Dr.WEB

Security Space for Aurora

User manual

This document is for information and reference purposes in relation to the specified software of the Dr.Web family. This document is not a ground for exhaustive conclusions about the presence or absence of any functional and/or technical features in the software of the Dr.Web family and cannot be used to determine whether the software of the Dr.Web family matches any requirements, technical task and/or parameters, and other third-party documents.

Trademarks

Disclaimer

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

Dr.Web Security Space for Aurora
Version 1.0.6
User manual
9/14/2021

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 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

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
⚠	Warning about possible errors or important notes to which you should pay 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.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

2. About Product

Dr.Web Security Space for Aurora (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 Security Space uses the Origins Tracing™ for Android technology that detects malware for Android and 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 version 3.2.2
CPU architecture	ARMv7 or ARMv8
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

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

Manual installation of Dr.Web

To install Dr.Web, you need to do the following:

1. Configure your device.
2. Copy certificate and installation file from PC to your device.
3. Connect to your device by SSH protocol.
4. Install certificate.
5. Install application.

Device configuration

Before you copy and install the certificate and the installation file, allow remote connection and configure USB connection.

To allow remote connection

1. Tap the ⚙ icon on App Grid. Settings menu will display.
2. In the **System** section, select **Developer tools**.
3. On the next screen, tap the **Remote connection** field.
4. Set password.
5. Tap **Save**.

To configure USB connection

1. Tap the ⚙ icon on App Grid. Settings menu will display.
2. In the **Connectivity** section, select **USB**. A screen with USB mode settings will display.
3. Tap **Default USB mode**.
4. In the list, select **Developer mode**.

Copy certificate and installation file

Connect your device to a PC with a USB cable.

To copy the installation file, execute the following command in the command line on your PC:

```
scp -p 22 C:\path\to\file\name.rpm nemo@192.168.2.15:/home/nemo/Downloads
```

where:

- `C:\path\to\file\name.rpm` is the path to the installation file;
- `/home/nemo/Downloads/` is the path where the file will be copied.

On password prompt, enter the password you set while configuring your device.

> ⚠ Changing the path for file copying is not recommended.

On your next step, copy the `DrWebBinaries-cert.der` certificate provided by Doctor Web.

To copy the certificate, execute the following command on your PC:

```
scp -p 22 C:\path\to\file\DrWebBinaries-cert.der
nemo@192.168.2.15:/home/nemo/Downloads
```

where:

- `C:\path\to\file\DrWebBinaries-cert.der` is the path to the certificate.
- `/home/nemo/Downloads/` is the path where the certificate will be copied.

Connecting to device

On your next step, connect to the device by SSH protocol.

To connect to the device, execute the following command in a new command line window on your PC:

```
ssh -p 22 nemo@192.168.2.15
```

On password prompt, enter the password you set while configuring your device.

Installing certificate

You can install the certificate only if you have root access.

> ⚠ Execute all of the following commands in the same window you opened to configure the device.

To get root access, execute the following command:

```
devel-su
```

On password prompt, enter the password you set while configuring your device.

Before installing, move the certificate to the `ima` folder located in `/etc/keys`.

To make sure you have the folder on your device, execute the following command:

```
ls /etc/keys/ima
```

If the response is

```
ls: cannot access /etc/keys/ima: No such file or directory
```

, that means that there is no such folder on the device and you need to create it.

To create the folder, execute the following commands:

```
mkdir /etc/keys

mkdir /etc/keys/ima
```

On your next step, move the certificate to the created folder. To do so, execute this command:

```
cp /home/nemo/Downloads/DrWebBinaries-cert.der /etc/keys/ima
```

Restart the device after installing the certificate so that the application opens and works properly.

Installing application

You can install the application only if you have root access.

If you did not get root access while installing the certificate, execute the following command:

```
devel-su
```

On password prompt, enter the password you set while configuring your device.

On you next step, go to the folder where you have copied the installation file by executing this command:

```
cd /home/nemo/Downloads/
```

To install the app, execute the following command:

```
rpm -ivh name.rpm
```

where: `name.rpm` is the name of the installation file.

After you finish the installation, Dr.Web will appear in the list of applications on Home screen.

Installation of Dr.Web through Aurora Center

Dr.Web can be installed by the administrator of the Management Platform through the Aurora Center application.

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 installed automatically.

Once the installation process is completed, information on the result of the operation will be displayed in Aurora Center. If the app was installed successfully, Dr.Web will appear on the list of applications.

> ⚠ After successful installation by either method you need to restart the device so that the application opens and works properly.

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

4. Uninstalling Dr.Web

Before removing the application, you need to configure your device, connect to your device by SSH protocol, and get root access.

Configuring device

Before removing Dr.Web, allow remote connection and configure USB connection.

To allow remote connection

1. Tap the ⚙ icon on App Grid. Settings menu will display.
2. In the **System** section select **Developer tools**.
3. On the next screen, tap the **Remote connection** field.
4. Set password.
5. Tap **Save**.

To configure USB connection

1. Tap the ⚙ icon on App Grid. Settings menu will display.
2. In the **Connectivity** section, select **USB**. Screen with USB mode settings will display.
3. Tap **Default USB mode**.
4. In the list, select **Developer mode**.

Connecting to device

On your next step, connect your device to PC with USB cable and configure SSH connection.

To configure SSH connection, execute the following command on your PC:

```
ssh -p 22 nemo@192.168.2.15
```

On password prompt, provide the password you set while configuring your device.

You can remove Dr.Web only if you have root access. To get root access, execute the following command:

```
devel-su
```

On password prompt, provide the password you set while configuring your device.

Uninstalling the application

To uninstall Dr.Web, execute the following command:

```
rpm -e name
```

where `name` is the name of the application.

> ⚠ Do not specify the .rpm extension for the application name.

5. Interface

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

- gestures,
- subpages,
- pulley menu,
- menu of available actions,
- remorse pop-up,
- app cover.

Gestures

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

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

Subpages

In Dr.Web, settings are grouped into subpages. The dot at the top left corner (see Figure 1) indicates that you are on a subpage. To go back to previous page, tap the dot.

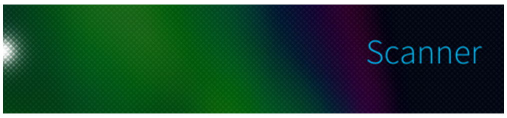


Figure 1. Back button

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

Pulley menu

Pulley menu opens the menu of Dr.Web. It also allows to perform actions with the page you are currently on.

