



Dr.WEB

Security Space for Android

User manual



© Doctor Web, 2023. All rights reserved

This document is intended for information and reference purposes regarding the Dr.Web software discussed herein. This document is not a basis for exhaustive conclusions about the presence or absence of any functional and/or technical features in Dr.Web software and cannot be used to determine whether Dr.Web software meets any requirements, technical specifications and/or parameters, and other third-party documents.

This document is the property of Doctor Web and may be used solely for the personal purposes of the purchaser of the product. No part of this document may be reproduced, published or transmitted in any form or by any means, without proper attribution, for any purpose other than the purchaser's personal use.

Trademarks

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are the property of their respective owners.

Disclaimer

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

Dr.Web Security Space for Android
Version 12.9
User manual
5/15/2023

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. Introduction	8
1.1. Dr.Web Functions	9
2. System Requirements	10
3. Installing Dr.Web	11
4. Updating and Uninstalling Dr.Web	15
5. Licensing	18
5.1. License Screen	18
5.2. Demo License	19
5.3. Purchasing License	20
5.4. Activating License	22
5.5. Restoring License	26
5.6. Pausing and Canceling Subscription	27
5.7. Renewing License	28
5.8. Configuring Notifications on License Expiration	30
6. Getting Started	31
6.1. License Agreement	31
6.2. Permissions	31
6.3. Interface	34
6.4. Notifications	36
6.5. Widget	39
6.6. My Dr.Web	40
7. Dr.Web Account	41
8. Dr.Web Components	44
8.1. Anti-Virus Protection	44
8.1.1. SplDer Guard: Real-Time Protection	44
8.1.2. Dr.Web Scanner: On-Demand Scan	47
8.1.3. Check Results	51
8.1.3.1. Threats in System Applications	51
8.1.3.2. Changes in System Area	51
8.1.3.3. Stagefright Exploits	51
8.1.4. Device Lockers	56
8.2. Call and SMS Filter	57



8.2.1. Blocking Filter	58
8.2.2. Allowing Filter	59
8.2.3. Editing Lists	60
8.2.4. Blocked Calls and SMS	61
8.3. URL Filter	62
8.4. Dr.Web Anti-Theft	65
8.4.1. Enabling Dr.Web Anti-Theft	65
8.4.2. Configuring Dr.Web Anti-Theft	66
8.4.3. Dr.Web Anti-Theft Commands	72
8.4.3.1. Push Commands	72
8.4.3.2. SMS Commands	72
8.4.4. Disabling Dr.Web Anti-Theft	77
8.5. Parental Control	77
8.5.1. Blocking Access to Apps and Components	80
8.5.2. Parental Control Settings	85
8.5.3. Parental Control Log	86
8.6. Dr.Web Firewall	89
8.6.1. Managing Network Activity of Apps	90
8.6.1.1. Active Apps	90
8.6.1.2. All Apps	90
8.6.1.3. Access to Data Transmission	90
8.6.1.4. Mobile Traffic Usage Limit	90
8.6.2. Managing Individual App Traffic	98
8.6.2.1. Internet Traffic Statistics	98
8.6.2.2. Application Settings	98
8.6.2.3. Connection Rules	98
8.6.2.4. Application Log	98
8.6.3. Dr.Web Firewall Log	108
8.7. Security Auditor	109
8.7.1. Vulnerabilities	110
8.7.2. System Settings	111
8.7.3. Conflicting Software	112
8.7.4. Hidden Device Administrators	112
8.7.5. Applications Exploiting Fake ID Vulnerability	112
8.7.6. Optimization Settings	112
8.7.6.1. Asus	112



8.7.6.2. Huawei	112
8.7.6.3. Meizu	112
8.7.6.4. Nokia	112
8.7.6.5. OnePlus	112
8.7.6.6. Oppo	112
8.7.6.7. Samsung	112
8.7.6.8. Sony	112
8.7.6.9. Xiaomi	112
8.8. Statistics	121
8.9. Quarantine	123
9. Settings	125
9.1. General Settings	126
9.2. Virus Database Update	127
9.3. Backup	128
9.4. Reset Settings	129
10. Centralized Protection Mode	130
10.1. Switching to Centralized Protection Mode	131
10.2. Administration	134
10.3. Switching to Standalone Mode	134
11. Dr.Web on Android TV	135
11.1. Events on Android TV	136
11.2. Anti-Virus Protection on Android TV	136
11.2.1. Real-Time SplDer Guard Protection on Android TV	136
11.2.2. Dr.Web Scanner on Android TV	137
11.2.3. Check Results on Android TV	138
11.3. Dr.Web Firewall on Android TV	140
11.3.1. Managing Network Activity on Android TV	141
11.3.2. Processing App Traffic on Android TV	144
11.3.2.1. App Statistics and Settings on Android TV	144
11.3.2.2. Connection Rules on Android TV	144
11.3.2.3. Application Log on Android TV	144
11.3.3. Dr.Web Firewall Log on Android TV	152
11.4. Security Auditor on Android TV	154
11.5. Miscellaneous	157
11.5.1. Dr.Web Settings on Android TV	158



12. Technical Support	160
13. Forgot Password?	161
Keyword Index	171



1. Introduction

Dr.Web Security Space for Android (hereinafter—Dr.Web) protects mobile devices running the Android™ operating system as well as TV sets, media players and game consoles running on the Android TV™ platform from various virus threats designed specifically for these devices.



On devices running Android TV, the centralized protection mode is not available. To check if your device and Dr.Web app version support the centralized protection mode, see [Centralized Protection Mode](#).

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™ for Android technology that detects malware. This technology allows to detect new families of viruses using information from existing databases. Origins Tracing™ for Android can identify recompiled viruses, e.g. Android.SmsSend, Spy, as well as applications infected by Android.ADRD, Android.Geinimi, Android.DreamExploid. Names of threats detected by Origins Tracing for Android are marked as Android.VirusName.origin.

About this manual

This manual is intended to help users of devices running the Android OS 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.
<i>Anti-virus network</i>	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.
Internal storage/Android/	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.



1.1. Dr.Web Functions

Dr.Web performs the following functions:

- Provides 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.
- Monitors changes in system area.
- Quarantines threats or completely removes them from your device.
- Unlocks your device if it is locked by ransomware.
- Filters incoming calls and SMS messages (SMS filtering does not work in app versions that are installed from Google Play).
- Downloads Dr.Web virus database updates from the internet.
- Gathers statistics on detected threats and performed actions; keeps the app log.
- Detects device location and locks its functions remotely when it gets lost or stolen.
- Restricts access to specific websites and website categories in the pre-installed Android browser, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser, and Atom.
- Analyzes device security and helps eliminate detected problems and vulnerabilities.
- Controls internet connections to protect your device from unauthorized access and prevents leakage of personal data through networks.
- Restricts access to applications installed on your device.
- Enables safe search in the main search systems.



Some of the listed functions are not available in the application installed on [Android TV](#) devices.



2. System Requirements

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

Parameter	Requirement
Operating system	Android version 4.4–13.0. Android TV (on TV sets, media players, and game consoles)
CPU	x86/x86-64/ARM7/ARM8
Free RAM	At least 512 MB
Free space on device	At least 45 MB (for data storage)
Screen resolution	At least 800×480
Other	Internet connection (for virus database updates). On devices running Android TV, the centralized protection mode is not available

- For compatibility with apps that lock other apps, the app lockers are required not to restrict Dr.Web from launching.
- Call and SMS filter and Dr.Web Anti-theft do not operate on devices that have no SIM card slot. Make sure your device supports SIM cards.
- URL filter operates in the Android embedded browser, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser, and Atom.
- URL filter requires access to your browser history on devices with Android 5.1 or earlier. Make sure to enable this option in your browser.



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

By default, the application is installed to the internal device memory. For correct operation of Dr.Web, do not transfer the installed application to a removable media.



3. Installing Dr.Web

You can install Dr.Web:

- [From original disk.](#)
- [From Doctor Web website.](#)
- [From Google Play.](#)
- [From HUAWEI AppGallery.](#)
- [By synchronizing your device with a computer.](#)

Installation from original disk

Some devices might require enabling file transfer when connecting to a computer with a USB cable.

To install Dr.Web, enable the following system setting:

- On devices with Android 7.1 or earlier:
 1. In your device settings, open the **Security** screen.
 2. Select the **Unknown sources** check box.
- On devices with Android 8.0 or later:
 1. In your device settings, open the **Install unknown apps** screen.
 2. Allow app installation from selected source.

Copying installation file from disk and launching the file on your device

1. Insert the disk into CD/DVD drive.
2. Copy installation file from the disk to computer.
3. With a USB cable, connect your mobile device to computer.
4. A file transfer window will open on your computer. Use it to drag the file.
5. Eject your mobile device from your computer and unplug the USB cable.
6. On your mobile device, use a file manager to find and launch the installation file.
7. On your next step, tap the **Install** button.
8. Tap **Open** to start using the app.

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

For further operation, you need to activate a [paid](#) or a [demo](#) license.



After the app is installed:

- On devices with Android 7.1 or earlier, in your device settings, disable the **Unknown sources** setting.
- On devices with Android 8.0 or later, in your device settings, open the **Install unknown apps** screen and disallow app installation from selected source.

Installation from Doctor Web website

To install Dr.Web, enable the following system setting:

- On devices with Android 7.1 or earlier:
 1. In your device settings, open the **Security** screen.
 2. Select the **Unknown sources** check box.
- On devices with Android 8.0 or later:
 1. In your device settings, open the **Install unknown apps** screen.
 2. Allow app installation from selected source.

You can download the Dr.Web installation file on the Doctor Web website at <https://download.drweb.com/android/>.

Launching the installation file on device

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

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

For further operation, you need to activate a [paid](#) or [demo](#) license.



After the app is installed:

- On devices with Android 7.1 or earlier, in your device settings, disable the **Unknown sources** setting.
- On devices with Android 8.0 or later, in your device settings, open the **Install unknown apps** screen and disallow app installation from selected source.

Installation from Google Play

Before installing Dr.Web from Google Play, make sure that:

- You have a Google account.
- You have logged in to your Google account from your device.



- Your device is connected to the internet.
- Your device meets the [system requirements](#).

To install the application

1. On your device, open Google Play, find Dr.Web in the list of applications and tap **Download** or **Purchase** (if you want to install Dr.Web Security Space Life version with an unlimited license).



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

2. If you have selected Dr.Web Security Space Life with an unlimited license, complete the purchase to continue.
3. On the next screen, you will be prompted to provide access to necessary features and data on your device.

Check the list of required permissions and tap **Accept**.

4. Tap **Open** to start using the app.

For further operation, you need to obtain a [paid](#) or [demo](#) license (except Dr.Web Security Space Life).

Installation from HUAWEI AppGallery

Before installing Dr.Web from HUAWEI AppGallery, make sure that:

- You have a Huawei account.
- You have logged in to your Huawei account from your device.
- Your device is connected to the internet.
- Your device meets the [system requirements](#).

To install the application

1. On your device, open HUAWEI AppGallery, find Dr.Web in the list of applications and tap **Install**.



If your device does not meet the [system requirements](#), Dr.Web will not be displayed in the list of applications in HUAWEI AppGallery.

2. On the next screen, you will be prompted to provide access to necessary features and data on your device.

Check the list of required permissions and tap **Accept**.

3. Tap **Open** to start using the app.



For further operation, you need to activate a [paid](#) or a [demo](#) license.

Installation by using synchronization software

Install the application by synchronizing the device with computer by using special synchronization software (e.g., HTC Sync™ etc.).

1. Synchronize your device with your computer.
2. Launch the installation manager included into the synchronization software package.
3. Specify the path to the file located on the computer, then follow the instructions of the installation wizard.
4. The application will be copied to the device where you can review the information on it and confirm the installation.
5. Close the installation wizard.

Dr.Web is successfully installed on your device and is ready to use. For further operation, you need to activate a [paid](#) or [demo](#) license.




4. Updating and Uninstalling Dr.Web

Updating Dr.Web

Configuring automatic updates for Dr.Web installed from the Doctor Web website


If you have downloaded your Dr.Web from the Doctor Web website, you can enable notifications about the availability of a new version. To do so:

1. On the Dr.Web main screen, tap **Menu**  and select **Settings**.
2. On the **Settings** screen, tap **Virus database update**.
3. On the **Virus database update** screen, select the **New app version** check box.

If the check box is selected, Dr.Web checks for new versions every time the virus databases get updated. If a new version is available, you will be prompted to download and install it.

Updating Dr.Web in Google Play manually

If your Google Play app is not configured to update installed apps automatically, you can update Dr.Web manually:

1. Open the **Play Store** app.
2. Tap your Google profile icon in the top-right corner of the screen.
3. Select **Manage apps & device**.
4. Select the **Manage** tab.
5. Tap the **Updates available** list and do one of the following:
 - Select **Dr.Web** and then tap **Update**.
 - Select the check box next to **Dr.Web** and tap the  icon.



The app is found on the **Updates available** list only if a new version of Dr.Web has been released.

6. Dr.Web may require new permissions when it is updated. In this case, a notification asking to grant new permissions will appear.

Tap **Accept** to grant Dr.Web the required permissions.

Tap **Open** to start using the app.



Updating Dr.Web in HUAWEI AppGallery

You can configure automatic updates for applications installed from HUAWEI AppGallery (including Dr.Web). To do so, in the **Manager** tab of the HUAWEI AppGallery app, use the **Auto-update over Wi-Fi** toggle button.

You can also update Dr.Web manually:

1. Open the **HUAWEI AppGallery** app and tap **Manager**.
2. Select Dr.Web on the list of installed apps and tap **Update**.



The **Update** option will not be available until a new version of Dr.Web is released.

3. Dr.Web may require new permissions when it is updated. In this case, a notification asking to grant new permissions will appear.

Tap **Accept** to grant Dr.Web the required permissions.

Tap **Open** to start using the app.

Uninstalling Dr.Web



Dr.Web Anti-theft is designed to complicate the process of deleting Dr.Web from your device. If Dr.Web Anti-theft is configured on your device, [disable](#) it and remove Dr.Web from device administrators before deleting the app.

To uninstall Dr.Web

1. In your device settings, select **Apps** or **Application manager**.
2. Select **Dr.Web** on the list of installed apps and tap **Uninstall**.

The quarantine folder and log files are not deleted automatically. You can delete them manually from the `Android/data/com.drweb/files` folder in the internal storage of your device.



On devices with Android 11.0 or later, logs are saved in `Download/DrWeb`.

Uninstalling Dr.Web through HUAWEI AppGallery

If you installed Dr.Web from HUAWEI AppGallery, you can uninstall the application by doing the following:

1. Open the HUAWEI AppGallery app.



2. Tap **Manager**.
3. On the next screen, tap **Installation manager**.
4. Select Dr.Web on the list of installed apps and tap **Uninstall**.
5. Confirm uninstallation.



5. Licensing

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

A license is required for all Dr.Web components to function in the following application versions:

- Downloaded from your personal account of the Dr.Web Anti-virus service provider.
- Received from the anti-virus network administrator of your company.
- For Dr.Web on Android TV.
- In the Dr.Web Security Space Life version.

A license is required for all Dr.Web components, except for [SpIDer Guard](#), [Scanner](#) and [Security Auditor](#), to function in the following application versions:

- Downloaded from the Doctor Web website <https://download.drweb.com/android/>.
- In the Dr.Web Security Space version installed from Google Play.
- In the app version installed from HUAWEI AppGallery.

If you want to try using the application before purchasing a license, you can activate a [demo license](#).

If you have a valid license for the products Dr.Web Security Space or Dr.Web Anti-virus (full packaged product or digital license), you can [activate](#) it.




If you have got an application version with the unlimited license (Dr.Web Security Space Life) from Google Play, the license is acquired and activated automatically.

If you use the application in the [centralized protection mode](#), the license is automatically downloaded from the centralized protection server.


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:

- In Dr.Web versions that [require a license for all the components to function](#):
 - Tap **More** in the notification about a missing license on the Dr.Web main screen.
 - On the Dr.Web main screen, tap **Menu**  and select **License**.
- In Dr.Web versions that [require a license for some of the components to function](#):



- On the Dr.Web main screen, select one of the components that require the purchase of a license.
- On the Dr.Web main screen, tap **Menu**  and select **License**.

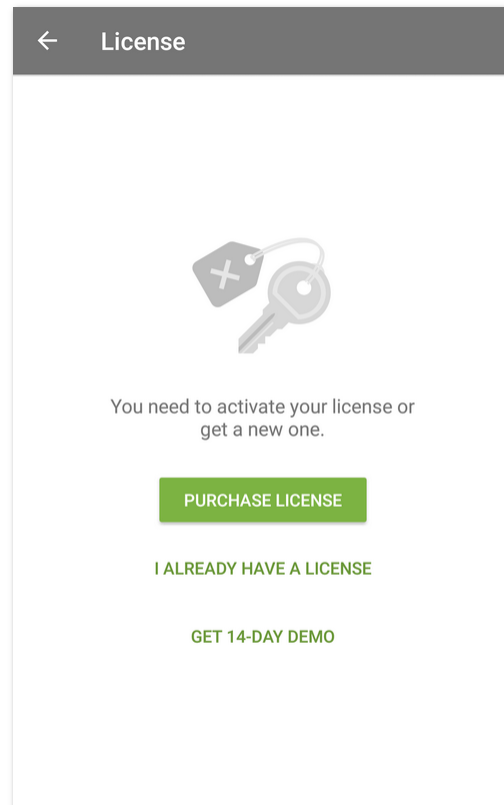


Figure 1. License screen

5.2. Demo License

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

To activate a demo license

1. Open 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.
 - Existing email address.
 - Country.
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.

← Demo version

To get a demo version, specify your name and email address.

Full name
John Doe

Email address
johndoe@example.com

Country
United Kingdom

☒ Get news by email

GET DEMO

Figure 2. Getting a demo license

5.3. Purchasing License

If the application is installed from Google Play

1. Open the application.
2. Open the [License](#) screen.
3. Select **Purchase license**.

If you do not have a Google account, enter an email address for license registration. If you reinstall the application or use it on another device, you will be able to restore your license with this email address.

On this step, the application may request access to your contacts. If you allow the access, the email address will be filled in automatically. Otherwise, enter it manually.

4. On the **Purchase license** screen (see [Figure 3](#)), select one of the following options:
 - **Monthly subscription.** Monthly subscription allows you to use the license for one month after you purchase the subscription. After that the subscription is automatically renewed and charged once a month.



- **1 year license.** This license is valid for one year after the purchase.
- **2 year license.** This license is valid for two years after the purchase.

If you select one of these options, a standard license purchase screen will open. After you complete the payment, your license will be activated automatically.

As a confirmation of your purchase of a 1 or 2 year license, a license key file will be sent to your email address. If the license is not activated because of a possible technical issue, contact our technical support: <https://support.drweb.com/>.

- **Lifetime license**

If you select a lifetime license, a Google Play screen for Dr.Web Security Space Life license purchase will be opened. After you complete your purchase, a new version of Dr.Web will be downloaded and installed. The license will be activated automatically.

Once you open a new version of Dr.Web, you are prompted to uninstall your previous version of Dr.Web. If you want to save your settings for further import to Dr.Web Security Space Life, you can [export](#) the settings before uninstalling the application.

Tap **OK** to uninstall the previous version of Dr.Web from your device.



Dr.Web Ant-theft is designed to complicate the process of Dr.Web removal from a device. If Dr.Web Anti-theft is configured on your device, [disable](#) it before proceeding.

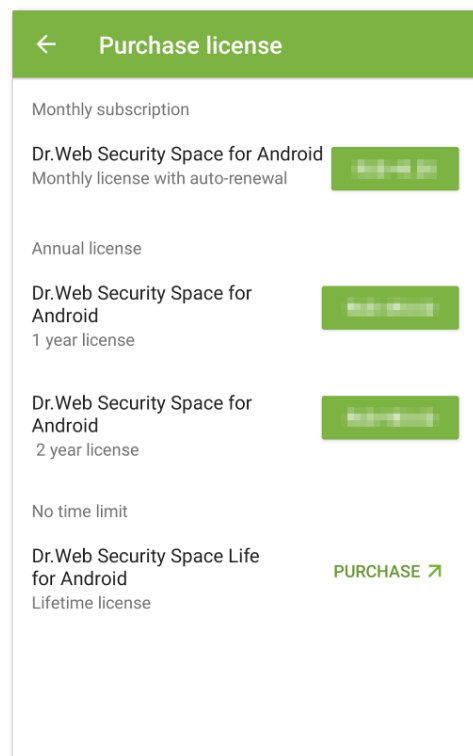


Figure 3. Purchasing license



If the application is installed from the Doctor Web website

1. Open 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. Select **Buy**.
6. Fill in the form and select **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. [Register the received serial number](#).

If the application is installed from Huawei AppGallery

1. Open the application.
2. Open the [License](#) screen.
3. Select **Purchase license**.

Create your Huawei account or log in to your current one. After logging in grant the application the necessary permissions.

On this step, the application may request access to your Huawei account. If you allow it, your email address will be filled out automatically. Otherwise, you will be prompted to select the email from the list in the pop-up window.

4. On the **Purchase license** screen, select one of the following options:

- **1 year license**
- **2 year license**

If you select one of these options, a standard license purchase screen will open. After you complete your payment, your license will be activated automatically. As a confirmation of your purchase, a license key file will be sent to your email address. If the license is not activated because of a possible technical issue, contact our technical support:

<https://support.drweb.com/>.

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 Android.

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](#) (only for an application installed from the Doctor Web website).

