Dr.WEB® for Android

User Manual

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

Dr.Web anti-virus for Android
Version 6.01.8
User Manual
05.04.2012

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 anti-virus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

Chapter 1. Introduction

Thank you for choosing **Dr.Web anti-virus**. This anti-virus solution offers a reliable protection of the mobile phones and communicators working under the Android™ operating system from various virus threats designed specifically for mobile devices.

The program employs the most advanced developments and technologies of **Doctor Web** aimed at detection and neutralization of malicious objects which may represent a threat to the device operation and information security.

Dr.Web anti-virus 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 mobile devices to install and adjust **Dr.Web anti-virus**. It also describes all the basic functions of the application.

Document Conventions

The following conventions and symbols are used in this document:

Convention	Description
Bold	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
Green and bold	Names of Dr.Web products and components.
Green and underlined	Hyperlinks to topics and web pages.
Italic	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values. In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
⚠	A warning about potential errors or any other important comment.

Main Features

Dr.Web anti-virus is a reliable anti-virus solution for users of mobile 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 removable memory cards
- 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
- 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, program log
- Detecting phone location or locking its functions in case it has been lost or stolen

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

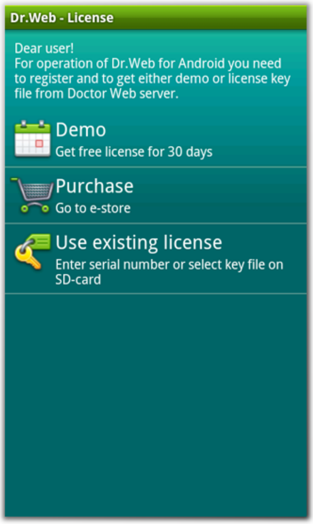
Chapter 2. Licensing

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

If the application was purchased and installed via Google Play, the license is registered automatically.

If you have the license for products **Dr.Web® Security Space** or **Dr.Web® Security Space Pro**, you can use the existing key file for operation of **Dr.Web anti-virus**.

To get or register the license, open the **Dr.Web - License** screen (see Figure 1). The **Dr.Web - License** screen opens on the first launch of the program and in case license key file is missing. You can also open this screen by pressing the **Menu** button on the main screen of the program (see Figure 2) and tapping **About** -> **Renew license**.



Dr.Web - License

Dear user!
For operation of Dr.Web for Android you need to register and to get either demo or license key file from Doctor Web server.

Demo
Get free license for 30 days

Purchase
Go to e-store

Use existing license
Enter serial number or select key file on SD-card

Figure 1. Dr.Web - License screen

Purchase license

You can purchase the license for **Dr.Web anti-virus** in the **Doctor Web** web store by tapping **Purchase** on the **Dr.Web - License** screen.

You will receive either the serial number or the license key file on the e-mail specified while ordering. You can also choose to receive the serial number in an SMS on the mobile number entered on registration.

To start using the purchased license you need to register the serial number or copy the key file on the device.

License Key File

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

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

There are two types of key files:

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

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

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

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

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

Acquire License Key File

For operation of the program you need to get either demo or license key file.

Get demo key file

If you installed the program in purposes of evaluation, you can download the free license for 30 days. To do this, tap **Demo** on the **Dr. Web - License** screen (see Figure 1), enter your personal data required for demo key file download and tap **Get key**. The key file will be downloaded and installed automatically.

Get license key file by registering serial number

You can download the key file directly to the device via Internet.

1. On the **Dr.Web - License** screen (see Figure 1) tap **Use existing license**.
2. Tap **Enter serial number**.
3. Enter the serial number and tap **Get key**.
4. Enter your personal data and select **Get key**. This information is necessary to receive the key file.
5. The key file will be downloaded and installed. The key file downloading procedure log is displayed on the screen:
   - If the license key is downloaded successfully, tap **OK**.
   - If an error occurred, the error details are displayed.

You can also get the key file by e-mail after the product registration on **Doctor Web** official web site.