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

You can open pulley menu by doing the following:

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

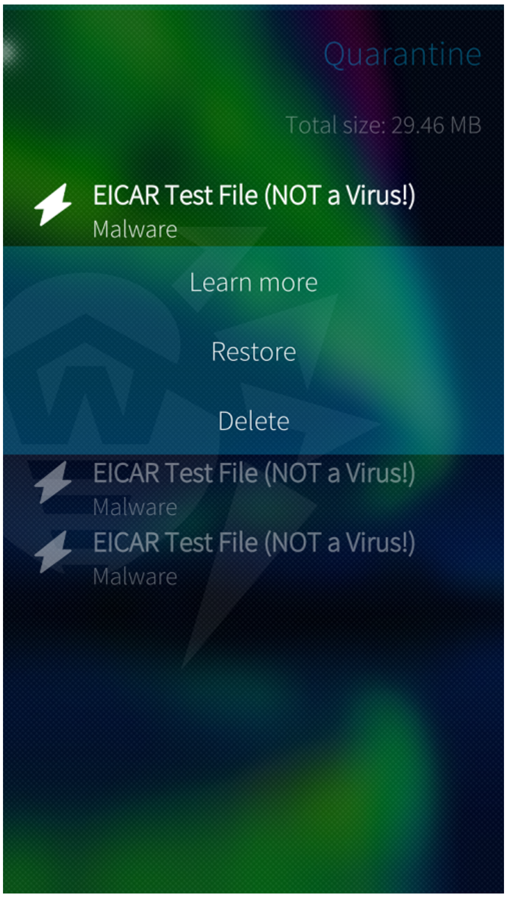
To select a necessary option from pulley menu, use one of the motions:

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

Menu of available actions

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

To open menu of available actions, long-press the necessary page element.



Quarantine

Total size: 29.46 MB

EICAR Test File (NOT a Virus!)
Malware

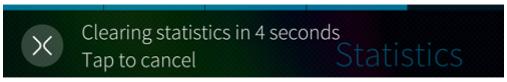
EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

Figure 2. Menu of available actions

Remorse pop-up

Remorse pop-up (see Figure 3) appears at the top of page after an action is performed (for example, after clearing statistics). To cancel action, tap remorse pop-up.



Clearing statistics in 4 seconds
Tap to cancel

Figure 3. Remorse pop-up

Application cover and stopping Dr.Web

If you close Dr.Web by swiping from the left or right edge, application cover displays on Home page (see Figure 4). Tap the cover to open the app.

If you close the app while scanning, app cover on Home page displays scan progress.

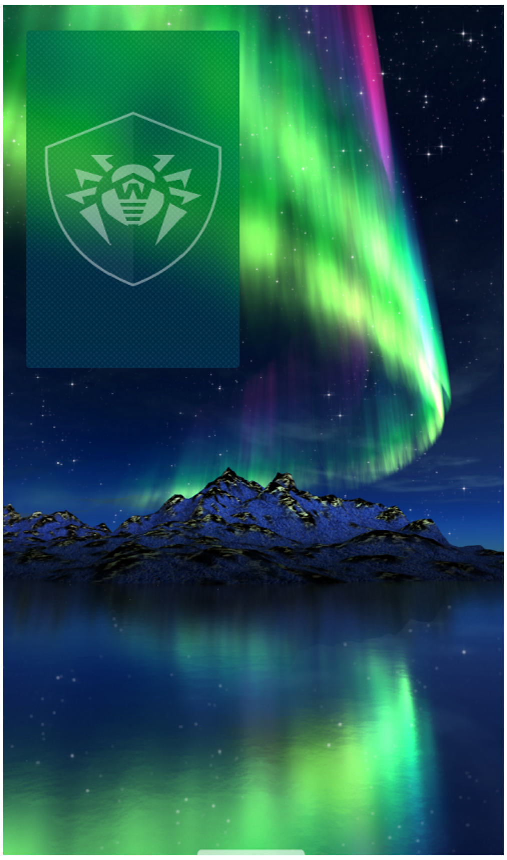


Figure 4. Application cover

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

- In the open app, tap 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 Home page of your device, long-press Dr.Web cover until the icon ⊗ appears.
  3. Tap the icon.

Main page

The main page (see Figure 5) contains the list of Dr.Web main components.

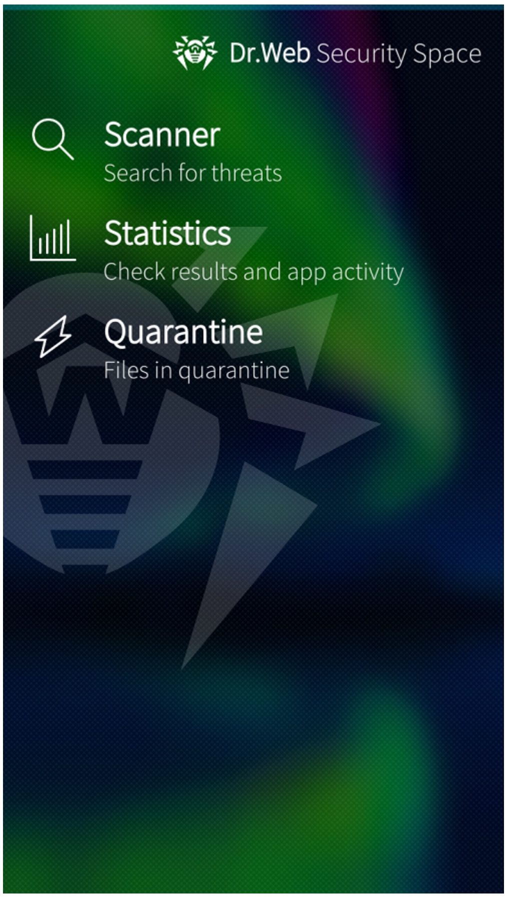


Figure 5. Main page of the application

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

In the pulley menu, (see Figure 6) you can

- update virus databases,
- open application settings,
- view license details,
- open online help,
- view information about the application.

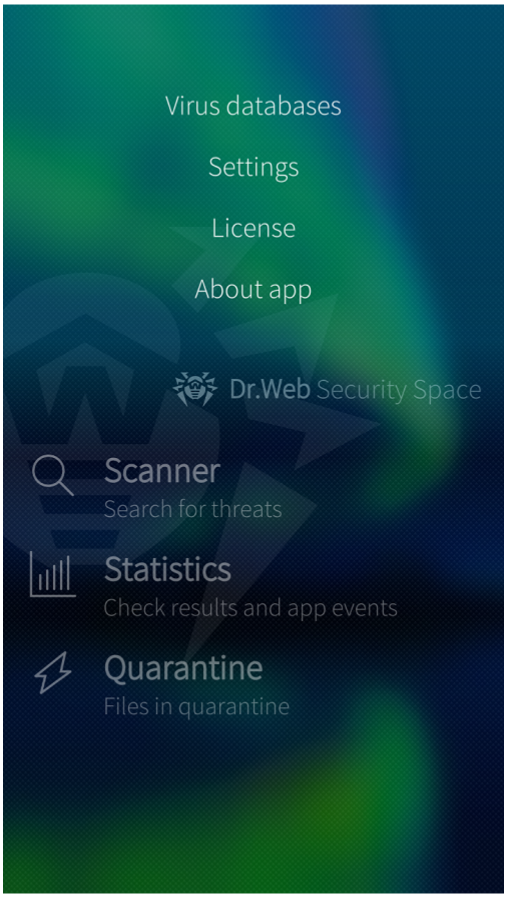


Figure 6. Application menu

6. Accounts

Type of your account defines whether you have or do not have access to some Dr.Web Security Space for Aurora features. Admin can use all features. User is unable to

- view statistics,
- neutralize threats in files added by admin.