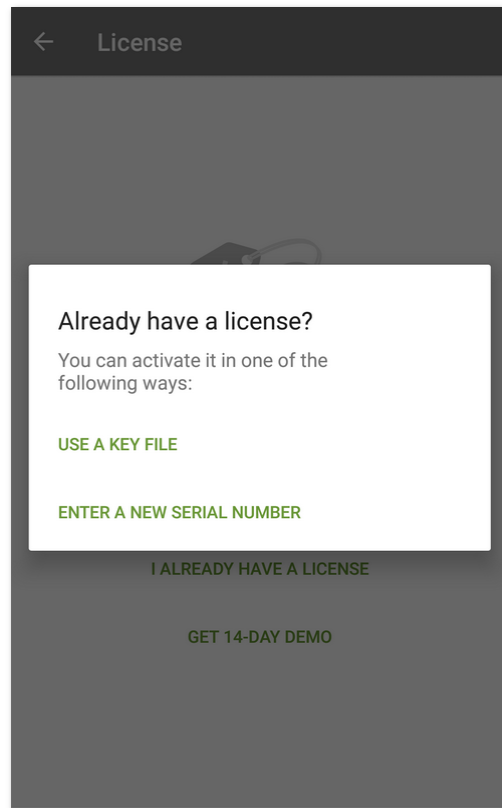


Figure 4. Activating license

Registering a serial number in the application

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

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

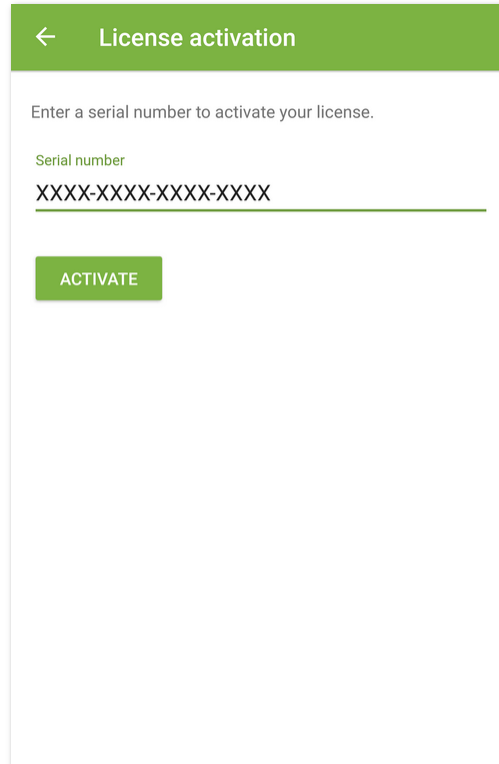


Figure 5. Registering a serial number

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

You will be redirected to the Dr.Web main screen. At the bottom of the screen, you will see a notification about a successful license activation.

Registering a serial number on the website

If your device with the installed application is not connected to the internet, you can use a computer or other device connected to the internet. In this case, you will receive a license key file that you will have to copy to your device to activate your license.

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. Fill in the registration form.



4. The license key file will be sent as a ZIP archive to your email address.

License key file

License key file contains the 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.
- 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.

Using a license key file

You can use the license key file only with an application installed from the Doctor Web website.

To use a license key file

1. Copy the key file to your device to a folder in the internal memory.
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](#) screen, tap **I already have a license**.
3. Select **Use a key file** (see [Figure 4](#)).
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 Dr.Web main screen. 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 editing makes it invalid. To prevent the license from compromise, do not save the file when you close the text editor.

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 the application is installed from Google Play

1. Open the application.
2. Open the [License](#) screen.
3. On the **License** screen, tap **I already have a license**.
4. Tap **Restore purchase from Google Play**.
5. Enter the email address you have previously used to register your license and your personal information.

License registered for this email address will be activated automatically.

If the application was installed from the Doctor Web website

You have two options to restore your license:

- [Register a serial number](#).
- [Use a key file](#).

If the application is installed from HUAWEI AppGallery

1. Open the application.
2. Open the [License](#) screen.
3. On the **License** screen, select **I already have a license**.
4. Tap **Restore purchase from HUAWEI AppGallery**.
5. Enter the email address you have previously used to register your license and your personal information.

License registered for this email address will be activated automatically.



Restoring demo license

1. Open 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. Pausing and Canceling Subscription

If you use the subscription-based license, you can pause your subscription for a set period of time or cancel the subscription using Google Play.

Pausing your subscription



The subscription will be paused at the end of the current billing period. The license will be valid until the subscription is paused.

To pause your subscription

1. Open the **Play Store** app.
2. Tap your Google profile icon in the top-right corner of the screen.
3. Select **Payments & subscriptions** > **Subscriptions**.
4. Select Dr.Web in the subscription list.
5. On the **Manage subscription** screen, select **Pause payments**.
6. Set the time period to pause payments.
7. Confirm that you want to pause the subscription.

You can resume your subscription at any moment before the end of the set time period to pause payments.

To resume your subscription

1. Open the **Play Store** app.
2. Tap your Google profile icon in the top-right corner of the screen.
3. Select **Payments & subscriptions** > **Subscriptions**.
4. Select Dr.Web in the subscription list.
5. On the **Manage subscription** screen, tap **Resume**.
6. Confirm that you want to resume payments.



Canceling your subscription



When you uninstall Dr.Web, your subscription won't cancel.


After you cancel your subscription, the license will be valid until the end of the current billing period.

To cancel your subscription

1. Open the **Play Store** app.
2. Tap your Google profile icon in the top-right corner of the screen.
3. Select **Payments & subscriptions** > **Subscriptions**.
4. Select Dr.Web in the subscription list.
5. On the **Manage subscription** screen, tap **Cancel subscription**.
6. On the **Would you rather pause your subscription?** screen, tap **No thanks**.
7. On the **What's making you cancel?** screen, select any option and tap **Continue**.
8. On the **Cancel subscription?** screen, tap **Cancel subscription**.

5.7. Renewing License

To view the details of your current license:

- **On Android.** On the Dr.Web main screen (see [Figure 8](#)), tap **Menu**  and select **License**.
- **On Android TV.** Open the Dr.Web [main screen](#) and go to **Miscellaneous** > **License**.

On the **License** screen, you can view the license serial number, license owner name, license activation and expiration dates.

If you are subscribed to the Dr.Web Anti-virus service, in the [centralized protection mode](#), the **License** screen also contains the subscription expiration date.

Renewing license



The Google Play subscription-based license does not require manual renewal. The subscription is automatically renewed and charged once a month.

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


You can renew your 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 website, you can:
 - [Purchase a license](#).
 - [Use a key file](#).
 - Renew your license on your [personal webpage](#) on the Doctor Web website.

To do so, tap **Menu** , select the **About** option, and tap **My Dr.Web**.

- If you have obtained your current license from Google Play:
 1. On the Dr.Web main screen, tap **Menu**  and select **License**.
 2. On the **License** screen (see [Figure 6](#)), tap **Extend Google Play license**.

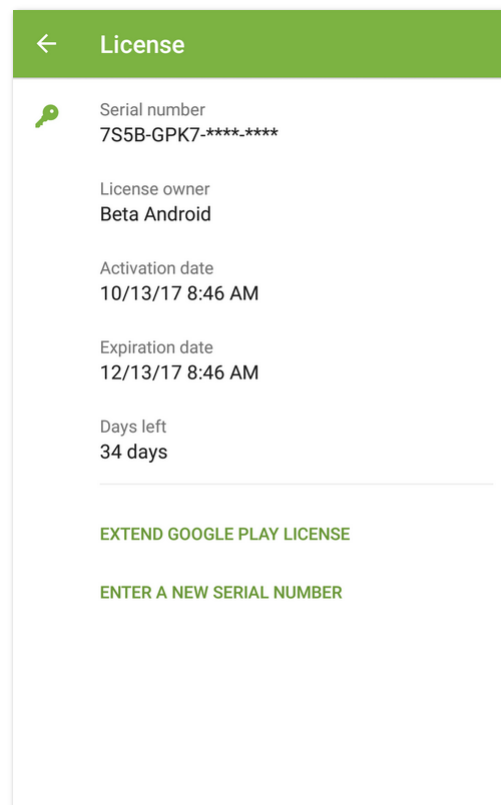


Figure 6. Renewing license


3. On the **Extend license** screen, select one of the following options:
 - **1 year license**
 - **2 year license**

If you select one of these options, a standard license purchase screen will open. After you complete your payment, your license will be activated automatically. As a confirmation of your purchase, a license key file will be sent to your email address. If your license is not activated due to possible technical issues, contact our technical support:

<https://support.drweb.com/>.

- **Lifetime license**
- If you have obtained your current license from HUAWEI AppGallery:



1. On the Dr.Web main screen, tap **Menu**  and select **License**.
2. On the **License** screen, tap **Extend HUAWEI AppGallery license**.
3. On the **Extend license** screen, select one of the following options:

- **1 year license**
- **2 year license**


If you select one of these options, a standard license purchase screen will open. After you complete your payment, your license will be activated automatically. As a confirmation of your purchase, a license key file will be sent to your email address. If your license is not activated due to possible technical issues, contact our technical support:

<https://support.drweb.com/>.

5.8. Configuring Notifications on License Expiration

On mobile devices, you can enable notifications about upcoming license expiration (unless you are using the Google Play subscription-based license or Dr.Web Security Space Life with an unlimited license).

To enable notifications

1. On the Dr.Web main screen, tap **Menu**  and select **Settings** (see [Settings](#)).
2. Tap **License**.
3. Select the **Notifications** check box.



6. Getting Started

After you install Dr.Web and activate a license, you can get acquainted with the interface and the main menu, configure notifications, and place the Dr.Web widget on your Home screen.

6.1. License Agreement

On the first launch of the application, you will be asked to read and accept the License Agreement. You must accept the License Agreement to use the application.

On the same screen, you will be notified about sending 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](#).



If your Dr.Web version is provided by the [anti-virus network](#) administrator of your company, you will not need to read and accept the License Agreement.

6.2. Permissions

On Android 6.0 or later, you can allow or block access to device features and personal data for your apps.

After you install Dr.Web and accept the License Agreement, grant the app the necessary permissions. Permissions might be also requested the first time you tap one of the [components](#) or enable them.

- Dr.Web requires the following permissions on the first launch of the application:
 - Access to photos, media, and files on your device.
 - All files access (on devices with Android 11.0 or later versions).

These permissions are mandatory for the application.

- Permission to send [notifications](#) (on devices with Android 13.0 or later versions).

Dr.Web needs this permission to use the notification bar for displaying messages about the device protection status and Dr.Web component activities. If the permission is not granted, Dr.Web cannot notify you about detected threats and component events until you open the app.

- [Call and SMS filter](#) requires the following permissions:
 - Make and manage phone calls.
 - Send and view SMS messages.
 - Access your contacts.



- Access notifications.
- Access the call log (on devices with Android 9.0 or later).
- Use Dr.Web as the default caller ID and spam app (on devices with Android 10.0 or later).
- [URL filter](#) requires access to Android accessibility features in order to operate in one of the supported browsers.
- [Dr.Web Anti-theft](#) requires the following permissions:
 - Make and manage phone calls.
 - Send and view SMS messages.
 - Access your contacts.
 - Access notifications.
 - Access your device's location.
 - Access Android accessibility features.
 - Make Dr.Web a device administrator.
- [Dr.Web Firewall](#) requires the following permissions:
 - Connect to a VPN in order to track traffic.
 - Drawing over other apps.
- [Dr.Web on Android TV](#) requires the following permissions:
 - Access to your contacts.
 - Access to photos, media, and files on your device.
 - All files access (on devices with Android 11.0 or later versions).



In the [centralized protection mode](#), the following permissions are requested:

- Basic permissions (access your photos, media, and files, contacts, etc.)—required for most of the app features.
- Permission to send notifications (on devices with Android 13.0 or later versions)—for displaying messages about the protection status and component events.
- All files access (on devices with Android 11.0 or later versions)—for performing device checks.
- Call and SMS filter (may vary depending on the Android version, see [above](#))—for call and SMS filtering.
- Device administration—to protect the app from uninstalling and to use the full functionality of Anti-theft.
- Access to accessibility features—for app filtering and full functionality of URL filter, Anti-theft, and Parental Control.
- Drawing over other apps—for app filtering and Firewall functionality.

If the requested permissions are not granted yet, the **Permissions required** screen appears (see [Figure 7](#)). You can grant all of the requested permissions or only the obligatory ones. Obligatory permissions are marked with a yellow icon. Non-obligatory permissions are marked with a gray icon. Once a permission is granted, its icon becomes green.



If you grant all of the permissions requested by a component, the app proceeds to the next screen automatically. If you grant only the obligatory permissions, you can proceed to the next screen by tapping the **Continue** button. You can grant the non-obligatory permissions the next time you access the component from the Dr.Web main screen or on the settings screen of your device.

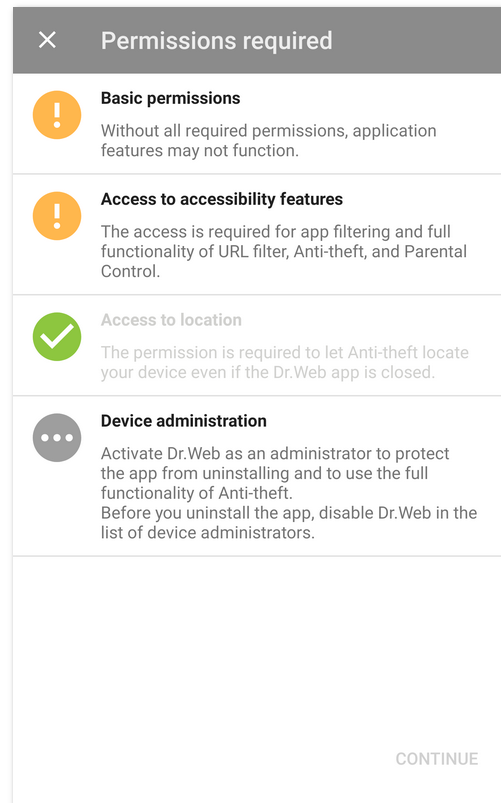



Figure 7. Permissions required

If you decline the at least one permission request, you will be prompted to go to settings:

- On devices with Android 9.0 or earlier:
 1. Tap **Go to Settings** and then select **Permissions**.
 2. Select **Storage** and grant the permission by using the toggle button.
- On devices with Android 10.0:
 1. Tap **Go to Settings** and then select **Permissions**.
 2. Select **Storage** in the **Denied** category and then select **Allow**.
- On devices with Android 11.0 or later:
 1. Tap **Go to Settings** and select **Permissions**.
 2. Select **Storage** in the **Denied** category and then select **Allow management of all files**. By selecting this option, you are granting access to your photos and media as well as access to all files.




To open the list of all permissions for Dr.Web

1. Open device settings .
2. Tap **Apps** or **Application manager**.
3. Find Dr.Web on the list of installed applications and tap it.
4. On the **App info** screen, select **Permissions**.
5. Tap the menu in the top-right corner and select **All permissions**.

6.3. Interface

Main screen

The main screen (see [Figure 8](#)) comprises the list of the main Dr.Web components.

The **menu**  in the top-right corner of the main screen allows you to:

- View license details.
- Open statistics.
- Open the list of quarantined files.
- Run virus database updates.
- Open the application settings screen.
- Open online help.
- Manage your Dr.Web account.
- View information about the application.

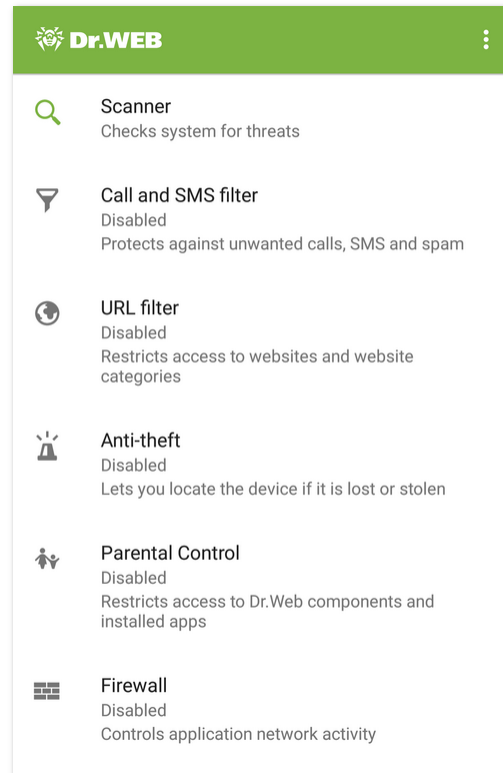


Figure 8. Dr.Web main screen

Status bar

In the top part of the Dr.Web main screen, there is a status bar with an indicator that shows the current protection status of your device (see [Figure 9](#)).

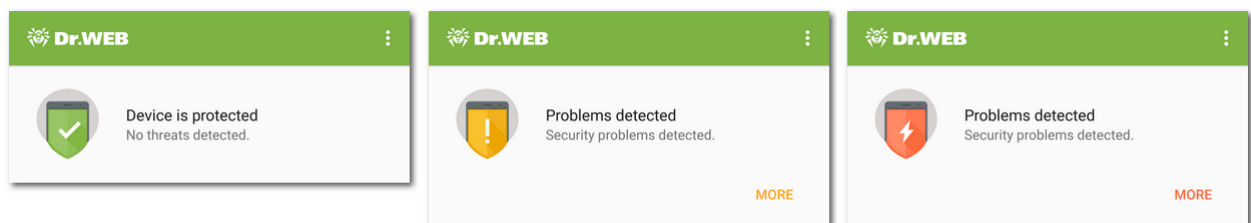


Figure 9. Status bar

- The green icon indicates that the device is protected. No additional actions are required.
- The yellow icon indicates that Dr.Web has detected security issues, e.g. a missing license or a vulnerability. To learn more about the detected issues and to eliminate them, tap **More**.
- The red icon indicates that Dr.Web has detected suspicious changes in the system area or threats. To open [check results](#) and neutralize the threats, tap **More**.

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



6.4. Notifications

On devices with Android 7.0 or later, all Dr.Web notifications are grouped into one extendable notification.

On devices with Android 8.0 or later, Dr.Web notifications are separated into categories, or channels. You can manage the behavior of each notification category separately in your device settings. If you disable one of the categories, you will stop receiving all notifications from this category. All the categories are enabled by default.

Notification categories


Category	Notifications
Threat detection	<ul style="list-style-type: none">• Notifications about threats detected by SpIDer Guard.• Notifications about threats detected by Dr.Web Scanner.
Safe applications	Notifications on the absence of threats in recently installed or updated applications. On devices with Android 7.1 or earlier, this notification category can be enabled or disabled in the general settings of Dr.Web .
Anti-virus protection status	<p>If the notification bar is disabled, this category contains the following notifications:</p> <ul style="list-style-type: none">• System is protected. Shown if SpIDer Guard is enabled and a scan is not being performed by Dr.Web Scanner.• Notifications about the type of scan being performed by Dr.Web Scanner. Shown if an express, full, or custom scan is in progress.• Notifications on scanning removable media. Shown if the SD card or the external storage is being scanned by SpIDer Guard. <p>If the notification bar is enabled and a scan has been started, a message about the ongoing scan is shown on the notification bar.</p>
Advanced components status	<ul style="list-style-type: none">• Advanced components enabled. Shown if Call and SMS filter, URL filter, Dr.Web Anti-theft, or Dr.Web Firewall is enabled.• Agent enabled. Shown in the centralized protection mode if Call and SMS filter (all incoming calls and SMS are accepted), URL filter, Dr.Web Anti-theft, and Dr.Web Firewall are enabled.• Agent and advanced components enabled. Shown in the centralized protection mode if Dr.Web Anti-theft, Dr.Web Firewall, Call and SMS filter, or URL filter is enabled.
Notifications from buddies	Notifications received from your buddies.
Protection components configuration	Configuring components... Shown when the location of your device is requested from a buddy's device if Dr.Web Anti-theft is enabled in the app version downloaded from Google Play.
Other	<ul style="list-style-type: none">• Permissions required. Shown when opening the application if access to photos, media, and files has been denied. In the app version received from





Category	Notifications
	<p>the anti-virus network administrator of your company or from the Dr.Web Anti-virus service provider, the notification is shown when opening the application if any of the requested permissions has been denied.</p> <ul style="list-style-type: none">• License notifications:<ul style="list-style-type: none">▫ An error occurred when verifying the license. Shown if an error occurred during the license verification. The license may be missing or not confirmed by the server.▫ Cannot confirm the license. Shown in the Dr.Web Security Space Life version with a lifetime license if the application does not receive the license confirmation for a long time.▫ Days remaining: <number of days>. Shown if your license is expiring and the Notifications check box is selected in the application settings.▫ License is expired. Shown if you use the Dr.Web Anti-virus service and your license has expired.▫ Please contact the anti-virus network administrator. Shown if you use the Dr.Web Anti-virus service and your license has been blocked.• New Dr.Web version available. Shown in the version downloaded from the Doctor Web website if a new version is released and the New app version check box is selected in the application settings.• Dr.Web Anti-theft notifications:<ul style="list-style-type: none">▫ No SIM card found.▫ New SIM card found.• Call and SMS filter notification: All incoming calls and SMS are rejected. Shown when you select the Block all check box.• Dr.Web Firewall notifications:<ul style="list-style-type: none">▫ Dr.Web Firewall is disabled. Shown if the VPN of Dr.Web is disconnected.▫ Mobile traffic limit reached. Shown if the specified mobile traffic limit is exceeded and, in the Firewall settings, the Notifications check box is selected.• New message. Shown if you receive a message from the anti-virus network administrator.
Group notifications	This category does not contain any specific notifications but allows you to group all Dr.Web notifications into one extendable notification.

Notification bar

The Dr.Web notification bar (see [Figure 10](#)) provides quick access to the main features of the application. It also notifies you of suspicious changes in the system area as well as threats.

If Dr.Web detects suspicious changes in the system area or threats, on devices running Android 11.0 or earlier, the application icon changes to  on the notification bar. On devices running



Android 12.0 or later, the application icon changes to , and the protection status indicator turns red .

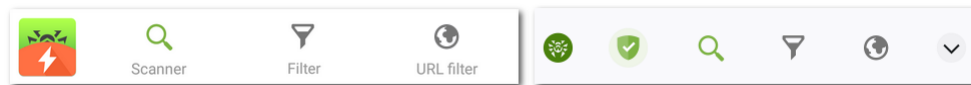



Figure 10. Notification bar on Android 11.0 (left) and Android 12.0 (right)



On [Android TV](#), the notification bar is unavailable.

To enable the Dr.Web notification bar

1. Select **Menu**  > **Settings** on the Dr.Web main screen.
2. Tap **General settings**.
3. Select the **Notification bar** check box.










On Android 5.0 and 5.1, if Dr.Web detects suspicious changes in the system area or threats, the notification bar is displayed over other applications until you apply an action to the detected object or until you swipe over the notification.





If your device does not support SIM cards, instead of the **Filter** option the notification bar contains the **Downloads** option, which allows you to scan downloaded files.

