Dr.WEB

Mobile Security Suite (Aurora)

User manual

Dr.Web Mobile Security Suite (Aurora)
Version 3.1
User manual
10/22/2024

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: https://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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

1. About Document 5
2. About Product 6
2.1. Main Features 6
2.2. System Requirements 6
3. Installing Dr.Web Mobile Security Suite 7
4. Uninstalling Dr.Web Mobile Security Suite 9
5. Interface 10
6. Accounts 16
7. Interaction with Aurora Center 17
8. Licensing 18
8.1. License Page 18
8.2. Trial Period 20
8.3. Purchasing License 21
8.4. License Activation 22
8.5. Restoring License 26
9. Dr.Web Components 27
9.1. Dr.Web Scanner: Scan at User Request 27
9.2. Statistics 32
9.3. Quarantine 36
10. Settings 39
10.1. General Settings 39
10.2. Scanner Settings 40
10.3. Update Settings 40
10.4. Reset Settings 41
11. Virus Database Update 42
12. Technical Support 44
Appendix A. Troubleshooting 45

1. About Document

This manual is intended to help admins and users of devices running on OS Aurora to install and configure the application. It also describes its basic features.

The following symbols and text conventions are used in this guide:

Convention	Comment
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`/home/user`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

2. About Product

Dr.Web Mobile Security Suite (hereinafter—Dr.Web) protects mobile devices, running on OS Aurora, from various virus threats.

The app features technologies of Doctor Web that are 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 for different paltforms, including OS Aurora. This technology allows to detect new families of viruses using the information from existing databases.

2.1. Main Features

Dr.Web performs the following features:

- scans entire file system or selected files at user request;
- scans archives;
- quarantines threats or completely removes them from your device;
- regularly updates Dr.Web virus databases over the internet;
- logs app activity (events related to Dr.Web Scanner operation, virus database update, actions applied to detected threats), keeps app log.

2.2. System Requirements

Before installing the app, make sure your device meets the requirements and recommendations listed below:

Component	Requirement
Operating system	Aurora 4.0.2 update 2 and later builds of version 4
CPU architecture	ARMv7
Free RAM	At least 512 MB
Free space on device	At least 20 MB (for data storage)
Screen resolution	At least 800×480
Other	Internet connection (for virus database updates)

3. Installing Dr.Web Mobile Security Suite

Dr.Web can be installed manually or by means of the Aurora Center application.

Manual installation of Dr.Web

You can install the application manually only if you have administrator access.

To install Dr.Web manually

1. Download the Dr.Web installation file or copy it to the device.
2. On the App Grid open the “Files” application.
3. Find the Dr.Web installation file and touch it.
4. In the dialog window tap **Install**.

If the app was installed successfully, you will see the corresponding notification at the top of the screen. Dr.Web will also appear on the App Grid of the user device.

For further operation, you need to activate a paid or demo license.

Installation of Dr.Web via Aurora Center

Dr.Web can be installed:

- by a Management platform administrator via the Aurora Center application software.
- by a mobile device user via the Aurora Market mobile app.

Dr.Web needs to be published in an Aurora Market app collection (dashboard) for it to be installed using either of the methods.

Installation by the administrator of the Management platform via Aurora Center

For Dr.Web to be installed on a mobile device, it has to be activated on the Aurora Center server first.

An administrator of the Aurora Center Management platform can install the app on the mobile device without involving the device user.

Before installing Dr.Web, make sure that the mobile device has been activated on the server. If the activation has been performed, the Management Platform administrator can distribute the

required policies on the device. As a result, the app will be automatically installed from the Aurora Market app collection specified by the administrator on the user device.

Once the installation process is completed, information on its result will be displayed in Aurora Center. If the app was installed successfully, Dr.Web will appear on the App Grid.

Installation by the user via the Aurora Market app

The mobile device user can install the app with the help of an administrator of the Aurora Center Management platform.

To install Dr.Web on a mobile device, the administrator of the Management platform needs to send the user the QR code or the link to the app collection the Dr.Web app is published in. After receiving the QR code or link, perform the following actions on the mobile device:

1. Connect the dashboard to the device in one of the following ways.
   - If you received a QR code:
     - Open the **Aurora Market** app.
     - Open the **Collections** tab at the bottom of the screen.
     - On the **Collections** page tap **Add** or select the **Add collection** option in the menu. To open the menu, with a fast motion, pull the page down or pull the page down starting from the middle without lifting your finger.
     - Scan the QR code.
     - If required, enter your login credentials.
   - If you received a link:
     - Follow the link sent to you by the administrator.
     - If required, enter your login credentials.
2. If the collection was not activated automatically, activate it:
   - On the **Collections** page, touch the dashboard.
   - Touch **Login**.
   - If required, enter your login credentials.
3. Open the **Applications** tab at the bottom of the screen.
4. Find **Dr.Web** on the app list and touch its icon.
5. On the Dr.Web app card screen, touch the **Install** button.

If the app was installed successfully, the **Launch** button will appear on the Dr.Web app card screen. Dr.Web will also appear on the **App Grid** of the user device.

For further operation, you need to activate a paid or demo license.

4. Uninstalling Dr.Web Mobile Security Suite

The Dr.Web app can be uninstalled using either of the following methods.

Uninstalling via Aurora Market

To uninstall Dr.Web via the Aurora Market app

1. Open the **Aurora Market** app.
2. If needed, activate the dashboard Dr.Web was installed from.
3. The main page of the **Aurora Market** app will display the app list of the activated dashboard. Find **Dr.Web** on the app list and touch its icon.
4. On the Dr.Web app card screen, touch the **Uninstall** button.

Uninstalling from the App Grid

To uninstall Dr.Web from the App Grid

1. Open the App Grid.
2. Touch and hold the App Grid until the  icons appear.
3. Touch  on the Dr.Web app icon to uninstall the app.

5. Interface

Use the following interface elements to configure and manage Dr.Web:

- gestures,
- back button,
- pulley menu,
- menu of available actions,
- switcher,
- alert panel,
- remorse pop-up,
- app cover.

Gestures

To open the application, swipe up from the bottom edge of the Home screen of your device. In the App Grid, select Dr.Web.

If you want to minimize the app and go back to the Home screen, in the open app, swipe to the center from the left or right edge. The cover of the Dr.Web app will appear on the Home screen.

If you want to minimize the app and go back to the App Grid, in the open app, swipe up from the bottom edge.

Back button

In Dr.Web, some interface components are located in subpages. A back button in the form of a glowing dot in the top-left corner (see Figure 1) indicates that you are on a subpage. To go back to previous page and save all your changes, touch the dot.

Figure 1. Back button

You can also return to the previous page by swiping from the left edge when you are on a subpage.

Pulley menu

The pulley menu opens the menu of Dr.Web. It also allows you to perform actions on the current page.

A highlighted horizontal line at the top indicates that a page contains a pulley menu.

You can open the pulley menu by doing the following:

- with a fast motion, pull the screen down;
- pull the page down starting from the middle without lifting your finger.

To select an option from the pulley menu, use one of the motions:

- With a fast motion, pull the screen down. Select the menu option.
- Pull the screen down starting from the middle without lifting your finger. Release when the necessary option is highlighted.

Menu of available actions

Menu of available actions opens a list of available actions or additional information depending on the selected page element. For example, the menu of available actions allows you to view the list of available actions for detected threats (see Figure 2).

To open the menu of available actions, touch and hold the necessary page element.