7. 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.

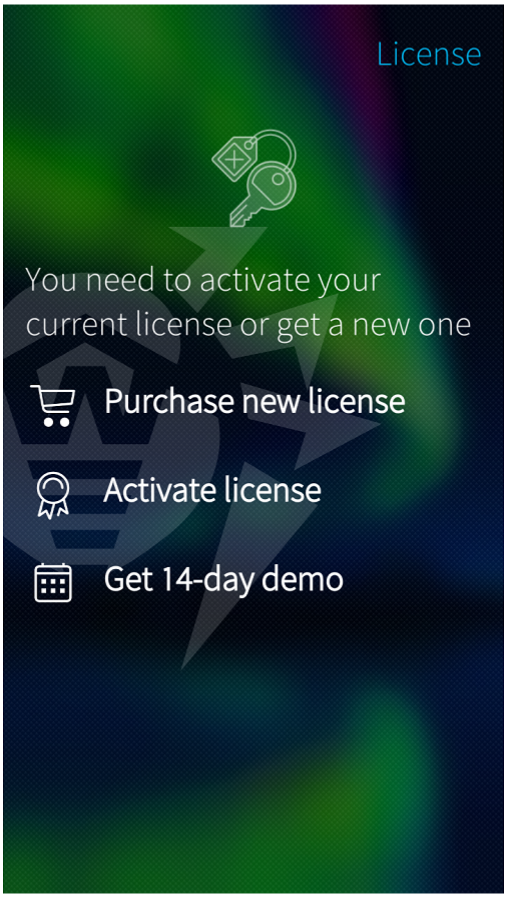
7.1. License Page

On the **License** page (see Figure 7) 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 without lifting your finger. Release when **License** is highlighted.



License

You need to activate your current license or get a new one

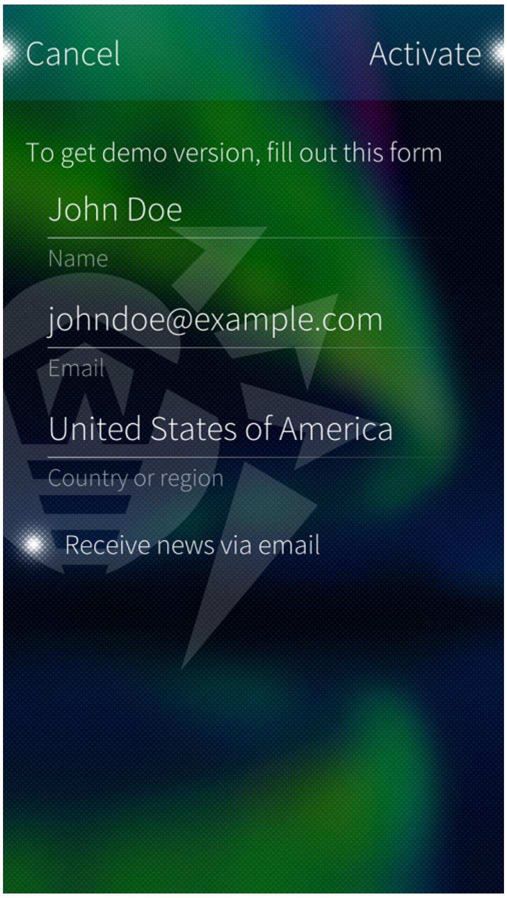
Figure 7. License page

7.2. 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 without lifting your finger.
2. In the pulley menu, select **License**.
3. Tap **Get 14-day demo**.
4. State your personal information (see Figure 8):
   - first and last name,
   - valid email address,
   - country.
5. Optionally, tap the **Receive newsletters to this email** field.
6. Tap **Activate**. Your trial period will be activated.



To get demo version, fill out this form

John Doe
Name

johndoe@example.com
Email

United States of America
Country or region

Receive news via email

Figure 8. Getting trial period

7.3. Purchasing License

To purchase a license

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

   > ⚠ Screen offering to purchase a license appears right after you open the application if you have not activated a demo license.

3. Tap **Purchase license**. You will be redirected to Doctor Web online store.

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

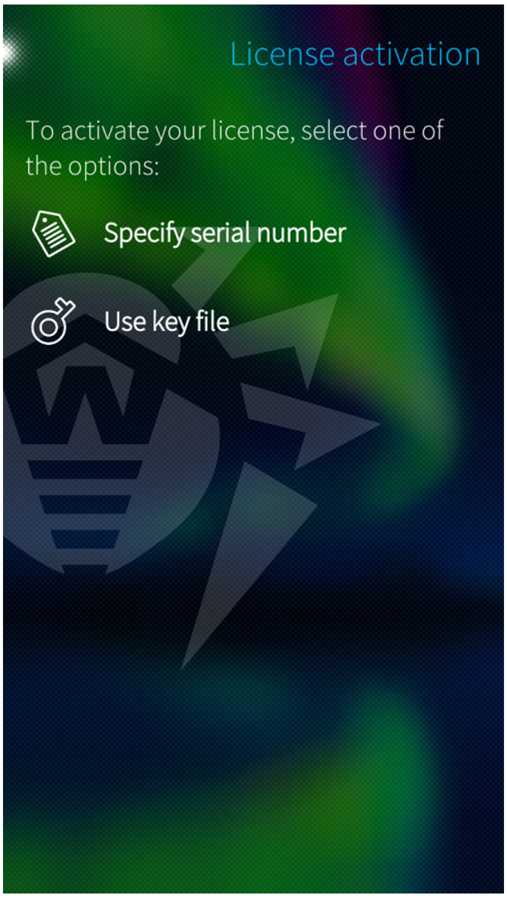
   After you complete your purchase, you will receive your serial number to the email you have provided. Optionally, you can choose to receive your serial number in SMS message if you provide your phone number.
7. Register the received serial number.

7.4. 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.



