Dr.WEB

Security Space for BlackBerry

User manual

Dr.Web Security Space for BlackBerry
Version 12.1
User manual
3/1/2018

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: http://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website 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

1. Introduction

Dr.Web Security Space for BlackBerry (hereinafter – Dr.Web) protects mobile devices running the BlackBerry™ operating system from various virus threats designed specifically for these devices.

The application features technologies of Doctor Web implemented to detect and neutralize malicious objects that may harm your device and steal your personal data.

Dr.Web uses the Origins Tracing™ technology that detects malware. This technology allows to detect new families of viruses using the information from existing databases.

About

This manual is intended to help users of the devices running BlackBerry to install and adjust the application. It also describes its basic features.

The following conventions and symbols are used in this document:

Convention	Description
	Warnings about potential mistakes or important issues that are worth special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples.

1.1. Dr.Web Features

Dr.Web performs the following features:

- Provides a real-time protection of your file system (scans files and apps when you install or download them, etc.).
- Scans the entire file system or selected files and folders on your demand.
- Scans archives.
- Scans files on SD cards (or other removable media).
- Detects threats in *.lnk files (defined by Dr.Web as Exploit.Cpllnk).
- Quarantines threats or completely removes them from your device.
- Unlocks your device if it is locked by ransomware.
- Downloads Dr.Web virus database updates from the Internet.
- Gathers statistics on detected threats and performed actions; keeps the application log.
- Analyzes device security and helps eliminate detected problems and vulnerabilities.

2. System Requirements

Make sure your device meets the requirements and recommendations listed below:

- BlackBerry of version 10.3.2 or later.
- Internet connection is required to update virus databases.

3. Installing the Application

Installing the application from Doctor Web website

The installation file of Dr.Web is available for downloading on the Doctor Web website at https://download.drweb.com/blackberry/.

Installing the application from the installation file on the device

1. Copy the installation file to the device.
2. Use a file manager to find and launch the installation file.
3. Tap **Install**.
4. Tap **Open** to start working with the application.

   Tap **Finish** to close the installation window and return to the application later.

4. Uninstalling the Application

To uninstall Dr.Web:

1. On the home screen, tap and hold the application sign.
2. Tap  on the application sign.

Note that the quarantine folder and the application log file remain in the device internal memory after uninstalling the application. If necessary, delete them manually.

5. Licensing

You need a license to use Dr.Web. A license allows you to use all features of the application during the validity period. It regulates the user rights for the purchased product according to the user agreement.

If you want to try the application before purchasing a license, you can activate a demo license.

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.

License key file

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

The license key file has *.key extension and 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 meets the following requirements:

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

If any of the conditions are violated, the license key file becomes invalid, the anti-virus 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.

5.1. License Screen

On the **License** screen (see Figure 1), you can purchase or activate a paid license, or you can get a demo license.

To open the **License** screen, do one of the following:

- Tap **More** in the notification about a missing license on the main screen of the application.
- Open the application main menu and select **License**.

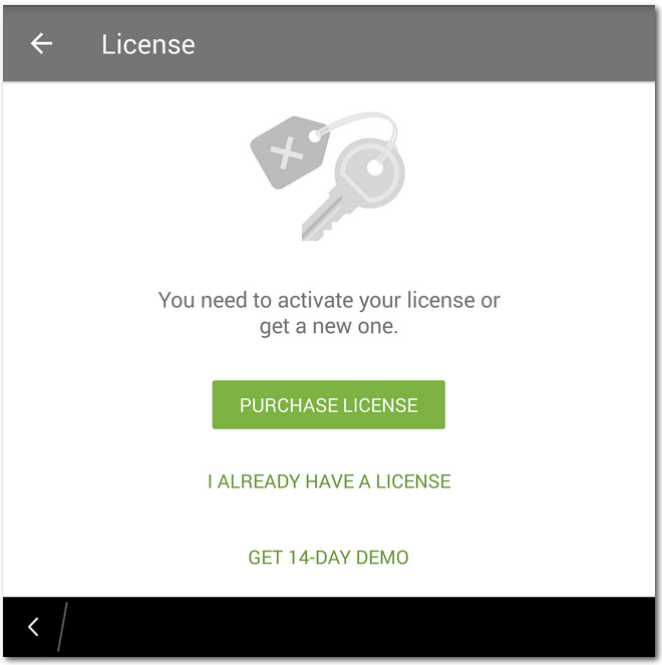

Figure 1. License screen

5.2. Activating Demo License

If you want to try the application before purchasing a license, you can activate a demo license for 14 days. To do so:

1. Start the application.
2. Open the License screen.
3. Select **Get 14-day demo**.
4. State your personal information (see Figure 2):
   - First and last name.
   - Country.
   - Existing email address.
5. Optionally, select the **Get news by email** check box.

   The application may request access to your contacts. If you allow the access, the **Email address** and **Country** fields are filled in automatically. Otherwise, you fill them in manually.
6. Tap **Get demo**. This will activate your demo license.

