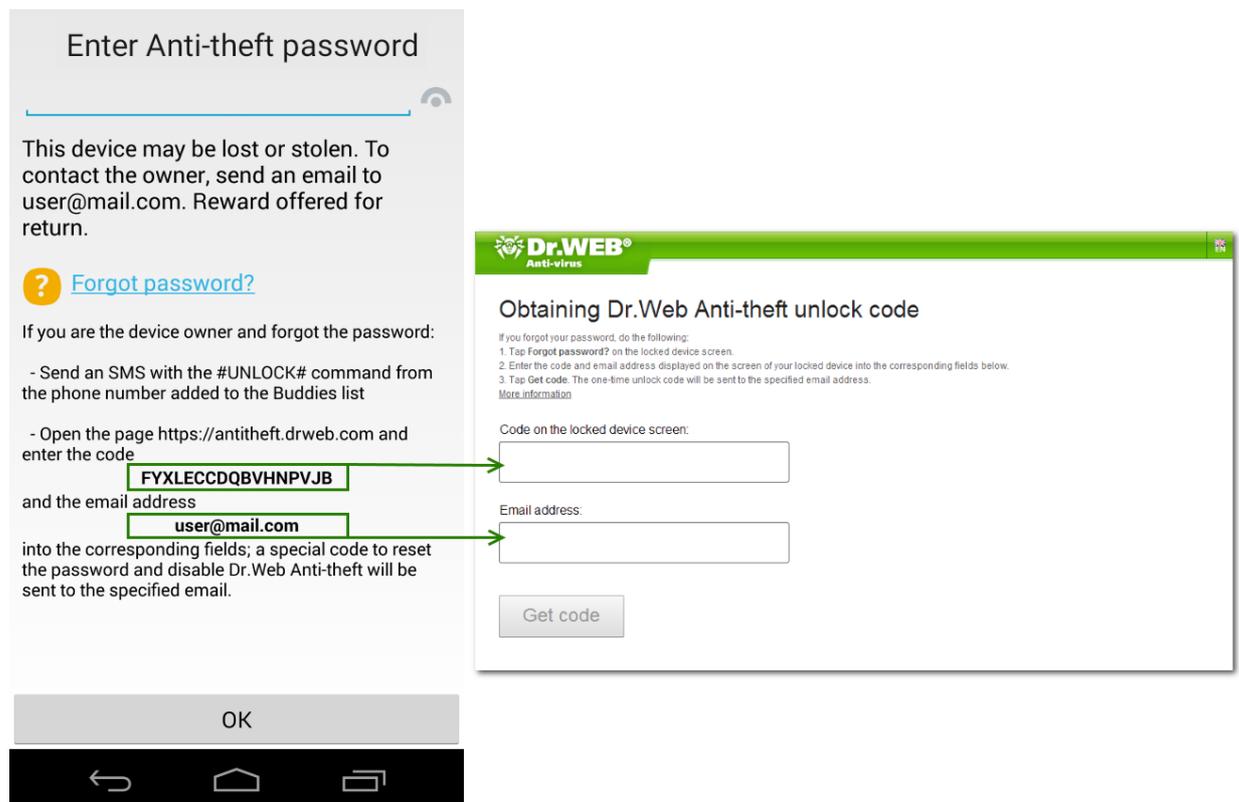


Figure 12. Unlock Dr.Web Anti-theft

Restricting Internet Access

Access to Internet resources is controlled by the URL filter **Cloud Checker**. It allows to protect user of the mobile device from unsolicited Internet sites.



Cloud Checker can be used only to control the Internet resources accessed via Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser and Boat Browser Mini.

In the [central protection mode](#) some features and settings of **Dr.Web Firewall** may be modified and blocked for compliance with the company security policy or according to the list of purchased services.

Cloud Checker allows to block access to the following categories of not recommended and potentially dangerous websites:

- Non-recommended sites
- Adult content
- Violence
- Weapons
- Gambling
- Drugs
- Obscene language
- Chats
- Terrorism
- Email
- Social networks
- URLs listed due to a notice from the copyright owner

By default, **Cloud Checker** blocks access to websites known as infection sources.



To ensure that **Cloud Checker** works correctly, enable saving history function in your browser.

Enable/disable the URL filter

1. On the main application screen (see [Figure 2](#)), tap **Cloud Checker**. This will open the URL filter settings screen (see [Figure 13](#)).

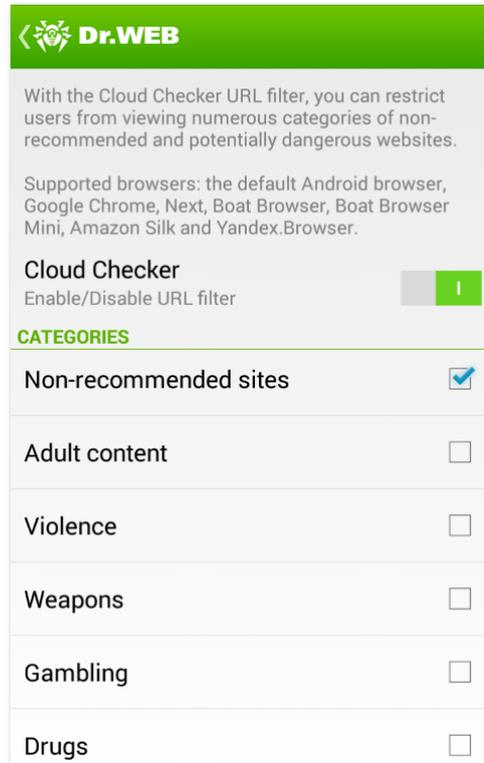


Figure 13. The Cloud Checker settings screen

2. The URL filtering can be enabled/disabled using the **Cloud Checker** option. By default, the URL filtering is enabled.
3. In the **Categories** list, select the categories of the websites to block access to.