License activation

To activate your license, select one of the options:

Figure 9. License activation

Registering a serial number in the application

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

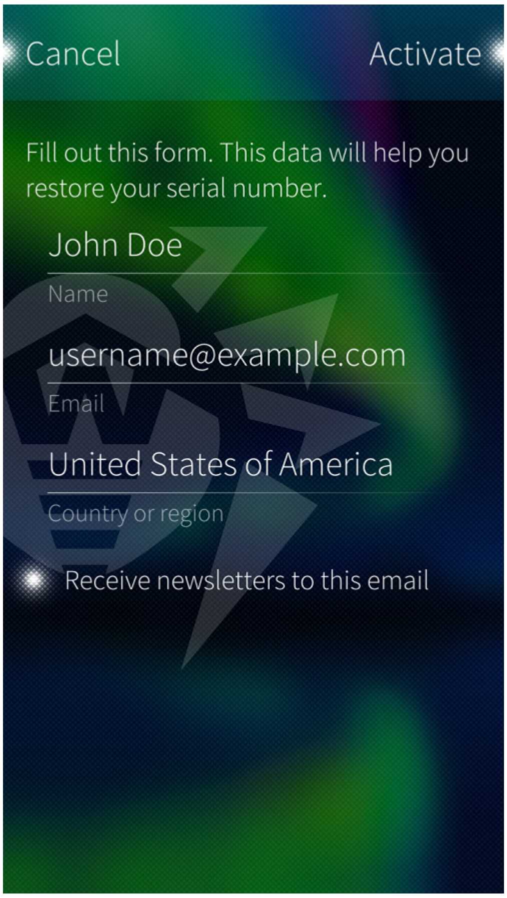
1. With a fast motion, pull the main page down or pull the page down without lifting your finger.
2. In the pulley menu, select **License**.

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

3. Tap the **Activate license** option.
4. On the next page (see Figure 9), tap **Specify serial number**.
5. On the next page, enter your purchased serial number.
6. If you haven't registered the entered serial number before, state your personal information (see Figure 10):
   - first and last name,
   - valid email address,

- country.

7. Optionally, tap the **Receive newsletters to this email** field.
8. Tap the **Activate** button.



Fill out this form. This data will help you restore your serial number.

John Doe
Name

username@example.com
Email

United States of America
Country or region

Receive newsletters to this email

Figure 10. License registration

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.

Registering a serial number on the website

If your device with the installed application is not connected to the internet, you can use other device connected to the internet. 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 a serial number that you received after you purchased Dr.Web.
3. Specify 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

License key file contains user rights for Dr.Web.

The file has the `.key` extension and contains, among other, 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, license key file becomes invalid, the anti-virus stops detecting and neutralizing malicious programs.

⚠ 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 compromise.

Using a license key file

You can activate your license using a key file.

To use a license key file

1. Copy 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, tap the **Activate license** field.
3. On the next page, tap the **Specify key file** option (see Figure 9).
4. Open the folder, where you have copied the key file or the entire ZIP archive to, and tap it.

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.

7.5. 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 other device.

You have two options to restore your license:

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

Restoring demo license

1. With a fast motion, pull the main page down or pull the page down without lifting your finger.
2. In the pulley menu, select **License**.
3. On the next step, tap the **Get 14-day demo** field.
4. Enter the email address, you have used previously to activate your demo license, and your personal information.
5. Tap the **Activate** button.

7.6. Extending License

To extend your Dr.Web license, you do not need to reinstall or stop the application.

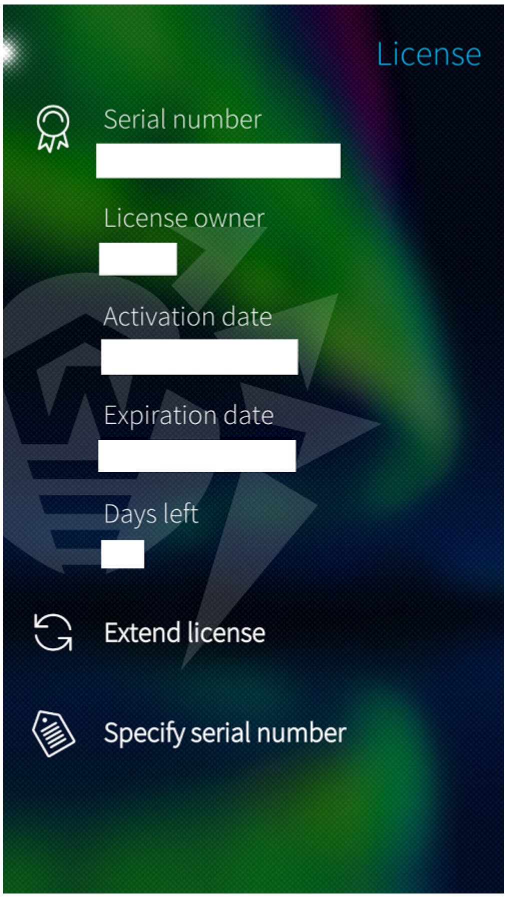
To open the page containing details on your current license

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

On the **License** page (see Figure 11), you can view license serial number, license owner name, license activation and expiration dates.

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

- If you already have a serial number, just specify it.
- You can also
  - purchase license,
  - use a key file.



License

Serial number

License owner

Activation date

Expiration date

Days left

Figure 11. Renewing license

To renew your license, tap **Extend license** on the **License** screen.

After your payment is complete, the serial number will be sent to the provided email. To extend your Dr.Web license, register the serial number.

If your license is not activated due to possible technical issues, contact our technical support: https://support.drweb.com/.

8. 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.

8.1. Dr.Web Scanner: Scan at User Request

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

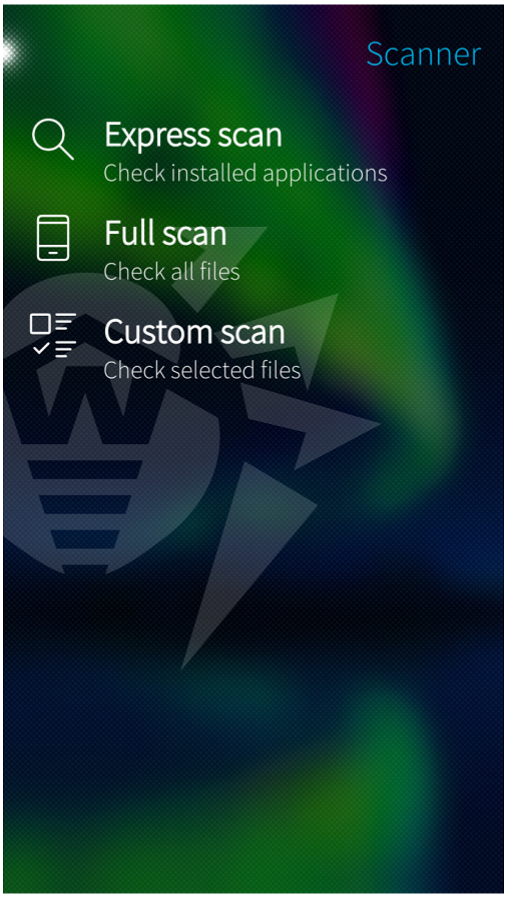


Figure 12. Dr.Web Scanner

Scanning

To scan the system, tap the **Scanner** option on the main page, then on the next page (see Figure 12) select one of the following actions:

- To only check installed applications, tap the **Express scan** option.
- To scan all files on your device, tap the **Full scan** option.
- To scan only selected files and folders, tap the **Custom scan** option. On the next page, select objects from the list (see Figure 13). Then tap **Scan**.