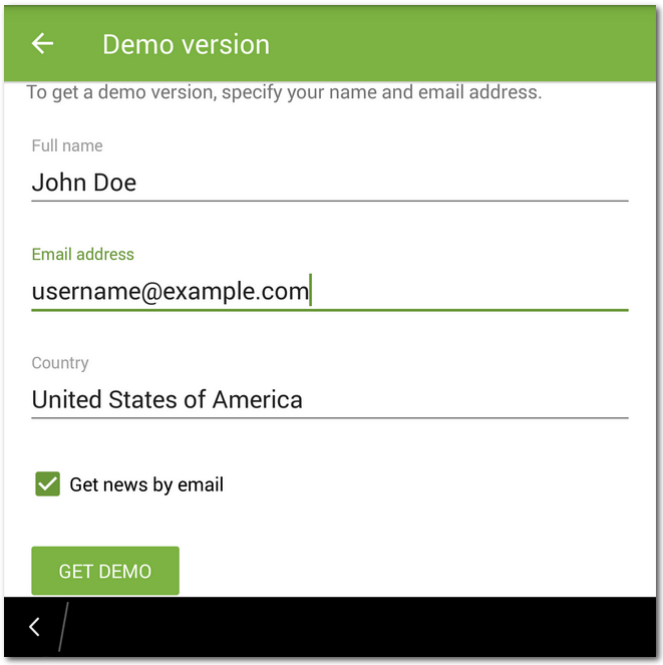

Figure 2. Getting a demo license

5.3. Purchasing License

If the application is installed from the Doctor Web website

To purchase a license for Dr.Web downloaded from the website:

1. Start the application.
2. Open the License screen.
3. Select **Purchase license**. You will be redirected to the Doctor Web online store.

   You can also open the online store at https://estore.drweb.com/mobile.
4. Select the license period and the number of devices to protect.
5. Click **Buy**.
6. Fill in the form and click **Continue**.

   After you complete your purchase, you will be sent a serial number. You can choose to receive the serial number via email or SMS message.
7. After that, register your serial number or copy the key file to your device.

5.4. Activating License

You should complete license activation if you have downloaded the application from Doctor Web website. Activation may also be necessary if you already have a valid Dr.Web license that covers Dr.Web Security Space for BlackBerry.

In order to activate your license, you have to register your serial number. To do so:

- Register your serial number in the application. In this case, your device must be connected to the Internet.
- Register your serial number on the Doctor Web website. Use this type of registration if your device has no Internet connection. In this case, you will receive a license key file that you will have to copy to your device to activate your license.

Registering a serial number and activating a license in the application

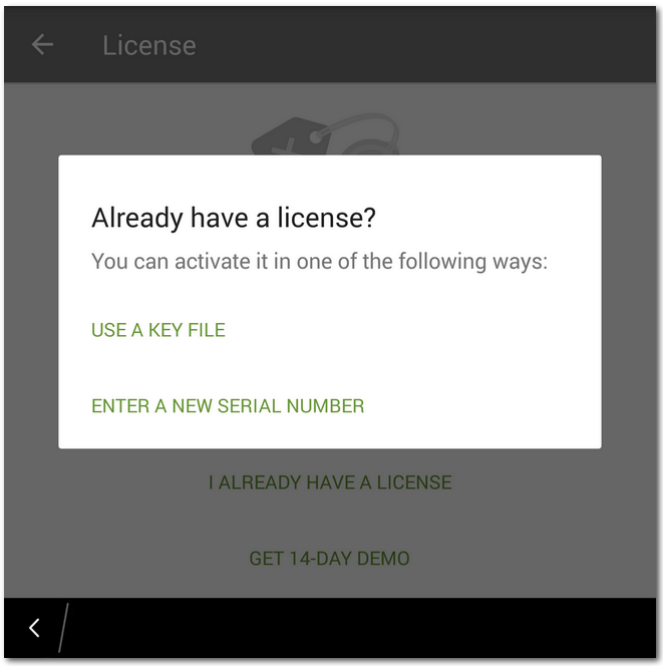

Figure 3. Activating License

To register your serial number and activate the license in the application:

1. Start the application.
2. Open the License screen.
3. Tap **I already have a license**.
4. On the next screen (see Figure 3), tap **Enter a new serial number**.
5. On the **License activation** screen (see Figure 4), enter your purchased serial number.
6. Tap **Activate**.