Dr.Web Firewall

Dr.Web Firewall protects your mobile device from unauthorized access and prevents leak of vital data through networks. This component monitors connection attempts and data transfer and helps you block unwanted or suspicious connections.



Dr.Web Firewall is based on VPN for Android technology. On some devices the protocol used by VPN may be disabled by manufacturer and is not available for non-system applications. In such cases the firewall functions are not available. For more information, please contact the manufacturer of your mobile device.

Enable/disable Dr.Web Firewall

1. On the main application screen (see [Figure 2](#)) tap **Firewall**. The firewall configuration screen will open (see [Figure 14](#)).

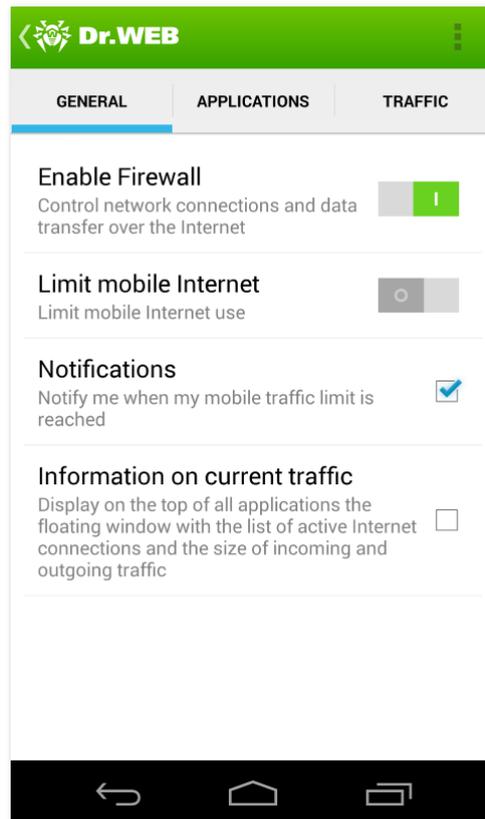


Figure 14. Firewall configuration screen. General tab

2. You can enable/disable firewall using the **Enable Firewall** option. By default, firewall is disabled. When you enable it, a dialog requesting to allow the use of VPN by **Dr.Web** opens. To start using the firewall you need to give this permission.



If another application gets the rights to use VPN during **Dr.Web Firewall** operation, the component is disabled. The user is notified by a corresponding warning in the notifications section. To re-enable **Dr.Web Firewall**, tap this warning.

Features

Dr.Web Firewall is based on VPN for Android technology, so it does not require root access on the device. Using VPN for Android technology sets the following limits:

- At any moment of time, only one application installed on the device can use VPN. This results in opening a dialog requesting to allow using the VPN by this application. If the user gives such permission, the application starts using VPN, but it blocks access to VPN to another application that was using it just before the new request appeared. Such request appears when **Dr.Web Firewall** is enabled and every time the device is rebooted. It can also appear when other applications try to access VPN. VPN is shared between the applications in time, and the firewall is operating only when it gets full rights to use VPN.
- Enabling **Dr.Web Firewall** can result in inability to connect the device on which **Dr.Web Firewall** runs to other devices directly using Wi-Fi or local network. It depends on the device model and applications which are used to establish a connection between devices.
- When **Dr.Web Firewall** is enabled, the device cannot be used as a Wi-Fi access point.



Dr.Web Firewall uses the VPN for Android technology only to perform its functions, without creating VPN tunnel, so the web traffic is not encrypted.

Limit the Use of Mobile Internet

Dr.Web Firewall allows you to limit the use of mobile Internet.

1. To enable/disable the limit for mobile Internet, use the **Limit mobile Internet** option on the **General** tab of the firewall configuration screen (see [Figure 14](#)).
2. Set up the limit for mobile traffic (in megabyte or gigabytes). You can select a duration period for the limit: a day, a week or a month.
3. If necessary, specify the amount of traffic that was already used since the selected limitation period has started:
 - If you selected a day as the limitation period, it begins at 00:00 of the current day
 - If you selected a week as the limitation period, it begins at 00:00 of the current day
 - If you selected a month as the limitation period, it begins at 00:00 of the first day of the current calendar month

When the mobile Internet limit is enabled, a graph showing the amount of the remaining traffic appears on the **General** tab of the firewall configuration screen. The specified limit and the countdown to the limit expiration are shown next to the graph (see [Figure 15](#)).