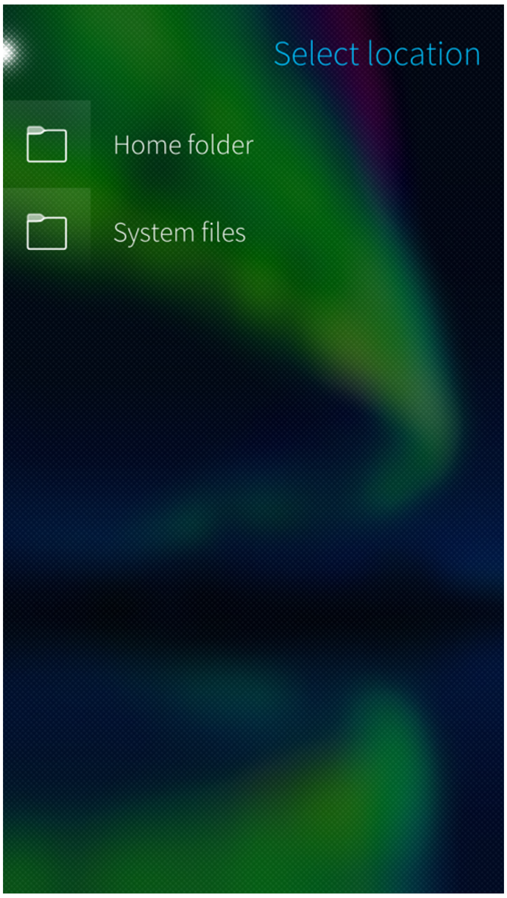
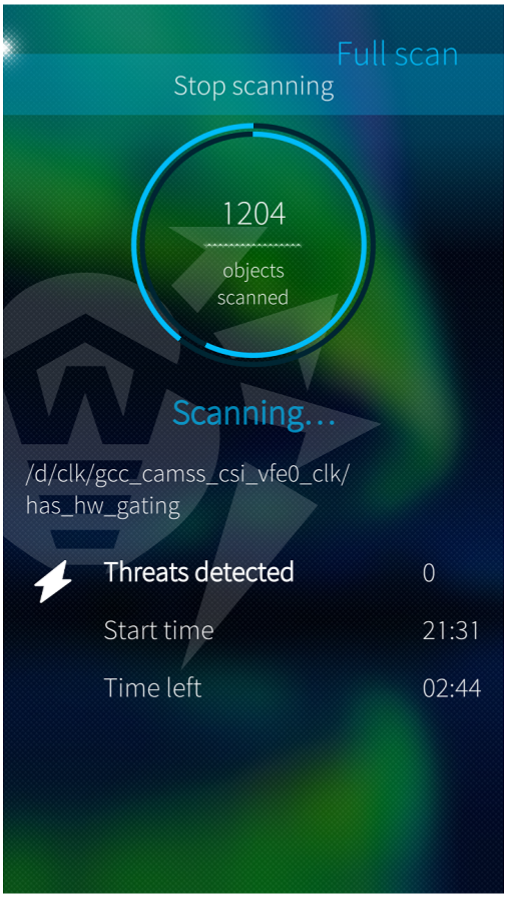


Figure 13. Custom scan

To stop scanning

1. With a fast motion, pull the page down or pull the page down without lifting your finger.
2. Tap **Stop scanning** (see Figure 14).
3. Confirm scan stop.



/d/clk/gcc_camss_csi_vfe0_clk/has_hw_gating

Threats detected	0
Start time	21:31
Time left	02:44

Figure 14. Stop scanning

Dr.Web Scanner settings

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

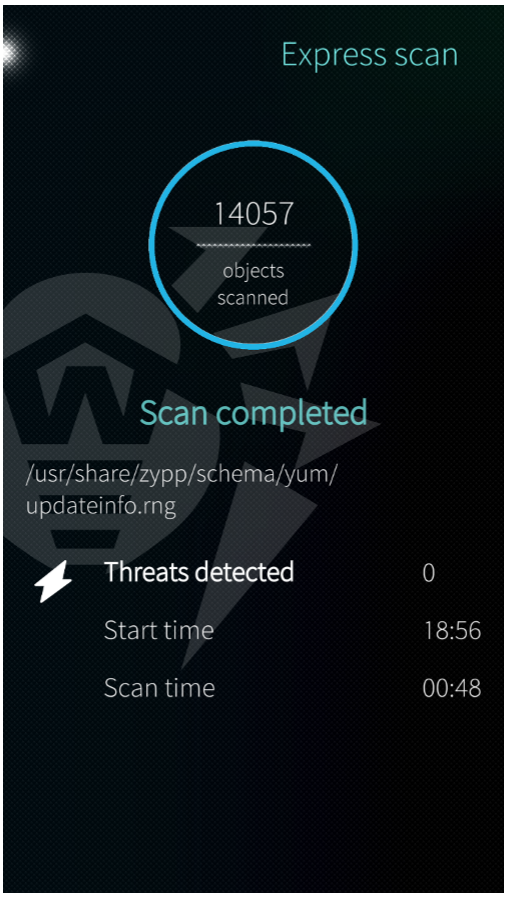
Statistics

The application registers events related to Dr.Web Scanner. They appear in the **Events** subsection on the **Statistics** page and are sorted by date (see Statistics).

Scan results

Once a scan is completed, you can view scan results by tapping **Threats detected** (see Figure 15).

If you close the app while scanning, scan results appear on the app cover. Tap the cover to view the results.



Express scan

14057 objects scanned

Scan completed

/usr/share/zypp/schema/yum/updateinfo.rng

Threats detected 0

Start time 18:56

Scan time 00:48

Figure 15. Scan results

Neutralizing threats

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

> ⚠ Users cannot neutralize threats detected in files added by an admin.