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

Use License Key File

If you already have a key file (e.g., received by e-mail) or you have the license for **Dr.Web Security Space** or **Dr.Web Security Space Pro** products and you want to use it for **Dr.Web anti-virus**, you need to copy the existing key file to the special folder on the SD-card.

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

To check whether such key file can be used:

- Open the key file in a text editor (e.g., Notepad).
- 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 anti-virus**.

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

Copy key file on the device with Dr.Web anti-virus

1. Synchronize your device with PC and copy the key file to the **Android/data/com.drweb/files** folder located on the SD-card.
2. On the **Dr.Web - License** screen (see Figure 1) select **Use existing license**.
3. Tap **Copy from file**. 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**.

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 anti-virus** supports hot license update without stopping or reinstalling the program.

Get information on license

1. On the main screen of the program (see Figure 2) press the **Menu** button and tap **About**.
2. You can review the following information on the licensing parameters on the **Dr.Web - About** screen:
   - License owner name
   - License activation and expiration dates

Update license

To update your license you need either register the new serial number or copy the new key file to the SD-card.

Chapter 3. Installation

Dr.Web anti-virus can be purchased and installed on the mobile device directly from Google Play or by launching the installation file **drweb-601-android.apk**. You can also install the application using the synchronization with PC.

The program can be removed via Google Play or by means of the operational system of the device.

System Requirements

To install and use **Dr.Web anti-virus**, ensure your mobile device works under the Android operating system of 1.6/2.0/2.1/2.2/2.3/3.0/3.1/3.2/4.0 version.

The Internet connection is also 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**, a working SIM card is required.

Install Program

You can install **Dr.Web anti-virus** either via Google Play or launch the program installation file on the device or via synchronization with PC.

Installation via Google Play

1. Open Google Play, find **Doctor Web** in the list of applications and tap **Purchase**.

> If your mobile device does not meet the system requirements, **Dr.Web anti-virus** is not displayed in the list of Google Play.

2. The screen with payment options will open. After the payment is made, on the screen with information on the application review the required access rights. The program requires access to the following data:

   - Device storage to check the files on SD-card and save the quarantine.
   - Internet to download virus databases updates.
   - Phone calls to pause scanning on calls.
   - System tools to save system information for further sending to Technical Support in case you experience problems while working with the application.

   Tap **OK**.

3. The application will be installed automatically.

For program installation without Google Play, you need to allow it on your device. To do this, select the **Unknown sources** check box on the **Settings** -> **Applications** screen.

Installation via launching the drweb-601-android.apk file directly on the device

1. Copy the installation file **drweb-601-android.apk** to the SD-card.

   To launch the installation file on the device a file manager is required.

2. Use the file manager to find and launch the installation file.
3. The application will be installed automatically.

Installation 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 **drweb-601-android.apk** 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 anti-virus was successfully installed on your device and is ready to use. In case you have installed the program without Google Play, you need to register the license for further operation of the application. If you do not have a valid key file, you can acquire it.

Update and Uninstall Program

The program can be updated or uninstalled via Google Play. If you do not have an Internet connection, you can uninstall the program by means of the operating system.

⚠ In case **Dr.Web Anti-theft** is enabled on your device, you need to clear the **Dr.Web anti-virus** checkbox on the **Location and Security** tab of the **Select device administrator** section in device settings before uninstalling the application.

Update or uninstall program via Google Play

1. Open Google Play and select **Downloads**.
2. Tap the sign of **Dr.Web anti-virus** in the list of downloaded applications.
3. On the screen with the information on the application tap **Update** or **Uninstall**.

4. Confirm the program update/removal:
    - In case you are updating the program, the next steps are similar to the ones described in the Install program section.
    - In case you are uninstalling the program, specify the reason of the program removal and tap **OK**. The program will be removed from the device.

Uninstall program without connecting to Internet

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

⚠ Quarantine and saved program log are not deleted by default. You can delete them manually from the Android/data/com.drweb/files folder on the SD-card.