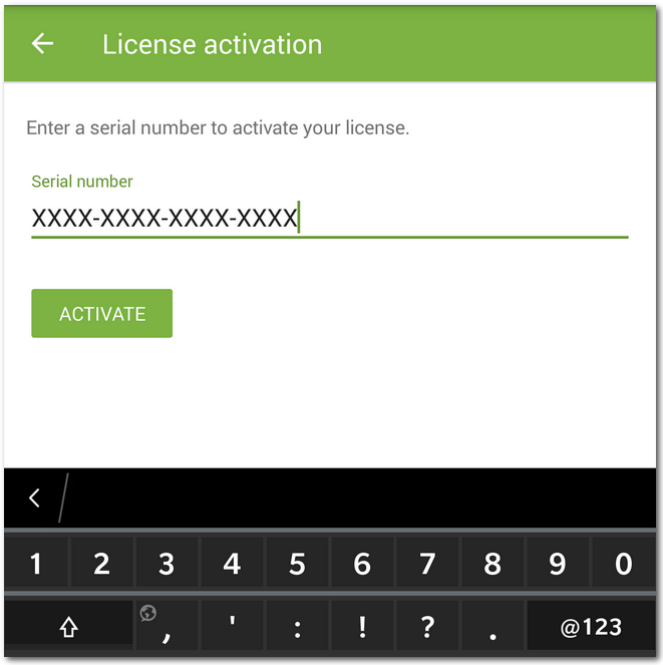

Figure 4. Registering a serial number

7. State your personal information:
   - First and last name.
   - Country.
   - Existing email address.
8. Optionally, select the **Get news by email** check box.
9. Tap **Activate**.

You will be redirected to the main screen of the application. You will see a notification about a successful license activation below.

Registering a serial number on the website

To register your serial number and receive your license key file, follow these steps:

1. Go to https://products.drweb.com/register/.
2. Enter the serial number that you received after you purchased Dr.Web.
3. Fill in the registration form.
4. The license key file with the *.key extension will be sent as a ZIP archive to your email address.

Using your license key file

1. Synchronize your device with computer and copy the key file to a folder in the internal device memory.

You can either copy the entire ZIP archive or you can extract the file on your computer and copy it to your device.

2. On the License screen, tap **I already have a license**.
3. Select **Use a key file** (see Figure 3).
4. Open the folder where you have copied the key file or the entire ZIP archive to, and tap it.

The key file will be installed and ready to use. You will be redirected to the main screen of the application. At the bottom of the screen, you will see a notification about a successful license activation.

A key file for Dr.Web Security Space or Dr.Web Anti-virus applications can be used with Dr.Web only if it supports DrWebGUI and Update components.

To check whether such a 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 and Update components are on 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.

5.5. Restoring License

You may need to restore your license if you have reinstalled the application, or if you are going to use Dr.Web on another device.

If you have purchased the application from the website, you have two options to restore your license:

- Enter a new serial number.
- Use your license key file.

Restoring demo license

To restore your demo license:

1. Start the application.
2. Open the License screen.
3. On the **License** screen, tap **Get 14-day demo**.
4. Enter the email address you have used to activate your demo license and your personal information.
5. Tap **Get demo**.

5.6. Renewing License

You can open the screen with details on your current license on the main screen (see Figure 5) tap menu and select **License**.

You can renew the license in one of the following ways:

- If you already have a new serial number, simply register it.
- If you have obtained your current license from the Doctor Web online store, you can:
  - Purchase license.
  - Use your license key file.
  - Renew license on your personal web page on the Doctor Web website.

    To do so, select the **About** option in the application menu and tap **My Dr.Web**.

5.7. Configuring Notifications on License Expiration

To enable and disable notifications about upcoming license expiration on mobile device:

1. On the main screen, open the menu and tap **Settings** (see Application settings).
2. Tap **License**.
3. Clear the **Notifications** check box to disable notifications. To enable notifications, select the check box.

6. Getting Started

After you install Dr.Web and activate a license , you can get acquainted with the interface and main menu.

6.1. License Agreement

On the first launch of the application you will be asked to read and accept the License agreement, that is necessary to accept using the application.

On the same screen, you will be notified about sending the statistics on the application operation and the detected threats to the Doctor Web, Google, and Yandex servers.

You can disable sending statistical information at any time by clearing the **Send statistics** check box in the **General Settings** section of the application settings.

6.2. Interface

Main screen

The main screen (see Figure 5) comprises the list of Dr.Web components.

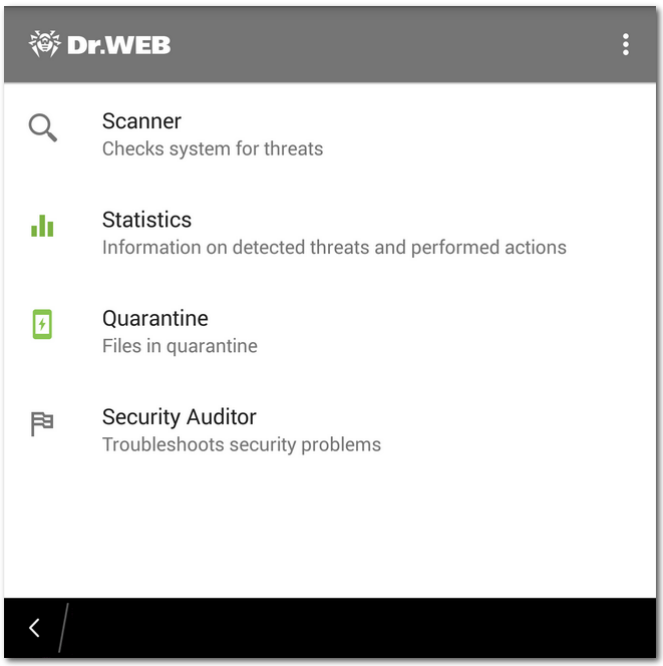

Figure 5. Application main screen

Menu in the top right-hand corner of the main screen allows you to:

- View license details.
- Run virus database update.
- Open application settings screen.
- View information about the application.