Neutralizing all threats at once

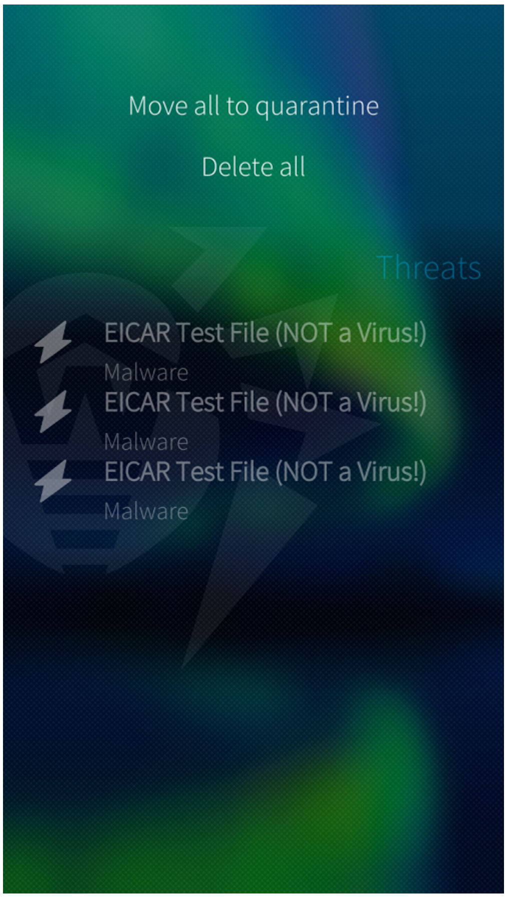
To delete all threats at once

1. With a fast motion, pull the **Threats** page down or pull the page down without lifting your finger.
2. Select **Delete all** (see Figure 16).

To quarantine all threats at once

1. With a fast motion, pull the **Threats** page down or pull the page down without lifting your finger.
2. Select **Move all to quarantine** (see Figure 16).

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



Move all to quarantine
Delete all
Threats
EICAR Test File (NOT a Virus!)
Malware
EICAR Test File (NOT a Virus!)
Malware
EICAR Test File (NOT a Virus!)
Malware

Figure 16. Neutralizing threats

Neutralizing one threat at a time

To view available actions for each threat, long-press the name of a threat in 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 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 description on the Doctor Web website.

8.2. Statistics

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

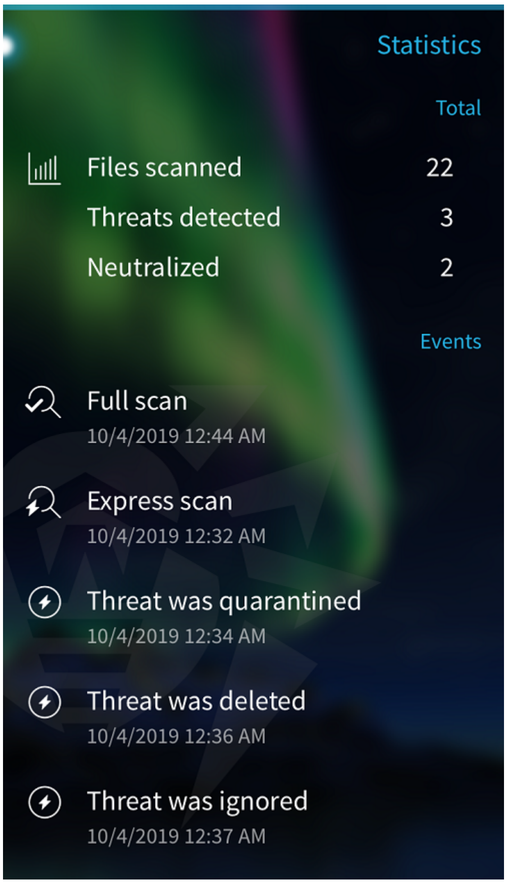
To view statistics, tap **Statistics** on the main page of the app.

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

Viewing statistics

The **Statistics** page contains two information sections (see Figure 17):

- **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.



Statistics

Total

Files scanned 22
Threats detected 3
Neutralized 2

Events

Full scan
10/4/2019 12:44 AM

Express scan
10/4/2019 12:32 AM

Threat was quarantined
10/4/2019 12:34 AM

Threat was deleted
10/4/2019 12:36 AM

Threat was ignored
10/4/2019 12:37 AM

Figure 17. Statistics

Viewing information on events

By tapping 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,
- file name,
- path to file.

Sorting events

You can sort events in Statistics

- by date,
- 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 without lifting your finger.
2. In the pulley menu, select **Filter events** (see Figure 18).
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 tapping any event type in the **Filter events** in the **Show** section of the menu.

Searching through events

You can search through events in Statistics.

To search events

1. With a fast motion, pull the **Statistics** page down or pull the page down without lifting your finger.
2. In the pulley menu, select **Search events** (see Figure 18).
3. On the next page, enter your search query.

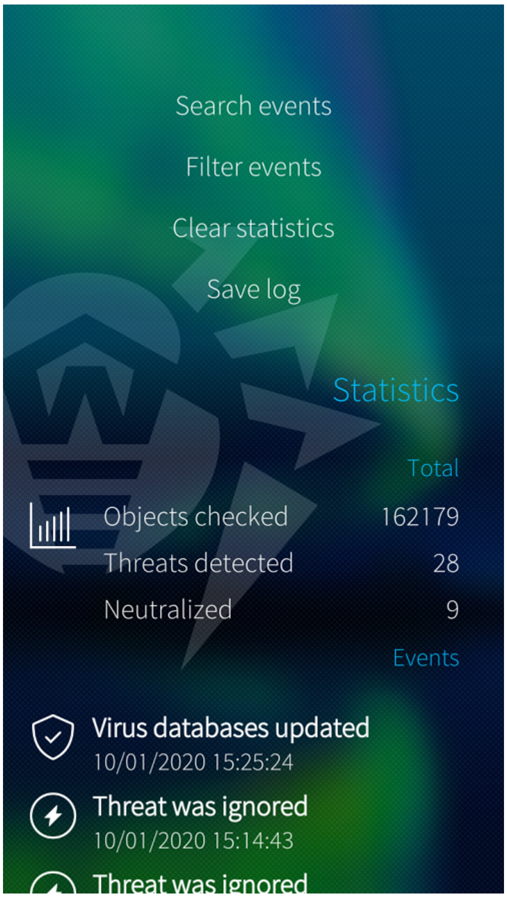


Figure 18. Filtering and searching through events

Clearing statistics

To clear all the statistics, pull the **Statistics** page down with a fast motion or pull the page down without lifting your finger and select **Clear statistics** (see Figure 18).