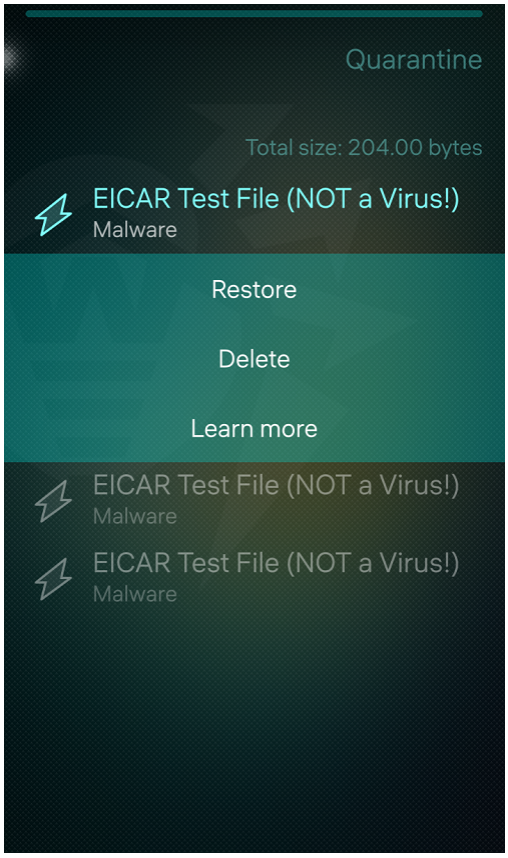

Figure 2. Menu of available actions

Switcher

The app settings can be changed with the help of switchers, which have two visual states:  represents an enabled option,  represents a disabled option. To enable or disable an option, touch the switcher.

Alert panel

An alert panel (see Figure 3) appears at the bottom of a page when a user action is needed after a process is completed. For example, an alert panel appears if threats were detected as a result of a scan.

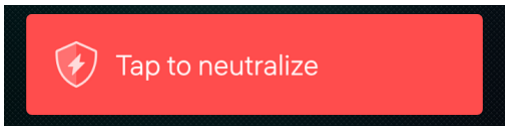

Figure 3. Alert panel

Touch the panel to go to a page with available actions.

Remorse pop-up

A remorse pop-up (see Figure 4) appears at the top of a page after an action is performed (for example, after resetting settings). To cancel the action, touch the remorse pop-up.

Figure 4. Remorse pop-up

Application cover and stopping Dr.Web

If you minimize Dr.Web by swiping from the left or right edge, the application cover displays on the Home screen (see Figure 5). Touch the cover to open the app again.

If you minimize the app while scanning, the app cover on the Home screen displays scan progress.

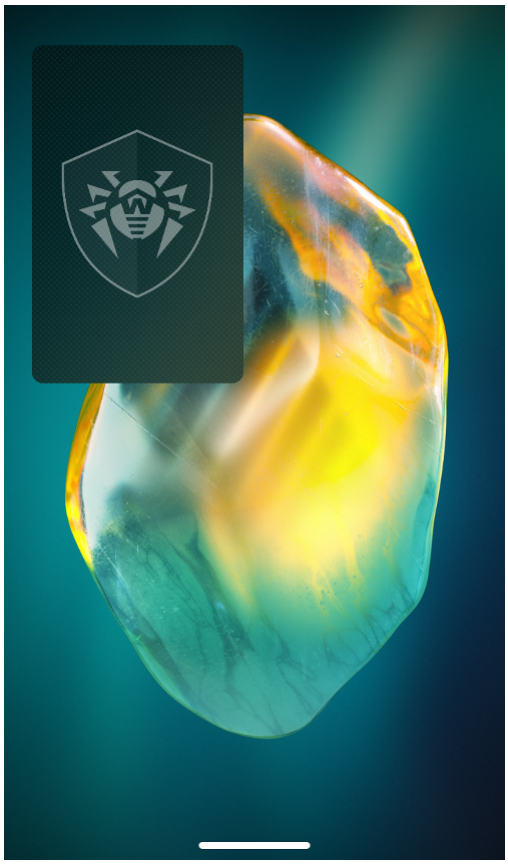

Figure 5. Application cover

To fully stop app operation and complete all related processes, do one of the following:

- In the open app, touch one of the top corners of the screen and pull down without lifting your finger.
- Do the following:
  1. In the open app, swipe from the left or right edge.
  2. On the Home page of your device, touch and hold the Dr.Web cover until the icon appears.
  3. Touch the icon.

If you fully stop the app operation while scanning, next time you open the app on its main page you will see an alert panel with the number of detected threats (see Figure 6). Touch it to go to the scan results. If the scan has not detected any threats, the alert panel does not appear. In this case, to see the scan results, open the page of the previously selected scan option.

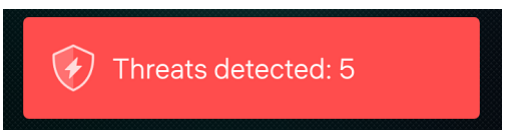

Figure 6. Alert panel with the number of detected threats

Main page

The main page (see Figure 7) contains the list of Dr.Web main components.

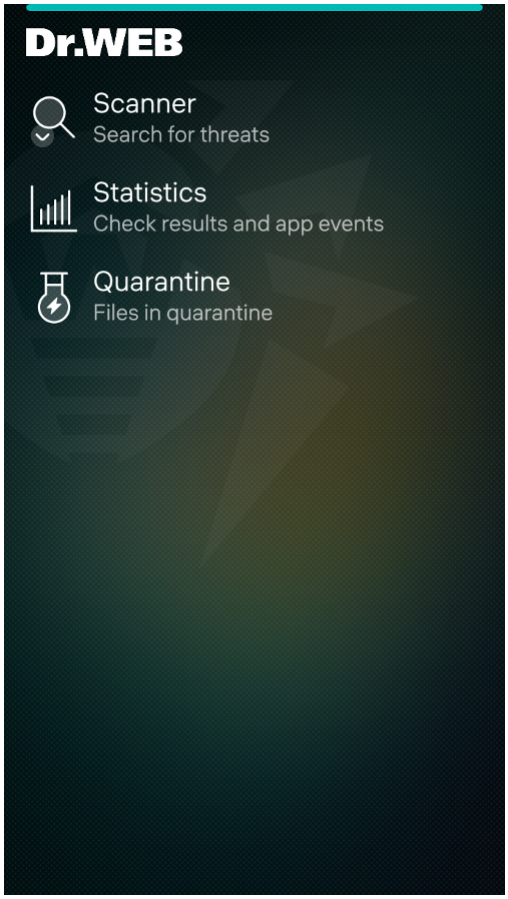

Figure 7. Main page of the application

To access other Dr.Web features and settings, with a fast motion pull the main page down or pull the page down from the middle without lifting your finger.

In the pulley menu (see Figure 8), you can:

- Update virus databases.
- Open application settings.
- View license details.
- View information about the application and open the online help.

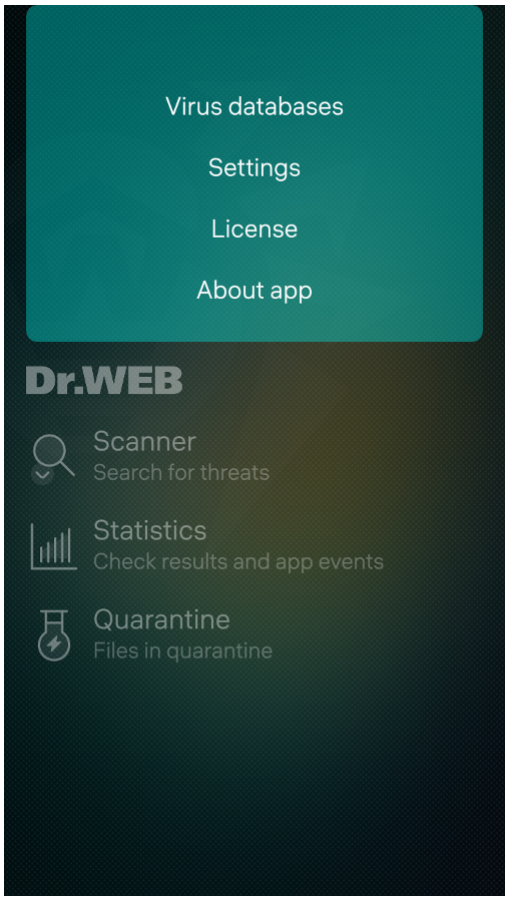

Figure 8. Application menu

6. Accounts

Some Dr.Web Mobile Security Suite features are available depending on the account type: administrator or user.

Unlike an administrator, a user cannot:

- view statistics;
- choose actions for threats quarantined under another account.

Both administrators and users can detect and neutralize threats only in the system areas they have read and modify permissions for.