Status bar

In the top part of the application main screen, there is a status bar with an indicator that shows current device protection status (see Figure 6).

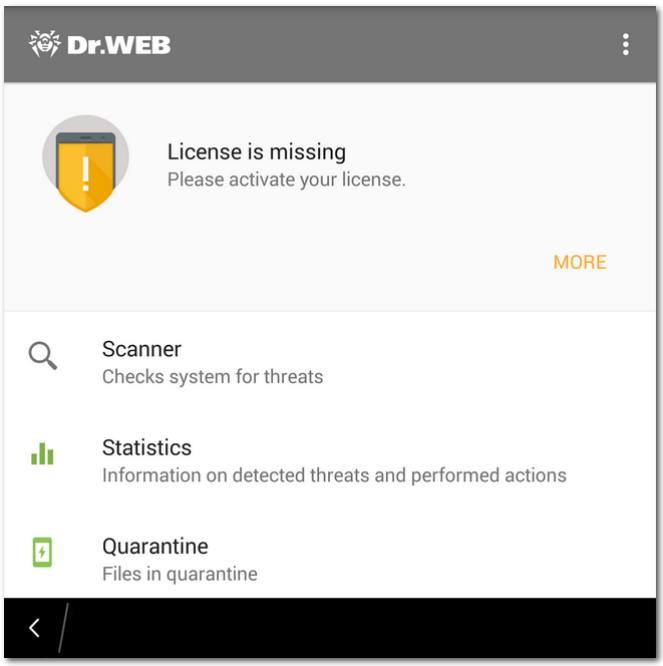

Figure 6. Status bar

- The green sign indicates that the device is protected. No additional actions are required.
- The yellow color indicates that the application has detected issues (for example, the license is missing). To learn more about detected threats or issues, and to eliminate them, tap **More** on the bar.
- The red color indicates that the application has detected security threats. In order to neutralize them, select **More**.

If the application has detected multiple events that require user attention, select **More** to open the **Events** screen, which will display all events.

6.3. My Dr.Web

My Dr.Web online service is your personal webpage on the official Doctor Web website. This page provides you with information on your license including usage period and serial number. It allows you 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 Dr.Web online service:

1. On the main screen, open the menu  and tap About.
2. Tap My Dr.Web.

7. Dr.Web Components

A list of application components is located on the main screen of the application. It also displays current state of the components (enabled or disabled).

Dr.Web comprises the following components:

- Scanner – scans your device on demand (3 scan types are available: full scan, express scan, and custom scan).
- Statistics – displays statistics of the detected threats and performed actions.
- Quarantine – allows you to view and process quarantined objects.
- Security Auditor – performs system diagnostics and resolves detected security problems and eliminate vulnerabilities.

7.1. Anti-Virus Protection

The SpIDer Guard component checks your file system in real time.

You can also scan your device manually with Dr.Web Scanner.

If any of the components detects a threat on your device, you are able to choose an action to neutralize it.

7.1.1. SpIDer Guard: Real-Time Protection

Enabling real-time protection

When you launch Dr.Web for he first time, the constant protection is enabled automatically after you accept the License Agreement. To disable or re-enable SpIDer Guard, select the **SpIDer Guard** on the Settings screen.

SpIDer Guard keeps protecting the device file system only when Dr.Web is launching. If you quit the application, SpIDer Guard will stop protecting your device.

If a security threat is detected, a notification about the detected threat appears in the status bar in the top part of the application main screen.

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

SpIDer Guard settings

To access SpIDer Guard settings, open the Settings screen.

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

  > By default, scanning of the archives is disabled. Enabling the scanning may influence the system performance and increase power consumption. Disabling the scanning does not decrease the protection level because SpIDer Guard checks installation *.apk and *.bar files even if the **Files in archives** option is off.

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

Statistics

The application registers the events related to SpIDer Guard operation (enabling/disabling SpIDer Guard, device memory and installed applications scan results, threat detections).

The application actions are displayed on the **Actions** section of the **Statistics** tab sorted by date (see Statistics section).

Testing SpIDer Guard

You can check if SpIDer Guard operates correctly using EICAR test file. The file is usually used to:

- Check if the anti-virus software is installed correctly.
- Show the anti-virus reaction if a threat is detected.
- Check the corporate procedures if a threat is detected.

The file is not a virus. It does not contain any fragments of viral code. Thus it is absolutely safe for your device. Dr.Web detects the file as “EICAR Test File (NOT a Virus!)”.

You can download it from the Internet or create it by yourself:

1. In any text editor, create a new file, which includes the only string:

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

2. Save the file with extension *.com.

As soon as you save EICAR file on your device, you will hear a distinguished sound and see a warning message from the SpIDer Guard: “Threat detected! EICAR Test File (NOT a Virus!)”. A red colored indicator will also appear on the status bar in the top part of the application main screen (see Figure 7).