If Dr.Web operates in the [centralized protection mode](#) and you do not have the permissions to change the Call and SMS filter settings or the URL filter settings, the corresponding options **Filter** and **URL filter** are unavailable on the notification bar.

The notification bar allows you to:

- On devices with Android 11.0 or earlier:
 - Open the app. Tap the  icon.
 - Start an express, full, or custom scan. Tap  **Scanner**.
 - Specify an action for all incoming calls and messages. Tap  **Filter**.
 - Select website categories that you want to restrict access to. Tap  **URL filter**.
- On devices with Android 12.0 or later:
 - Open the app (when the protection status indicator is green). Tap .
 - Grant necessary permissions (when the protection status indicator is yellow). Tap .
 - Open check results (when the indicator is red). Tap .



- Start an express, full, or custom scan. Tap .
- Specify an action for all incoming calls and messages. Tap .
- Select website categories that you want to restrict access to. Tap .
- View protection status, current and recommended actions. Tap .

6.5. Widget

Dr.Web widget allows you to quickly enable and disable real-time SplDer Guard protection. You can add the widget to your Home screen.



On [Android TV](#), the widget is unavailable.

To add the Dr.Web widget

1. Open the list of widgets available on your device.
2. Select the Dr.Web widget.

The green widget indicates that the SplDer Guard component is enabled and the device is under its active protection. The widget with a yellow icon indicates that the SplDer Guard component is disabled (see [Figure 11](#)). Tap the widget to re-enable SplDer Guard.

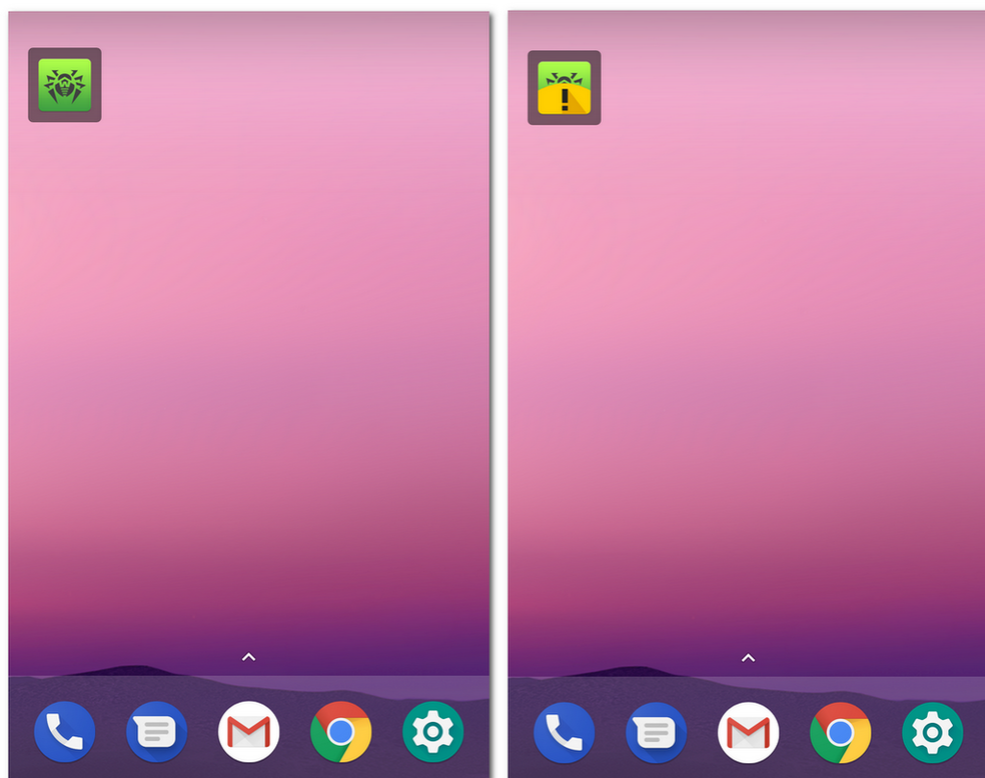


Figure 11. Dr.Web Widget



6.6. 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 the My Dr.Web online service








1. On the Dr.Web [main screen](#), tap **Menu**  and select **About**.
2. Tap **My Dr.Web**.



7. Dr.Web Account

Dr.Web account protects access to Dr.Web components and device settings with a password or a fingerprint.

The Dr.Web account password or a fingerprint is required:

- To access the following Dr.Web components:
 - Dr.Web Anti-theft.
 - Parental Control.
- To access the following application settings if Dr.Web Anti-theft is enabled:
 - **Reset settings.**
 - **Backup.**
 - **Administration.**
- To access the following settings of your device if Dr.Web Anti-theft is enabled:
 - **Settings**  > **Apps** or **Application manager** >  **Dr.Web Security Space** (for Android 6.0 or later).
 - **Settings**  > **Accessibility features.**
 - **Settings**  > **Privacy** > **Location** (for Android 6.0 or later).
 - **Settings**  > **Privacy** > **Device Administrators** >  **Dr.Web Security Space.**
 - **Settings**  > **Advanced Settings** > **Reset Settings** (settings name and location depend on your device).




On Xiaomi devices, access to the **Restrict data usage** setting is also protected.

If Parental Control is enabled on the device, the sections and settings mentioned above can be accessed by fingerprint if the **Unlock with fingerprint** option is enabled in the Parental Control settings.

You can protect access to Call and SMS filter, URL filter, and Dr.Web settings with your password (see [Parental Control](#) section).

Creating Dr.Web account

1. Tap **Menu**  in the top right-hand corner of the Dr.Web main screen.
2. Select the **Account** option.
3. On the **Account** screen, tap **Create**.
4. Enter your email address.



The email can be useful later if you forget your password. Enter an email address you have access to.

Note that you will not be able to change your email address after signing up. To use another address, you will have to delete the account and create it again with a new address.



A working internet connection is required for registering the email address.

5. Tap **Next**.
6. Set a password. The password must contain at least 4 characters.
7. Confirm the password and tap **Next**.

On the next screen, you will see a notification confirming that your account is created and registered successfully.

8. Tap **Finish**.

Managing your account

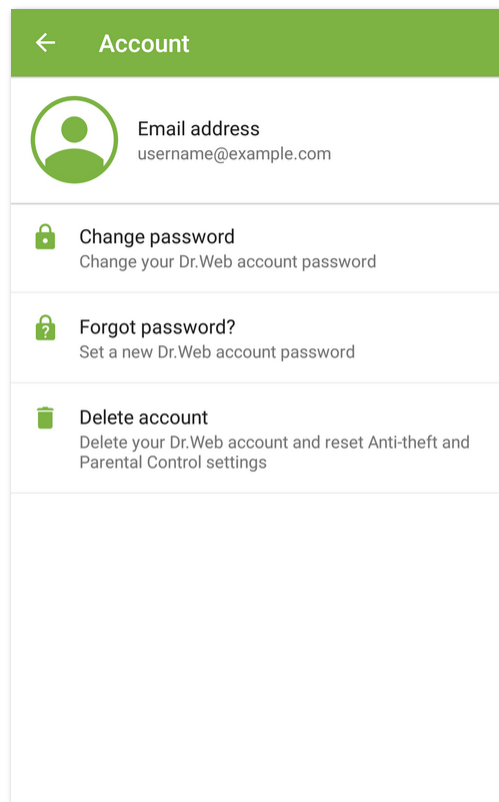


Figure 12. Account

On the **Account** screen (see [Figure 12](#)), you can do the following:

- Change your password.
- [Set a new password](#) if you have forgotten your current one.



- Delete your account.



After you delete your account, Anti-theft and Parental Control will be disabled, and their settings will be reset.

To change your password or delete your account, enter the current account password or scan your fingerprint.



8. Dr.Web Components

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

- [Scanner](#) scans your device on demand. Three scan types are available: full scan, express scan, and custom scan.
- [Call and SMS filter](#) blocks unwanted calls and SMS messages.
- [URL filter](#) restricts access to specific internet resources.
- [Anti-theft](#) allows you to locate and lock your device if it is lost or stolen.
- [Parental Control](#) restricts access to app components and installed applications.
- [Firewall](#) controls internet connections and data transfers over the network.
- [Security Auditor](#) performs system diagnostics, resolves detected security problems and eliminates vulnerabilities.




If your device does not support SIM cards (there is no slot for a SIM card on your device), **Call and SMS Filter** and **Dr.Web Anti-theft** are unavailable.

8.1. Anti-Virus Protection

- [SpIDer Guard](#) checks your file system in real time.
- [Dr.Web Scanner](#) allows you to scan your device for threats manually.
- On the [Check results](#) screen, you can select actions to neutralize the detected security threats.

8.1.1. SpIDer Guard: Real-Time Protection






SpIDer Guard is enabled automatically after you accept the License Agreement. The component keeps protecting the file system even if you close the application. If SpIDer Guard is enabled, the Dr.Web icon  is displayed on the Android status bar.

On some devices, the Dr.Web icon may not show when the app is functioning in the background. It happens because the device firmware optimizes background processes to save power or improve performance. To pin the Dr.Web icon to the Android status bar, remove background app restrictions: check your device settings and the built-in app manager settings. The settings may vary by device. Oftentimes all you need to do is tap the lock icon next to the Dr.Web app in Recent apps.

SpIDer Guard protects the file system even if the Dr.Web icon is not displayed on the Android status bar. If you install a malicious app, the component reacts and shows a notification about the threat. You can [test SpIDer Guard](#) by using the EICAR test file.



If SplDer Guard detects a suspicious change in the system area or a threat, the following items appear on the screen:


- An icon on the Android status bar in the top-left screen corner:
 -  on Android 4.4,
 -  on Android 5.0–11.0,
 -  on Android 12.0 or later.
- A pop-up notification about detection of a threat (see [Picture 13](#)).
- The  (on Android 11.0 or earlier) or  (on Android 12.0 or later) icon on the [notification bar](#).
- A message with a red indicator on the [status bar](#).

To open check results, tap the  () icon or the status bar message.



SplDer Guard will stop working if the internal device memory is cleared using the default Task Manager. To restore real-time anti-virus protection, open Dr.Web again.

To disable or re-enable SplDer Guard


1. On the Dr.Web main screen, tap **Menu**  and select **Settings**.
2. On the **Settings** screen, tap **SplDer Guard**.

SplDer Guard settings



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

To open SplDer Guard settings

1. On the Dr.Web main screen, tap **Menu**  and select **Settings**.
2. On the **Settings** screen, tap **SplDer Guard**.

Files in archives

To enable scanning of files in archives, select the **Files in archives** check box.



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



Built-in SD card and removable media

To enable scanning of the built-in SD card and removable media on each mounting, select the **Built-in SD card and removable media** check box. If the setting is enabled, the scan starts every time SplDer Guard is enabled. You will see the corresponding [notification](#).

System area

To monitor [changes in the system area](#), select the **System area** check box. If the setting is enabled, SplDer Guard monitors changes (addition, change, and deletion of files) and notifies only on deletion of any files as well as addition and change of executable files: .jar, .odex, .so, APK, ELF files, etc.

Recheck system area

To run a recheck of the system area, tap **Recheck system area**. SplDer Guard will check the previously ignored changes in the system area again.

Notifications about system area

To enable notifications on changes of any files in the system area (not only executables), select the **Notifications about system area** check box.

Additional options

To enable detection of adware and riskware (including hacktools and jokes), tap **Additional options**, then select the **Adware** and **Riskware** check boxes respectively.

Statistics

The application registers events related to the operation of SplDer Guard: enabling/disabling of SplDer Guard, threat detections, and check results of the device storage and installed applications. SplDer Guard statistics appear in the **Actions** section of the **Statistics** tab and are sorted by date (see [Statistics](#)).

Testing SplDer Guard

You can test SplDer Guard by using the 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 a 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 only the string:

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

2. Save the file with the .com extension.

As soon as you save the EICAR file on your device, a warning message from SpIDer Guard appears (see [Figure 13](#)).

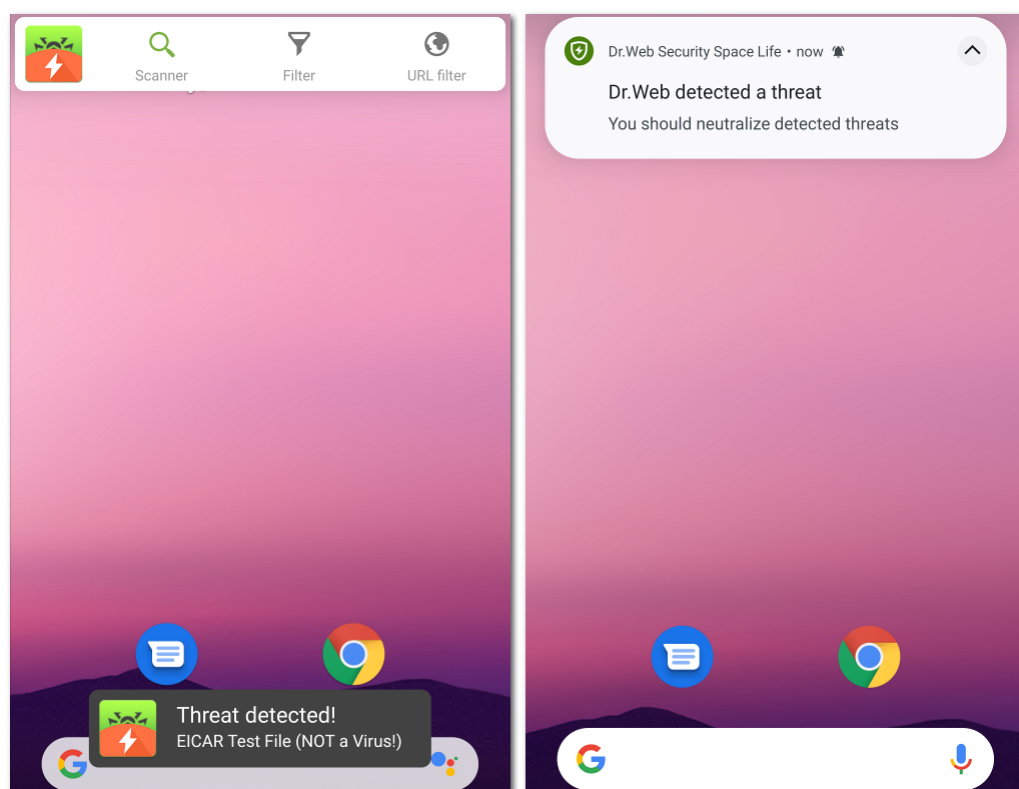


Figure 13. EICAR test file detection on Android 10.0 (left) and Android 12.0 (right)

8.1.2. Dr.Web Scanner: On-Demand Scan

On-demand scan of the file system is performed by Dr.Web Scanner. It can execute an express or full scan of the whole file system or scan critical files and folders only.

It is recommended to scan the system periodically, especially if SpIDer Guard has been deactivated for a while. Usually the express scan is sufficient for this purpose.



In the [centralized protection mode](#), Dr.Web Scanner settings may be modified or blocked in compliance with your company's security policy or according to the list of purchased services. The scan may start in accordance with a schedule set by the network administrator.

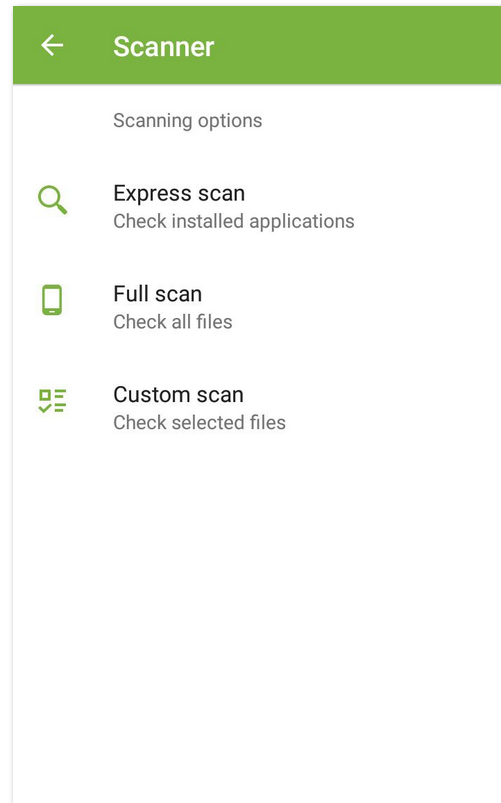


Figure 14. Dr.Web Scanner

Scanning

To scan the system, on the Dr.Web main screen, select **Scanner**. Then on the **Scanner** screen (see [Figure 14](#)), do one of the following:

- To scan only the installed applications, select **Express scan**.
- To scan all the files, select **Full scan**.
- To scan files and folders of your choice, select **Custom scan**, then select objects from the list (see [Figure 15](#)). To select all objects in the current location, use the check box at the top right. Then tap **Scan**.

If your device is rooted, you can also scan the `/sbin` and `/data` folders located in the root directory.




On devices with Android 11.0 or 12.0, to scan the `/Android/data` and `/Android/obb` folders, a permission is required for Dr.Web to access these folders.

To grant the permission to access `/Android/data` or `/Android/obb`

1. Tap **Custom scan**.
2. Select the `/Android/data` or `/Android/obb` folder on the list of objects.
3. In the dialog window, tap **Grant**.
4. Tap **Use this folder**.

On devices with Android 13.0 or later versions, the `/Android/data` and `/Android/obb` folders are system-protected and thus cannot be scanned.

If Dr.Web Scanner detects threats, the  icon appears at the bottom of the scan screen. Tap the icon to open check results (see [Figure 16](#)) and [neutralize threats](#). If you switch to another screen or application, you can open check results by tapping the icon on the [notification bar](#).

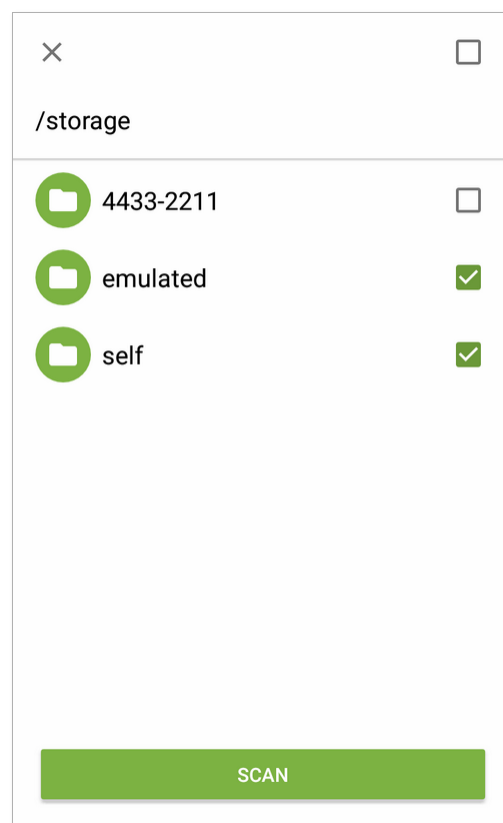


Figure 15. Custom scan



Sending suspicious files to the Doctor Web anti-virus laboratory

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

To send a file to the laboratory

1. Tap and hold the file in the hierarchical list (see [Figure 15](#)), then tap **Send to laboratory**.
2. On 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** if you think that the file was identified as a threat by mistake.
4. Tap **Send**.



The Doctor Web anti-virus laboratory accepts files of 250 MB or less.

Dr.Web Scanner settings

To access Dr.Web Scanner settings, open the [Settings](#) screen and select **Scanner**.

- To enable the scanning of files in archives, select the **Files in archives** check box.



By default, the scanning of archives is disabled. Enabling archive scanning may impact system performance and increase power consumption. Disabling archive scanning does not decrease the protection level because Dr.Web Scanner checks APK installation files even if the **Files in archives** check box is not selected.

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







Statistics

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



8.1.3. Check Results

How to open check results

- If Dr.Web Scanner detects threats, the  icon appears on the screen.
To open check results, tap the icon.
- If SplDer Guard detects a suspicious change in the system area or a threat, the following items appear on the screen:
 - An icon on the Android status bar in the top-left screen corner:
 -  on Android 4.4,
 -  on Android 5.0–11.0,
 -  on Android 12.0 or later.
 - A pop-up notification about detection of a threat (see [Figure 13](#)).
 - The  (on Android 11.0 or earlier) or  (on Android 12.0 or later) icon on the notification bar.
 - A message with a red indicator on the status bar.

To open check results, tap the  () icon or the status bar message.



On Android 5.0 or later, the threat notification will also appear on the lock screen. Tap it to access check results.

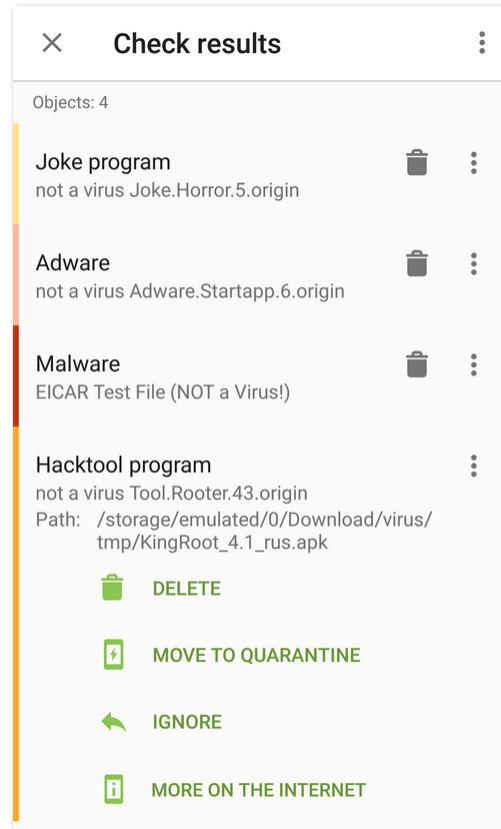


Figure 16. Check results

Neutralizing Threats

On the **Check results** screen, you can review the list of threats and changes in the system area. For each object, its type and name are specified, as well as the icon of the recommended option for the object.

Objects are marked in different colors depending on the degree of danger. Listed below are the threat types in decreasing danger order:

1. Malware.
2. Riskware.
3. Hacktool program.
4. Adware.
5. Changes in the system area:
 - New files in system area.
 - Change of system files.
 - Deletion of system files.
6. Joke program.