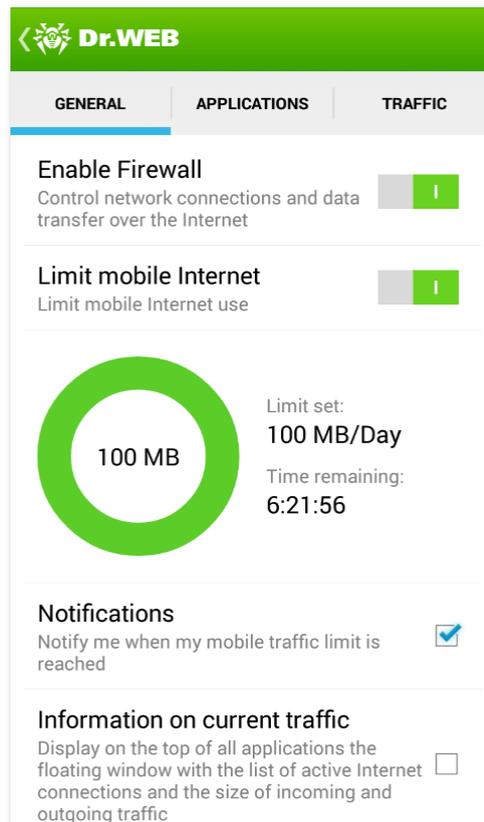


Figure 15. Firewall configuration screen with enabled mobile traffic limit



The specified mobile traffic limit may be overrun by up to 4 KB.

Notifications

You can set up notifications about reaching the mobile traffic limit by selecting the **Notifications** check box on the **General** tab of the firewall configuration screen (see [Figure 14](#)).

Processing Applications Traffic

Dr.Web Firewall allows to filter traffic on the application level and, therefore, control the access of applications to network resources. To view the information on the Internet traffic of applications installed on your mobile device, as well as to configure the connection rules for them, open the **Applications** tab of the firewall configuration screen (see [Figure 16](#)).

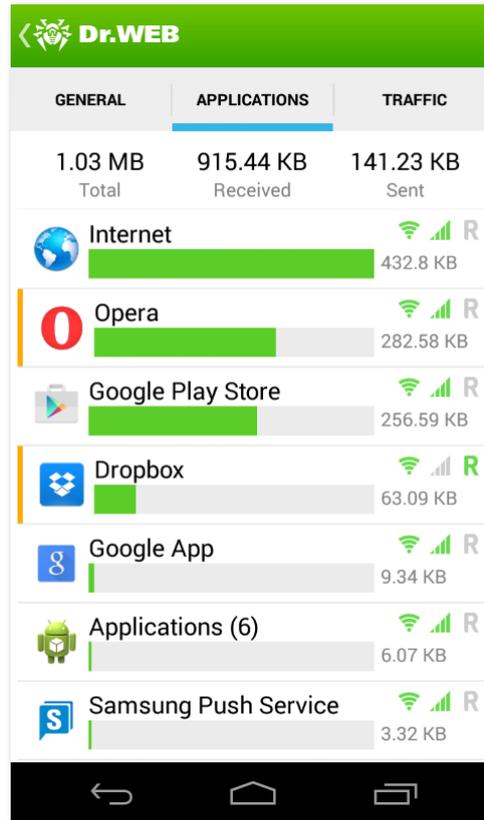


Figure 16. Firewall configuration screen. Applications tab

On the **Applications** tab, you can review the total amount of data transferred over the networks and the amount of sent and received data.

The **Applications** tab also features a list of applications (and application groups) with information on the traffic used by each of them. To open the list of all applications installed on your device, including those without any Internet traffic, select the **All applications** check box in the menu on the **Applications** tab.

You can enable/disable the use of Wi-Fi, mobile Internet and roaming for each application in the list using the corresponding options to the right of the applications names.



If the application settings are changed, this application appears highlighted in the list.

To review the detailed information on the use of Internet by an application (or an application group) from the list, tap it. On the application information screen, you can perform the following actions:

- Enable/disable the use of Wi-Fi, mobile Internet and roaming for this application (or application group)
- View the application [log](#)
- View the Internet traffic [statistics](#) for this application (or application group)
- Configure [connection rules](#) for this application (or application group)



Internet Traffic Statistics

On the application (applications group) traffic screen, you can review the statistics of Internet traffic used by this application shown as a graph (see [Figure 17](#)).

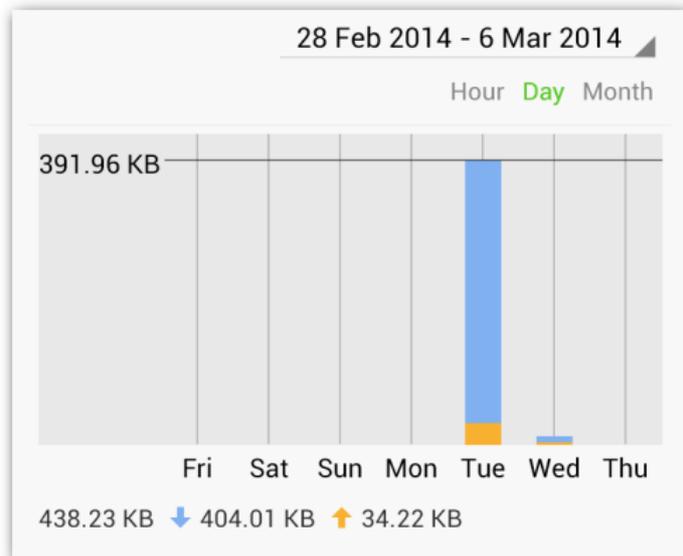


Figure 17. Application traffic statistics

The yellow color on the graph shows the outgoing application traffic, the blue one shows the incoming traffic. The numeric values of the application traffic amount (total, incoming and outgoing) are shown under the graph.