7. Interaction with Aurora Center

Aurora Center application software (AS) is designed for centralized management of mobile devices running Aurora and Android OS. The Aurora Center subsystems help manage user accounts, distribute policies and scenarios to user devices, maintain and manage app collections, monitor audit events, and perform other administrative functions. Aurora Center AS runs on a server. The Aurora Center subsystems are accessed via a web interface.

To manage a mobile device by means of the Aurora Center AS, the device needs to be activated via the Aurora Center mobile application.

Aurora Center AS and its subsystems allow for the following forms of interaction with the Dr.Web application:

- publication of the app in the Market subsystem as well as in app collections;
- distribution of the app installation policy to a mobile device;
- monitoring of audit events of the app installed on a device.

The Market subsystem of the Aurora Center AS can be used to upload mobile apps to the subsystem for their subsequent publication in app collections (dashboards) available for specified user groups. The Dr.Web app needs to be uploaded to a collection for the app to be available for installation on user devices (by means of policy distribution or from the Aurora Market mobile app). The Dr.Web app can be uploaded to the Market subsystem and then added to existing or newly created collections.

The security subsystem of the Aurora Center AS can monitor the following Dr.Web audit events:

- application started,
- application stopped,
- anti-virus service started,
- scan started,
- scan stopped,
- update finished,
- threat detected.

By default, the information about Dr.Web events is sent to the server once an hour. The frequency can be adjusted in the Aurora Center AS settings.

8. Licensing

You need a license to use Dr.Web. License allows you to use all features of the application during validity period. It regulates 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.

8.1. License Page

On the **License** page (see Figure 9) you can purchase or activate a paid license and get a trial period.

To open the page, do one of the following:

> License activation screen displays right after you open the application, provided you do not have an activated demo license.

- With a fast motion, pull the main page down. In the pulley menu, tap **License**.
- Pull the page down starting from the middle without lifting your finger. Release when **License** is highlighted.

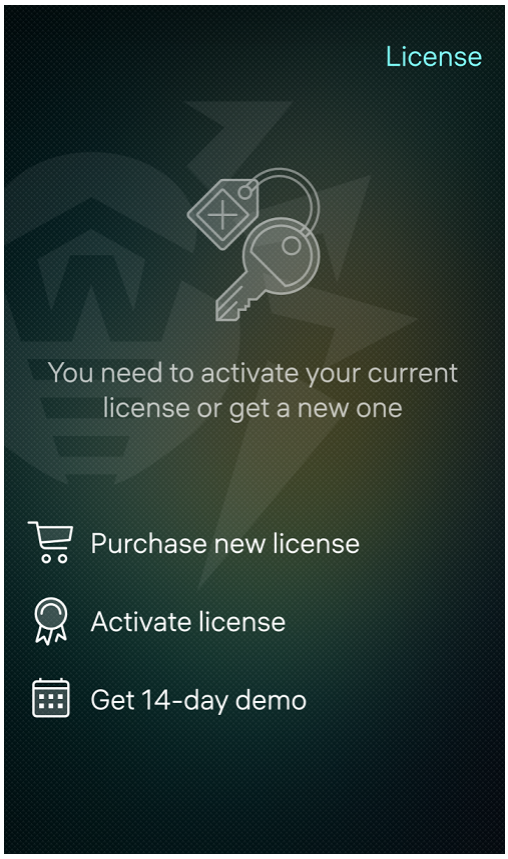

Figure 9. License page

When you have an active license, on the **License** page (see Figure 10), you can view license info: serial number, license activation and expiration dates, and days left until expiration.

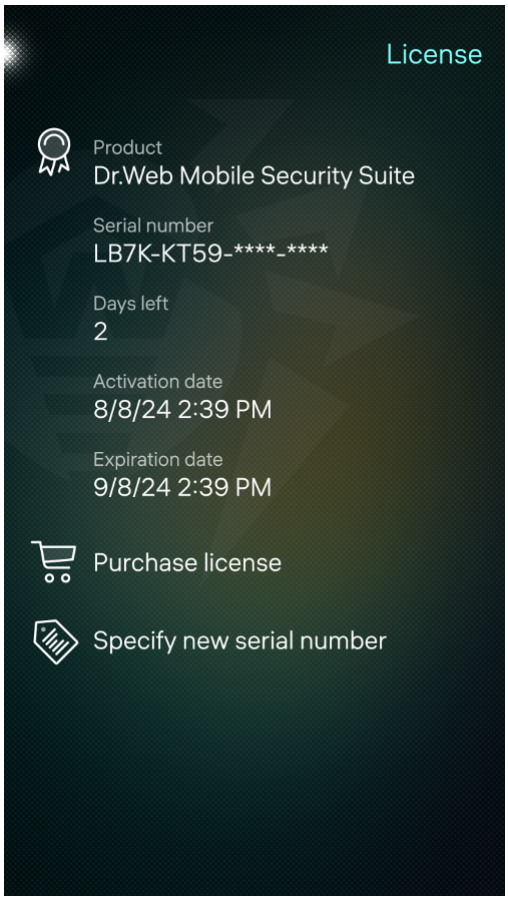

Figure 10. License info

If your license expires soon, you can purchase a new one and use it without reinstalling the app. To do so, touch **Purchase license** and follow the instructions from the Purchasing License and License Activation sections.

8.2. Trial Period

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

To activate a trial period

1. With a fast motion, pull the main page down or pull the page down starting from the middle without lifting your finger.
2. In the pulley menu, select **License**.
3. Touch **Get 14-day demo**.
4. State your personal information (see Figure 11):
   - first and last name,
   - valid email address,

- country.

5. Optionally, select the **Receive newsletters to this email** check box.
6. Touch the **Activate** button. Your trial period will be activated.

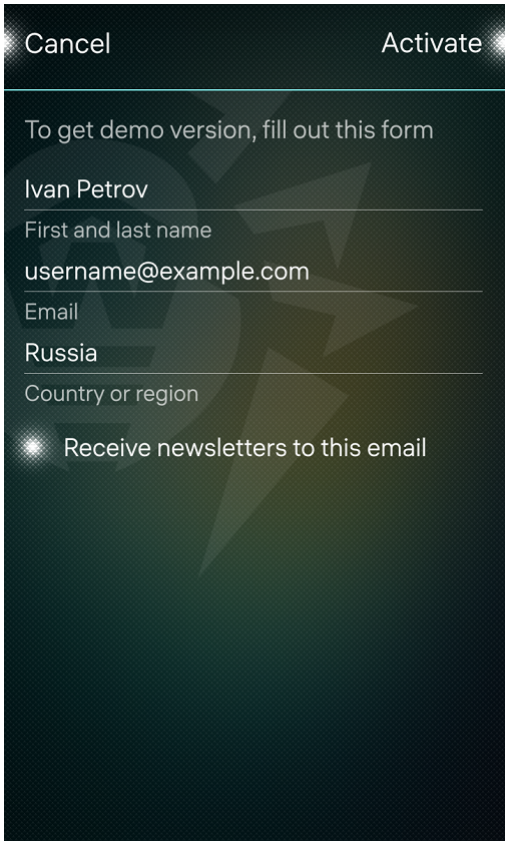

Figure 11. Getting trial period

8.3. Purchasing License

Purchase is available only in the Russian Federation.

To purchase a license

1. With a fast motion, pull the main page down or pull the page down starting from the middle without lifting your finger. In the pulley menu, select **License**.

   If you have not activated a demo license, a screen offering to purchase a license appears right after you open the application.
2. Tap **Purchase license**. You will be redirected to the license constructor at Doctor Web online store.

   You can also visit it at https://products.drweb.ru/biz/v4/.
3. Specify your company's scope of activity and whether you are transitioning under the migration program.

4. In the **Protection for mobile devices Dr.Web Mobile Security Suite** section select **OS Aurora** and number of protected devices. The minimal number of protected devices is 5. To expand the section, tap "plus".

   

   Free additional component "Control Center" does not allow you to control Aurora devices.

5. Select the license period.

   

   By default, the cart also contains a **Dr.Web Desktop Security Suite** license for 5 PCs protection. If you do not need a license for PC protection, remove it from the cart by tapping “minus” to the left of the specified PC number.