To view the file path, select the object. For threats that are detected in apps, the app package name is also specified.

Neutralizing all threats

To delete all threats

- In the top-right corner of the **Check results** screen, select **Menu** ⋮ > **Delete all**.

To move all threats to the quarantine

- In the top-right corner of the **Check results** screen, select **Menu** ⋮ > **All to quarantine**.

Neutralizing one threat at a time

Each object has its own set of available options. To expand the option list, select the object. Recommended options are placed first. Select one of the options:



Cure to cure the infected application.

The option is available for some [threats in system applications](#) if root access is enabled on the device.



Delete to delete the threat from your device.

In some cases, Dr.Web cannot delete applications that use Android accessibility features. If Dr.Web does not delete the app after you select the **Delete** option, reboot to safe mode and delete the app manually. If access to accessibility features has been granted to Dr.Web, the app will be deleted automatically once you select the **Delete** option.

The option is not available for [threats in system applications](#) in the following cases:

- If root access is not allowed on your device.
- If the application cannot be safely deleted.
- If a threat modification is detected. To identify if the app does pose a threat, report a false positive.



Move to quarantine to move the threat to an isolated folder (see [Quarantine](#)).

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



Ignore to temporarily leave the change in the system area or the threat as it is.




Send to laboratory or **False positive** to send the file to the Doctor Web anti-virus laboratory for analysis. The analysis will show if there is a threat or it is a false positive. If it is a false positive error, it will be fixed. To receive the analysis results, enter your email address.

If the file is sent to the laboratory successfully, the **Ignore** option is automatically applied to the object.



The **Send to laboratory** option is available only for added or changed executable files in the system area: .jar, .odex, .so, APK, ELF files, etc.

The **False positive** option is available only for threat modifications and for threats detected in the system area.

 **More on the Internet** to view the detected object description on the Doctor Web website.

8.1.3.1. Threats in System Applications

Applications installed in the system area can in some cases perform functions that are typical for malware. Therefore, Dr.Web may identify such applications as threats.

For system applications, as well as for any installed application, the **Move to quarantine** option is not available.

If a system application can be safely deleted or cured, the corresponding option is available for it if your device is rooted.

If a system application cannot be safely deleted, the **Delete** option is not available, but you can use the following guidelines:

- Stop the application from the device settings: open **Settings** > **Applications** and select the application detected as a threat. Then tap **Stop** on the application information screen.



Repeat this action every time after you restart your device.

- Stop the application from the device settings: open **Settings** > **Applications** and select the application detected as a threat. Then tap **Disable**.
- If a custom operating system (ROM) is installed on the device, you can restore the official software of your device manufacturer by yourself or in a service center.
- If you use official software of the device manufacturer, try to contact the vendor for more information on this application.
- If your device is rooted, you can try deleting the problem application using specialized utilities.

To disable notifications about threats in system applications that cannot be safely deleted, select the **System applications** check box in **Settings** > **General settings** > **Additional options**.



On Android TV, select the **System applications** check box in **Miscellaneous** > **Settings** > **General settings** > **Additional options**.



8.1.3.2. Changes in System Area

System area is a storage area that is used by system applications. It contains sensitive user data and data critical to device operation. If your device is not rooted, the system area is not available to you.

Malicious applications can gain root access and make changes to the system area: delete, add, or change files or folders.

The SplDer Guard component can monitor changes in the system area. You can enable system area monitoring in the [SplDer Guard settings](#). If the component detects suspicious changes in the system area, it notifies you about it.

Change	Name	Type
Deletion of folder with files	read-only.area.dir.deleted.threat	Deletion of system files
File deletion	read-only.area.deleted.threat	Deletion of system files
Addition of folder with files	read-only.area.dir.added.threat	New files in system area
File addition	read-only.area.added.threat	New files in system area
File modification	read-only.area.changed.threat	Change of system files

If SplDer Guard detects one of the changes listed, the files or folders themselves are not necessarily malicious. However, the change could have been made by a malicious application.

For the detected changes, the following options are available:

- [Ignore](#).
- [Send to laboratory](#) (available only if executable files have been added or changed: .jar, .odex, .so, APK, ELF files, etc.).
- [More on the Internet](#).

SplDer Guard merely informs you about the changes listed above. To detect the malicious application that could have made the change to the system area, run the [full scan](#).


8.1.3.3. Stagefright Exploits

Stagefright is an Android vulnerability that makes hacking into your device possible by means of a multimedia file with built-in malicious code.

Stagefright exploits are detected and neutralized by [Dr.Web Firewall](#). Enable it to protect your device from Stagefright exploits.



Dr.Web Firewall scans all multimedia files you download in real time. If Dr.Web detects malicious code in a file you are downloading:

- The download is stopped.
- A notification with the  icon appears at the bottom of the screen. The threat name has the postfix *<threat.name>.Stagefright*.
- Information on the detected threat is added to the [app statistics](#).

8.1.4. Device Lockers

Dr.Web protects your device from ransomware. These programs may be extremely harmful for Android smart phones and tablets. They can encrypt files located in the built-in memory or on your removable media (such as an SD card). The malicious programs can lock the device screen and display a ransom demand for decrypting and unlocking the device.

Ransomware can compromise your photos, videos, and documents. In addition, the programs may steal various information about the infected device (including IMEI) and information from the phone book of the infected device (contact names, phone numbers and email addresses) and transmit it to the cybercriminals' servers. Ransomware programs monitor incoming and outgoing communications and can block those communications if desired. All the information collected, including phone call data, is also transmitted to the control server.

Dr.Web detects and removes ransomware when it attempts to get on your device. However, the number of malicious programs increases every day. That is why it is extremely important to update Dr.Web virus databases on your device regularly, as it may prevent your device from getting infected.

If your mobile device is locked by a ransomware program and SplDer Guard is enabled on the device, you can use Dr.Web to unlock it.

To unlock your device

1. Within 5 seconds, plug and unplug a charger.
2. In the next 10 seconds, plug in earphones.
3. In the next 5 seconds, unplug earphones.
4. In the next 10 seconds, shake your device vigorously.
5. Dr.Web finishes all active processes on the device, including the one that is run by the application locker, then activates a vibration signal (on devices that have this feature). After that, the Dr.Web screen opens.



Finishing active processes can result in losing data of other applications that were active when the device was locked.

6. Once the device is unlocked, it is recommended to [update](#) the Dr.Web virus databases and perform an [express scan](#) of the system, or to delete the malicious application.



8.2. Call and SMS Filter

Call and SMS filter blocks unwanted calls and SMS messages including advertising messages, calls and messages from unknown and private numbers.

You can enable either the blocking or the allowing filter.

- Blocking filter blocks the added contacts or keywords. In addition, you can add [masks](#) to the blocking filter.
- Allowing filter allows calls and SMS only from added contacts.

By enabling one filter you disable the other.

For filtering, you can select one of the standard lists or create your own.



SMS filter does not work in app versions from Google Play.

The filter may not work correctly on devices with two SIM cards.

SMS filter may not work correctly due to system restrictions of Android. Blocked messages might appear in the SMS log.

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

Permissions

Once you enable Call and SMS filter, it can request the following permissions:

- Access your contacts.
- Make and manage phone calls.
- Send and view SMS messages.

Tap **Allow** in each window.

On devices with Android 9.0 and later, Call and SMS filter also requests access to the call log.

On devices with Android 10.0 and later, Call and SMS filter also requests the permission to use Dr.Web as the default caller ID and spam app.

The component does not work without the required permissions.



If you use a Xiaomi phone with installed **Security** app, grant Dr.Web the permission to manage SMS messages in this app.




8.2.1. Blocking Filter

Blocking filter blocks calls and SMS from added contacts.






How to use blocking filter

- Enable the **Block all** option to block all incoming calls and SMS messages.
- Add contacts to **Black List**.
- Create your own lists.


To create a list

1. Open blocking filter.
2. Tap the  icon.
3. Specify a list name.
4. Add contacts or keywords. You cannot save an empty list.

To add contacts to the list

1. On a screen with the necessary list, tap the  icon. Select one of the options:
 -  **Contacts** to add a contact from your contacts on your device.
 -  **Call log** to add a contact from your recent calls. Available only in the version downloaded from the website.
 -  **SMS log** to add a contact from your recent SMS messages. Available only in the version downloaded from the website.
 -  **Keyword** to add a keyword for blocking SMS messages. Available only in the version downloaded from the website.

Dr.Web will check all incoming text messages for the word or phrase you have added. If you want the application to block messages by words that may not stand next to each other, add them one by one.

 **Private number** to block calls from any hidden numbers. Available only in the version from Google Play. In the version from the website and from Huawei AppGallery, you can add a hidden number from your call or SMS log.

 **New contact** to create a new contact or [mask](#).

 **Import contacts** to import a contact list that was saved earlier.

2. If necessary, edit a name and phone for each contact, select what to block: **Calls** or **SMS**. You cannot edit a private number or number added from your contacts.

To save contacts from a list to a device

1. Select the necessary list.





2. Tap the  icon in the top right corner.

Masks

Masks let you block similar numbers:

- Numbers beginning with a certain sequence of digits (or other characters)
- Numbers ending with a certain sequence of digits (or other characters)
- Numbers containing a certain sequence of digits (or other characters)

To add a mask

1. On a screen with the necessary list, tap the  icon and select  **New contact**.
2. If necessary, edit a name.
3. When typing a number, use a star * at the beginning, end, or both.
A star replaces any sequence of characters. Do not use a star in the middle of a number or two stars in a row: such mask will not work.
4. Select what to block: **Calls** or **SMS**.

Mask examples

Example	Description
+7*	All numbers beginning with +7
0	All numbers containing 0 at the beginning, in the middle or at the end of the number
*0	All numbers ending with 0
* +7*0 *0*0 **0 +7**	Examples of incorrect masks

8.2.2. Allowing Filter


Allowing filter allows calls and SMS only from the added contacts.

How to use allowing filter







- Enable the **Contacts** option to accept calls and SMS messages only from your contacts.
- Create your own lists.




To create a list

1. Open allowing filter.
2. Tap the  icon.
3. Specify a list name.
4. Add contacts. You cannot save an empty list.

To add contacts to the list

1. On a screen with the necessary list, tap the  icon. Select one of the options:
 -  **Contacts** to add a contact from your contacts on your device.
 -  **Call log** to add a contact from your recent calls. Available only in the version downloaded from the website.
 -  **SMS log** to add a contact from your recent SMS messages. Available only in the version downloaded from the website.
 -  **New contact** to create a new contact.
 -  **Import contacts** to import a contact list that was saved earlier.
2. If necessary, edit name and phone for each contact. You cannot edit a number added from your contacts.

To save contacts from a list to a device

1. Select the necessary list.
2. Tap the  icon in the top right corner.

8.2.3. Editing Lists

To edit a list

1. Tap the list you need to edit.
2. Make changes.
3. Tap **Save**.


To delete a list

- Swipe the list name to the left.

If you accidentally delete a wrong list, you can restore it by tapping **Undo**. You cannot delete the standard lists.




To delete several lists

1. Tap and hold one list.
2. After a vibration, tap other lists you need to delete.
3. Tap the  icon in the top right corner.

To delete a contact from the list

- Swipe it to the left.

To delete several contacts from the list

1. Tap and hold one contact.
2. After a vibration, tap other contacts you want to remove from the list.
3. Tap the  icon in the top right corner.


To cancel an accidental contact deletion, tap **Undo**.



A contact deleted from the list is not deleted from your contacts on your device.

8.2.4. Blocked Calls and SMS

To open a list of blocked calls and SMS messages

1. On the Dr.Web main screen, select **Call and SMS filter**.
2. Tap **Menu**  and select **Blocked calls** or **Blocked SMS**.

If calls or SMS messages are blocked, the corresponding information is displayed on the [status bar](#). To view details, tap **More** on the status bar.

The following information is available for each blocked call and SMS message:

- Date and time of the call or SMS.
- Number and name of the caller or SMS sender.
- Text of the message.

Actions available for blocked calls and SMS

To call

1. Tap the number in the list of blocked calls or SMS.
2. Tap **Call**.




To send SMS

1. Tap the number in the list of blocked calls or SMS.
2. Tap **Send SMS**.

To delete a call or SMS message

- Swipe it to the left.

To delete all calls or SMS messages

1. At the top right, tap **Menu** .
2. Tap **Clear the list**.

8.3. URL Filter

URL filter controls access to websites. URL filter lets you restrict access to unwanted internet resources. To configure URL filter, you can select specific websites or website categories.

In an attempt to open a restricted webpage, you will see a relevant notification and will not be able to access its contents.



URL filter operates in a default Android browser as well as in Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser, and Atom.

Enabling URL filter

On the Dr.Web [main screen](#), tap **URL filter** (see [Figure 17](#)).

URL filter may request access to Android accessibility features in order to work in one of the supported browsers. Without this access, URL filter will not be able to operate.

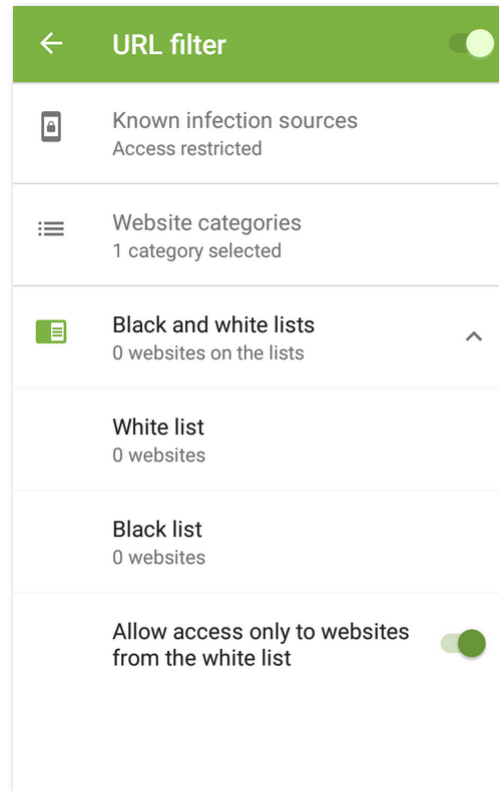


Figure 17. URL filter

Website categories

Dr.Web allows you to select specific website categories with a restricted access. Open the **Website categories** list and select necessary categories:

- Non-recommended sites
- Adult content

If you select this option, you will enable *safe search* in Google, Yandex, Bing, Yahoo, and Rambler. It means that adult content will be completely excluded from the search results.

- Violence
- Weapons
- Gambling
- Drugs
- Obscene language
- Online games
- Terrorism
- Email
- Social networks
- Chats



- URLs listed due to a notice from the copyright owner
- Anonymizers
- Cryptocurrency mining pools




By default, URL filter restricts access to websites known as infection sources.

Black and white lists

You can configure lists of websites with restricted or permitted access. This access will not depend on other URL filter settings. By default, the lists are empty.

To add a website to a black or white list

1. In the URL filter screen, open the **Black and white lists** section.
2. Select a list.
3. Tap the  icon in the bottom right-hand corner.
4. Specify a website URL in any of the following formats:
 - example.com
 - http://example.com
 - https://www.example.com
 - www.example.com



You can add only specific website URLs. Adding masks or keywords is not supported.

5. Tap **Add URL**.

If you try to add a URL that is already on the opposite list, you will be prompted to move it.

Allow access only to websites from the white list

Enable this option to be able to view only those websites you have added to the **White list**. Access to other websites will be restricted.



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



8.4. Dr.Web Anti-Theft

Dr.Web Anti-theft allows you to manage your device if it is lost or stolen. For example, you can remotely remove your personal data, locate the device or lock it. To unlock the device, enter your password:

- to your [Dr.Web account](#) if it is set up,
- to Anti-theft if the account is not set up yet.

How to manage your device using Dr.Web Anti-theft

- [Configure Dr.Web Anti-theft](#) in advance. For example, enable device lock if a SIM card is changed.
- Send a [command](#) to Dr.Web Anti-theft, for example, to locate the device.


8.4.1. Enabling Dr.Web Anti-Theft

1. On the Dr.Web main screen, select **Anti-theft**.
2. On the **Anti-theft** screen, tap **Enable**.
3. If it is the first time you enable Dr.Web Anti-theft, allow the app to access Android accessibility features as well as your device features and data.



If you use the app version downloaded from [Doctor Web website](#) on a Xiaomi phone with installed **Security** app, grant Dr.Web the permission to manage SMS messages in this app.

Dr.Web Anti-theft works only if all permissions are granted.

4. If Dr.Web account is not created on your device, [create it](#).
If the account is already created, enter your account password. If you enter an incorrect password 10 times in a row, the password field will be temporarily blocked. You will see how much time is left until the next attempt.
5. If Dr.Web is not a device administrator, activate the app as an administrator:
 - To avoid unwanted app deletion.
 - To allow Dr.Web Anti-theft to reset device settings to default. This protects your personal data if the device is lost or stolen.
6. To [add buddies](#), tap the  icon. [Buddies](#) help you manage your device remotely if the device is lost or stolen or if you forget your Dr.Web account password. Tap **Next**.
7. Edit the text that will be displayed on locked screen. You can also specify how to contact you to return the device to you here. Tap **Next**.
8. Edit the notification text that your buddies will receive if Dr.Web Anti-theft locks your device and you forget your password. Tap **Next**.
9. Enable the necessary settings and tap **Finish**.




8.4.2. Configuring Dr.Web Anti-Theft



In the [centralized protection mode](#), some features of Dr.Web Anti-theft can be modified or blocked for compliance with your company security policy or according to the list of purchased services.

To open Anti-theft

1. On the Dr.Web main screen, select **Anti-theft**.
2. If the  icon is displayed next to the password field, touch the fingerprint sensor.

If fingerprint authentication is unavailable, enter your Dr.Web account password. If you enter an incorrect password 10 times in a row, the password field will be temporarily blocked. You will see how much time is left until the next attempt.



If you upgrade to version 12, your Dr.Web Anti-theft password automatically becomes your Dr.Web account password.

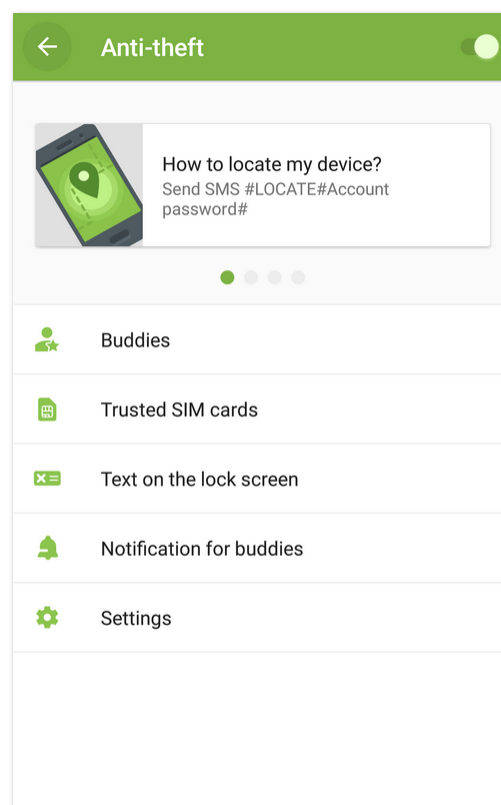


Figure 18. Dr.Web Anti-theft



Cards with SMS commands



Available only in the version downloaded from the Doctor Web [website](#).

Cards with [SMS commands](#) are located at the top of the **Anti-theft** screen (see [Figure 18](#)).

- To view all commands, swipe the cards to the right.
- To open a detailed description of an SMS command or [to send a command](#), tap the card with the command.

Buddies

Buddies are contacts you trust to manage your device with [commands](#), or contacts that trust you. In the app, buddies are separated into two tabs: [I trust](#) and [They trust me](#).

I trust





On this tab, you can see the list of buddies you trust to manage your device with commands. You have added these contacts as buddies using their phone numbers or email addresses.

Icon	App version	Description
	Website version	You have added a phone number. The buddy can send SMS commands to your device without a password.
	Any	You have added an email address. The buddy has confirmed your buddy request. Now they can send push commands to Dr.Web Anti-theft. To confirm your request, the buddy needs to have Dr.Web Security Space or the free Dr.Web Light installed on their device. Your request may have gone unnoticed. Send another request if necessary.
	Any	You have added an email address. The buddy has confirmed your buddy request. Now they can send push commands to Dr.Web Anti-theft. <ul style="list-style-type: none">• If Dr.Web Security Space is installed on your buddy's device, the buddy can send any commands.• If Dr.Web Light is installed on your buddy's device, the buddy can help unlock your device if it gets locked and you forget your password.
	Any	You have added an email address, but the buddy has rejected your buddy request. They cannot send push commands to Dr.Web Anti-theft. In this case, you can remove the contact from your buddy list.

To add a buddy



- On the **I trust** tab, tap the icon.



- **For the app version from the Doctor Web website.** Add a phone number. SMS commands can be sent to your device without a password from this number. Select one of the options:
 -  **Contacts**—select a contact from the contacts on your device.
 -  **Call log**—select a phone number from recent calls.
 -  **Call log**—select a phone number from recent messages.
 -  **New contact**—enter a new phone number.
- **For any app version.** Add an email address. An email with your buddy request will be sent to the address. The request can be confirmed in either Dr.Web Security Space or the free Dr.Web Light app. Once they confirm your request, your buddy can send commands to Dr.Web Anti-theft using notifications. If your device is locked, unlock commands and reset password commands can be sent from Dr.Web Light. Any command can be sent from Dr.Web Security Space.

You can add up to five email addresses. In the version downloaded from the Doctor Web website, you can add up to five phone numbers.

To edit a buddy's contact

1. Select the contact on the **I trust** tab.
2. Tap the  icon.
3. Edit the contact info.
4. Tap the  icon to save the changes.



You cannot edit a buddy's profile if they rejected your buddy request.

To remove a buddy

- Swipe the contact to the left.




If you accidentally remove the wrong contact from the list, you can restore it by tapping **Undo**.

They trust me

The **They trust me** tab contains the list of buddies who trust you to manage their devices. They added you as a buddy in Dr.Web Anti-theft using your email address. Confirm the buddy request to be able to manage your buddy's device remotely.