Chapter 4. Start to Use

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

Launch and Exit Program

To launch the application

To launch **Dr.Web anti-virus** open the **All programs** screen and tap **Dr.Web anti-virus** sign . On the first launch of the program the License agreement will open. You need to accept it to start using the program.

To exit the application

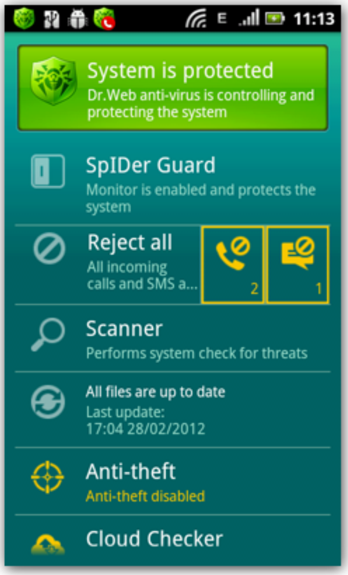
To exit **Dr.Web anti-virus** press the **Home** ⌂ button.

You can use the **Dr.Web anti-virus** sign in the recently launched programs section to activate the application from the background operation. When you first launch **Dr.Web anti-virus**, 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 program main screen (see Figure 2) the current protection status is displayed. It also provides access to the following program 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.
- **Scanner** – provides the on-demand scanning of the system (3 scan types are possible: full scan, quick scan and custom scan).
- **Update** – contains information on the date of the last update and launches the program update if required.
- **Anti-theft** – allows to configure **Dr.Web Anti-theft**.
- **Options** – allows to access to the application settings, review the quarantine list, the program statistics and the information on the application.



11:13

System is protected
Dr.Web anti-virus is controlling and protecting the system

SpIDer Guard
Monitor is enabled and protects the system

Reject all
All incoming calls and SMS a...

Scanner
Performs system check for threats

All files are up to date
Last update:
17:04 28/02/2012

Anti-theft
Anti-theft disabled

Cloud Checker

Figure 2. Main screen of the program

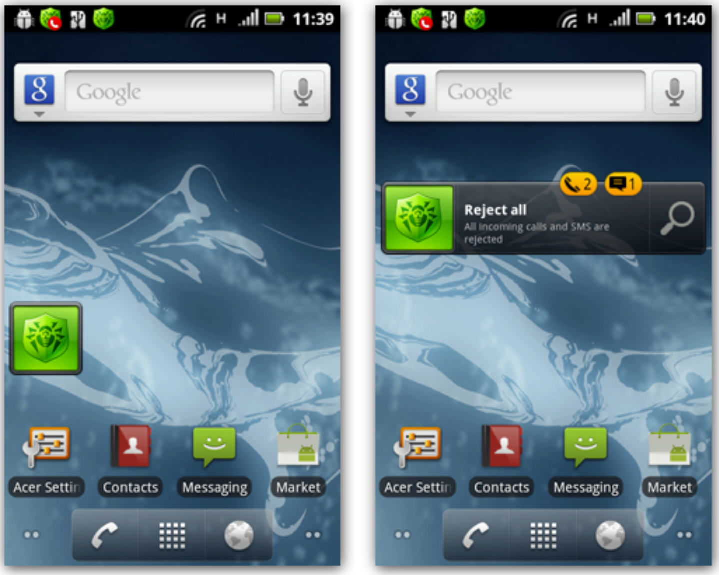
Widgets

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

To add widget

1. Press and hold an empty area on the Home Screen until the menu of adding options appear. Alternatively, to open this menu, you can press the **Menu** button on the Home Screen and select **Add**.
2. Select **Widgets** in the list of objects types.

3. Select one of **Dr.Web anti-virus** widgets in the list:
   - **Dr.Web 1x1 (small)** – displays the current protection status and allows to enable/disable the monitor **SpIDer Guard** (see Figure 3).
   - **Dr.Web 4x1 (medium)** – displays the current protection status, the selected filtering profile, the number of blocked calls and messages and allows to enable/disable the monitor **SpIDer Guard**, open the scanner screen (see Figure 4).