Saving event log

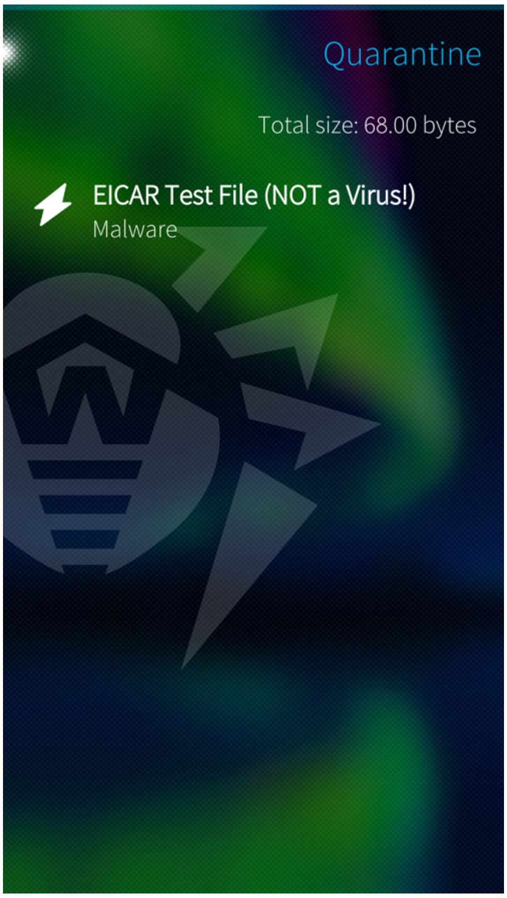
You can save application event log for further analysis in case you experience problems while using the application.

1. With a fast motion, pull the **Statistics** page down or pull the page down without lifting your finger.
2. Select **Save log**.
3. The log is saved in the `DrWeb_Log.txt` and `DrWeb_Err.txt` files located in the `home/nemo/Documents/DrWeb/` folder in the internal memory of your device.

8.3. Quarantine

You can move detected threats to quarantine folder, where they are isolated and cannot damage the system (see Figure 19).

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



Quarantine

Total size: 68.00 bytes

EICAR Test File (NOT a Virus!)
Malware

Figure 19. Quarantine

Viewing quarantined files

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

List of all threats in quarantine will open.

Viewing information on quarantined threats

If you tap a threat in the list, the following information will display:

- file name,
- path to the file,
- date and time the threat was quarantined.

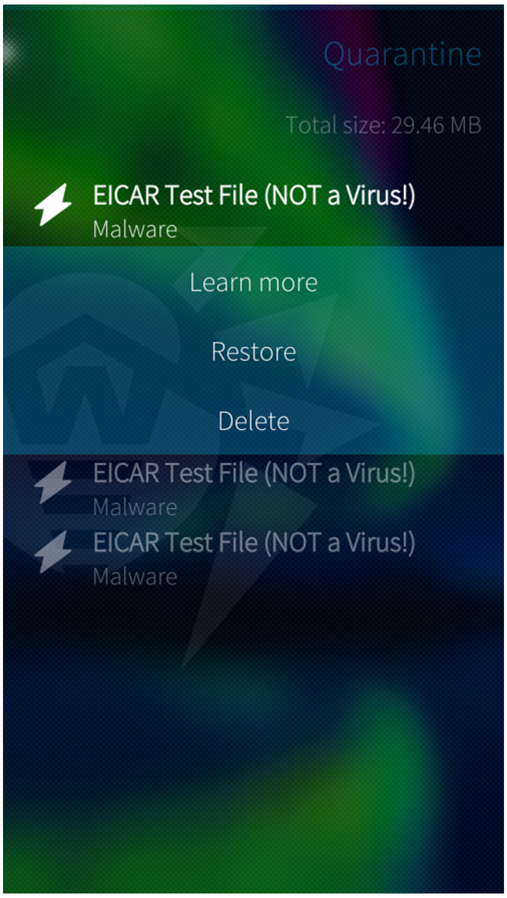
Available options

To view available options, long-press a threat in the list.

For each threat, the following options are available (see. Figure 20):

- **Learn more** to view threat description on Doctor Web website;
- **Restore** to move 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 file from quarantine and device system.

> ⚠ **Delete** is unavailable for system threats since deleting this type of threat can affect functionality of your device.



Quarantine

Total size: 29.46 MB

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

Figure 20. Actions for threat

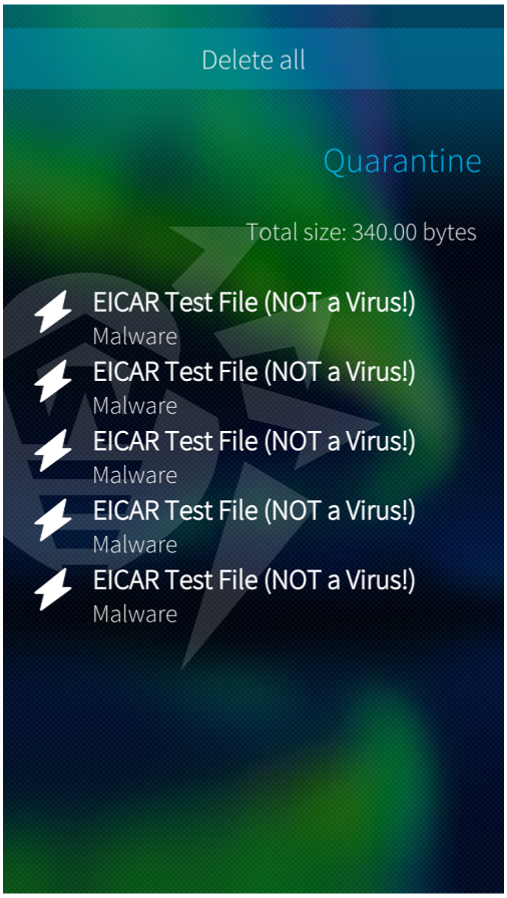
Deleting all objects from quarantine

To remove all quarantined objects at once:

1. With a fast motion, pull the **Quarantine** page down or pull the page down without lifting your finger.
2. Select **Delete all** (see Figure 21).
3. Confirm delete.

Delete all is unavailable for system threats since deleting this type of threats can affect functionality of your device.

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



Delete all

Quarantine

Total size: 340.00 bytes

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

EICAR Test File (NOT a Virus!)
Malware

Figure 21. Deleting all threats from quarantine

9. Settings

To go to app settings (see Figure 22), with a fast motion, pull the main page down or pull the page down without lifting your finger and select the **Settings** option.