Buddy request statuses

Icon	Description
	You have not confirmed the buddy request yet. Confirm the request to be able to send push commands to the buddy's device.
	You have confirmed the buddy request. You can manage your buddy's device remotely using push commands .
	You have been removed from the buddy list. Your buddy needs to send you another request for you to be able to send push commands .

To confirm a buddy request

Do one of the following:



- Tap the request notification that you received after someone added you as a buddy and then tap **Confirm**.
- Select the contact on the **They trust me** tab and tap **Confirm**.

To reject a buddy request

Do one of the following:

- Tap the request notification that you received after someone added you as a buddy and then tap **Decline**.
- Select the contact on the **They trust me** tab and tap **Decline**.
- Remove the contact from your buddy list.

To edit a buddy's contact

1. Select the contact on the **They trust me** tab.
2. Tap the  icon.
3. Edit the contact info.
4. Tap the  icon to save the changes.



You cannot edit a buddy's profile if they removed you from their buddy list.

To remove a buddy

- Swipe the contact to the left.

If you accidentally remove a contact of your buddy whose buddy request you have not confirmed yet, you can restore the contact by tapping **Undo**.



To unlock a buddy's device

1. Tap the notification you received from your buddy.
2. Contact your buddy to obtain the verification code. Do not trust messages that contain the verification code. They can be sent by fraudsters.
3. Enter the verification code.
4. Tap **Unlock**.

Trusted SIM cards

Trusted SIM cards are the SIM cards you use on your device. By default, Anti-theft is configured to lock your device if it detects a SIM card that is not found on the trusted list. In this case, even if your device is stolen, an attempt to use another SIM card will make the device impossible to use. If you change your SIM card to another trusted SIM card, Anti-theft will not lock your device.

If you use two SIM cards on a device with Android 5.1 or later, both SIM cards are added to the trusted list automatically. If you use a device with Android 5.0 or earlier, you can add only one SIM card to the trusted list (you cannot add both SIM cards at the same time).

For every SIM card on the list, its name, as well as its ID number (on devices with Android 5.0 or earlier) or the mobile network operator (on devices with Android 5.1 or later) are displayed.

New SIM cards are added to the trusted list when you reboot your device or launch Dr.Web.

Tap **Trusted SIM cards** to open or edit the list:

- For more detailed information on a SIM card, tap it on the list. Depending on the OS version, the following fields may be available: name, operator, ID.
- To rename a SIM card, tap it on the list. On the SIM card details screen, enter a new name in the **Name** field and tap **Save**.
- To remove a SIM card from the trusted list, swipe it left.



You cannot remove a SIM card that is currently used on your device.

Text on the lock screen

Here you can change the text that will be displayed on the screen of your locked device if it gets lost or stolen. For example, you can specify your other phone number or your email address.



To edit the text on the lock screen

- Tap **Text on the lock screen**, edit the text and then tap **Save**.

Notification for buddies

Notification for buddies is a notification that you can send to your buddies if your device is locked by Dr.Web Anti-theft and you forget your password. After your buddies receive your notification, they need to get the verification code from you to reset your password. After that, you will be able to set a new password.

To change the notification text

- Tap **Text on the lock screen**, edit the text and then tap **Save**.

Settings

Lock after restart

This option is disabled by default.

Enable this option to force Dr.Web Anti-theft to lock your device after every reboot. To unlock your device, you will be prompted to enter your Dr.Web account password. Your device will stay locked until you enter your password.

Lock if SIM card is changed

This option is enabled by default.

Dr.Web Anti-theft will lock your device as soon as it detects a SIM card that is not on the trusted SIM card list. To unlock your device, you will be prompted to enter your Dr.Web account password. Your device will stay locked until you enter your password.

Inform buddies if SIM card is replaced



Available only in the version downloaded from the Doctor Web [website](#).

This option is disabled by default.

Enable this option to make Dr.Web Anti-theft send SMS messages to your buddies when a SIM card which is not on the trusted list is detected on your device. Dr.Web Anti-theft also identify the phone number linked to the SIM card.



Anti-theft resends SMS messages to your buddies at every device reboot with the changed SIM card. Anti-theft can send a maximum of five of such SMS broadcasts a day.

Remove data

This option is disabled by default.

If your device is stolen and locked, a stranger can try to unlock it by means of a direct password search. In order to protect your data, enable the **Remove data** option.

After 10 failed attempts to enter the password on a locked device:

- If Dr.Web is activated as a device administrator, Dr.Web will trigger a factory reset. This uninstalls all of your apps and removes your personal data, photos and videos, messages and contacts. Information on your SD card will also be removed. Note that a factory reset will also uninstall Dr.Web from your device.
- If Dr.Web is not activated as a device administrator, your personal data will be deleted (except for your SMS since Dr.Web is not set as the default app for sending and receiving messages). Dr.Web will not be uninstalled and will continue to lock your device.

No SIM mode

This mode is enabled when a SIM card is missing on your device or when your device configuration blocks access to SIM card information for installed apps. This concerns devices that feature a SIM card slot.

Once Dr.Web Anti-theft detects that it has no access to SIM card information, you are prompted to enter your Dr.Web account password. The notification bar also shows a notification that a SIM card is not found. Enter your Dr.Web account password to make the no SIM card mode trusted. You will not be able to send SMS commands, but the other Anti-theft functions will be available.

8.4.3. Dr.Web Anti-Theft Commands

Use Dr.Web Anti-theft commands to manage your device remotely.

- [Push commands](#) are sent via push notifications and are not displayed on the recipient's device.
- [SMS commands](#) are sent via SMS messages and are displayed on the recipient's device.



Anti-Theft commands requirements

Device	Push commands	SMS commands
Sender	Device with any app version. Anti-theft is enabled, the recipient's buddy request is confirmed in Anti-theft.	Dr.Web is not required to be installed. <ul style="list-style-type: none">Any device if the password is specified in the command.Device with a phone number that is added to the recipient's Buddy list if the password is not specified in the command.
Recipient	Device with any app version. Anti-theft is enabled.	Device with the app version from the website or with the version from HUAWEI AppGallery. Anti-theft is enabled.



The **Show on Lock screen** system setting found on some devices may prevent you from entering your Dr.Web account password on a device that was blocked with a command. This setting is disabled by default. If you have enabled it, open your device settings, select **Apps > Dr.Web > Other permissions**, and disable the **Show on Lock screen** setting.

8.4.3.1. Push Commands

What are push commands

Push commands are commands for managing Dr.Web Anti-theft that are sent over Android push notifications. Push notifications that contain push commands are not displayed on the recipient's device but they are processed by the app.



Please note that correct operation of push commands is not guaranteed in the app version from Huawei AppGallery installed on non-Huawei devices. That is because outdated mobile services might be used for sending push commands.

What is required to use push commands

1. To send and receive push commands, the devices must be connected to the internet.
2. The Dr.Web Security Space app must be installed on the recipient's device. Dr.Web Security Space or Dr.Web Light must be installed on the sender's device.
3. Anti-theft must be enabled on the recipient's device.
4. A push command can be sent only from a device where the recipient's buddy request has been confirmed before.
 - From the Dr.Web Security Space app, a buddy can send any push commands.



- From the Dr.Web Light app, a buddy can unlock the recipient's device by using the Help Your Buddy component.

To send a push command

1. On the **Anti-theft** screen, tap **Buddies**.
2. Select the **They trust me** tab.
3. Select a buddy whose device you want to send a command to.
4. Select a command.



Push command delivery might take up to 15 minutes.

Commands



The **Show on Lock screen** system setting found on some devices may prevent you from unlocking a device locked with a command. Make sure in advance that this setting is [disabled](#).

Command	Action
Locate device	<p>Get coordinates of the mobile device.</p> <p>You will receive a notification with a link to a map showing the device location.</p> <p>When you tap the link, the special Doctor Web service called Dr.Web Anti-theft Locator opens a browser tab with a map and the location of your device on the map. The location accuracy depends on the GPS receiver, Wi-Fi networks and GSM transmitting stations. Thus, depending on the available data, the received coordinates may be exact (showing a position on the map) or approximate (showing a circle).</p> <p>You can select a map service from the list at the top of the map page.</p>
Lock device	<p>Lock the device. To unlock it, the Dr.Web account password needs to be entered.</p>
Lock device and turn on a sound alert	<p>Lock the device and enable a sound alert that is impossible to switch off even by rebooting the device. To unlock it, the Dr.Web account password needs to be entered.</p>
Remove data	<p>Remove all data from the device. If Dr.Web is activated as an administrator on the buddy's device, the command will restore the default device settings.</p> <p>This action is also performed if your device is locked and the Remove data option is enabled in the Dr.Web Anti-theft settings.</p>



Command	Action
Reset password	Unlock the device and reset Dr.Web account password. To send the command, a verification code is required. The code is displayed on the buddy's device .

8.4.3.2. SMS Commands



You can only send SMS commands to devices with the app version installed from the Doctor Web [website](#).

In order for SMS commands to work on a Xiaomi phone with the **Security** app installed, Dr.Web has to have the permission to manage SMS in this app.

You can manage Dr.Web Anti-theft remotely by sending SMS commands. SMS commands allow you to get the location of a device, lock it, or delete personal data.

You can send an SMS command as follows:

- If you specify your password—from any device.
- Without specifying your password—from your [buddy's phone](#).

It is not recommended to send SMS commands with your password to a lost or stolen device. Cybercriminals can view the SMS with the password and unlock the device. To send an SMS command without a password, [add phone numbers](#) to your buddy list in advance.

SMS commands



The **Show on Lock screen** system setting found on some devices may prevent you from unlocking a device locked with a command. Make sure in advance that this setting is [disabled](#).

Command	Action
#LOCK# <i>Password#</i>	Locks the device. In response to the command, you will receive the following SMS message: "Dr.Web Anti-theft - The <device name> phone is locked".
#SIGNAL# <i>Password#</i>	Locks the device and enables a sound alert that is impossible to switch off even by rebooting the device. In response to the command, you will receive the following SMS message: "Dr.Web Anti-theft - The <device name> phone is locked".
#LOCATE# <i>Password#</i>	Requests the coordinates of the device that you will receive in an SMS message.



Command	Action
	<p>This SMS contains a link to a map showing the device location.</p> <p>When you tap the link, the special Doctor Web service called Dr.Web Anti-theft Locator opens a browser tab with a map and the location of your device on the map. The location accuracy depends on the GPS receiver, Wi-Fi networks and GSM transmitting stations. Thus, depending on the available data, the received coordinates may be exact (showing a position on the map) or approximate (showing a circle).</p> <p>You can select a map service from the list at the top of the map page.</p>
#UNLOCK#Password#	Unlocks the device without resetting the Dr.Web account password.
#WIPE#Password#	<p>Restores the factory settings of the device and deletes all data from the device memory and the SD card.</p> <p>In response to the command, you will receive the following SMS message: "Dr.Web Anti-theft - Deleting data on the phone <device name>".</p> <p>This action is also performed if your device is locked and the Remove data option is enabled in the Dr.Web Anti-theft settings.</p>
#RESETPASSWORD#	Unlocks the device and sets a new password. This command can be performed only if sent from a number from the buddy list.



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

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

Sending SMS commands via Dr.Web Anti-theft

Using Dr.Web Anti-theft, you can send SMS commands to devices on which Dr.Web Anti-theft is also enabled.

To send an SMS command

1. On the **Anti-theft** screen (see [Figure 18](#)), tap any [card with an SMS command](#).
2. Tap **Send SMS command**.
3. On the **Sending SMS command** screen:
 1. From the **Command** list, select a necessary command:
 - **Lock device**—corresponds to the [#LOCK#](#) command.
 - **Lock device and enable sound alert**—corresponds to the [#SIGNAL#](#) command.



- **Track device location**—corresponds to the [#LOCATE#](#) command.
 - **Unlock device**—corresponds to the [#UNLOCK#](#) command.
 - **Delete all data**—corresponds to the [#WIPE#](#) command.
 - **Unlock and set a new password**—corresponds to the [#RESETPASSWORD#](#) command.
2. In the **To** field, specify the recipient's phone number.
 3. In the **Recipient's password** field, enter the recipient's account password.
If your phone number is on the recipient's [buddy list](#), you can leave the field blank.
 4. On the **From** list, select a SIM card that you want to send the command from.
The option is available on devices with two SIM cards with Android 5.1 or later.
 5. Tap **Send**.

8.4.4. Disabling Dr.Web Anti-Theft

To disable Dr.Web Anti-theft

1. On the Dr.Web main screen, select **Anti-theft**.
2. Enter your Dr.Web account or Anti-theft password.
3. On the **Anti-theft** screen (see [Figure 18](#)), use the toggle button in the top-right corner of the screen to disable Dr.Web Anti-theft.
4. In the next window, tap **OK**.



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

8.5. Parental Control

Using Parental Control, the Dr.Web account owner can restrict access to any application or group of applications installed on the device and to Dr.Web component settings.

How Parental Control works

The Dr.Web app must be installed on the device of the user whose access to apps and Dr.Web component settings you want to restrict. You activate the Parental Control component on the user's device and provide your Dr.Web account details. After activating the component, you create rules restricting the device owner's access to apps, app groups or Dr.Web component settings. When attempting to launch a blocked app or access component settings, the device user sees the [blocked app screen](#) or the account login screen. A blocked app or component can be accessed only by entering your Dr.Web account password or scanning your fingerprint.



Parental Control main features

Parental Control allows you to:

- block access to an app or group of apps;
- block access to Dr.Web component settings;
- restrict access to an app or group of apps within a set time interval;
- create custom app groups;
- keep track of events related to blocked apps and components.

Enabling Parental Control

To enable Parental Control

1. On the Dr.Web main screen, select **Parental Control**.
2. If a Dr.Web account has not been created on the device yet, [create it](#).
If the account is already created, enter the account password. If you enter an incorrect password 10 times in a row, the password field will be temporarily blocked. You will see how much time is left until the next attempt.
3. On the **Parental Control** screen, tap **Enable**.
4. If Dr.Web is not a device administrator, activate the app as an administrator:
 - To avoid unwanted app deletion.
 - To allow Dr.Web Anti-theft to reset device settings to default. This protects your personal data if the device is lost or stolen.

Disabling Parental Control

To disable Parental Control

1. On the Dr.Web main screen, select **Parental Control**.
2. Enter your Dr.Web account password.
3. Disable Parental Control using the toggle button in the top-right corner of the screen and tap **OK**.

Training mode

The top part of the Parental Control main screen (see [Figure 19](#)) displays mini-slides that allow you to go to the training mode. The training mode helps you quickly learn how to use the main features of Parental Control.

The training mode consists of four sections:



- [Apps](#): blocking access to apps and app groups.
- [Time-restricted access](#): restricting access to apps and app groups for the specified time.
- [Components](#): blocking access to Dr.Web component settings.
- [Settings](#): Parental Control settings and log.

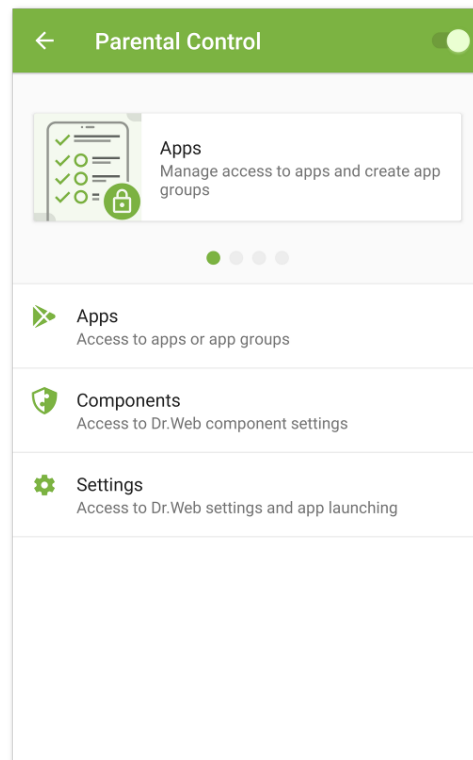


Figure 19. Parental Control

Each of the mini-slides leads to a training mode section. Swipe a mini-slide left or right to move to the next or previous mini-slide. Tap the mini-slide to open the corresponding training mode section.

In the training mode, you can view fullscreen slides that tell you how to use the main features of Parental Control (see [Figure 20](#)). Swipe the current slide left to move to the next one.

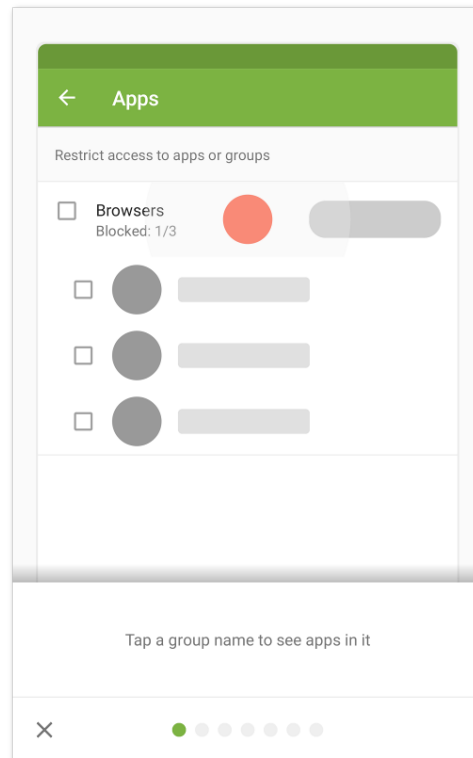



Figure 20. Training mode slide

To exit the training mode, tap  in the bottom-left corner of the screen.

8.5.1. Blocking Access to Apps and Components

Apps

The **Apps** section contains the list of all apps installed on the device.

Blocking access to apps and app groups

The Parental Control component allows you to block access to individual apps or app groups. When an app with blocked or restricted access is launched, the [blocked app screen](#) appears. The screen prevents access to the app itself. The app can only be accessed by entering the Dr.Web account password or by scanning your [fingerprint](#).

To block access to an app or all apps in a group, select the check box next to the name of the app or app group. To restore access, clear the check box.



App groups




By default, all apps are separated into system groups by category. To see apps within a group, tap the group name.



On devices with Android 8.0 or earlier, all apps are found in the **Other** system group.



You can also create your own app groups.

To create a user app group


1. Tap the  icon in the bottom-right corner of the screen.
2. Select the **New group** option.
3. Enter the name of the new group.
4. Tap the  icon next to the apps you want to add to the new group.
5. Tap the  icon to save the new group.

User-defined groups are displayed at the top of the app group list.


To edit a user group

1. Swipe the group name left.
2. Tap the  icon.
3. Make changes.
4. Tap the  icon in the top-right corner of the screen.

To delete a user group

1. Swipe the group name left.
2. Tap the  icon.

To delete multiple user groups

1. Tap and hold the name of one of the groups to be deleted.
2. Select the other groups to be deleted.
3. Delete the groups by tapping the  icon in the top-right corner of the screen.



System groups cannot be edited or deleted.




If the **Block browsers without URL filter** or **Block new apps** option is enabled in the [Parental Control settings](#), the **Browsers without URL filter** or **New apps** system group will appear on the app list. To restore access to apps in these groups, disable the corresponding option in the Parental Control settings.

Searching through the list of apps

You can use the search function to navigate the app list.

To search by app or app group name

1. Tap the  icon in the bottom-right corner of the screen.
2. Select the **Search** option.
3. Enter your query in the search field at the bottom of the screen.

Time-restricted access



You can block access to app groups all the time or in the set time intervals.

Restriction type is shown to the right of the group name. Two restriction types are available:

- **Always**—access to the app group is always blocked.
- **Interval**—access to the app group is blocked within a set time interval.

By default, when blocking an app group, the access is always blocked.

To set a time-based restriction



1. Tap the restriction type to the right of the app group.
2. Tap  in the bottom-right corner of the screen.
3. Select the days of the week when the restriction will be active.
4. Tap **Start** and set the start of the interval when access will be blocked.
5. Tap **OK** to confirm the selected time.
6. Tap **End** and set the end of the interval when access will be blocked.
7. Tap **OK** to confirm the selected time.
8. Tap  in the top-right corner of the screen to save the restriction.

Only one time interval can be set for one restriction. To block the app group at other times, create more restrictions.


You can edit and delete restrictions.



To edit a restriction

1. Tap the restriction type to the right of the app group.
2. Swipe the restriction left.
3. Tap the  icon.
4. Make changes.
5. Save the changes by tapping the  icon in the top-right corner of the screen.

To delete a restriction

1. Tap the restriction type to the right of the app group.
2. Swipe the restriction left.
3. Tap the  icon.

Components

In addition to apps and app groups, you can also block access to Dr.Web component settings: Call and SMS Filter, URL filter, Firewall, and the Dr.Web app settings.

To block access to Dr.Web component settings

1. On the Parental Control main screen, select **Components**.
2. Select the check boxes next to the Dr.Web components you want to block access to:
 - [Call and SMS Filter](#). Allows the account owner to configure lists of phone numbers the device user will be able to receive calls and messages from. For example, you can allow calls and SMS messages from specific numbers or only from numbers from the contact list. The device user will not be able to change the list of the allowed or blocked numbers.
 - [URL Filter](#). Allows the account owner to restrict access to specific websites as well as website categories (e.g., Drugs, Weapons, Terrorism, Adult content, etc.). The device user will not be able to change the list of websites and website categories they have access to.
 - [Firewall](#). Allows the account owner to limit the use of mobile traffic, monitor data transmission, and manage internet connections established by apps on the user device. The user will not be able to change any rules and restrictions.
 - [Dr.Web Settings](#). Allows the account owner to restrict access to Dr.Web settings for the device user. For example, the user will not be able to reset Dr.Web settings.



Time-restricted access is not available for Dr.Web components. Access will be blocked at all times.

To access a blocked component, enter the Dr.Web account password or scan your fingerprint (if the [corresponding setting](#) is on).

Blocked app screen

The blocked app screen appears when a blocked app is launched (see [Figure 21](#)). To access the app, enter the Dr.Web account password and tap **Unlock**. Access to the app can be granted by means of scanning a fingerprint if the **Unlock with fingerprint** option is enabled in the [Parental Control settings](#).