Reject all

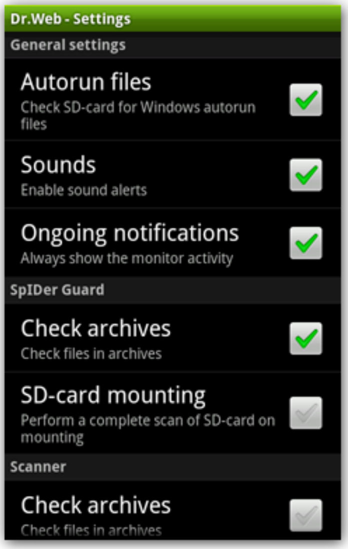
All incoming calls and SMS are rejected

Figures 3 and 4. Dr.Web widgets

Chapter 5. Application Functions

This section describes main features of **Dr.Web anti-virus** and provides step-by-step procedures of setting up the anti-virus check, SMS and calls filtering, the operation of **Dr.Web Anti-theft** for configuring protection of your device.

The main components of **Dr.Web anti-virus** can be configured on the **Dr.Web - Settings** screen (see Figure 5). To open the settings screen, on the main screen tap **Options** or press the **Menu** button and select **Settings**.



Dr.Web - Settings

General settings

Autorun files ☑
Check SD-card for Windows autorun files

Sounds ☑
Enable sound alerts

Ongoing notifications ☑
Always show the monitor activity

SpIDer Guard

Check archives ☑
Check files in archives

SD-card mounting ☑
Perform a complete scan of SD-card on mounting

Scanner

Check archives ☑
Check files in archives

Figure 5. Dr.Web - Settings screen

Reset settings

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

1. Tap **Restore default settings** on the **Dr.Web - Settings** screen (see Figure 5).
2. Confirm the return to the default settings.

Import and export settings

You can also save all current application settings to the file on the SD-card. You will be able to re-use them in future by downloading from the file.

1. To save the current configuration, on the **Dr.Web - Settings** screen (see Figure 5) tap **Backup** and then tap **Export data**. In the **Export data** window enter the password to set up for the settings file and tap **OK**. All settings are saved in the Android/data/com.drweb/files/DrWebPro.bkp file on the SD-card.
2. To load the saved settings from the file, on the **Dr.Web - Settings** screen (see Figure 5) tap **Backup** and then tap **Import data**. Confirm the settings and parameters loading from the file and enter the password set for file. All current application settings will be replaced by the settings from the file.

Anti-Virus Protection

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

Constant Anti-Virus Protection

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

Enable constant protection

On the first launch of the program the constant protection is disabled. To enable it, tap the **SpIDer Guard** section of the main screen.

When monitor 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 program sign appears in the status bar on the screen as well as a popup window with notification on the threats detection. After opening the Notifications panel you can review the information on the number of the detected threats and access to the list of the threats to choose actions for their neutralization.

Monitor settings

To access the **Dr.Web anti-virus** settings, tap **Options** or press the **Menu** button on the main screen and tap **Settings**. To configure the monitor, perform the following actions on the **Dr.Web - Settings** screen (see Figure 5):

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

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

- To enable check of the files on the SD-card on each mounting, select the **SD-card mounting** check box on the **SpIDer Guard** section.
- To enable the SD-card 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 🛡 in the status bar on monitor activity, select the **Ongoing notifications** check box on the **General settings** section.

Statistics

Dr.Web anti-virus registers the events concerning the monitor operation (enable/disable, SD-card and installed applications check results, threats detection). The program actions are displayed on the **Actions** section of the **Statistics** screen.