6. Tap **Check out**.
7. Fill out the form and touch **Continue**.

   After you complete your purchase, you will receive your serial number to the email you have provided. Optionally, you can choose to receive your serial number in SMS message if you provide your phone number.

8. Register the received serial number.

8.4. License Activation

After you purchase a license, you need to activate it.

To activate a license

- Register a serial number
  - in the application if your device with the installed application is connected to the internet;
  - on the Doctor Web website if your device with the installed application is not connected to the internet.
- Use a key file.

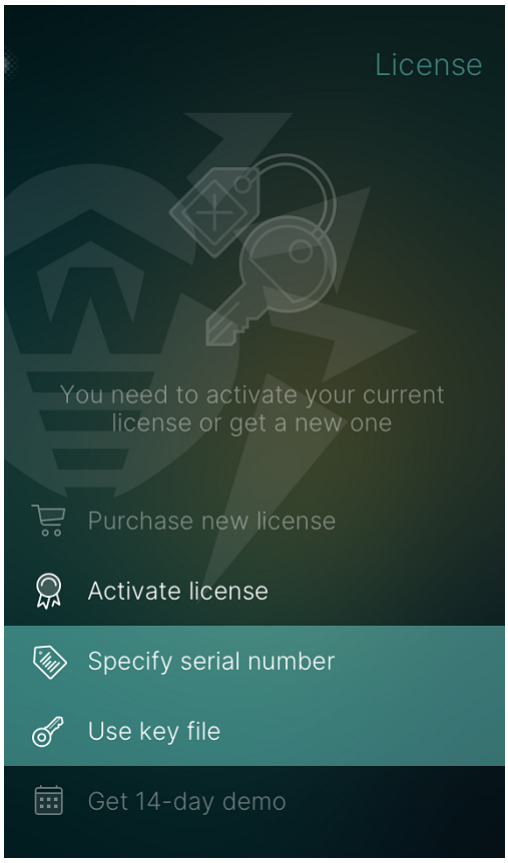

Figure 12. License activation

Registering a serial number in the application

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

1. With a fast motion, pull the main page down or pull the page down starting from the middle without lifting your finger.
2. In the pulley menu, select **License**.

   The license activation screen displays right after you open the application, provided you do not have an activated demo license.

3. If you don't have an active license, select the **Activate license** option and touch **Specify serial number** (see Figure 12). If you have an active license, select **Enter a new serial number**.
4. On the next page, enter your purchased serial number.
5. If you haven't registered the entered serial number before, state your personal information (see Figure 13):
   - first and last name,
   - valid email address,

- country.

6. Optionally, select the **Receive newsletters to this email** check box.
7. Touch the **Activate** button.

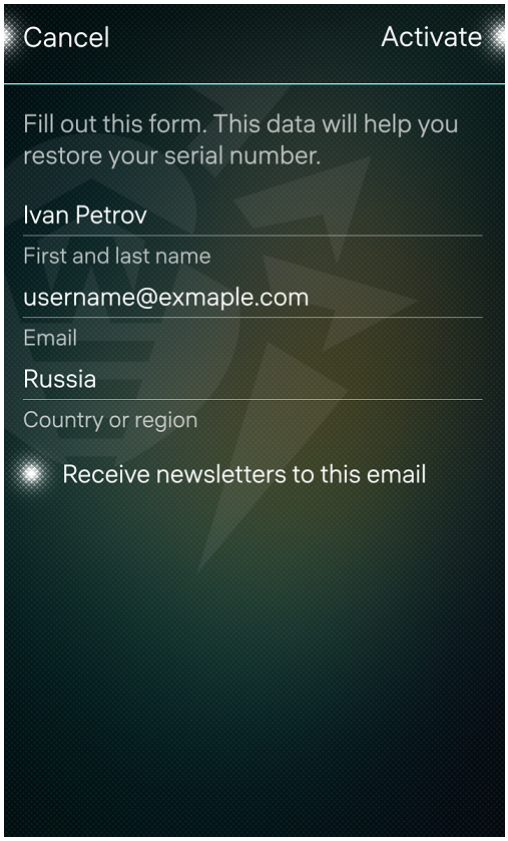

Figure 13. License registration

You will be redirected to the page containing information about the license owner. At the top of the screen, a notification about a successful license activation appears.

Registering a serial number on the website

If your device with the installed application is not connected to the internet, you can use another device connected to the internet to register your serial number. In this case, you will receive a license key file that you will need to copy to the device which you intend to use for license activation.

To register a serial number on the website

1. Go to https://products.drweb.com/register/.
2. Enter the serial number that you received after you purchased Dr.Web.
3. Specify the license owner's registration data.
4. The license key file will be sent as a ZIP archive to the email address you have provided.

License key file

The license key file contains user rights for Dr.Web.

The file has the `.key` extension and contains, among others, the following information:

- licensed period for the application;
- list of components the user is allowed to use;
- other limitations.

A valid license key file meets the following requirements:

- license is not expired;
- 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, and the anti-virus stops detecting and neutralizing malicious programs.

The license key file becomes invalid if you edit it. Do not save changes after opening the file in a text editor to prevent your license from being compromised.

Using a license key file

You can activate your license using a key file.

If you have an active license, you cannot use a key file. Wait until your license expires or use a serial number.

To use a license key file

1. Copy the key file to your device.

   You can either copy the entire ZIP archive, or you can unpack the archive and copy only the `.key` file to your device.
2. On the License page, touch the **Activate license** option.
3. Touch the **Use key file** option (see Figure 12).
4. Open the folder which you have copied the key file or the entire ZIP archive to and touch the file.

The key file is ready to use after you install it. You will be redirected to the page containing info about license owner. At the top of the screen, a notification about a successful license activation appears.

8.5. 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.

You have two options for restoring your license:

- register a serial number,
- use a key file.

To restore your demo license

1. On the screen that appears after you launch the application, touch **Get 14-day demo**.
2. State your personal information:
   - first and last name,
   - valid email address,
   - country.
3. Touch the **Activate** button.

Demo license is bound to the device. If you change devices, instead of restoring the demo license, you will get a new one.

9. Dr.Web Components

On the main page of the app, you will find a list of components:

- Scanner scans your device on demand. Three scan types are available: full scan, express scan, and custom scan.
- Statistics logs events related to Dr.Web Scanner operation, virus databases update, and actions applied to detected threats.
- Quarantine allows you to view and process quarantined threats.

9.1. Dr.Web Scanner: Scan at User Request

Dr.Web Scanner checks the system at user request. You can run an express or full scan of the whole file system or scan critical files and folders only.

Both administrators and users can detect and neutralize threats only in the system areas they have read and modify permissions for.

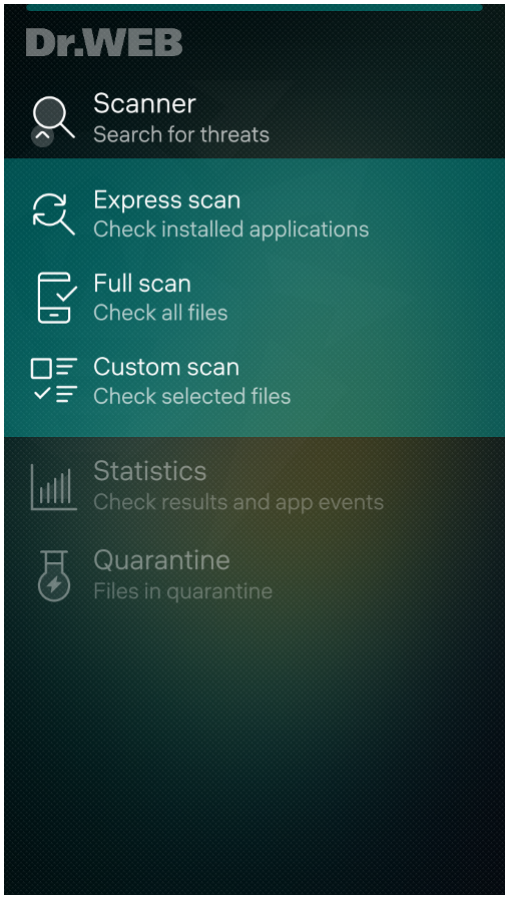

Figure 14. Dr.Web Scanner

Scanning

To scan the system, touch the **Scanner** option on the main page, then on the submenu (see Figure 14) select one of the following actions:

- To only check installed applications, touch the **Express scan** option.
- To scan all files on your device, touch the **Full scan** option.
- To scan only some files or folders, touch the **Custom scan** option. On the next page, select file system objects from the list. To open a folder, touch it. To select a folder, touch and hold it (see Figure 15). To select a file, touch it. After you have selected the objects, touch **Accept**.