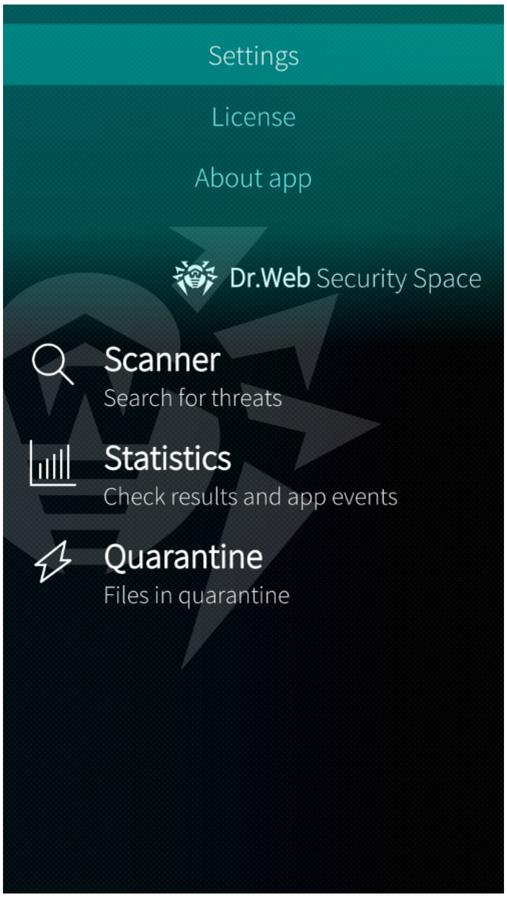


Figure 22. Settings

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

- **General settings**—allows to configure sound alerts.
- **Scanner**—allows you to configure Dr.Web Scanner that scans your device on your request (see Scanner Settings).

9.1. 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.

9.2. Scanner Settings

To access Dr.Web Scanner settings, with a fast motion pull the main page down or pull the page down without lifting your finger and select Settings.

- to enable scanning files in archives, in the **Scanner** section, tap the **Files in archives** field (○—option is disabled, ●—option is enabled);

> ⚠ By default, scanning of archives is disabled. Enabling scanning may impact system performance and increase power consumption. Also, disabling scanning does not decrease protection level since Dr.Web Scanner checks installation APK and RPM files even if the **Files in archives** option is off.

- to toggle detection of adware and riskware (including hacktools and jokes), tap the **Adware** and **Riskware** fields respectively (○—option is disabled, ●—option is enabled).

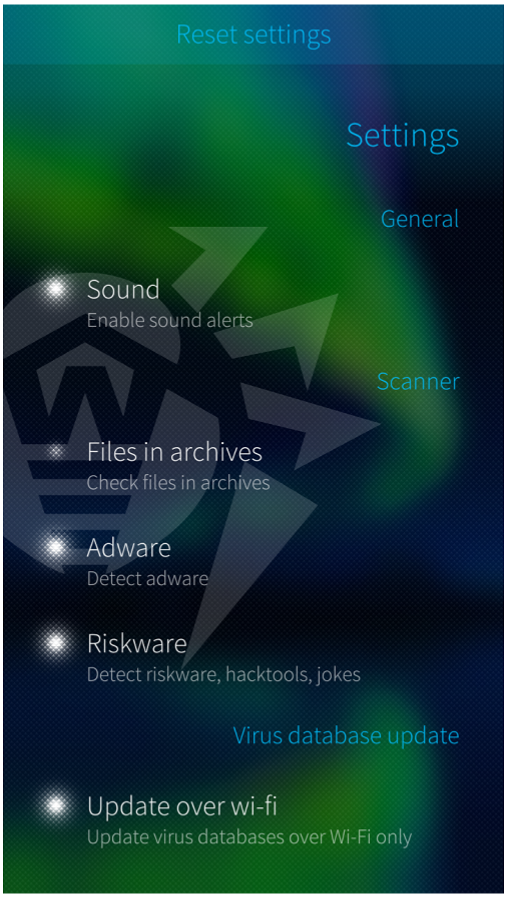
9.3. Reset Settings

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

To reset settings

1. With a fast motion, pull the **Settings** page down or pull the page down without lifting your finger.
2. Tap **Reset settings** (see Figure 23).
3. Confirm restoring default settings.

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



Reset settings

Settings

General

Sound
Enable sound alerts

Scanner

Files in archives
Check files in archives

Adware
Detect adware

Riskware
Detect riskware, hacktools, jokes

Virus database update

Update over wi-fi
Update virus databases over Wi-Fi only

Figure 23. Resetting settings

10. Virus Database Update

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

Update

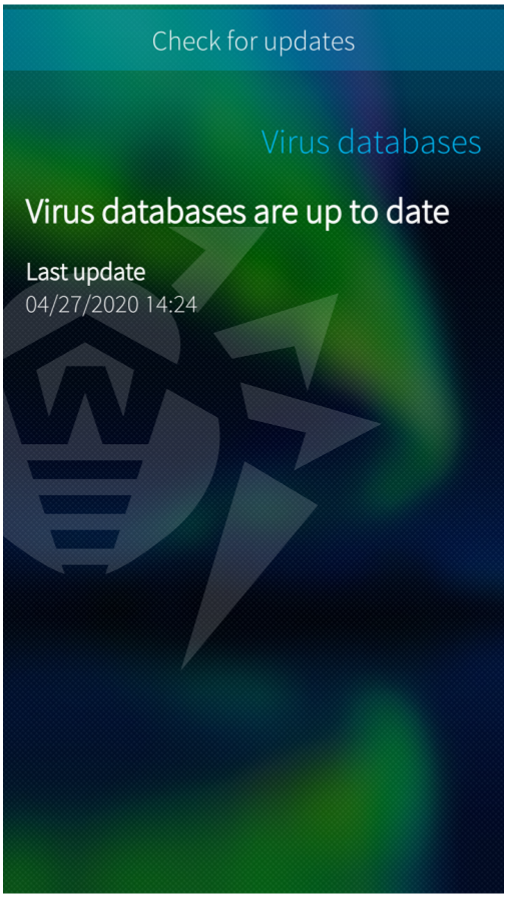
If virus databases are out of date, a notification appears at the bottom of the app. Tap the notification to update virus databases. You can also start the update in the **Virus databases** section of the pulley menu.

⚠ It is recommended to update 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 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 update

1. With a fast motion, pull the main page down or pull the page down without lifting your finger.
2. In the pulley menu, select **Virus databases**.
3. The next page contains 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 without lifting your finger.
5. Tap **Check for updates** (see Figure 24).

Update will start automatically.



Check for updates

Virus databases

Virus databases are up to date

Last update
04/27/2020 14:24

Figure 24. Virus database update

11. 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:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

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

- Fill in the web form in the corresponding section at https://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

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