On-demand Scan

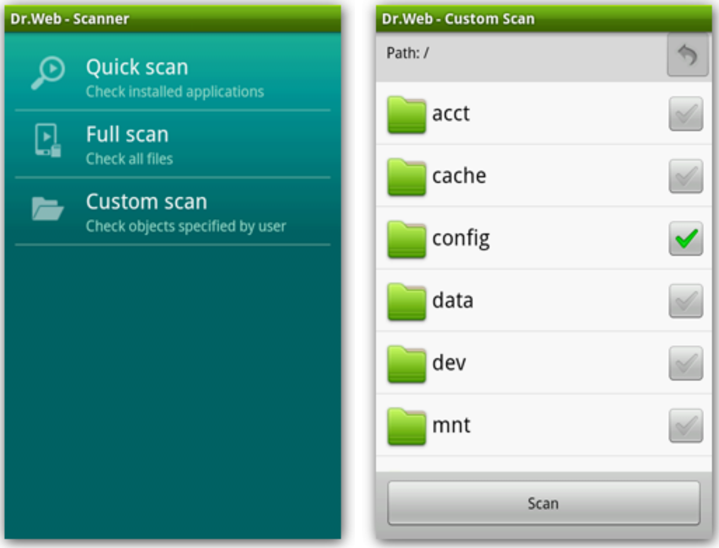
Dr.Web anti-virus provides on-demand scanning of the file system. You can perform quick or full check of the whole file system or scan the critical files and folders only. This function is performed by the Dr.Web *scanner*.

Scanning

To scan the system, on the **Dr.Web - Scanner** screen (see Figure 6) do one of the following actions:

- To launch only the installed applications check, tap **Quick scan**.
- To scan all the files, tap **Full scan**.
- To scan only critical files and folders, tap **Custom scan**, select the objects in the hierarchical list (see Figure 7) and then tap **Scan**.

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



Figures 6 and 7. Scanner and Custom Scan screens

Scanner settings

To access to the scanner settings, on the main screen tap **Options** or press the **Menu** button and tap **Settings**. To configure the scanner, perform the following actions on the **Dr.Web - Settings** screen (see Figure 5):

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

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

- To enable the SD-card 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.

It is strongly recommended to periodically scan the system in case the monitor had not been active for some time. Usually, the quick scan is sufficient for this purpose.

Statistics

Dr.Web anti-virus registers the events concerning the scanner operation (check type and results, threats detection). The program actions are displayed on the **Actions** section of the **Statistics** screen.

Threats Neutralization

On the scan completion, **Dr.Web anti-virus** allows to choose one of the following actions for each detected threat:

- **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.

You can set up sound notifications on threats detection, deletion or moving to quarantine. To do this, on the main screen press the **Menu** button and tap **Settings**, then select the **Sounds** check box on the **General settings** section of the **Dr.Web - Settings** screen (see Figure 5).

Calls and SMS Filter

Dr.Web anti-virus 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.

The filtering mode is specified by user. The program provides you with the predefined profiles, which determine the filters. You can also create user profiles with separate filtering settings.

The information on the blocked calls and messages is available on the **Blocked calls and SMS** section.

Filtering Mode

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

- **Accept all**. In this case all the incoming calls and SMS are accepted.
- **Reject all**. In this case all the incoming calls and SMS are blocked.
- **Phone book**. In this case calls and SMS only from the phone book contacts are accepted.
- **Black list**. This filter type means that the phone calls and SMS from the numbers included into the black list are blocked.

Alternatively, you can use the custom filter. **Dr.Web anti-virus** 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. Therefore, the calls and SMS are not filtered by black list only if **Accept all** filtering mode is selected.

Create black list

1. To create the black list, on the main screen of the program tap the filtering section and then select **Configure** on the **Choose profile** menu.
2. On the **Profiles/Black list** screen tap the **Black list** tab.
3. Tap **Add number** 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** phone 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 it in the list and then 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 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, press the **Menu** button and select **Clear the list**.

Create Filtering Profile

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

Create a new profile

1. In the list of available profiles tap **Configure**.
2. On the **Profiles** tab tap **Add profile**.
3. On the Add profile screen 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
    - **Block contacts from the list** – to block calls and SMS from the contacts of current profile

5. Tap **Add number** 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** phone 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 it and modify the information entered in the **Name** and **Number** fields. Then 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 it and hold to make appear a menu, where tap **Delete**.