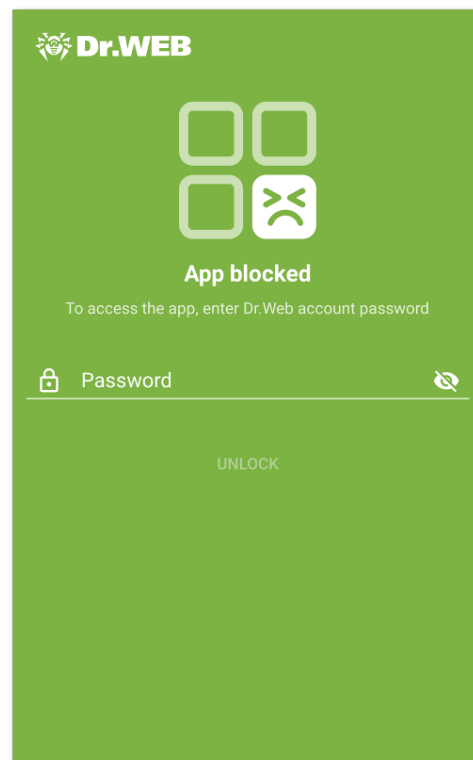


Figure 21. Blocked app screen

New apps

If the **Block new apps** option is enabled in the Parental Control settings, all apps installed after enabling the option will be placed into the **New apps** system group. When an app from the **New apps** group is launched, the blocked app screen shows an option that allows you to grant access to the app from now on.

To allow access to a new app

1. Launch the app.
2. On the blocked app screen, enter your Dr.Web account password.
3. Select the check box next to the **Remove from "New apps" group** option.
4. Tap **Unlock**.

8.5.2. Parental Control Settings

You can access the **Settings** section (see [Figure 22](#)) from the main screen of the component. The section allows you to manage Parental Control settings, as well as open the Parental Control log.

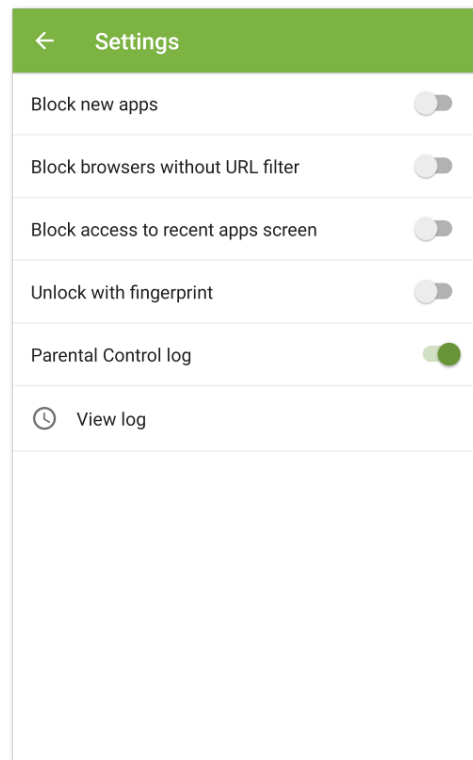


Figure 22. Parental Control settings

In the **Settings** section, the following options are available:

- **Block new apps.** Allows you to block access to apps installed after enabling this option. New apps are added to the **New apps** system group. Access to apps from this group is always blocked.



You can grant access to an individual app by using the **Remove from “New apps” group** option on the blocked app screen.

- **Block browsers without URL filter.** Allows you to block access to [browsers not supported by URL filter](#). The browsers are added to the **Browsers without URL filter** system group. Access to apps from this group is always blocked.



URL filter must be enabled before enabling this option.

- **Block access to recent apps screen.** Allows you to block the recent apps screen. The blocked app screen will be shown when the recent apps screen is opened.



The option might not work as intended if you use a third-party system shell.

- **Unlock with fingerprint.** Allows you to use your fingerprint instead of the Dr.Web account password for gaining access to apps and components.



Before enabling this option make sure that only the Dr.Web account owner's fingerprints are registered on the device.

After multiple fingerprint recognition errors, the fingerprint sensor will be disabled. To enable it again, unlock the device by means of another unlock option (pattern, PIN code, or password).

- **Parental Control log.** Enables the [Parental Control log](#). Once the option is enabled, the **View log** option is available.

8.5.3. Parental Control Log

The Parental Control log registers all events related to apps and components with blocked or restricted access.

By default, Parental Control log events are shown as a list of events grouped by date. The following events are registered in the log:


- App events:
 - launch attempt,
 - unlocking.
- Dr.Web component and Parental Control events:
 - enabling,
 - disabling.

For each event, its time is given.

Event listing in the log

You can manage the way events are listed in the Parental Control log. You can sort, filter, or group events. Searching by events is also available.

Event filter

To sort or filter events by a set parameter, tap the  icon in the bottom-right corner of the screen and select **Filter**.

The following sort types are available:



- oldest on top,
- newest on top,
- A to Z,
- Z to A.


You can also filter events by event type: app unlocking, launch attempt; component enabling, disabling.

To sort or filter the event list, select the desired parameters and go back to the event list.

You can restore the default view by tapping  in the top-right corner of the **Event filter** screen.


Searching

To search through Parental Control log events

1. Tap the  icon in the bottom-right corner of the screen.
2. Select **Search**.
3. Enter your query in the search field at the bottom of the screen.

Grouping

You can group events by app or component. When grouping is enabled, the Parental Control log is displayed as a list of apps and components whose events have been registered in the log (see [Figure 23](#)).

To group Parental Control log events, on the log screen, tap **Menu**  in the top-right corner of the screen and select the **Group** check box. Tap the app or component name to expand the list of relevant events.

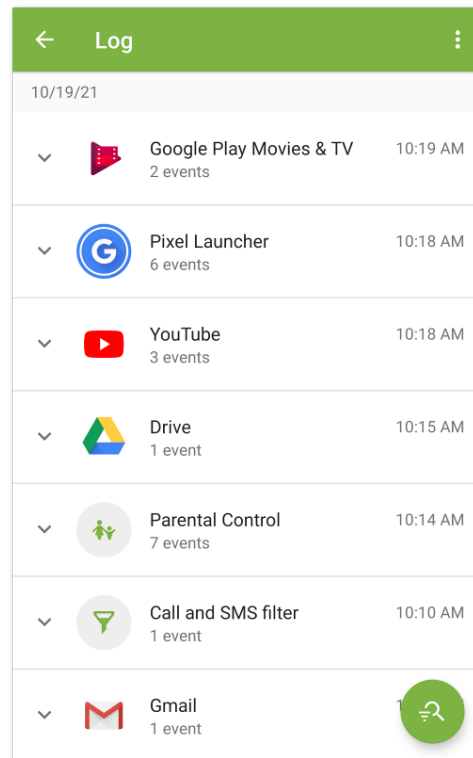




Figure 23. Grouped events

Group filter


You can sort groped events by a set parameter.

To sort grouped events

1. Tap the  icon in the bottom-right corner of the screen.
2. Select the **Filter** option.
3. On the **Group filter** screen, select the sort type.
4. Go back to the event list.

You can restore the default view by tapping  in the top-right corner of the **Group filter** screen.

Saving event log


To save the event log to a file, on the log screen, tap **Menu**  in the top-right corner and select **Save log**.

The log will be saved in the `DrWeb_Parental_Log.txt` file located in the `Android/data/com.drweb/files` folder in the device internal storage.



On devices with Android 11 or later, the log will be saved in `Download/DrWeb`.

Clearing the log

To delete all Parental Control log events, on the log screen, tap **Menu**  and select the **Clear log** option.

8.6. Dr.Web Firewall

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

Certain aspects of Dr.Web Firewall operation

Dr.Web Firewall is based on the VPN for Android technology, so it does not require root access on the device. However, the VPN for Android technology sets a number of limitations:

- Only one app can use VPN at a time. As a result, before enabling VPN, the app prompts you to provide it the corresponding permission. If you give the permission, the app starts using VPN, but it also blocks access to VPN for other apps. Dr.Web Firewall requests the VPN permission the first time you enable the component. It can also request the permission after a device reboot and after VPN requests from other apps. VPN is shared between the apps over time. Dr.Web Firewall can operate only when it gets the full rights to use VPN.
- Enabling Dr.Web Firewall can result in inability to connect the device on which Dr.Web Firewall runs to other devices directly using Wi-Fi or a local network. It depends on the device model and the apps which are used to establish a connection between devices.
- When Dr.Web Firewall is enabled, you cannot use your device as a Wi-Fi access point.



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

To enable Dr.Web Firewall

1. On the Dr.Web [main screen](#), select **Firewall**.
2. Tap the **Enable** button or use the toggle button in the top-right corner of the screen.

Dr.Web requests the permission to set up a VPN connection. You need to grant the permission in order for Dr.Web Firewall to function.

To enable Firewall after the device boots, open Dr.Web.



On devices with Android 7.0 or later, you can set your OS to automatically enable Dr.Web Firewall after the device boots. To do so:

1. In your device settings, select **VPN**.
2. Open the Dr.Web Security Space (Dr.Web Security Space Life) network settings.
3. On the **Dr.Web Security Space (Dr.Web Security Space Life)** screen, enable the **Always-on VPN** setting.

On devices with Android 8.0 or later, you can block access to the internet after the device boots until the VPN successfully connects. To do so, enable the **Block connections without VPN** setting.



If another app starts using VPN, Dr.Web Firewall will be disabled. You will see a corresponding notification. Tap this notification to enable Dr.Web Firewall again.

If you use a restricted profile (guest profile) on your device, Dr.Web Firewall is disabled.

Main screen

The Firewall main screen displays cards containing information from its sections:

- [Traffic limit](#) (when a limit is set): displays information on the current traffic limit.
- [Active apps](#): displays a diagram of the incoming and outgoing traffic used by active app connections.
- [All apps](#): displays the total sum of all incoming and outgoing traffic used by apps installed on the device.

Tap **More** on the app traffic or traffic limit card to go to the corresponding section.

The menu in the top-right corner of the main screen allows you to:

- open [mobile traffic limit](#) settings;
- open the [Dr.Web Firewall log](#).

8.6.1. Managing Network Activity of Apps

Dr.Web Firewall allows you to control the use of internet traffic on the device and manage the general settings of network access of apps. General management includes the following features:


- monitoring of [active app traffic](#) in real time;
- access to the [list of apps that used internet traffic](#), and the amount of the used traffic;
- management of [access to data transmission](#) of apps over Wi-Fi, mobile networks, and when roaming;
- ability to [limit data usage](#) over a set period of time.

8.6.1.1. Active Apps

The **Active apps** section displays a real-time list of active connections initiated by apps installed on the device. The section provides easy access to managing current app traffic.

The section card on the main Firewall screen displays apps with the highest active traffic use. Tap **More** to open the full list of apps with active connections.

The following information is provided on every app on the **Active apps** screen (see [Figure 24](#)):

- Total amount of incoming and outgoing traffic used by established connections.
- [Access to data transmission](#) over Wi-Fi, mobile networks, or when roaming.
- User settings. Icons of apps with a changed access to data transmission are marked with the  icon.

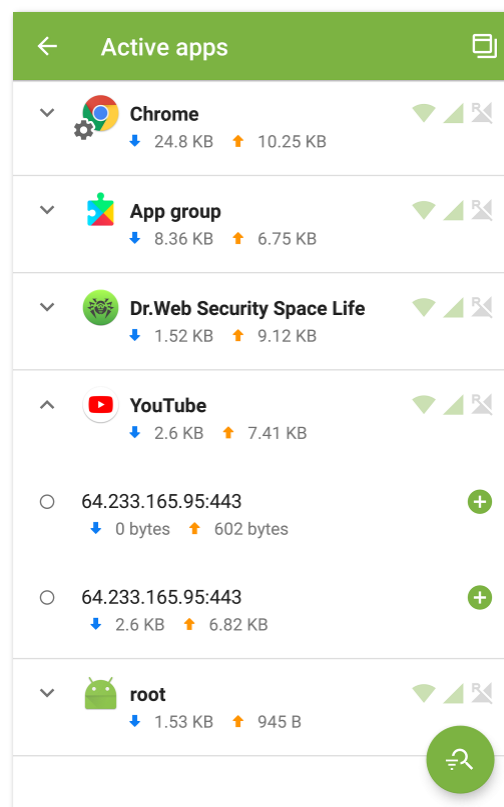







Figure 24. Active apps

App connections

Tap the  icon to the left of the name of an app on the **Active apps** screen to see detailed information on connections established by the app:

- list of established connections;
- total amount of incoming and outgoing traffic used by each of the established connections;





- connection rule:
 -  allowing,
 -  blocking,
 -  redirecting,
 -  not set.


To copy a connection address to the clipboard, tap and hold the connection row. The address will be copied to the clipboard.

Tap the connection row to go to the [Connection](#) screen.


Connection rules

You can create allowing, blocking, and redirecting rules to manage connections established by apps (see [Connection Rules](#)). To create or edit a rule, tap the  or  icon to the right of the connection.


App sorting

To sort the list of apps, tap the  icon in the bottom-right corner of the screen, then tap **Filter** and select a sorting option:

- highest traffic first—apps with the highest traffic will be at the top of the list;
- lowest traffic first—apps with the lowest traffic will be at the top of the list;
- A to Z;
- Z to A.

By default, apps are sorted by traffic (apps with the highest traffic are at the top of the list). To restore the default sorting, tap the  icon on the **Filter** screen.

Search

To quickly navigate to a certain app, use the search by app name function. To do so, tap the  icon in the bottom-right corner of the screen, then tap **Search** and enter your query in the search field at the bottom of the screen.

Floating window

To see all active internet connections in real time and control the amount of incoming and outgoing traffic, enable the floating window that is displayed on top of all other apps (see [Figure 25](#)).

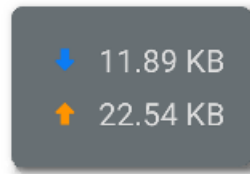




Figure 25. Floating window


To enable the floating window

1. Go to the **Active apps** screen and tap the  icon in the top-right corner (see [Figure 24](#)).
2. Allow the app to display its floating window on top of the other apps.

If the permission to draw over other apps is removed, the floating window cannot be displayed. To enable it again, tap the  icon in the top-right corner of the screen and grant the requested permission.



Total traffic size is calculated since the moment you enable the window.

- To open the list of apps that are using internet connections (see [Figure 26](#)), tap the floating window.
- To close the list of apps, tap .

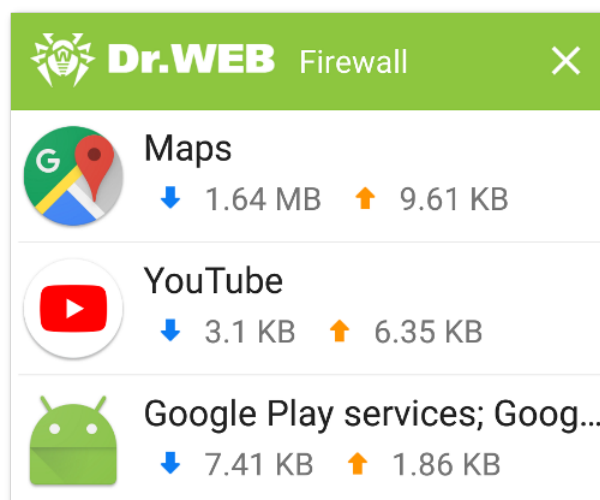



Figure 26. List of apps that are using internet connections

To disable the floating window

- Go to the **Active apps** screen and tap the  icon in the top-right corner.






8.6.1.2. All Apps

The **All apps** section contains a list of all connections established by apps since enabling Dr.Web Firewall (including apps removed from the device if the [corresponding setting](#) is on). The section allows you to manage the access of any app to internet traffic.

The section card on the main Firewall screen displays the total amount of incoming and outgoing traffic used by applications since enabling Firewall. Tap **More** to open the full list of apps.

The following information is provided on every app on the **All apps** screen:


- total amount of incoming and outgoing traffic used by established connections;
- access to data transmission over Wi-Fi , mobile networks , or when roaming .

Tap the name of an app to go to the [Application](#) screen and see the statistics, settings, and rules for this app.


Access to data transmission

On the **All apps** screen, you can manage access to data transmission over Wi-Fi, mobile networks or when roaming for all or some apps on the list using the **Access to data transmission** panel (for more information see [Access to Data Transmission](#)).

App filtering and sorting

To filter or sort the list of apps, tap the  icon in the bottom-right corner of the screen, then tap **Filter** and select the options:

- Display apps:
 - with no traffic.
- Sort:
 - highest traffic first—apps with the highest traffic will be at the top of the list;
 - lowest traffic first—apps with the lowest traffic will be at the top of the list;
 - A to Z;
 - Z to A.

By default, apps are sorted by traffic (apps with the highest traffic are at the top of the list), apps with no traffic are displayed. To restore the default list view, tap the  icon on the **Filter** screen.




Search

To quickly navigate to a certain app, use the search by app name function. To do so, tap the



icon in the bottom-right corner of the **All apps** screen, then tap **Search** and enter your query in the search field at the bottom of the screen.

All app settings

To manage settings for all apps, on the **All apps** screen, tap **Menu**  and select the **Settings** option.

The following settings are available:

- **Use IPv6.** Allows you to enable or disable the use of IPv6 in parallel with IPv4.
- **Allow DNS over TCP.** Allows you to enable or disable the use of the DNS over TCP protocol for DNS query redirection and the hiding of domain names.



The use of the DNS over TCP protocol may prevent domain names from being displayed on some Firewall screens.


The setting works on devices which support this protocol type. The setting is disabled by default.

- **Block connections for new apps.** Allows you to block access to networks for apps installed after enabling the setting. You can block connections over Wi-Fi and mobile networks by selecting the corresponding check boxes below the setting.
- **Store rules and statistics after deleting apps.** Allows you to store data of apps removed from your device for the selected period of time: one week, month, or year.


All rules

The **All rules** screen contains the list of all [connection rules](#) of all apps (app groups).

To open the list of all rules, on the **All apps** screen, tap **Menu**  and select **All rules**.


The rules are grouped by the name of the app (or app group) that established the connection. Apps are sorted in alphabetical order. To expand the list of rules of an app, tap the  icon to the left of the app (app group) name. App rules are listed in the order of their execution.

To change the order of rule execution

- Tap and hold the  icon next to the rule you want to move, then drag the rule to the desired position on the list.




To search through all app rules

- Tap the  icon in the bottom-right corner of the **All rules** screen and enter your query in the search field at the bottom of the screen.

App rules can be stored on the device for the specified period of time after the app is deleted if the [corresponding setting](#) is enabled.

Clearing app data

To delete settings, rules and statistics for all apps

1. On the **All apps** screen, tap **Menu**  and select **Clear**.
2. Select the check boxes next to the data you want to delete.
3. Tap **Clear**.

8.6.1.3. Access to Data Transmission

You can manage access to data transmission for all installed apps as well as for individual apps:

- over Wi-Fi ,
- over mobile networks ,
- over mobile networks when roaming .

Allowed access types are marked with green icons, blocked access types are marked with gray.



By default, data transmission is allowed over Wi-Fi and mobile networks and blocked over mobile networks when roaming for all apps.

To change access to data transmission for all apps

- On the **All apps** screen, tap **Wi-Fi**, **Mobile data**, or **Roaming** at the top of the screen.





To change access to data transmission for multiple apps

1. On the **All apps** screen, tap and hold one of the apps.
2. Select the rest of the apps you want to change access for.
3. Use the icons in the top-right corner of the screen to allow/block the corresponding access to data transmission for all selected apps.

To exit the access editing mode, tap the  icon in the top-left corner of the screen.



To change access to data transmission for one app

- On the [Application](#) screen, open the **Settings** tab and tap the , , or  icon.
- Icons of apps with a changed access to data transmission are marked with the  icon.



8.6.1.4. Mobile Traffic Usage Limit

Dr.Web Firewall allows you to limit the use of mobile traffic within a set period of time.



This function is unavailable if your device does not support SIM cards (there is no slot for a SIM card on your device).

To set a traffic limit

- On the main Dr.Web Firewall screen, tap **Menu**  and select the **Traffic limit** option.
- Tap **Limit**.
- Set a traffic limit (in megabytes or gigabytes).
- If necessary, specify the amount of traffic that has already been used since the selected limitation period started (which begins at 00:00 of the current day).
- Tap **Save**.
- Set the duration period for the limit: a day, a week, or a month. When selecting **Week** or **Month**, specify the day of the week or the day of the month on which the limit will restart within the current selected period.
- You can select the **Notify me when my mobile traffic limit is reached** check box to receive a notification upon reaching the traffic usage limit.
- Tap the  icon in the top-right corner of the screen.

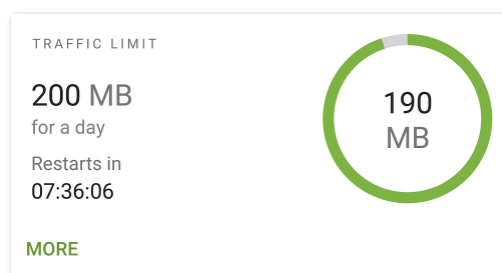


Figure 27. Traffic limit


When the traffic usage limit is enabled, a diagram showing the amount of the remaining mobile traffic is displayed on the **Traffic limit** card on the main Dr.Web Firewall screen. The specified limit and the countdown to the restart of the period are shown next to the diagram (see [Figure 27](#)).



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

Tap **More** on the traffic limit card to go to the **Traffic limit** screen.

To change the current traffic limit

1. Go to the **Traffic limit** screen.
2. Make changes.
3. Tap the  icon in the top-right corner of the screen to save changes.

To disable the traffic limit


- On the **Traffic limit** screen, tap the **Disable** button and confirm the action.

8.6.2. Managing Individual App Traffic

Dr.Web Firewall allows you to manage and monitor internet traffic of individual apps and connections established by them. This helps you control the access of apps and processes to network resources.

The **Application** screen displays the statistics of traffic usage for every app (or, in some cases, app group) and allows you to set custom connection rules and traffic use settings, as well as view all Firewall events related to this app.

To go to the **Application** screen (see [Figure 28](#)), do one of the following:

- On the **Active apps** or **All apps** screen, tap the name of an app on the app list.
- On the [Connection](#) screen, tap the  icon to the right of the name of an app.