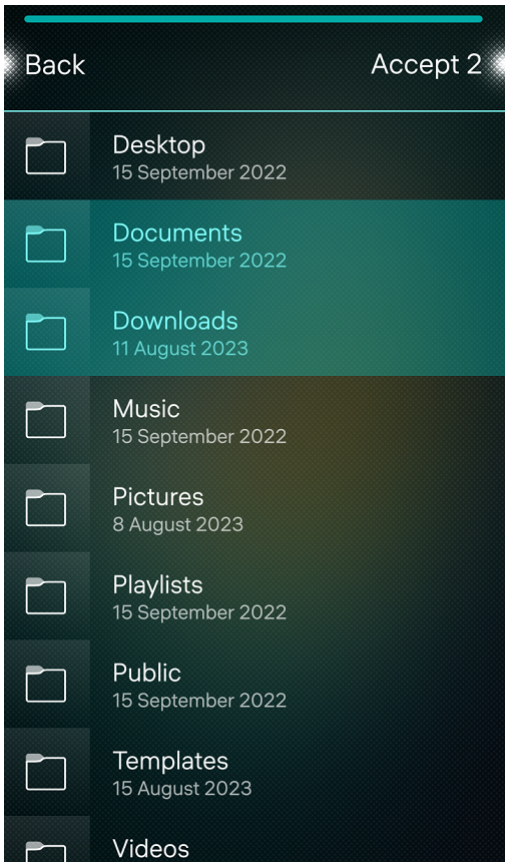

Figure 15. Custom scan

Stop scanning

To stop scanning, touch the dot in the top-left corner.

To cancel scanning stop, tap the remorse pop-up at the top of the application (see Figure 16).

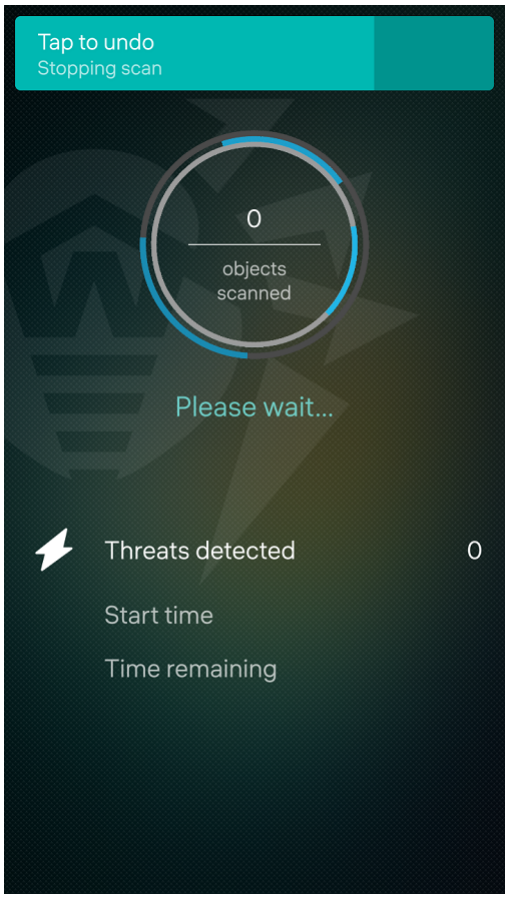

Figure 16. Stop scanning

Dr.Web Scanner settings

You can change Dr.Web Scanner settings (see Scanner Settings).

Statistics

The application registers events related to the operation of Dr.Web Scanner. They appear in the **Events** subsections on the **Statistics** page and depending on the filter settings are sorted by date or in alphabet order (see Statistics).

Scan results

Once a scan is completed, you can view scan results by touching **Tap to neutralize** (see Figure 17) or the dot in the upper-left corner.

If you minimize the app while scanning, touch the cover to return to the **Scan completed** page and proceed to the scan results.

If you fully stop the app operation while scanning, next time you open the app on its main page you will see an alert panel with the number of detected threats. Touch it to go to the scan results. If the scan has not detect any threats, the alert panel does not appear. In this case, to see the scan results, open the page of the previously selected scan option.

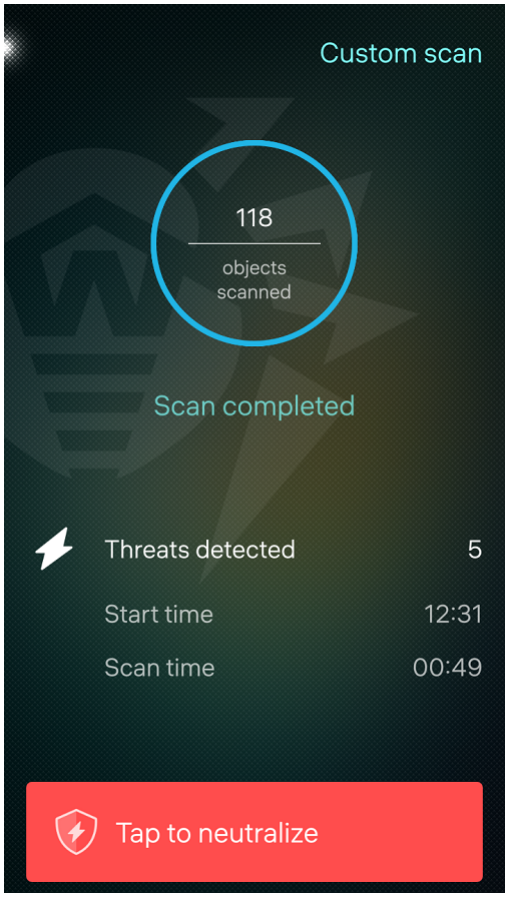

Figure 17. Scan completed

Neutralizing threats

Scan results are available on the **Threats** page, where you can view the list of detected threats and neutralize them.

Neutralizing all threats at once

To delete all threats at once

1. With a fast motion, pull the **Threats** page down or pull the page down starting from the middle without lifting your finger.
2. Select **Delete all** (see Figure 18).

To quarantine all threats at once

1. With a fast motion, pull the **Threats** page down or pull the page down starting from the middle without lifting your finger.
2. Select **Move all to quarantine** (see Figure 18).

> System threats cannot be deleted or quarantined since it can affect functionality of your device.

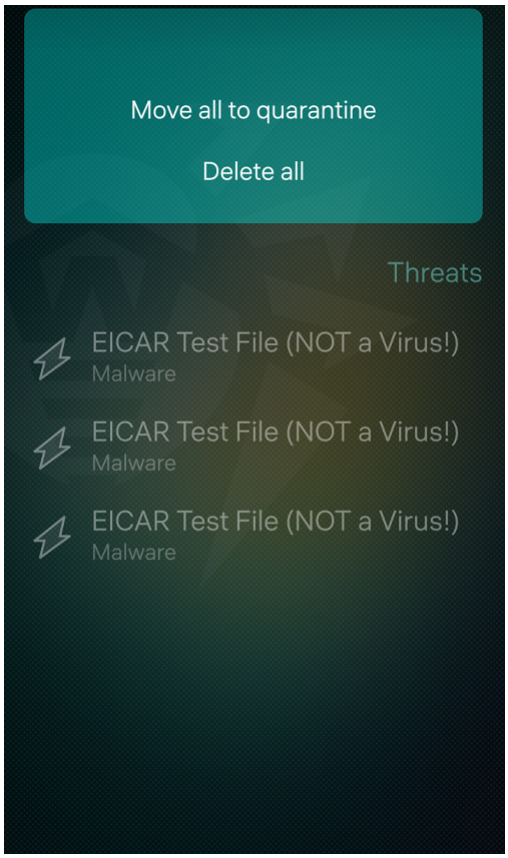

Figure 18. Neutralizing threats

Neutralizing one threat at a time

To view the available actions for each threat, touch the name of a threat on the list. Select one of the actions:

- **Move to quarantine** to move the threat to an isolated folder (see Quarantine).
- **Delete** to erase the threat from the device memory. If the threat is detected in an installed application, deletion is not possible. Thus, the **Delete** action is not on the list.
- **Ignore** to temporarily leave the threat as it is.
- **Learn more** to view a description of the detected threat on the Doctor Web website.