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

View Blocked Calls and SMS

The filtering section on the main screen of the program contains the information on the number of blocked calls and messages. 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/message sender

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
   - **Delete** – to delete the SMS

Update

Dr.Web anti-virus uses **Dr.Web virus databases** to detect threats. These databases contain details and signatures for all viruses and malicious programs for mobile devices known at the moment of the application release. However modern computer viruses are characterized by the 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 program the date of the last update is displayed on the section **Update**.

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

Configure updates

Virus databases updates can be configured on the **Update** section of the **Dr.Web - Settings** screen (see Figure 5). You can specify the following options:

- Select the **Automatic** check box to choose the daily automatic updates. By default, the automatic update is disabled. If you prefer launching updates manually, clear this check box.

- Select the **Do not use mobile networks** check box to disable the use of the mobile networks to download the updates. If such networks are unavailable, you will be offered to use 3G or GPRS.

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

Quarantine

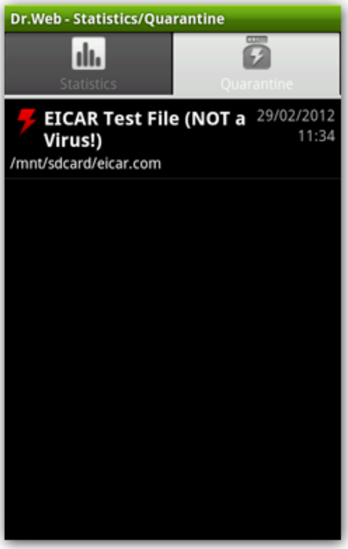
Dr.Web anti-virus allows you to move the detected threats to quarantine, where they are isolated from the rest of file system and therefore cannot damage the system.

Manage files in quarantine

1. To review the list of the threats moved to quarantine, tap **Options** or press the **Menu** button on the main screen and then tap **Quarantine**.
2. The list of all threats in quarantine will open (see Figure 8).
3. Tapping the threat in the list brings you to the window with the following information on the threat:
   - File name
   - Path to the file
   - Date of moving to quarantine

   You can also open the link on the **Information on the web** section to read the detailed information on the threat on **Doctor Web** official web-site.

4. For each threat in the list one of the following action can be performed:
   - **Restore** – to return the file back to the folder where it was moved from (use this action only if you are sure that the file is safe);
   - **Delete** – to completely remove the file from the device.



EICAR Test File (NOT a Virus!) 29/02/2012 11:34
/mnt/sdcard/eicar.com

Figure 8. Quarantine

Quarantine size

You can also review the information on the memory occupied by quarantine and on the free space on SD-card. To do this, press the **Menu** button on the **Quarantine** tab and select **Quarantine size**.

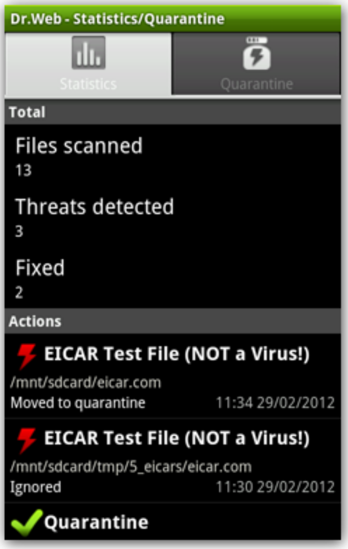
Statistics

Dr.Web anti-virus compiles the statistics of detected threats and program actions. To view the statistics, on the main screen tap **Options** or press the **Menu** button and then tap **Statistics**.

The **Statistics** tab contains two following information sections (see Figure 9):

- **Total** section contains the information on the total number of scanned files, detected and neutralized threats

- **Actions** section contains the information on scanner start/stop, monitor enable/disable, detected threats and performed actions of the program



Total

Files scanned
13

Threats detected
3

Fixed
2

Actions

EICAR Test File (NOT a Virus!)
/mnt/sdcard/eicar.com
Moved to quarantine 11:34 29/02/2012

EICAR Test File (NOT a Virus!)
/mnt/sdcard/tmp/5_eicars/eicar.com
Ignored 11:30 29/02/2012

✓ Quarantine

Figure 9. Statistics

Clear statistics

To clear all the statistics, press the **Menu** button and tap **Clear statistics**.