When reviewing the Internet traffic statistics, you can perform the following actions:

- Use the corresponding list to select the period to show statistics. You can review the statistics for the current day, last week, current month, previous month or specify any other period by selection the start and end dates.
- Configure showing the statistics for the hours, days or months within the selected period.

Clear statistics

- To clear statistics for all applications:
 1. On any tab of the firewall configuration screen (see [Figure 14](#)) open the menu and tap **Clear**.
 2. On the opened window, select the **Clear statistics** check box and tap **OK**.
- To clear statistics for an application:
 1. On the **Applications** tab of the firewall configuration screen (see [Figure 16](#)), select the application to delete the statistics for.
 2. On the application information screen, open the menu and tap **Clear**.
 3. On the opened window, select the **Clear statistics for this application** check box and tap **OK**.

Connection Rules

On the application (applications group) traffic screen, you can set up the rules for connections of this application to certain IP addresses and ports.



Configure rule sets

1. To create a new rule, tap **Add rule**. You can add allowing or blocking rules depending on the option selected in the **Connection rules** section:
 - **Block connections from the list**—you can add blocking rule
 - **Allow only the connections from the list**—you can add allowing rule
2. In the opened window, **IP address** enter a valid IP address in the **IP address** field (in the a.b.c.d format), an IP addresses range (in the a1.b1.c1.d1-a2.b2.c2.d2 format) or a network (in the a.b.c.0/n format, where n is a number from 1 to 32) or leave this field blank (in this case entering the port is obligatory). Enter the valid port in the **Port** field or leave it blank (in this case entering the IP address is obligatory). In case one of the fields is blank, the rule is valid for all the IP addresses or ports respectively. Tap **OK** to save the rule.
3. To edit an existing rule, tap and hold it, then tap **Edit**.

You can also add allowing and blocking rules when browsing the [applications logs](#) or the list of [current Internet connections](#).

Delete connection rules

- To delete a rule, tap and hold it, then tap **Delete**.
- To clear all rules for a certain application:
 1. Select this application in the list (see [Figure 16](#)).
 2. In the application menu, select **Clear**.
 3. In the opened window, select the **Clear rules for this application** checkbox.
- To clear all rules for all applications:
 1. On the applications screen (see [Figure 16](#)), open the application menu and select **Clear**.
 2. In the opened window, select the **Clear rules for applications** checkbox.

Incoming connections

The **Allow incoming** check box in the menu on the application information screen excludes the incoming connections from the firewall check. The information on the connections from any external addresses with the port opened by the application is only partially added to the [application log](#) and firewall [statistics](#). Moreover, any connections with such addresses may be excluded from the processing by firewall for all other applications. Such operation mode is not safe and generally, it is not recommended to use it.

Allowing the incoming connections is useful in case the firewall cannot be disabled by other means, for example, when a server receiving connections from external networks is configured on the device.

Current Internet Activity

You can get the information on current Internet activity using the following:

- The **Traffic** tab of the firewall configuration screen (see [Figure 14](#))



The **Traffic** tab contains information on current Internet connections initiated by applications installed on the mobile device. To open the detailed information on connections of a certain application (IP addresses and ports of the connections and the amount of the sent and received data), tap it in the list.

You can create allowing or blocking rules for connections from the list. Tap and hold the connection in the list, then tap the corresponding option:

- **Add allowing rule**—to create a rule allowing the connections from the specified IP address and port for the selected application
- **Add blocking rule**—to create a rule blocking all the connections from the specified IP address and port for the selected application
- Floating window with the information on current traffic

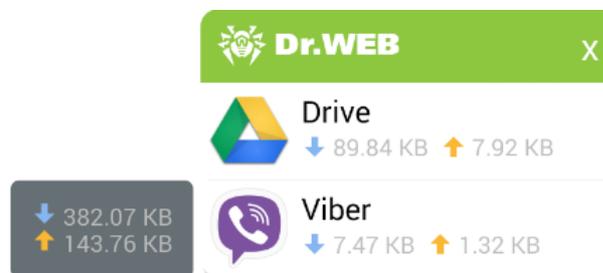
To display the window, select the **Information on current traffic** check box on the firewall configuration screen (see [Figure 14](#)). The floating window with the size of incoming and outgoing traffic will be displayed on the top of all applications (see [Figure 18a](#)).



Traffic size is calculated after opening the window.

Work with the floating window

- To open the list of applications that use Internet connections (see [Figure 18b](#)), tap the window. Select an application in the list to open the **Traffic** tab containing detailed information on current connections.
- To close the list of applications, tap **X**.
- To hide the floating window, clear the **Information on current traffic** check box.