9.2. Statistics

Dr.Web logs termination or completion of all types of scans, virus database updates, and actions applied to detected threats.

To view statistics, touch **Statistics** on the main page of the app.

> Only the **Save log** option is available for users. To view statistics, you must have administrator privileges (see Accounts).

Viewing statistics

The **Statistics** page contains two information sections (see Figure 19):

- **Total** contains information on the total number of scanned files, detected threats, and neutralized threats.
- **Events** shows the following information:
  - completion or termination of full, express, and custom scans;
  - virus database updates or update failures;
  - actions applied to detected threats—deletion, moving to quarantine, ignoring.

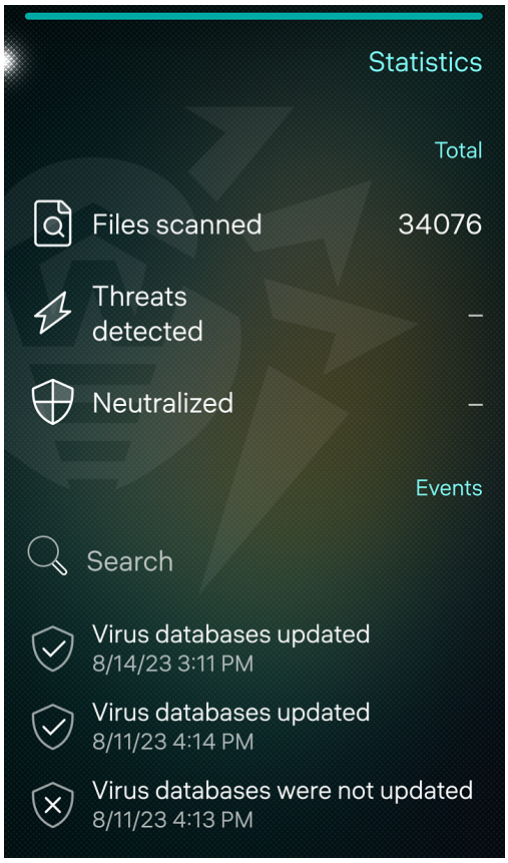

Figure 19. Statistics

Viewing information on events

By touching the name of an event, you can see the following information about the event:

- type of event,
- date and time of event,
- who initiated event.

Depending on the type of the event, additional information may be available, such as:

- number of detected threats,
- event status,
- number of scanned files,
- threat type,
- threat name,
- file name,
- path to file.

Searching through events

You can search through events in Statistics:

- by event name,
- by event date,
- by event time,
- by threat name,
- by file name.

To search events, enter your search query to the **Search** bar on the **Events** subsection (see Figure 19).

Sorting events

You can sort Statistics events by date or A to Z.

To sort events by date or A to Z

1. With a fast motion, pull the **Statistics** page down or pull the page down starting from the middle without lifting your finger.
2. In the pulley menu, select **Filter events** (see Figure 20).
3. On the next page, in the **Sort by** section select how you want the events to be sorted.

You can also view only particular events by touching any event type in the **Filter events** in the **Show** section of the menu.

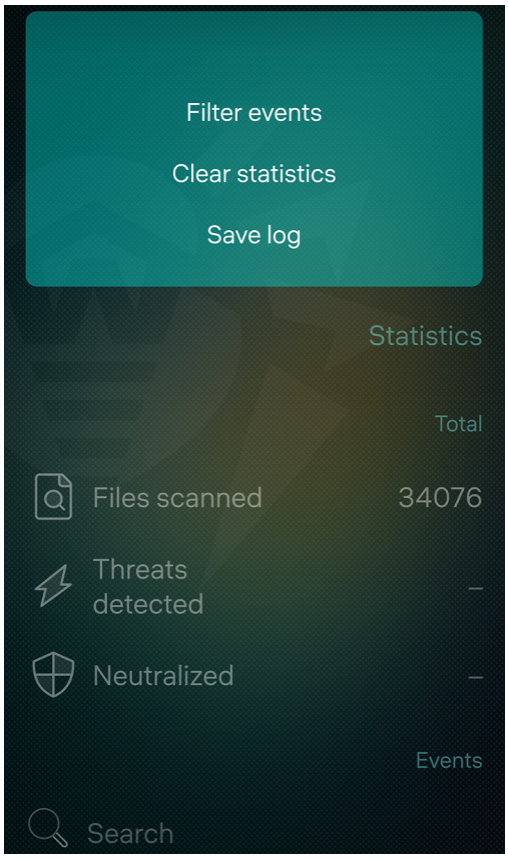

Figure 20. Statistics menu

Clearing statistics

To clear all the statistics, pull the **Statistics** page down with a fast motion or pull the page down starting from the middle without lifting your finger and select **Clear statistics** (see Figure 20).

Saving event log

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

1. With a fast motion, pull the **Statistics** page down or pull the page down starting from the middle without lifting your finger.
2. Select **Save log**.
3. The log is saved in the `DrWeb_Log.txt` file located in the internal memory of your device in the `/home/<user>/Documents/drweb/` folder where *<user>* stands for the current user.

9.3. Quarantine

You can move detected threats to the quarantine folder, where they are isolated and cannot damage the system (see Figure 21).

Total size of all quarantined files displays at the top-right corner of the **Quarantine** page.

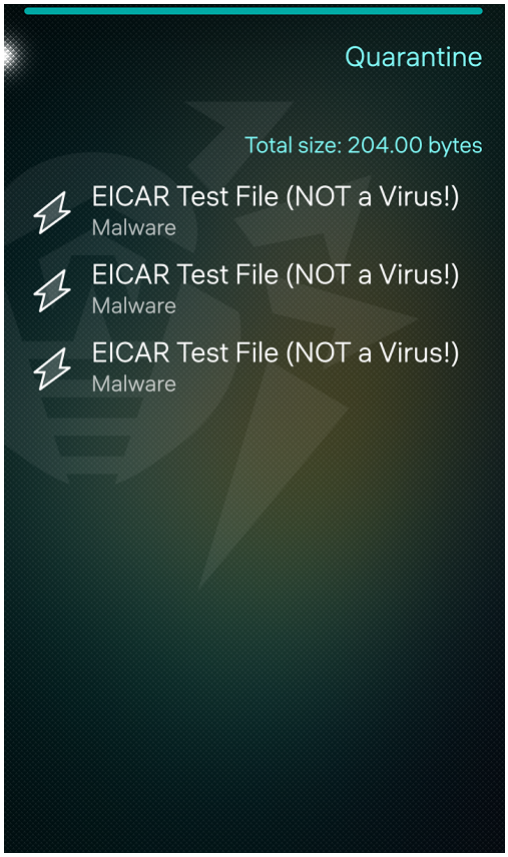

Figure 21. Quarantine

Viewing quarantined files

To view the list of threats moved to quarantine, touch **Quarantine** on the main page.

A list of all threats in quarantine will open.

Viewing information on quarantined threats

If you touch the name of a threat on the list, the following information will display:

- file name,
- threat type,
- path to the file,

- date and time the threat was quarantined.

Available options

To view the available options, touch and hold a threat on the list.

The following options are available for threats (see Figure 22):

- **Restore** to move the file back to the folder where it was quarantined from. Use this action only if you are sure the file is safe.
- **Delete** to delete the file from quarantine and the device system.
- **Learn more** to view the threat description on the Doctor Web website.