Event log

Dr.Web anti-virus also logs the events related to its operation in a special file that can be saved on SD-card for further sending to **Doctor Web** Technical Support in case you experience troubles while using **Dr.Web anti-virus**.

To save the event log:

1. Press the **Menu** button on the **Statistics** tab and then tap **Save log on SD-card**.
2. The log will be saved in DrWeb_Log.txt file located in the Android/data/com.drweb/files folder on SD-card.

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.

You can manage **Dr.Web Anti-theft** using special SMS commands. **Dr.Web Anti-theft** also allows to create a Buddies list, from whose devices you will be able to send SMS commands even if you forgot your password for **Dr.Web Anti-theft**.

Configure General Settings

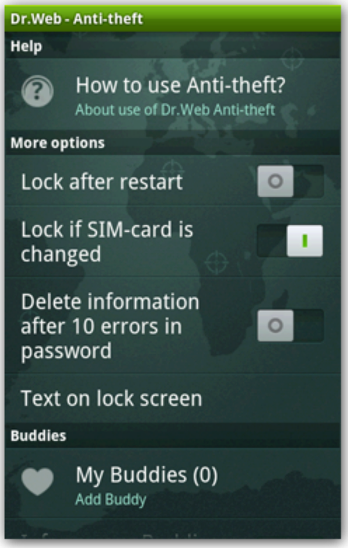
On the first start of **Dr.Web Anti-theft** a wizard window opens to help you to set you the main functions of Dr.Web Anti-theft:

- 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.

Configuring 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. Tap **Next**.
2. Confirm the entered password. Tap **OK**.
3. Configure the Buddies list. Tap **Next**.
4. Enter the text which will be displayed on the screen of the locked device. Tap **Continue**.

5. This completes the general configuration. Tap **OK** to exit the Wizard and to open the **Dr.Web - Anti-theft** screen (see Figure 10).



Dr.Web - Anti-theft

Help

How to use Anti-theft?
About use of Dr.Web Anti-theft

More options

Lock after restart ○

Lock if SIM-card is changed ●

Delete information after 10 errors in password ○

Text on lock screen

Buddies

My Buddies (0)
Add Buddy

Figure 10. Dr.Web - Anti-theft screen.

Before opening the main screen of **Dr.Web Anti-theft** a screen prompting to grant **Dr.Web anti-virus** the device administrator privileges, which you need to accept for correct operation of **Dr. Web Anti-theft**.

Getting help

To open the help on **Dr.Web Anti-theft**, on the **Dr.Web - Anti-theft** screen, tap **How to use Anti-theft?** on the **Help** section.

To change password

To change the password set for **Dr.Web Anti-theft**, on the **Dr.Web - Anti-theft** 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**.

Additional Functions

To configure **Dr.Web Anti-theft**, on the main application screen tap **Anti-theft**. To access to the **Dr.Web Anti-theft** settings screen, enter the password set for the **Dr.Web Anti-theft** on its first start. If you forgot your password, send and SMS with the **#RESETPASSWORD#** command to your device from the number included into the Buddies list or contact **Doctor Web Technical Support**.

Additional settings

To configure **Dr.Web Anti-theft**, on the **Dr.Web - Anti-theft** screen (see Figure 10), perform the following actions on the **More options** section:

- 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 errors in password** 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**.

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.

Create Buddies list

1. On the **Dr.Web - Anti-theft** screen (see Figure 10), tap **My Buddies** on the **Buddies** section.
2. Tap **Add number** 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** phone 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 **Delete**.
5. To notify your Buddies about changing the SIM-card in your phone, enable the **Inform your Buddies about SIM-card change**.
6. To allow sending SMS commands from the Buddies numbers without entering the **Dr.Web Anti-theft** password, enable the **Allow SMS commands without password** option.