Figures 18a and 18b. Current traffic floating window

Logging

Dr.Web logs the events related to the operation of **Dr.Web Firewall**. You can review the [full log](#) or the lists of events related to the use of Internet by separate [applications](#).

Dr.Web Firewall Log

To open the list of all the events related to **Dr.Web Firewall** operation, open the menu and tap **Log** on any tab of the firewall configuration screen (see [Figure 14](#)).

View the log

To simplify searching the information when viewing the event log, use the sorting and fast scrolling (by moving a special graphical element in the right part of the screen) functions. To sort the records in the



log, select the sorting criterion in the menu on the log screen.

You can review following information for each event in the log:

- Connection date and time (for TCP) or the time required to receive the packets with the corresponding traffic amount (for UDP). Example: 18/02/2014 2:07:11–18/02/2014 2:07:12.
- Local address and port. Example: src: 10.2.3.5:6881.
- Incoming and outgoing traffic (in bytes) or the number of blocked packets. Example: in:103 out:112 or blocked packets:1.
- ID of the application related to the traffic on the device (User ID). Example: uid=10071.
- Number of traffic jams (only for TCP). Example: traffic jam=0. Traffic jams are the special situations, when the client application struggles to unload all data from the TCP buffer, that results in "clogging", so the data transfer speed significantly decreases.

Clear log

1. On any tab of the firewall configuration screen (see [Figure 14](#)) open the menu and tap **Clear**.
2. In the opened window, select the **Clear log** check box and tap **OK**.

Log file size

By default, the maximum size for the log file is set to 5 MB. You can change his value:

1. On any tab of the firewall configuration screen (see [Figure 14](#)) open the menu and tap **Clear**.
2. In the opened window, enter a new value for the maximum log file size and tap **OK**.

Application Logs

To review the list of events related to the network connections of a certain application installed on your device, tap **Log** on the application information screen.

View the application log

All the events related to the application are grouped by date. To open the list of events for a certain date, tap it in the list. You can review the following information for each event:

- Connection time (for TCP) or the time required to receive the packets with the corresponding traffic amount (for UDP)
- Local address and port
- Incoming and outgoing traffic (in bytes) or the number of blocked packets

You can create allowing or blocking rules for connections from the application log. Tap and hold the connection in the list, then tap the corresponding option:

- **Add allowing rule**—to create a rule allowing the connections from the specified IP address and port for the selected application
- **Add blocking rule**—to create a rule blocking all the connections from the specified IP address and port for the selected application

Clear application log

1. On the application information screen, open the menu and tap **Clear**.
2. In the opened window, select the **Clear log for this application** check box and tap **OK**.

Disable logging for application

1. On the application information screen, open the menu and tap **Clear**.
2. In the opened window, select the **Disable logging for this application** check box and tap **OK**.



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.

Resolve security problems

To review the list of the detected problems and vulnerabilities (see [Figure 19](#)), tap the **Security Auditor** section on the main application screen.

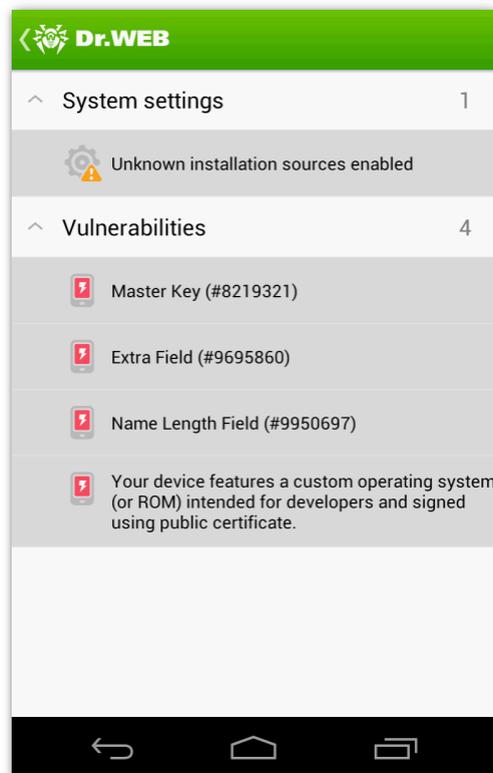


Figure 19. List of security problems detected on the device

Dr.Web detects the following categories of security problems: applications with highest priority of SMS processing, hidden device administrators, vulnerabilities and system settings that affect the device security. 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.

Applications with highest priority of SMS processing

This category contains the list of applications installed on the device that have the higher priority in SMS processing than **Dr.Web**. Such applications can block the operation of [Dr.Web Anti-theft](#) and [SMS filtering](#), since they are first to process all incoming messages and [commands](#). Sometimes such applications are malicious and may present a threat to the security of your device.



If you notice that the SMS filtering or **Dr.Web Anti-theft** does not work properly, try to change the priority settings of the applications in the list, if possible. These applications will disappear from the list of security problems. If you are not sure that these applications are totally safe, it is recommended to delete them from the device. 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.

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.