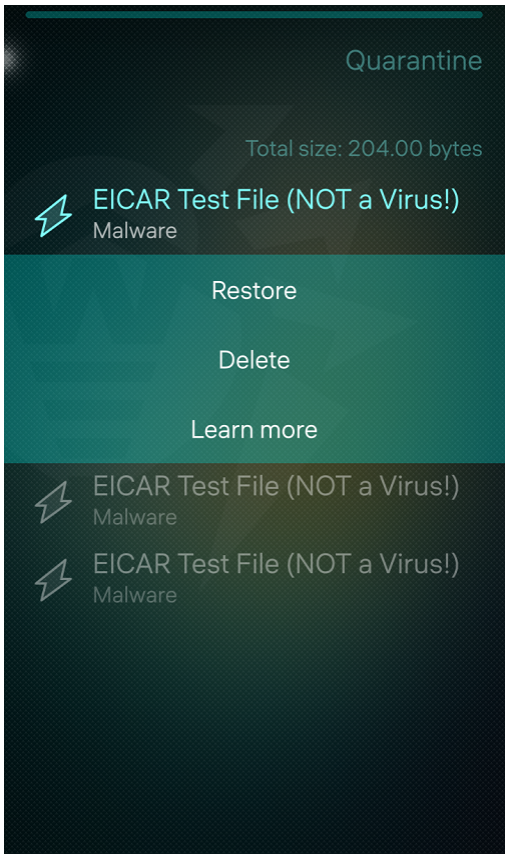

Figure 22. Actions for threat

Deleting all objects from quarantine

To remove all quarantined objects at once

1. With a fast motion, pull the **Quarantine** page down or pull the page down starting from the middle without lifting your finger.
2. Select **Delete all** (see Figure 23).
3. Confirm the action.

To cancel, tap the remorse pop-up at the top of the application.

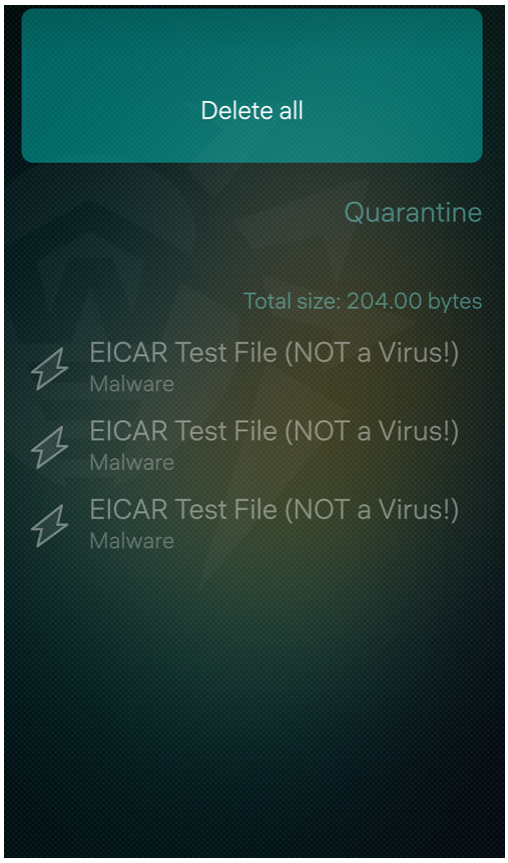

Figure 23. Deleting all threats from quarantine

10. Settings

To go to app settings, with a fast motion, pull the main page down or pull the page down starting from the middle without lifting your finger and select the **Settings** option (see Figure 24).

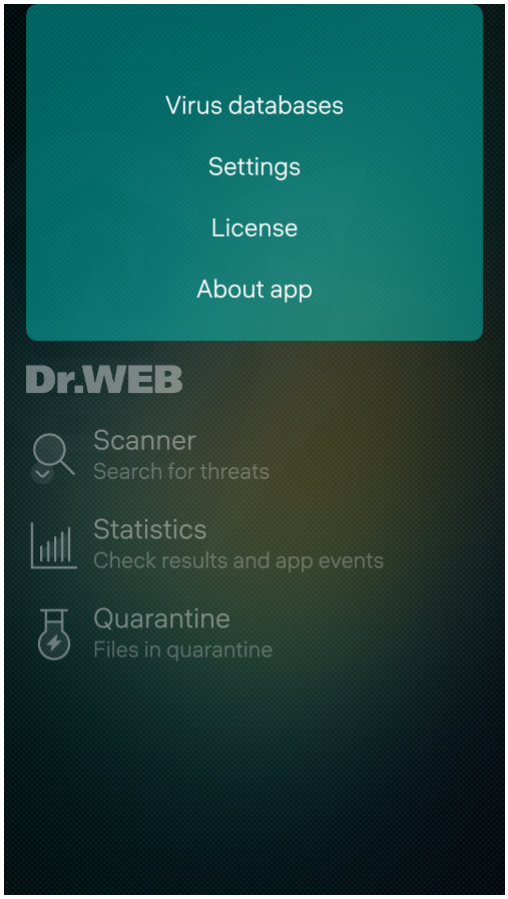

Figure 24. Settings

On the **Settings** page, the following sections are available:

- **General settings**. Allows to configure sounds alerts.
- **Scanner**. Allows you to configure Dr.Web Scanner, which scans your device on your request (see the Scanner Settings section).
- **Virus databases**. Allows you to manage automatic database updates as well as updating over mobile networks (see the Update Settings section).

10.1. General Settings

In the **General settings** section you can configure sound alerts about threat detection, deletion, or moving to quarantine (—option is disabled, —option is enabled).

By default, sound alerts are enabled.

10.2. Scanner Settings

The **Scanner** section allows you to specify Dr.Web Scanner scan parameters.

- To enable scanning of files in archives, in the **Scanner** section, touch the **Files in archives** field ( —option is disabled,  —option is enabled). Archive scanning is enabled by default.
- To enable/disable detection of adware and riskware (including hacktools, joke programs, dialers and exploitable software), touch the **Adware** and **Riskware** fields respectively ( —option is disabled,  —option is enabled). Both options are enabled by default.

10.3. Update Settings

In the **Virus databases** section, you can either allow or prohibit virus database updates over mobile networks, as well as specify auto-update parameters.

To enable or disable the use of mobile networks for downloading updates

- In the **Virus databases** section, touch the **Update over Wi-Fi only** field ( —option is disabled,  —option is enabled). The option is enabled by default.

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

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

To enable or disable automatic updating of virus databases

- In the **Virus databases** section, touch the **Auto-update** field ( —option is disabled,  —option is enabled). The option is enabled by default.

You can also change the following update settings:

- To change the frequency of virus database status checks and updates, touch the **Update interval** field and select one of the available options in the drop-down list: **30 minutes**, **1 hour**, **4 hours**, **8 hours**, or **1 day**. The databases are checked and automatically updated every 4 hours by default.
- To change the protocol used for connecting to the update server, touch the **Connection** field select one of the connection types in the drop-down list: **Secure (HTTPS)** or **Non-secure**

(HTTP). Virus databases will be updated over the selected protocol only. Updates will use the HTTPS protocol by default.

If you receive custom updates via the **Dr.Web Custom Updates** package, the protocol used for connecting to the update server that you choose in the app settings should match the one specified in **Dr.Web Custom Updates**.

10.4. Reset Settings

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

To reset settings

1. With a fast motion, pull the **Settings** page down or pull the page down starting from the middle without lifting your finger.
2. Touch the **Reset settings** option (see Figure 25).
3. Confirm restoring the default settings.

To cancel resetting settings, touch the remorse pop-up at the top of the application.

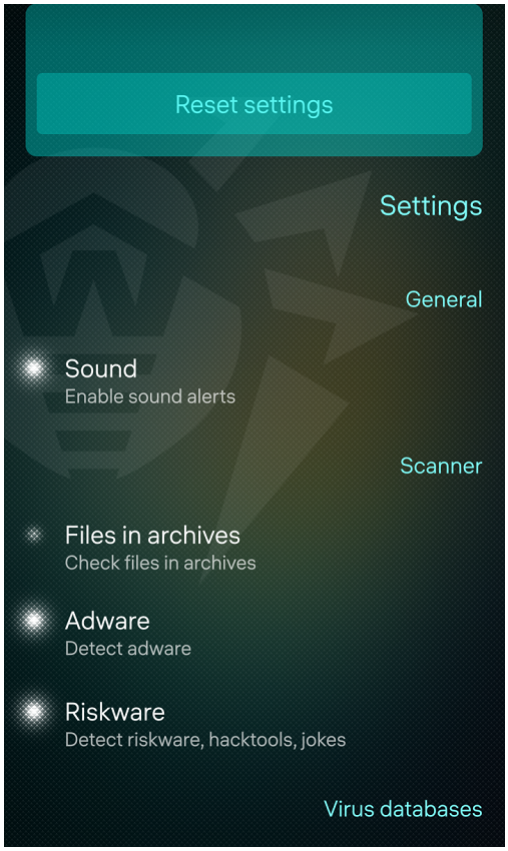

Figure 25. Resetting settings

11. Virus Database Update

Dr.Web uses special virus databases to detect threats. These databases contain details and signatures of all viruses and malicious programs for devices running on Android and Aurora OS that are known by Doctor Web experts. The virus databases need to be regularly updated as new malicious programs appear all the time. The application features an option for updating the virus databases over the internet.