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

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
#SIGNAL#*Password***#**	Lock the device and enable a sound alert which remains active even after restarting the device.
#LOCK#*Password***#**	Lock the device.
#UNLOCK#*Password***#**	Unlock the device without resetting the **Dr.Web Anti-theft** password.
#LOCATE#*Password***#**	Get the GPS coordinates of the device in ans SMS. This SMS contains a link to the Google Maps indicating the device location.
#WIPE#*Password***#**	Restore the factory settings of the device and delete all the information on the SD-card. This action will be also performed in case of 10 error when entering the password and the **Delete information after 10 errors in password** option is enabled in the **Dr.Web Anti-theft** settings.
#RESETPASSWORD#*Password***#**	Unlock the device and rest the password of **Dr. Web Anti-theft**. 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 phone, you can send the **#LOCK#*Password*#** command written as **#Lock#*Password*#**, **#lock#*Password*#**, **#lOck#*Password* #**, etc.

To 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. Do the following:

1. On the **Dr.Web - Anti-theft** screen (see Figure 10), 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;
   - **Unlock phone** – corresponds to the #UNLOCK# command;
   - **Delete all data** – corresponds to the #WIPE# command;
   - **Detect phone location** – corresponds to the #LOCATE# 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 don't need to enter the password.
5. Tap **Send**.

Recovering Password

Please send the following information with your request to recover your **Dr.Web Anti-theft** password to the **Doctor Web** Technical Support:

- The photo of your mobile device box with IMEI or MEID/ESN on it.
- Device ID, if you use a tablet. The Device ID is displayed on the screen of the blocked device.
- Google order reference, if you have purchased **Dr.Web anti-virus** via Google Play. The order reference is available on the https://checkout.google.com/main page.

After verifying the provided information, an individual unlock password will be generated and sent to the e-mail indicated during the license registering/purchase.

Operation Mode

If necessary, you can use your installation of **Dr.Web anti-virus** 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 anti-virus**.

To use central protection mode

1. Contact an anti-virus network administrator of your company or IT provider for parameters of connection to the central protection server.
2. On the main application screen, tap **Options** or press the **Menu** button and select **Settings**.
3. To connect to to central protection server of your company or IT provider, on the **Dr.Web - Settings** screen (see Figure 5) select the **Dr.Web Agent** checkbox on the **Mode** section.

In the central protection mode, the option of manual start and configuring updates is blocked. Some features and settings of **Dr.Web anti-virus**, particularly concerning the constant protection and on-demand scanning, may be modified and blocked for compliance with the company security policy or according to the list of purchased services. A key file for operation in this mode is received from central protection server. Your personal key file is not used.

4. On switching to the central protection mode **Dr.Web anti-virus** 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. If necessary, enter the port number separated by a colon.
    - Enter the authentification parameters: ID, which is assigned to your mobile 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.
    - Tap **Connect**.

To use standalone mode

1. On the main application screen, tap **Options** or press the **Menu** button and select **Settings**..
2. To switch to the standalone mode, clear the **Dr.Web Agent** checkbox on the **Mode** section of the **Dr.Web - Settings** screen (see Figure 5).

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

3. For correct operation in standalone mode **Dr.Web anti-virus** requires a valid personal key file. The key files received from central protection server cannot be used in this mode. If necessary, you can receive or update a personal key file with License Manager.

To configure the available applications list

If you are the administrator of the anti-virus network, you can specify the list of application available for the users on their devices. To do this:

1. On the main screen of the application tap **Administrator**.
2. On the **Dr.Web - Applications control** select the application which will be available for the anti-virus network users on their mobile devices.
3. Tap **Allow selected**.

Appendices

Appendix A. Technical Support

Support is available to customers who have purchased a commercial version of **Doctor Web** products. Visit **Doctor Web Technical Support** web site at http://support.drweb.com/.

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

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse the Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

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

Index

Index

Index

Index