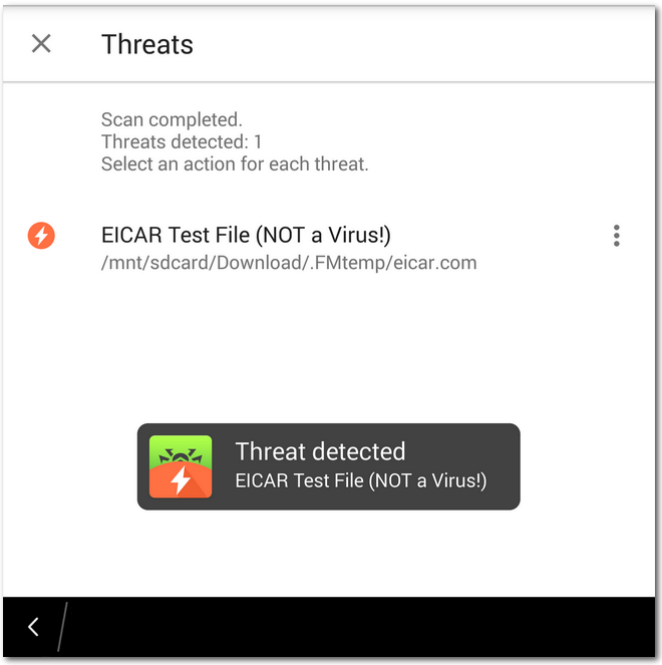

Figure 7. EICAR test file detection

7.1.2. Dr.Web Scanner: On-Demand Scan

On-demand scanning of the file system is provided by Dr.Web Scanner. It performs express or full scan of the whole file system or scans critical files and folders only.

You should scan the system periodically, especially if SpIDer Guard have not been active for a while. Usually, the express scan is sufficient for this purpose.

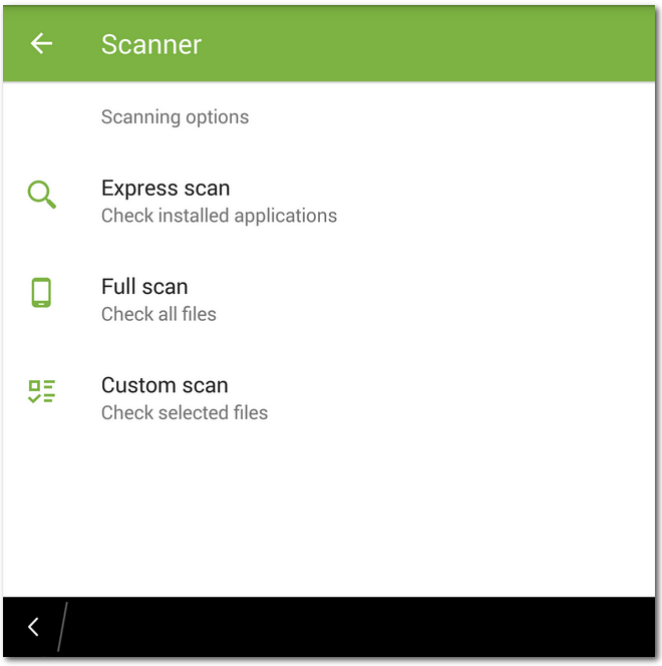

Figure 8. Dr.Web Scanner

Scanning

To scan the system, on the application main screen, tap **Scanner**, then on the **Scanner** screen (see Figure 8) select one of the following actions:

- To check installed applications, tap **Express scan**.
- To scan all the files, tap **Full scan**.
- To scan only selected files and folders, tap **Custom scan**, select the objects from the list (see Figure 9) and then tap **Scan**. You can select all objects in the current location (use the check box above the list).

If Dr.Web Scanner finds threats on your device, the sign will appear at the bottom of the Scanner screen. Tap it to view the list of detected threats and neutralize them.

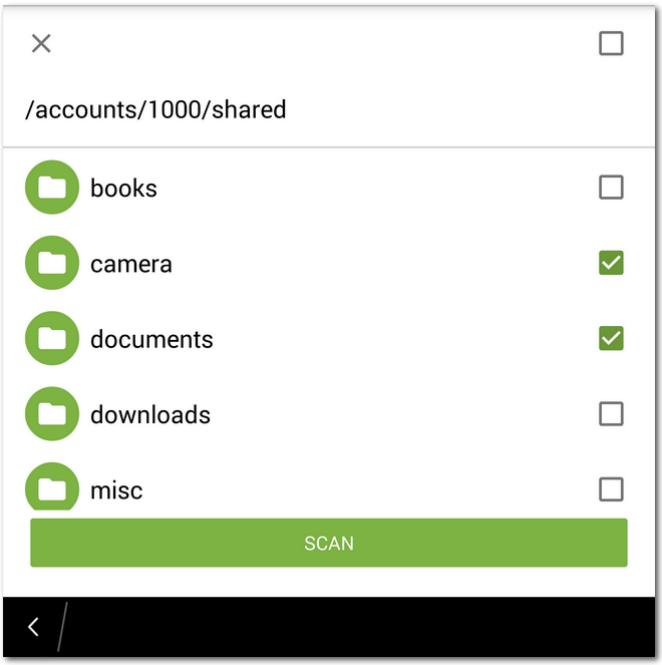

Figure 9. Custom scan screen

Sending suspicious files to Doctor Web anti-virus laboratory

You can submit to Doctor Web anti-virus laboratory suspicious ZIP archives (files with the *.jar and *.apk extensions) presumably containing viruses, *.dex, *.odex, *.so files, or clean ZIP-archives that has been identified as so-called false positive:

1. Tap and hold the file in the hierarchical list (see Figure 9), then tap **Send to laboratory**.
2. In the next screen, enter your email address if you want to receive the results of the file analysis.
3. Select a category for your request:
   - **Suspicious file** – if you think that the file is a threat.
   - **False positive** or **False positive by Origins Tracing** – if you think that the file was identified as a threat by mistake.

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

Doctor Web anti-virus laboratory accepts files of 50 MB or less.

Dr.Web Scanner settings

To access Dr.Web Scanner settings, open the application settings screen and select **Scanner**.

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

> By default, scanning of the archives is disabled. Enabling the scanning may influence the system performance and increase power consumption. Disabling the scanning does not decrease the protection level because Dr.Web Scanner checks installation *.apk and *.bar files even if the **Files in archives** option is off.

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

Statistics

The application registers events related to Dr.Web Scanner operation (scan type and results, detected threats). All registered actions are displayed in the **Actions** section, on the **Statistics** tab sorted by date (see Statistics).

7.1.3. Neutralizing Threats

Viewing the list of detected threats

If threats are detected by SpIDer Guard, the  appears in the status bar on the screen. You will also see a notification about detected threats.

If Dr.Web Scanner detects threats on your device, the  sign will appear at the bottom of the Scanner screen. Tap it to view the list of detected threats and neutralize them.

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

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

If the detected threat is not a virus (which still could be potentially harmful for your device), Dr.Web will add a clarification in brackets: adware, riskware, joke or hacktool program.

Neutralizing threats

Select a threat in the list and apply one of the following actions:

- **Delete** – to delete the threat from your device.
- **Move to quarantine** – to isolate the threat in the quarantine folder.

If the threat is detected in an installed application, it cannot be moved to quarantine. In this case, the **Move to quarantine** option will not be available.

- **Ignore** – to temporary ignore the threat with no action applied.
- **Report false positive** – to 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 to receive the results of the file analysis and tap **Send**.

The **Report false positive** action is available for threat modifications with the ".origin" postfix.

7.2. Statistics

Dr.Web compiles statistics of detected threats and application actions.

To view the statistics, tap **Statistics** on the main screen.

Viewing statistics

The **Statistics** tab contains two 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, enabling and disabling SpIDer Guard, on detected threats and performed actions.

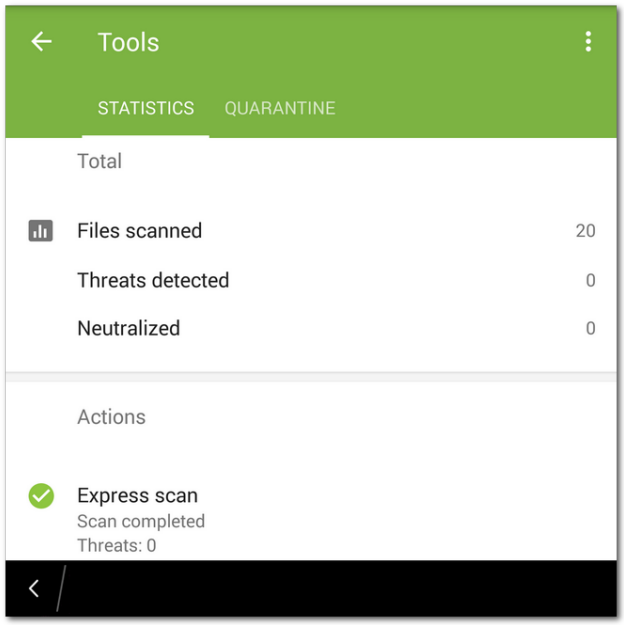

Figure 10. Statistics

Clearing statistics

To clear all the statistics, open the application menu in the **Statistics** section and tap **Clear statistics**.

Saving event log

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

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

7.3. Quarantine

Dr.Web allows you to move the detected threats to quarantine folder, where they are isolated and cannot damage the system (see Figure 11).