You can use your own update mirror instead of the Dr.Web Global Update System servers. This option is provided by the additional **Dr.Web Custom Updates** package. For more information on this package, contact your Doctor Web company manager.

Update

The virus databases are updated automatically by default. You can disable auto-updates or change their frequency and the type of the connection established with the update server in the Update Settings section of the app settings.

If auto-updates are disabled, the application performs a virus database status check at a rate selected in the settings. By default, a check is performed every 4 hours.

If the virus databases are out of date, a corresponding alert appears at the bottom of the screen in the app. The alert is displayed until the virus databases are updated. Touch the alert to update the virus databases manually. You can also start an update from the **Virus databases** section of the pulley menu.

It is recommended to update the virus databases as soon as you install the application. This will allow Dr.Web to use up-to-date information about known threats. As soon as the experts of the Doctor Web anti-virus laboratory discover new threats, an update for virus signatures, behavior characteristics, and attributes is issued. In some cases, updates can be issued several times per hour.

To start an update

1. With a fast motion, pull the main page down or pull the page down starting from the middle without lifting your finger.
2. In the pulley menu, select **Virus databases**.
3. The next page displays the virus database update status and when the virus databases were last updated. If the databases are not up to date, the status will notify you about it.
4. With a fast motion, pull the **Virus databases** page down or pull the page down starting from the middle without lifting your finger.
5. Select **Check for updates** (see Figure 26).

An update will start automatically.

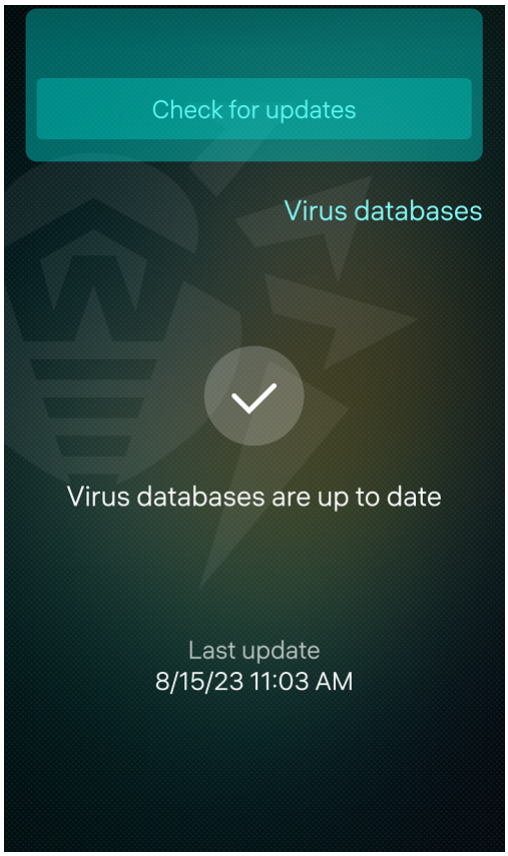

Figure 26. Virus database update

12. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

1. Download and review the latest manuals and guides at https://download.drweb.com/doc/.
2. See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
3. Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

1. Fill out a web form in the appropriate section at https://support.drweb.com/.
2. Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.

Appendix A. Troubleshooting

When a system failure interfering with anti-virus operation occurs, Dr.Web will try to fix the error by itself. If you open the application, you will see the troubleshooting screen (see Figure 27).

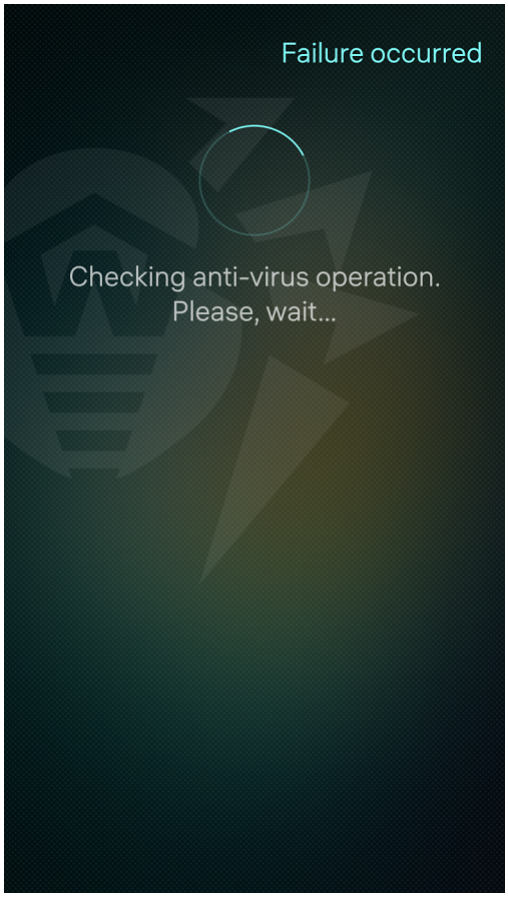

Figure 27. Troubleshooting screen

If Dr.Web manages to correct the failure, you will receive a notification that the application has been restarted and will be able to continue using it.

If the failure is not corrected, you will see a corresponding screen (see Figure 28) when you open the application. Contact the device administrator to fix errors.

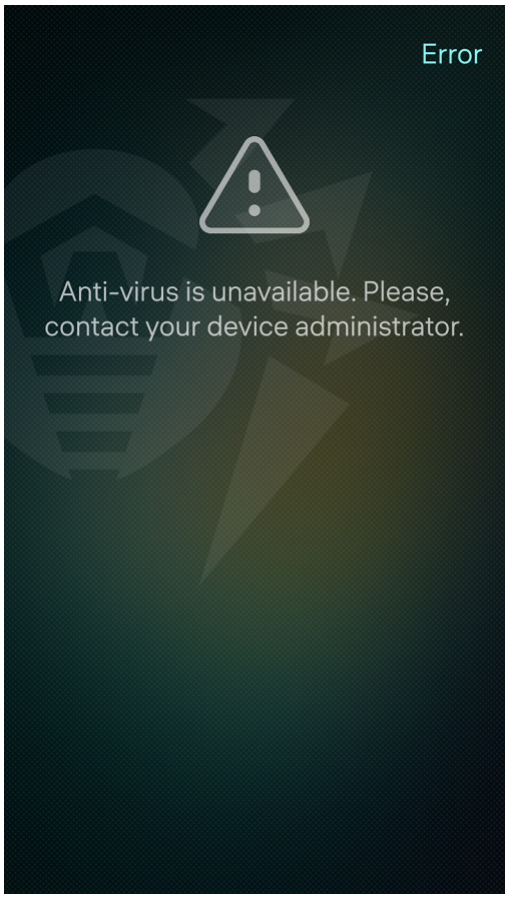

Figure 28. Error message

To correct failures

1. Open the “Terminal” application.
2. Enable root access.
3. Relaunch `av-service` with the command `systemctl restart av-launcher`.
4. If the failure continues to occur, view the Dr.Web background process event log to determine the reason for the failure and remedy it. The log is kept in the `DrWebService_Log.txt` file located in the `/srv/shared/ru.drweb/drweb/log/` folder in the internal memory of your device.
5. If the reason for the failure cannot be identified, reinstall Dr.Web.

   For details on how to install and uninstall the application, refer to sections 3. Installing Dr.Web Mobile Security Suite and 4. Uninstalling Dr.Web Mobile Security Suite.