System settings

USB debugging and installing applications from unknown sources are the system settings that affect the security of the device. It is insecure to use conflicting software as well:

- **USB debugging** is intended for developers and allows copying data from PC to the device and vice-versa, installing the applications on the device, viewing their logs and deleting them in some cases. If you are not developer and do not use the debug mode, it is recommended to turn it off. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem.
- **Installing applications of unknown origin** is the main source of threats. Application downloaded from other source than official market (Google Play) are likely to be unsafe and present a threat to the device security. To mitigate risks of installing the unsafe applications, it is recommended to disable installation of the applications from unknown sources. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem. It is also recommended to scan for viruses all the applications you install on your device. Make sure that **Dr.Web** virus databases are [up-to-date](#) before scanning.
- **Software conflicts.** Use of conflicting software, including web browsers that are not compatible with [Cloud Checker URL filter](#), decreases the security level of your device, as it is not protected against the undesirable and malicious web resources. It is recommended to use and to assign as the default browser on your device one of the following browsers: Google Chrome, Google Chrome Beta, Next, Amazon Silk, Yandex.Browser, Boat Browser and Boat Browser Mini.

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 and Stagefright 2.0 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.

The device may become vulnerable to different types of threats if it is rooted, i.e. the procedure of rooting has been performed to attain control (known as "root access") over the device system. It results in ability to modify and delete system files, that may potentially damage the device. If you rooted your device yourself, it is recommended to rollback the changes for security reasons. If root access is the integral feature of your device or you need it for your everyday tasks, be extremely cautious when installing applications from the unknown sources.

URL Shortening Service

Sometimes, for example, when you have to deal with limits on the number of characters in SMS or social networks posts, you may need to use short URLs. **Dr.Web** allows shortening URLs and scanning them for viruses using a special link shortening service in order to protect users from security threats.

Check and shorten a URL

1. Select the URL you want to check and shorten, then use the sharing function of your browser.
2. In the menu that opens, tap **Shorten URL**. The page that the selected URL links to will be scanned for threats and, if it is safe, the shortened URL will be created and copied to clipboard. If the page contains security threats, the service will show the corresponding notification.



Chapter 6. Operation in Central Protection Mode

You can use **Dr.Web** installed from the **Doctor Web** website to connect to corporate networks managed by **Dr.Web Control Center** or to access **Dr.Web AV-Desk** anti-virus service of your IT provider. To operate in such central protection mode, you do not need to install additional software or uninstall **Dr.Web**.



Operation in central protection mode is not supported by the version of **Dr.Web** installed from Google Play.

Components controlled from the central protection server

Some features and settings of **Dr.Web** may be modified and blocked for compliance with the company security policy or according to the list of purchased services.

The following **Dr.Web** components can be controlled from the central protection server:

- [Dr.Web Scanner](#). Scanning can be performed on user demand or according to the schedule. Also the remote launch of anti-virus scan of stations from the the central protection server is supported.
- [SpIDer Guard](#).
- [Calls and SMS Filter](#).
- [Dr.Web Anti-theft](#).
- [Cloud Checker](#).
- [Dr.Web Firewall](#).
- [Application filter](#).

Licensing in the central protection mode

A [license](#) for operation in this mode is received from the central protection server. Your personal license is not used. When the license is expired or blocked, contact your company anti-virus network administrator in order to obtain a new license or extend your **Dr.Web AV-Desk** subscription, after receiving the corresponding notification.

Update in the central protection mode

In the central protection mode the option of manual start of update is blocked, updates are downloaded automatically from the central protection server. Update settings can be modified and blocked for compliance with the company security policy or according to the list of purchased services. If on the central protection server the mobile mode is enabled, the manual start of update will be available while the connection to the central protection server is lost.

Switching to Central Protection Mode

To start operating in the [central protection mode](#), you need to connect to the central protection server.

Automatic connection

If **Dr.Web** was installed with the *.apk file provided by the anti-virus network administrator, connection to the central protection server will be established automatically. It requires that your device to be on the same Wi-Fi network as the central protection server.

Connection with parameters

To connect to the central protection server, the parameters of connection received from the anti-virus



network administrator or from your IT-provider are required.

1. Make sure your device is connected to the network.
2. On the settings screen (see [Figure 6](#)), select the **Dr.Web Agent** check box on the **Mode** section.



In the application installed with the *.apk file provided by the anti-virus network administrator, the **Dr.Web Agent** check box is selected by default.

3. On switching to the central protection mode **Dr.Web** restores parameters of the previous connection. If you are connecting to the server for the first time or connection parameters have changed, do the following:
 - Enter the IP address of the central protection server provided by administrator of anti-virus network.
 - Enter the authentication parameters: ID, which is assigned to your device for registration at the server, and password. The entered values are saved and you need not enter them again when reconnecting to the server. To connect as a new station ("Newbie"), open the application menu and tap **Connect as "Newbie" station**.
4. Tap **Connect**.

Connection using configuration file

The install.cfg file received from the anti-virus network administrator or your IT-provider contains settings to connect to the central protection server.

1. Make sure your device is connected to the network.
2. Place the install.cfg file to the root folder or any of the folders at the first nesting level of the internal device memory.
3. On the settings screen (see [Figure 6](#)), select the **Dr.Web Agent** check box on the **Mode** section. If the file is downloaded to the device, fields for entering the connection settings will be filled in automatically.