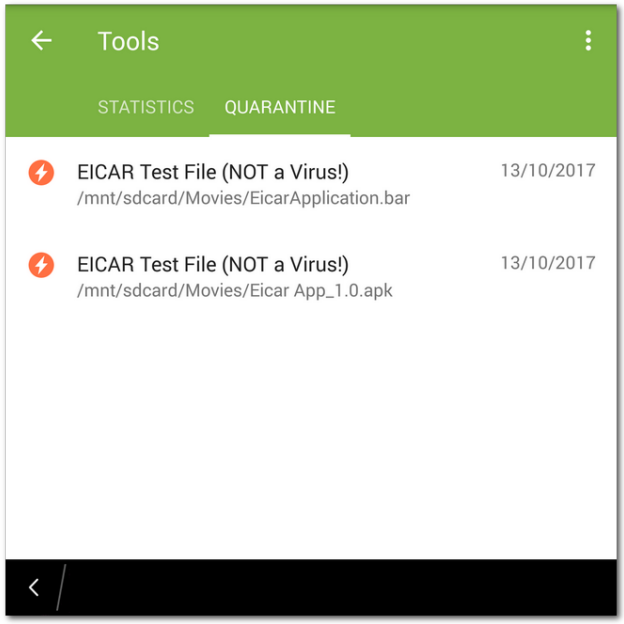

Figure 11. Quarantine

Viewing quarantined files

To view the list of threats moved to quarantine, select the Quarantine option on the application main screen.

Viewing information on quarantined threats

To view information on a threat, tap it in the list.

For each threat, the following information is available:

- File name.
- Path to the file.
- Date and time the threat has been quarantined.

Actions you can apply to quarantined objects

For each threat, you can apply the following actions:

- **More on the Internet** – to view detailed information on this type of threats on the Doctor Web website;
- **Restore** – to return the file back to the folder where it was quarantined from (use this action only if you are sure that the file is safe).
- **Delete** – to completely remove the file from the device.

Removing all objects from the quarantine

To remove all quarantined objects at once:

1. Open the **Quarantine** section.
2. Open the menu in the **Quarantine** section and select **Remove all**.
3. Tap **OK** to confirm the removal.

   Tap **Cancel** to cancel the action and return to the **Quarantine** screen.

Quarantine size

To view the information on the internal device memory free space and space occupied by the quarantine:

1. Open the **Quarantine** section.
2. Open the menu in the **Quarantine** section and select **Quarantine size**.
3. Tap **OK** to return to the **Quarantine** screen.

7.4. Security Auditor

Dr.Web uses a special component — Security Auditor — to diagnose the security of your device and help resolving the detected problems and vulnerabilities. The component is enabled automatically when the application is launched for the first time and after registering the license.

Resolving security problems

To review the list of the detected problems and vulnerabilities (see Figure 12), select the **Security Auditor** section on the application main screen.

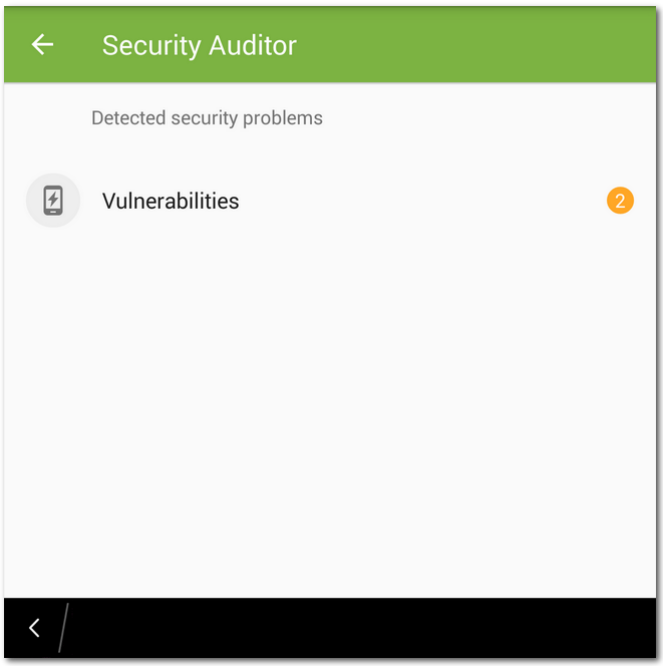

Figure 12. List of security problems detected on your device

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

Vulnerabilities

Vulnerability is a weakness in the source code which allows cybercriminals to impair the correct operation of a system.

Dr.Web detects the following vulnerabilities in the system: BlueBorne, 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, SIM Toolkit (CVE-2015-3843). 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 — an error in OpenSSL, that can be used by cybercriminals to access 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. Recent versions may have these vulnerabilities fixed. If there are no available updates, you are recommended to install applications only from trusted sources.

7.5. URL Shortener

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.

Checking and shortening a URL

1. Select the URL you want to check and shorten, then use the sharing function of your browser.
2. In the menu, select **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 application detects threats, you will see a warning.

8. Dr.Web Settings

To open the settings screen (see Figure 13), on the main screen open the application menu and select **Settings**.

On the **Settings** screen, you can use the following option to configure the application:

- **General Settings** allows you to enable and disable sound alerts and edit statistics sending preferences (see section General Settings).
- **SpIDer Guard** allows you to configure the SpIDer Guard component, that constantly scans your device for security threats (see section SpIDer Guard settings).
- **Scanner** allows you to configure Dr.Web Scanner that scans your device on your request (see section Dr.Web Scanner Settings).
- **Updating Virus Databases** allows you to disable virus database update over mobile networks (see section Updating Virus Databases).
- **License** – allows you to enable and disable notifications on upcoming license expiration (see section Configuring notifications on license expiration).
- **Reset settings** allows you to reset user settings and restore default configuration (see section Resetting Settings).