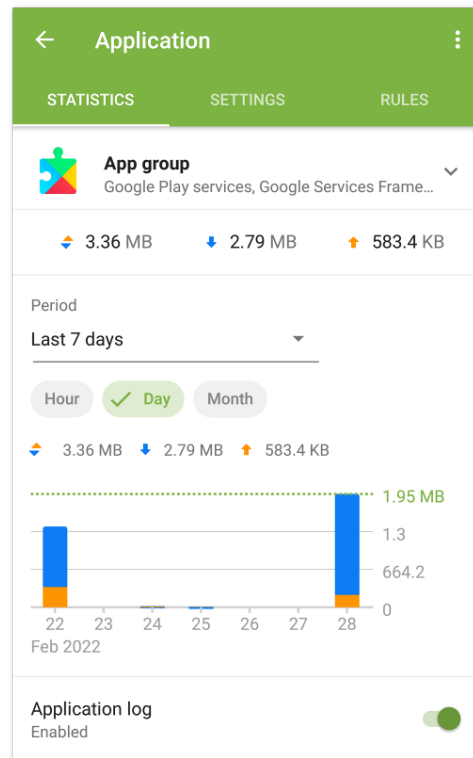


Figure 28. Application screen

Three tabs are available on the **Application** screen: **Statistics**, **Settings**, and **Rules**.

8.6.2.1. Internet Traffic Statistics

You can review statistics on traffic use of any app on the device. The statistics are shown in the form of a graphical diagram (see [Figure 29](#)).

To go to the traffic use statistics, on the **Active apps** or **All apps** screen, tap the name of an app on the app list.

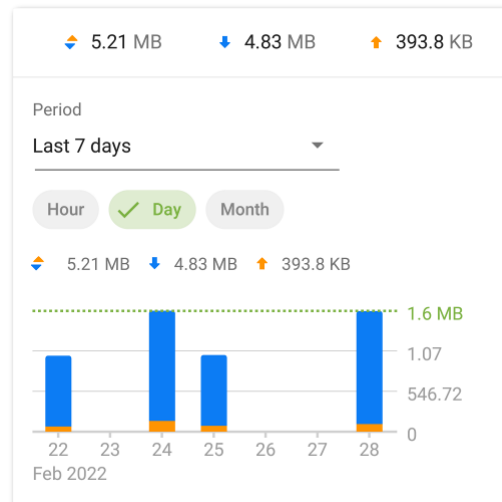


Figure 29. Internet traffic statistics of an app

On the **Statistics** tab, the amount of traffic used by the app since enabling Firewall is shown below the name of the app.



Outgoing app traffic is marked with orange on the graph, incoming traffic is marked with blue. The numeric values of the amount of traffic (total, incoming, and outgoing) spent over a specified period of time are shown above the graph.

When reviewing internet traffic statistics, you can do the following:

- Select the period of time over which you want to review the statistics. You can review the statistics for the current day, last 7 days, current month, previous month, or specify any other period manually by setting the start and end dates. Select the period in the **Period** drop-down list above the diagram.
- Change the scale of the displayed statistical data within the selected period: hour, day, or month. Select one of the options above the diagram.

You can swipe the diagram left or right to the desired value if the graphic does not fit on the screen.

Clearing statistics

- To clear statistics for a specific app:
 1. On the **Active apps** or **All apps** screen, tap the name of the app you want to clear the statistics of.
 2. On the **Application** screen, tap **Menu**  in the top-right corner and select **Clear**.
 3. In the next window, select the **App statistics** check box and tap **Clear**.
- To clear statistics for all apps:
 1. On the **All apps** screen, tap **Menu**  and select **Clear**.
 2. In the next window, select the **App statistics** check box and tap **Clear**.






Once you remove an app from the device, its statistics will be cleared automatically within the next 5 minutes.

Application log

Events related to the network activity of apps installed on the device are registered in [application logs](#). Use the toggle button to enable or re-enable the application log. To go to the log, tap **View log**.

8.6.2.2. Application Settings

Access to data transmission

You can allow or deny access to data transmission over Wi-Fi , mobile networks , or over mobile networks when roaming  for an app by tapping the corresponding icon (see [Access to Data Transmission](#)).

Block all connections not allowed by the rules

To block all connections for an app by default, select the **Block all connections not allowed by the rules** check box. With no allowing rules set, the app will be unable to initiate any connections.

An allowing rule for port 53 is automatically added when enabling the **Block all connections not allowed by the rules** setting for this app. This rule (set for the DNS, UDP, or ALL protocols) is mandatory for the functioning of allowing rules with domain names.



To ensure that this setting works as intended in the presence of allowing rules with domain names, disable the use of a private DNS server in your device settings.

Do not control the app



The setting is available on devices running Android 5.0 or later.

The setting is not available for some system apps.

Dr.Web Firewall is based on the VPN for Android technology. VPN prevents apps from functioning if they use a technology which is incompatible with VPN, e.g. Wi-Fi Direct. This can result in inability to connect your device to other devices. In this case you should disable Dr.Web Firewall control for the app (or app group) by selecting the **Do not control the app** check box.



It is recommended to disable Dr.Web Firewall control only for your trusted apps.

When the option is enabled, Dr.Web Firewall does not control network connections of the app even if you customize traffic settings for it in the Dr.Web Firewall settings. The app traffic is not monitored.

8.6.2.3. Connection Rules

App traffic is managed through connections established by apps. You can set up allowing, blocking, or redirecting rules for connections with specified IP addresses and ports for every app installed on the device.

Connection rules are displayed on the [Rules](#) tab of the **Application** screen, as well as on the [All rules](#) screen.

Connections

General information on each connection is shown on the **Connection** screen (see [Figure 30](#)). To go to this screen, do one of the following:

- On the [Active apps](#) screen, tap the ▼ icon to the left of the name of an app and then tap a connection row.
- In the [Firewall log](#):
 - When events are grouped by date: tap a connection row.
 - When events are grouped by app name: expand the list of app connections by tapping the ▼ icon to the left of the name of an app and then tap a connection row.
- In an [application log](#): expand the list of app connections by tapping the ▼ icon to the right of an event date and then tap a connection row.

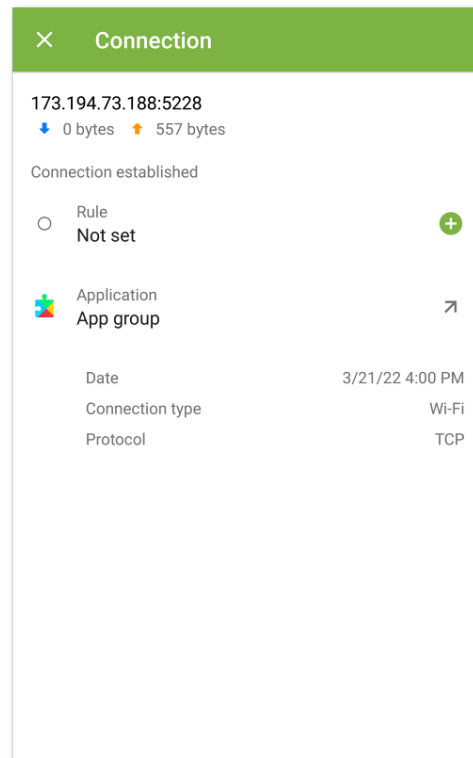




Figure 30. Connection screen

The **Connection** screen contains the following information:

- connection address and port;
- host name (if available);
- amount of incoming and outgoing traffic received or transmitted by the connection;
- connection status;
- connection rule;
- app that established the connection;
- date and time;
- connection type;
- protocol.

To copy a connection address

1. Tap and hold the connection row. You will enter the copying mode. The address will be highlighted in gray.
2. Tap the  icon in the top-right corner of the screen. The address will be copied to the clipboard.



To exit the copying mode, tap the  icon in the top-left corner.








Connection rules

Creating rules

To create a new connection rule

1. For connections without rules:
 - On the **Connection** screen, tap the  icon to the right of the **Rule** section.
 - On the **Active apps** screen, expand the list of established connections and tap the  icon to the right of the connection address.

For any connection:

 - On the **Application** screen, open the **Rules** tab and tap the  icon in the bottom-right corner of the screen.
2. On the next screen, select the rule type:
 -  allowing,
 -  blocking,
 -  redirecting.
3. Check the IP address/host name. If the address is not specified, enter a valid IP address (in the a.b.c.d format for IPv4 addresses or [a:b:c:d:e:f:g:h] for IPv6), an IP address range (in the a1.b1.c1.d1-a2.b2.c2.d2 or [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2] format), or a network (in the a.b.c.0/n format, where n is a number from 1 to 32). If you are creating a redirecting rule, enter the redirection address in the field below. You can specify a host name instead of an address.
4. Tap **More** for the additional **Protocol** setting to choose a network protocol for the connection.
5. Tap the  icon to save the changes.

Icons of apps with set connection rules are marked with the  icon.


Viewing rules


To view connection rules

- For an individual app:
 - Go to the **Application** screen and open the **Rules** tab.


The tab contains the list of all rules set for the app, in the order of their execution.
- For all apps:
 1. On the main Firewall screen, tap **More** on the **All apps** section card.




2. On the **All apps** screen, tap **Menu**  and select **All rules**.

The **All rules** screen contains the list of all connection rules grouped by the name of the app (or app group) that established the connection. Apps are sorted in alphabetical order. To expand the list of rules of an app, tap the  icon to the left of the app (app group) name. App rules are listed in the order of their execution.

To change the order of rule execution

- Tap and hold the  icon next to the rule you want to move, then drag the rule to the desired position on the list.






To search through all app rules

- Tap the  icon in the bottom-right corner of the **All rules** screen and enter your query in the search field at the bottom of the screen.

App rules can be stored on the device for the specified period of time after the app is deleted if the [corresponding setting](#) is enabled.

Editing rules

To edit an existing rule


1. Do one of the following:
 - On the **Connection** screen, tap the  icon to the right of the rule.
 - On the **Active apps** screen, tap the  icon to the left of the name of an app and then tap the  icon next to the connection with the rule you want to change.
 - On the **Application** screen, open the **Rules** tab and tap the rule row.
 - On the **All rules** screen, tap the  icon to the left of the name of an app and then tap the rule row.
2. Make changes.
3. Tap the  icon to save the changes.

Deleting rules


To delete a rule

- On the rule editing screen:
 1. Tap **Delete rule**.
 2. On your next step, tap **Delete**.
- On the **Rules** tab or the **All rules** screen:




1. Swipe the rule left and tap the  icon.
2. On your next step, tap **Delete**.

To delete all rules for a certain app

1. On the **Application** screen, tap **Menu**  in the top-right corner and select **Clear**.
2. On your next step, select the **App rules** check box. Tap **Clear**.



To delete all rules for all apps

1. On the **All rules** screen, tap **Menu**  and select **Clear**.
2. Tap **Clear**.

Importing and exporting rules

You can export rule lists to a file in the internal device memory. This allows you to import them from the file later (for example, in case you reinstall Dr.Web or use it on another device).

To export rules to a file


- For an individual app:
 1. On the **Rules** tab of the **Application** screen, tap **Menu**  in the top-right corner and select **Export rules**.
 2. Tap **OK**.
- For all apps:
 1. On the **All rules** screen, tap **Menu**  in the top-right corner and select **Export rules**.
 2. Tap **OK**.

Rules are exported to the `DrWeb_Firewall_Rules_<app_name>.hsts` file if these are app-specific rules, or the `DrWeb_Firewall_Rules_ALL.hsts` file if these are the rules for all apps. The file is saved in the `Internal storage/Android/data/com.drweb/files/` folder.




On devices with Android 11.0 or later, the file is saved in `Download/DrWeb`.

To import rules from a file

- For an individual app:
 1. On the **Rules** tab of the **Application** screen, tap **Menu**  in the top-right corner and select **Import rules**.
 2. Locate the file with rules in the file tree and tap it.



- For all apps:
 1. On the **All rules** screen, tap **Menu**  in the top-right corner and select **Import rules**.
 2. Locate the file with rules in the file tree and tap it.

Block all connections not allowed by the rules

You can block all connections except for those allowed by rules for an app by selecting the [corresponding check box](#) on the app settings screen.

8.6.2.4. Application Log

Network connection events are registered in application logs.





To enable application logging

- On the **Application** screen, open the **Statistics** tab and use the **Application log** toggle button.

To open an application log

- On the **Application** screen, open the **Statistics** tab and select the **View log** option.

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

- connection address and port;
- used up traffic;
- connection time;
- connection rule:
 -  allowing,
 -  blocking,
 -  redirecting,
 -  not set.

Tap the connection row to go to the [Connection](#) screen and set up rules.

To copy a connection address

- Tap and hold the connection row. The address will be copied to the clipboard.

To clear an application log

1. On the application log screen, tap the  icon in the top-right corner of the screen.




2. On your next step, tap the **Clear** button.

To disable application logging

- On the **Application** screen, open the **Statistics** tab and use the **Application log** toggle button.

8.6.3. Dr.Web Firewall Log

Events related to Firewall activities are registered in the Dr.Web Firewall log.


To open the list of all the events related to the operation of Dr.Web Firewall, on the main Firewall screen, tap **Menu**  and select **Log**.


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

- name of the app;
- connection address and port (as well as the redirection address if such a rule is set);
- used up traffic;
- event date and time;
- connection rule.

When an event is tapped, the [Connection](#) screen opens.

To filter or sort events in the Firewall log

1. Tap the  icon in the bottom-right corner of the **Log** screen and then tap **Filter**.
2. Select the options:
 - Sort:
 - newest on top—newest events at the top of the log;
 - oldest on top—oldest events at the top of the log;
 - A to Z;
 - Z to A.
 - Display connections:
 - established,
 - reset,
 - redirected,
 - with errors.

By default, events are sorted by date (newest events are at the top of the log), all connections are displayed. To restore the default log view, tap the  icon on the **Filter** screen.




You can group events by app for easier log navigation.

To group events by app

- On the **Log** screen, tap **Menu**  in the top-right corner and select the **Group** check box.


To search through the Firewall log

1. Tap the  icon in the bottom-right corner of the **Log** screen and then tap **Search**.
2. Enter your query in the search field at the bottom of the screen.

To copy a connection address

- Tap and hold the connection row. The address will be copied to the clipboard.


To clear the Firewall log

1. Tap **Menu**  and select **Clear**.
2. Confirm the action by tapping **Clear**.

Maximum log size

By default, the maximum size for the log file is set to 5 MB.

To change the maximum size for the log:

1. On the Firewall log screen, tap **Menu**  and select **Maximum log size**.
2. On the next screen, change the value and tap **OK**.



The maximum log file size must exceed 0 MB.

8.7. 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

Dr.Web detects the following security problems:

- [Vulnerabilities](#).
- [System settings](#) that affect device security.
- [Conflicting software](#).
- [Hidden device administrators](#).
- [Applications exploiting Fake ID vulnerability](#).
- [Optimization settings](#).

To open the list of the detected problems (see [Figure 31](#)), select **Security Auditor** on the Dr.Web main screen.

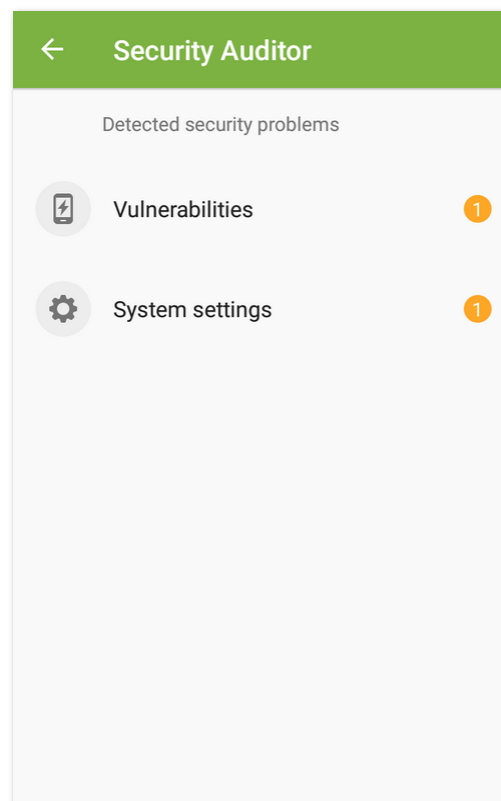


Figure 31. Security Auditor

8.7.1. Vulnerabilities

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

Security Auditor detects the following vulnerabilities in the device system: [BlueBorne](#), [EvilParcel](#), [Extra Field](#), [Fake ID](#), [Janus](#), [ObjectInputStream Serialization](#), [OpenSSLX509Certificate](#),



[PendingIntent](#), [SIM Toolkit](#), [Stagefright](#), and [Stagefright 2.0](#).

The vulnerabilities allow adding malicious code to some applications, that may result in performing of dangerous functions by these applications and damage the device.

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.

Root access

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

8.7.2. System Settings

Security Auditor detects the following system settings that affects the device security:

- **Debugging enabled.** USB debugging is intended for developers and allows copying data from PC to the device and vice versa, installing the applications on the device, viewing their logs and deleting them in some cases. If you are not a developer and do not use the debug mode, you are recommended to turn this mode off. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem.
- **Installation of apps from unknown sources is enabled.** Installing application from unknown sources is one of the main reasons devices with Android 7.1 and earlier get infected.

Applications downloaded from elsewhere other than the official store are likely to be unsafe and become a threat to device security. To mitigate risks of installing the unsafe applications, you are recommended to disable installation of the applications from unknown sources. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem.

You should scan for threats all the applications you install on your device. Before scanning, make sure that Dr.Web virus databases are [up to date](#).

- **Dr.Web notifications are blocked.** In this case, Dr.Web cannot immediately inform you on detected threats. This compromises security of your device. That is why, you are recommended to enable Dr.Web notifications in the settings of your device.
- **User root certificate installed.** If any user certificates are detected on your device, Security Auditor detects and displays them. Certificates may be used by a third party to monitor your network activity. If you are not aware why these certificates are installed on your device, you are recommended to remove them.



8.7.3. Conflicting Software

Use of conflicting software, including web browsers that are not compatible with URL filter, decreases the security level of your device. While using these browsers you will not be protected against the undesirable and malicious web resources. We recommend that you make one of the following browsers default on your device: Android embedded browser, Google Chrome, Yandex.Browser, Microsoft Edge, Firefox, Firefox Focus, Opera, Adblock Browser, Dolphin Browser, Sputnik, Boat Browser, and Atom.

8.7.4. Hidden Device Administrators

Applications that are activated as device administrators but not shown on the list of administrators on the corresponding section of the device settings cannot be deleted by means of the operation system. Most likely, such applications are potentially harmful for your device.

If you do not know why an application is not displayed in the list of device administrators, you are recommended to delete it from the device. To delete the application, tap **Delete** on the screen with the detailed information on the problem related to this application.

8.7.5. Applications Exploiting Fake ID Vulnerability

If applications exploiting Fake ID vulnerability are detected on the device, they are displayed in the separate Security Auditor section. These applications can be malicious, therefore you are recommended to delete them. To delete the application, tap **Delete** on the screen with the detailed information on the problem related to this application, or use standard OS tools.

8.7.6. Optimization Settings

The operating system of your device can terminate background processes of apps you are not actively using at the moment. Such optimization of background processes helps save power or improve system performance, but it can affect app performance.

The Dr.Web app should work continuously to achieve real-time anti-virus protection and efficiency of the advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#) and [Firewall](#).

Remove background restrictions for Dr.Web so that the app works as expected. To do that, check your device settings and the settings of the built-in app manager.

Settings can vary by device:

- [Asus](#)
- [Huawei](#)
- [Meizu](#)



- [Nokia](#)
- [OnePlus](#)
- [Oppo](#)
- [Samsung](#)
- [Sony](#)
- [Xiaomi](#)



The instructions provided in these sections may not fully correspond to some devices as settings may vary on different device models and OS versions. In case of inconsistencies, please refer to the user manual provided by your device manufacturer. If this does not solve your problem, please contact [our technical support](#).

Permission auto-reset



This warning appears only when Dr.Web has not been granted access to accessibility features.

Starting with Android 6.0, the system resets permissions granted by the user if an app has not been used for a few months. Additionally, on Android 12.0 and later, the app cache is cleared and the app can no longer send you notifications. This is done to save storage space and protect user data. However, Dr.Web cannot provide continuous device protection if the [permissions](#) required for its main functions and the app components will be reset. To ensure seamless operation of Dr.Web, it is recommended to disable permission auto-reset in the device settings. To open the corresponding device settings section, tap **Settings** on the screen with detailed information on the problem.

Restricted settings

On devices with Android 13.0 or later, the operating system restricts access to certain settings to apps by default. This is done to protect sensitive info from being acquired and used by harmful apps. However, Dr.Web components use some of these settings, such as accessibility features and notification access, to protect your data and block unwanted content. To open the system setting that grants access to settings required for Dr.Web to function as intended, follow the instructions on the screen with detailed information on the problem.

8.7.6.1. Asus

In order for the Dr.Web app to work properly on Asus devices, proceed as follows:

- [Allow autostart](#)

Autostart allows the app to start its processes right after the device startup. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).



- [Allow running in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To allow autostart

1. In your device settings, open **Auto-start manager**.
2. Allow autostart for the Dr.Web app.

To allow running in the background

1. In the **Mobile manager** app, open **Settings**.
2. Disable the **Clean up in suspend** setting.

8.7.6.2. Huawei

Devices supporting manual management

On the Huawei devices that support automatic and manual management of app launch, allow the Dr.Web app to be managed manually.

Manual management allows the app to keep running even if it is not active, and to start its processes right after the device startup. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

To enable manual management

- On devices running Android:
 1. In your device settings, open **Battery > App launch**.
 2. Select **Manage manually**.
- On devices running Harmony OS:
 1. In your device settings, open the app launch settings.
 2. Find Dr.Web on the list and use the toggle button on the right to enable manual management.
 3. On the next screen, enable all the additional management settings and tap **OK**.



Other Huawei devices

In order for the Dr.Web app to work properly on other Huawei devices, change the following settings:

- [Allow running in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Disable battery optimization](#)



If Dr.Web is set as a device administrator, this optimization setting is unavailable.

To optimize battery consumption, the operating system can stop the Dr.Web app. This interrupts constant anti-virus protection and the work of the enabled advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Allow running after screen is off](#)

Running when the screen is off is necessary for constant anti-virus protection and for the advanced components to work as expected: [Call and SMS filter](#), [Anti-theft](#), and [Firewall](#).

- [Allow pop-up windows](#) if [Anti-theft](#) or [Parental Control](#) is enabled.