In the application installed with the *.apk file provided by the anti-virus network administrator, the **Dr.Web Agent** check box is selected by default. After the application is installed, it starts to search the configuration file and tries to connect to the server. If the file is not found or it contains incorrect connection parameters, you need to clear and select again the **Dr.Web Agent** check box and enter the parameters [manually](#) or use the configuration file with correct settings.

4. Tap **Connect**.

Reset connection settings

1. Open the application menu on the connection settings entering screen.
2. Tap **Reset connection settings**.

When the settings are reset, the install.cfg file, which contains the connection parameters, will be deleted. If the other install.cfg file is present on the device, the connection parameters of this file will be used. Thus the connection settings will be reset only when all the install.cfg files will be deleted.

Errors during connection

Unsupported option. The error occurs if traffic encryption and/or compression options not supported by **Dr.Web** are enabled on the server. To resolve the problem, contact anti-virus network administrator or IT-provider.

License (subscription) has expired. To connect to the central protection server, contact anti-virus network administrator in order to get a license or expire your **Dr.Web AV-Desk** subscription.



Subscription is blocked. To connect to the central protection server, contact your **Dr.Web AV-Desk** service provider in order to unblock the subscription.

Not connected. Running Dr.Web for Android is denied on central protection server. The error occurs if your tariff plan does not provide for using **Dr.Web for Android** or running **Dr.Web for Android** is denied by the anti-virus network administrator.

Application Filter

If the ability to configure application filter is enabled on the [central protection server](#), you can specify the list of applications, which can be run on your device.

1. On the main screen of the application tap **Administrator**.
2. Select the applications, which will be available on your device.
3. Tap **Allow selected**. The specified settings will be transferred to the server and saved as your device personal settings.

If you are an anti-virus network administrator, on the central protection server, you can configure the lists of available applications for all devices in the network based on your personal settings saved on the server.

Switching to Standalone Mode

To use standalone mode, clear the **Dr.Web Agent** check box on the **Mode** section of the settings screen (see [Figure 6](#)).

On switching to this mode, all settings of **Dr.Web** are unlocked and restored to their previous or default values. You can once again access all features of anti-virus.

For correct operation in standalone mode **Dr.Web** requires a valid personal [license](#). The license received from central protection server cannot be used in this mode. If necessary, you can [activate or update](#) a personal license.



Chapter 7. Working with Dr.Web on Android TV

On the devices running Android TV, the following **Dr.Web** features are available:

- [Constant anti-virus protection](#)
- [On-demand scan](#)
- [Update](#)
- [Statistics](#)
- [Quarantine](#)
- [Security troubleshooting](#)

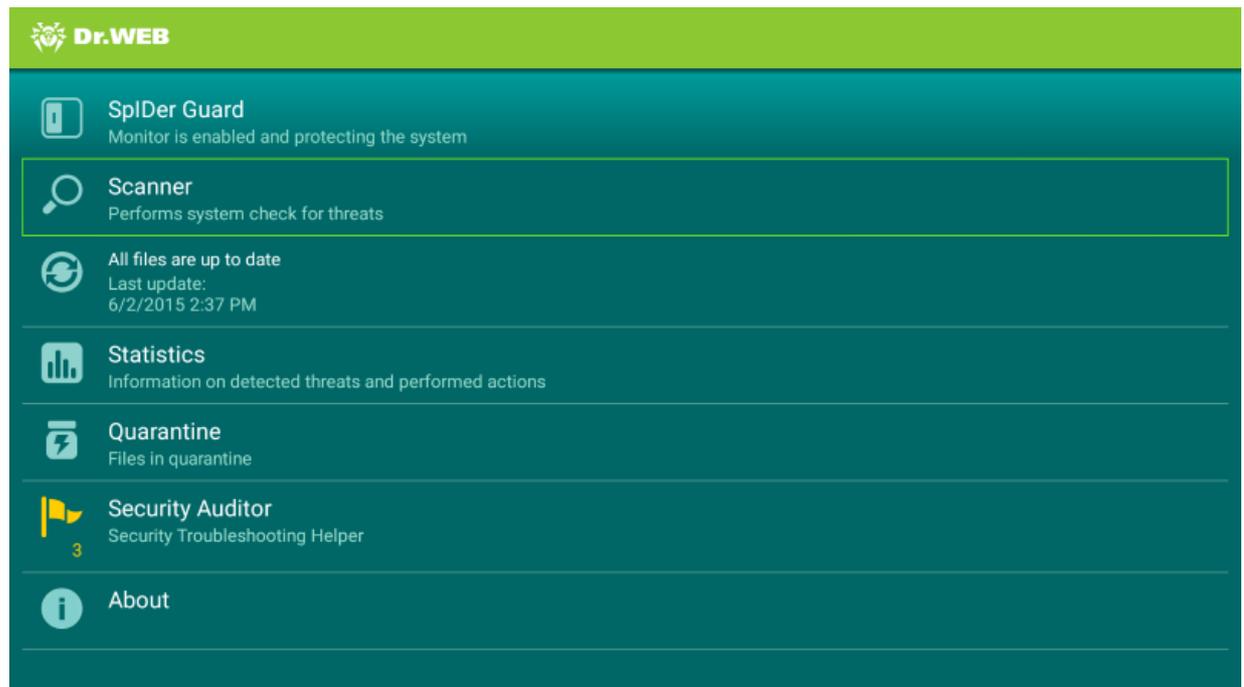


Figure 20. Dr.Web for Android TV

Features of Dr.Web operation on Android TV devices

Licensing

- The feature of purchasing a license is unavailable in the application.
- To renew a license, you need to select the **About** section on the main screen and tap the **Renew license** button.