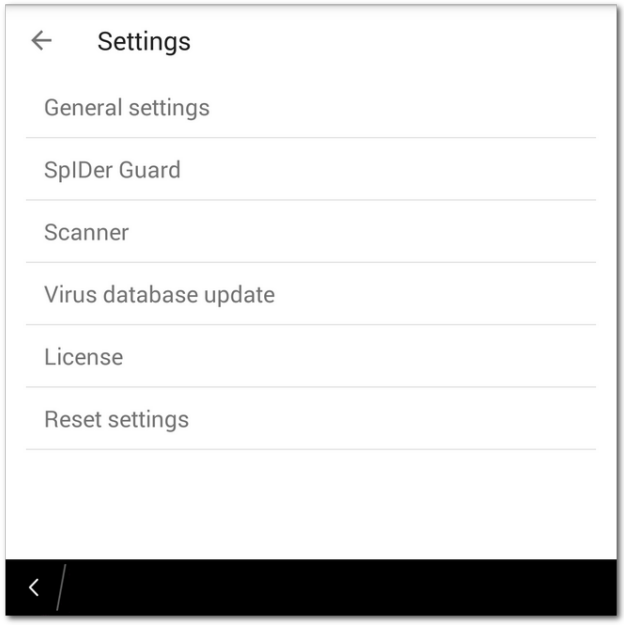

Figure 13. Application settings

8.1. General Settings

The **General Settings** section (see Figure 14) contains the following options:

- **Sounds** enables and disables sound notifications on threat detection, deletion or moving to quarantine. By default, sound notifications are enabled.
- **Send statistics** enables and disables sending statistics to Doctor Web.

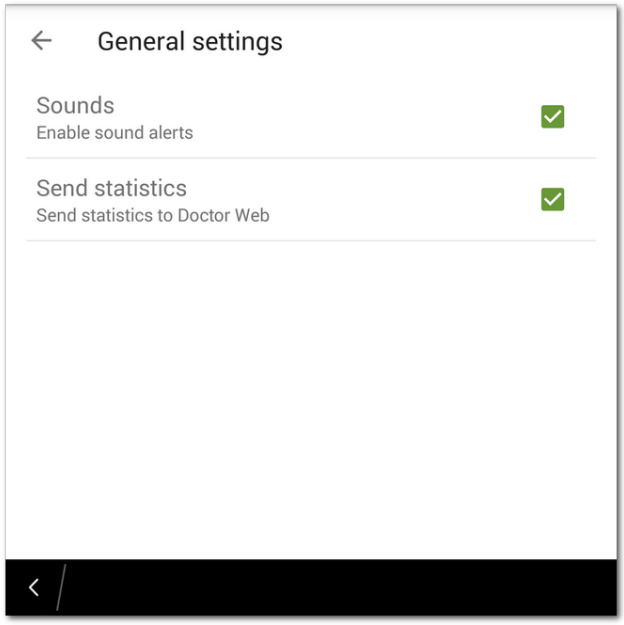

Figure 14. General settings

8.2. Updating Virus Databases

Dr.Web uses special virus databases to detect threats. These databases contain details and signatures of all viruses and malicious programs for devices running BlackBerry known by Doctor Web experts. Virus databases have to be regularly updated as new malicious programs appear every day. The application features a special option for updating virus databases over the Internet.

Update

The virus databases are updated via Internet several times a day automatically. If virus databases have not been updated for a long time (for example, if the device is not connected to the Internet) you should update them manually.

To check whether you need to update virus databases, do the following:

1. Open the application main menu and select **Virus databases**.
2. In the opened screen you will see virus databases update status, and when virus databases were last updated. If the bases are not up to date, you should update them manually.

To update virus databases manually:

1. Open the application main menu and select **Virus databases**.
2. In the next window, tap **Update**.

> You are recommended to update virus databases as soon as you install the application. This will allow Dr.Web to use the most up-to-date 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 are issued. In some cases, updates can be issued several times per hour.

Configuring updates

By default, the updates are automatically downloaded several times a day.

To enable or disable the use of mobile networks to download updates:

1. Open the menu and select **Settings** (see Figure 13).
2. Select section **Updating Virus Databases**.
3. To disable the use of mobile networks to download updates select the **Update over Wi-Fi** check box.

If no Wi-Fi networks are available, you will be prompted to use mobile Internet. Changing this setting does not affect the use of the mobile networks by other application and device functions.

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

8.3. Reset Settings

You can reset custom settings of the application at any time and restore default settings.

1. Tap **Reset settings** on the settings screen (see Figure 13). Then tap **Reset settings**.
2. Confirm you want to restore default settings.

9. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Review the latest manuals and guides at https://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/.

If you have not found solution for the problem, you can request direct assistance from Doctor Web technical support in one of the following ways:

- Fill in the web form in the corresponding section at http://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86. Free phone call (within Russia): 8-800-333-7932.

Refer to the official website at http://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.

Keyword Index

Keyword Index