Interface

- [Widgets](#) are unavailable.
- [Notification pane](#) is unavailable.
- The application menu and **Dr.Web** components settings are unavailable.



Appendices

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

- [Appendix A. Technical Support](#)

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

A

- anti-spam 27
- anti-virus network 54
- application filter 56
- applications
 - connection rules 47
 - incoming connections 47
 - statistics 47
 - traffic 47

B

- black list 28

C

- central protection 54
- Cloud Checker 40
 - settings 40
 - supported browsers 40
 - web sites categories 40
- connection rules 47
- constant protection 22
- custom scan 23

D

- demo key file 10
- device lockers 27
- document conventions 6
- Dr.Web 6
 - actions 25
 - anti-spam 27
 - black list 28
 - Cloud Checker 40
 - Dr.Web Anti-theft 34, 35, 37, 38, 40
 - Dr.Web Anti-theft Locator 38
 - Dr.Web Firewall 42
 - export settings 22
 - filtering 27, 28, 30
 - filtering profiles 29
 - functions 21
 - import settings 22
 - install 13
 - interface 16
 - key file 8
 - launch 16
 - license 8

- log 33
- main features 6
- My Dr.Web 20
- notifications 18
- operation mode 54
- quarantine 32
- reset settings 21
- scanner 23
- security troubleshooting 51
- settings 21
- SpIDer Guard 22
- start to use 16
- statistics 33
- switching to central protection mode 54
- switching to standalone mode 56
- system requirements 7
- technical support 58
- uninstall 13, 14
- update 31
- URL shortening 53
- widgets 18

- Dr.Web Anti-theft 34
 - buddies list 38
 - disable 35, 40
 - password 35
 - registration 35
 - reset password 40
 - settings 35, 37
 - SMS commands 38
 - trusted SIM cards 37
 - wizard 35
- Dr.Web Anti-theft Locator 38
- Dr.Web Firewall 42
 - applications traffic 45, 47
 - incoming connections 47
 - Internet traffic 48
 - limit mobile Internet 44
 - logging 49, 50
 - network connections 48

E

- export settings 22
- express scan 23

F

- false positive 23, 25, 32



Index

filtering 27
 black list 28
 calls 27
 messages 27
 mode 28
 profiles 29
 view blocked 30

filtering mode 28

filtering profiles 29

filters 28
 black list 28
 user 29

full scan 23

G

Google Play 13, 14

H

hidden device administrators 51

I

import settings 22

install application 13

interface 16

Internet traffic
 applications 45, 47
 mobile 44

K

key file
 acquire 10
 copy from file 11
 download 10
 update 12
 use 11

L

launch application 16

license
 acquire 10
 copy from file 11
 download 10
 purchase 10
 register serial number 11
 renew 12
 update 12

use 11

licensing 8

log 33
 applications 50
 Dr.Web Firewall 49
logging 33

M

main features 6

market 13, 14

mobile Internet
 limit 44
 notifications 44

My Dr.Web personal page 20

N

network connections
 current activity 48
notifications 18
 license 12
 mobile Internet 44
notifications pane 18

O

operation mode 54

P

processing threats 26, 27, 32
 quarantine 25
 sounds 25
protection status 16
purchase license 10

Q

quarantine
 processing threats 32
 size 32

R

ransomware 27
register serial number 11
reset settings 21
root access 51
rooting 51



Index

S

- scan
 - custom 23
 - express 23
 - full 23
- scanner
 - custom scan 23
 - express scan 23
 - full scan 23
 - settings 23
 - statistics 23
- security troubleshooting
 - hidden device administrators 51
 - incompatibility 51
 - root access 51
 - sms processing priority 51
 - software conflicts 51
 - system settings 51
 - vulnerabilities 51
- send file to laboratory 23, 25, 32
- settings
 - Dr.Web Anti-theft 35, 37
 - export 22
 - import 22
 - reset 21
 - scanner 23
 - SpIDer Guard 22
 - update 31
 - URL filter 40
- sms processing priority 51
- software conflicts 51
- SpIDer Guard
 - enable 22
 - settings 22
 - statistics 22
- start to use 16
- statistics 33
 - applications traffic 47
 - scanner 23
 - SpIDer Guard 22
- support 58
- supported browsers 40
- system requirements 7
- system settings 51

T

- technical support 58
- threats
 - actions 26
 - device lockers 27
 - system applications 26
- trusted SIM cards 37

U

- uninstall application 13
- uninstall program 14
- update
 - automatic 31
 - settings 31
- URL filter 40
- URL shortening 53

V

- view blocked 30
- virus databases
 - automatic 31
 - update 31
- vulnerabilities 51

W

- widgets 18