[Anti-theft](#) and [Parental Control](#) use pop-up windows in the background to restrict access to a single app or the whole device.



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To allow running in the background

1. Open recent apps.
2. Tap the lock icon next to the Dr.Web app.

To disable battery optimization

1. In your device settings, open **Advanced settings** > **Battery manager** > **Protected apps**.
2. Select **Protected** for the Dr.Web app.

To allow running after screen is off

1. In your device settings, select **Apps** > **Dr.Web** > **Battery**.
2. Enable the **Keep running after screen is off** option.



To allow pop-up windows

1. In your device settings, select **Apps**.
2. Select Dr.Web on the list of apps.
3. On the list of permissions, enable displaying pop-up windows in the background.

8.7.6.3. Meizu

In order for the Dr.Web app to work properly on Meizu devices, change the following settings:

- [Disable battery optimization](#)



If Dr.Web is set as a device administrator, this optimization setting is unavailable.

To optimize battery consumption, operating system can stop the Dr.Web app. This interrupts constant anti-virus protection and work of advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Lock Dr.Web in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Allow running after screen is off](#)

Running when the screen is off is necessary for constant anti-virus protection and for the advanced components to work as expected: [Call and SMS filter](#), [Anti-theft](#), and [Firewall](#).



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To disable battery optimization

1. In your device settings, open **Advanced settings** > **Battery manager** > **Protected apps**.
2. Select **Protected** for the Dr.Web app.

To lock Dr.Web in the background

1. Open recent apps.
2. Tap the lock icon next to the Dr.Web app.

To allow running after screen is off

1. In your device settings, select **Apps** > **Dr.Web** > **Battery**.
2. Enable the **Keep running after screen is off** option.



8.7.6.4. Nokia

In order for the Dr.Web app to work properly on Nokia devices, force close the Power saver app.



If Dr.Web is set as a device administrator, this optimization setting is unavailable.

The Power saver app optimizes battery consumption that can cause the Dr.Web app to stop. This interrupts constant anti-virus protection and work of advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To force close Power saver

1. In your device settings, go to **Apps** > **All apps**.
2. Tap the menu in the top-right corner and select **Show system**.
3. Select **Power saver** and tap **Force close**.

The app will remain stopped until the next device reboot.

8.7.6.5. OnePlus

In order for the Dr.Web app to work properly on OnePlus devices, change the following settings:

- [Disable battery optimization](#)



If Dr.Web is set as a device administrator, this optimization setting is unavailable.

To optimize battery consumption, operating system can stop the Dr.Web app. This interrupts constant anti-virus protection and work of advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Lock Dr.Web in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

In addition, it is necessary to [disable deep optimization](#) and [autostart](#) on some devices.



After you install an update of the operating system, the optimization settings may be reset. In this case you will need to change them again.



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To disable battery optimization

1. In your device settings, open **Battery** > **Battery optimization**.
2. Select the Dr.Web app.
3. Select the **Don't optimize** option and tap **Done**.

To lock Dr.Web in the background

1. Open recent apps.
2. Tap the lock icon next to the Dr.Web app.

To disable deep optimization

1. In your device settings, open **Battery** > **Battery optimization**.
2. Tap the settings icon in the top-right corner.
3. Disable deep optimization.

To disable autostart

1. In your device settings, open **Apps**.
2. Tap the settings icon in the top-right corner.
3. Select **App auto-launch**.
4. Disable autostart for the Dr.Web app.

8.7.6.6. Oppo

In order for the Dr.Web app to work properly on Oppo devices, change the following settings:

- [Allow autostart](#)

Autostart allows the app to start its processes right after the device startup. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Lock Dr.Web in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Allow running in the background](#) if you have the Security center app on your device



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To allow autostart

1. In your device settings, open **App management**.
2. Select the Dr.Web app.
3. Allow autostart.

To lock Dr.Web in the background

1. Open recent apps.
2. Tap the lock icon next to the Dr.Web app.

To allow running in the background

1. Open **Security Center**.
2. Select **Privacy permissions** > **Startup manager**.
3. Grant Dr.Web the permission to work in the background.

8.7.6.7. Samsung

In order for the Dr.Web app to work as expected, it is necessary to lock Dr.Web in the background.

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To lock Dr.Web in the background

1. Open recent apps.
2. Open the menu in the top-right corner and select **Lock apps**.
3. Tap the lock icon next to the Dr.Web app.

8.7.6.8. Sony

In order for the Dr.Web app to work properly on Sony devices, disable battery optimization for Dr.Web.





If Dr.Web is set as a device administrator, this optimization setting is unavailable.

To optimize battery consumption, operating system can stop the Dr.Web app. This interrupts constant anti-virus protection and work of advanced components: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To disable battery optimization

1. On the device home screen, tap .
2. Select **Settings** > **Battery**.
3. Tap  and select **Battery optimization**.
4. Tap **Apps**. A list of optimized apps will appear.
5. Select Dr.Web. The app will appear in the **Not optimized** tab.



In the Ultra STAMINA mode you are not able to exclude apps from optimization.

8.7.6.9. Xiaomi

In order for the Dr.Web app to work properly on Xiaomi devices, change the following settings:

- [Allow autostart](#)

Autostart allows the app to start its processes right after the device startup. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Allow running in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Lock Dr.Web in the background](#)

Running in the background allows the app to keep running even if it is not active. It is necessary for constant anti-virus protection and for the following advanced components to work as expected: [Call and SMS filter](#), [URL filter](#), [Anti-theft](#), [Parental Control](#), and [Firewall](#).

- [Allow pop-up windows](#) if [Anti-theft](#) or [Parental Control](#) is enabled.

[Anti-theft](#) and [Parental Control](#) use pop-up windows in the background to restrict access to a single app or the whole device.



Settings and their location may vary on different device models and OS versions. If the instruction does not solve your problem, please contact our [technical support](#).

To allow autostart

1. In your device settings, select **Apps**.
2. Select Dr.Web on the list of apps.
3. Allow autostart.


To allow running in the background

1. In your device settings, select **Apps**.
2. Select Dr.Web on the list of apps.
3. Select the **Battery saver** setting.
4. Tap **No restrictions**.

To lock Dr.Web in the background

1. Open recent apps.
2. Tap the lock icon next to the Dr.Web app.

Some OS versions also allow you to lock apps in the background via the pre-installed **Security** app:


1. In the **Security** app, open the **Boost speed** section.
2. Tap the  settings icon in the top-right corner of the screen.
3. Tap **Lock apps**.
4. Find Dr.Web on the list of apps.
5. Use the toggle button to the right of Dr.Web to lock the app in the background.

To allow pop-up windows

1. In your device settings, select **Apps**.
2. Select Dr.Web on the list of apps.
3. Select **Other permissions**.
4. On the list of permissions, enable displaying pop-up windows in the background.

8.8. Statistics

Dr.Web collects statistics on detected threats and application actions.

To view the statistics, on the Dr.Web main screen, tap **Menu**  and select **Statistics**.



Viewing statistics

The **Statistics** tab contains two information sections (see [Figure 32](#)):

- **Total.** Contains information on the total number of scanned files, detected and neutralized threats.
- **Events** Contains the information on Dr.Web Scanner check results, enabling and disabling of SplDer Guard, detected threats and performed actions.

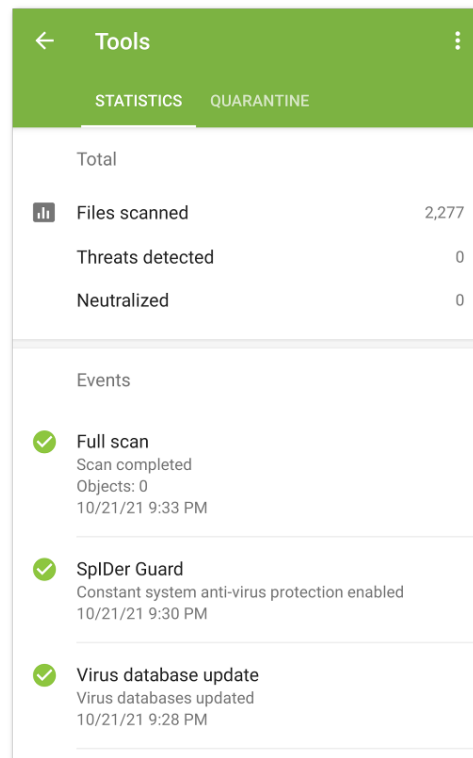



Figure 32. Statistics

Clearing statistics

To clear all the statistics, on the **Statistics** tab, tap **Menu**  and select **Clear statistics**.

Saving event log

You can save the application event log to send it to the Doctor Web technical support if you experience problems while using the application.

1. On the **Statistics** tab, tap **Menu**  and select **Save log**.
2. The log will be saved in the `DrWeb_Log.txt` and `DrWeb_Err.txt` files located in the `downloadsAndroid/data/com.drweb/files` folder in the device internal storage.



On devices with Android 11.0 or later, logs are saved in `Download/DrWeb`.

8.9. Quarantine

Dr.Web allows you to move detected threats to the quarantine folder, where they are isolated and cannot damage the system (see [Figure 33](#)).

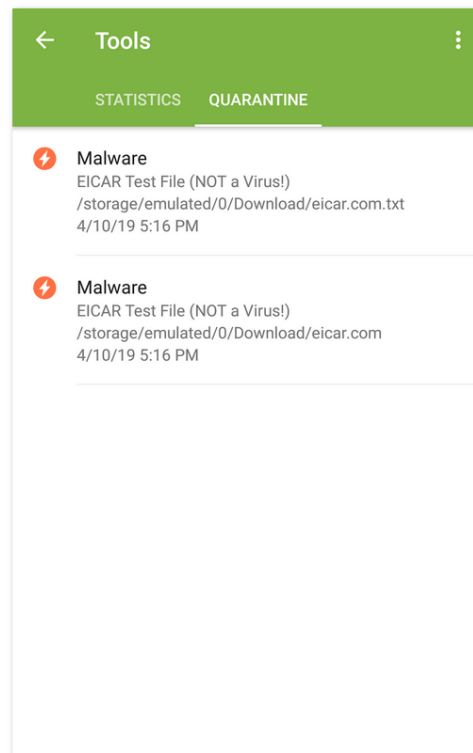


Figure 33. Quarantine

Viewing quarantined files

To view the list of threats moved to the quarantine:

1. On the Dr.Web main screen, tap **Menu** .



On Android TV, select **Miscellaneous**.

2. Select **Quarantine**.

The list of all threats in the quarantine opens.



Viewing information on quarantined threats

To view information on a threat, tap its name on the list.

For each threat, the following information is available:

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

Available options

For each threat, the following options are available:


- **More on the Internet** to view the threat description 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 delete the file from the quarantine and from the device.
- **False positive** to send the file to the Doctor Web anti-virus laboratory for analysis. The analysis will show if the file does pose a threat or it is a false positive. If it is a false positive error, it will be fixed. To receive the analysis results, enter your email address.



The **False positive** option is available only for threat modifications.

Deleting all objects from the quarantine

To remove all quarantined objects at once:

1. Open the **Quarantine**.
2. On the **Quarantine** tab, tap **Menu**  and select **Delete all**.
3. Tap **OK** to confirm the removal.
Tap **Cancel** to cancel the action and return to the **Quarantine**.


Quarantine size

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

1. Open the **Quarantine**.
2. On the **Quarantine** tab, tap **Menu**  and select **Quarantine size**.
3. Tap **OK** to return to the **Quarantine**.



9. Settings

To open the settings screen (see [Figure 34](#)), on the Dr.Web main screen, tap **Menu**  and select **Settings**.

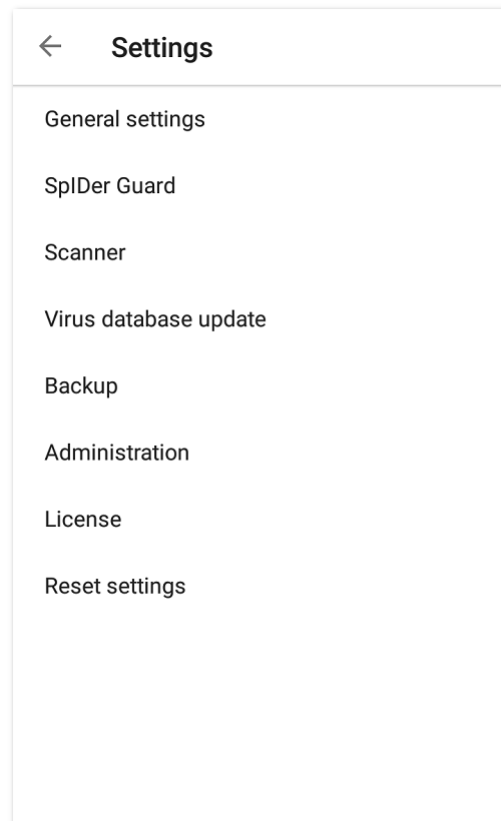


Figure 34. Settings

If you have set a password to access application settings, enter your account password.

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

- **General settings.** Allows you to configure the notification bar, enable and disable sound alerts and opt out of sending statistics (see [General Settings](#)).
- **SpIDer Guard.** Allows you to configure the SpIDer Guard component, which constantly scans the file system for threats and monitors changes in the system area (see [SpIDer Guard settings](#)).
- **Scanner.** Allows you to configure Dr.Web Scanner, which scans your device on your request (see [Dr.Web Scanner settings](#)).
- **Virus database update.** Allows you to disable virus database updates over mobile networks (see [Virus Database Update](#)).
- **Backup.** Allows you to import and export application settings (see [Backup](#)).



- **Administration.** Allows you to switch to the [centralized protection mode](#) (this option is available for the application version downloaded from the Doctor Web website).
- **License.** Allows you to enable and disable notifications on upcoming license expiration (except application versions with an unlimited license in Dr.Web Security Space Life) (see [Configuring Notifications on License Expiration](#)).
- **Reset settings.** Allows you to reset user settings and restore the default configuration (see [Reset Settings](#)).



If [Dr.Web Anti-theft](#) is enabled on the device, to change some application settings (**Reset settings**, **Backup** and **Administration**), enter your Dr.Web account password.

9.1. General Settings

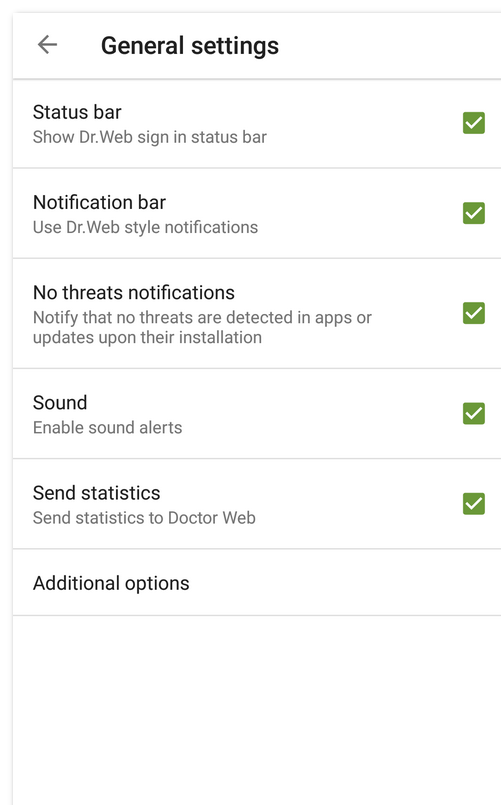


Figure 35. General settings

On the **General settings** screen (see [Figure 35](#)), you can use the following options:

- **Status bar.** Enables and disables the Dr.Web icon in the Android status bar. Using this option, you can also remove the Dr.Web bar from the notification area (see [Notification bar](#)).



The setting is not available on devices with Android 8.0 or later.



- **Notification bar.** Allows you to manage the appearance of the Dr.Web notification bar. If the option is enabled, the Dr.Web notification bar is used. If the option is disabled, the standard Android notification bar is used.
- **No threats notifications.** Enables and disables notifications informing that no threats have been detected in apps or updates that were just installed.



The setting is not available on devices with Android 8.0 or later. In this case, notifications from the **Safe applications** category can be enabled or disabled in the device settings.

- **Sound.** Enables and disables sound alerts on threat detection, deletion, or moving to quarantine. By default, sound alerts are enabled.
- **Send statistics.** Allows you to opt out of sending statistics to Doctor Web.
- **Additional options.** Contains additional settings:
 - **System applications.** Allows you to enable and disable notifications on [detecting threats in system applications](#) that cannot be safely deleted. This option is disabled by default.

9.2. 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 Android 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.




In the [centralized protection mode](#), you cannot update virus databases manually; updates are downloaded automatically from the centralized protection server. If the mobile mode is enabled on the server and the connection with the centralized protection server is lost, you can update the virus databases manually.

Update


The virus databases are updated via the internet several times a day automatically. If the 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

1. On the Dr.Web main screen, tap **Menu**  and select **Virus databases**.
2. In the pop-up window, you will see the virus database update status and when the virus databases were last updated. If the databases are not up to date, you should update them manually.



To start the update

1. On the Dr.Web main screen, tap **Menu**  and select **Virus databases**.
2. Tap **Update**.




It is recommended to update the virus databases as soon as you install the app so that Dr.Web can use the most up-to-date information about known threats. As soon as the Doctor Web anti-virus laboratory experts 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.

Update settings

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

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

1. On the Dr.Web main screen, tap **Menu**  and select **Settings** (see [Figure 34](#)).
2. Select **Virus database update**.
3. To disable the use of mobile data for downloading updates, select the **Update over Wi-Fi** check box.

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



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

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

9.3. Backup

You can export your current settings to a file in the internal device memory. This allows you to import them from the file (for example, in case you reinstall Dr.Web or use it on another device).



In the [centralized protection mode](#), you cannot import or export settings.



To export your current settings to a file

1. On the Settings screen (see [Figure 34](#)), tap **Backup**.
2. Enter your account password.
The password is required only if Dr.Web Anti-theft is enabled and configured.
3. In the next window, tap **Export settings**.
4. After that, specify a password to protect the settings file, and tap **OK**.

All settings are saved in the
Internal storage/Android/data/com.drweb/files/DrWebPro.bkp file.



On devices with Android 11 or later, the file will be saved in Download/DrWeb.

To import settings from a file

1. On the settings screen (see [Figure 34](#)), tap **Backup**.
2. Enter your account password.
The password is required only if Dr.Web Anti-theft is enabled and configured.
3. Select **Import settings**.
4. Confirm that you want to import settings from a file.
5. Locate a file with settings in the file tree and tap it.
6. Enter the password the file is protected with and tap **OK**.
All current application settings will be replaced by the settings from the file.

9.4. Reset Settings

You can reset custom settings of the application, including Call and SMS filter, Dr.Web Anti-theft, Dr.Web Firewall and URL filter settings, at any time and restore the default settings.



In the [centralized protection mode](#), you cannot reset settings.

To reset settings

1. Tap **Reset settings** on the settings screen (see [Figure 34](#)). Then tap **Reset settings**.
2. Enter your Dr.Web account password.
3. Confirm that you want to restore the default settings.



10. Centralized Protection Mode

Computers and other devices on which Dr.Web cooperating components are installed form an *anti-virus network*. The anti-virus network has a client-server architecture. The server controls the client using Dr.Web Agent. Centralized protection mode is the operating mode of the application under the Dr.Web Agent control.

The Dr.Web Security Space for Android version detailed in this manual is compatible with Dr.Web AV-Desk 10 and 13 and Dr.Web Enterprise Security Suite 10, 11, 12 and 13.

Centralized protection mode is available for the following Dr.Web versions:

- Downloaded from the Doctor Web website <https://download.drweb.com/android/>.
- Downloaded from your personal account of the Dr.Web Anti-virus service provider.
- Received from the anti-virus network administrator of your company.

Centralized protection mode is not available:

- For Dr.Web installed from Google Play.
- For Dr.Web installed from Huawei AppGallery.
- For Dr.Web on Android TV.

Components controlled from the centralized protection server

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

The following components can be controlled from the centralized protection server:

- [Dr.Web Scanner](#). Allows you to scan your device on demand and according to a schedule. It also allows you to launch scanning from the centralized protection server remotely.
- [SpIDer Guard](#).
- [Call and SMS Filter](#).
- [Dr.Web Anti-Theft](#).
- [URL Filter](#).
- [Application Filter](#).

Licensing in the centralized protection mode

In the centralized protection mode, the [license key file](#) is automatically downloaded from the server; your personal license is not used. If the license expires or gets blocked, contact the anti-virus network administrator of your company in order to obtain a new license, or extend your Dr.Web Anti-virus service subscription, after receiving the corresponding notification.



Virus database update in the centralized protection mode

In the centralized protection mode, you cannot update the virus databases manually. Updates are downloaded automatically from the centralized protection server. Update settings may be modified and blocked for compliance with your company security policy or according to the list of purchased services. If the mobile mode is enabled on the server and the connection with the centralized protection server is lost, you can update the virus databases manually.

Application update in the centralized protection mode

Some versions of the centralized protection server support updating Dr.Web Security Space for Android. If you select the **New version** check box in the application settings, you will receive a notification whenever a new version of the application is available and will be prompted to install it. Contact the anti-virus network administrator of your company for details.

Application versions downloaded from the Doctor Web website cannot be updated from the centralized protection server. In these application versions, only the virus databases can be updated in the centralized protection mode.

10.1. Switching to Centralized Protection Mode

To switch the app to the centralized protection mode, [connect](#) to the centralized protection server.



To connect to the centralized protection server 11.0.0 or later, Dr.Web 11.0.0 or later is required.

After you connect to the server, the following permissions can be requested:

- Basic permissions (access your photos, media, and files, contacts, etc.)—for functionality of most app features.
- Call and SMS filter (set Dr.Web as a default phone app)—for call and SMS filtering.
- Device administration—to protect the app from uninstalling and to use the full functionality of Anti-theft.
- Access to accessibility features—for app filtering and full functionality of URL filter, Anti-theft, and Parental Control.
- Drawing over other apps—for app filtering and Firewall functionality.



Connecting to the centralized protection server

Automatic connection

If you have received your Dr.Web version from the anti-virus network administrator of your company or from the Dr.Web Anti-virus service provider, Dr.Web connects to the centralized protection server automatically. For that, the installation package must be run from the internal memory of your device.

Entering connection settings

To connect to the centralized protection server, you need to specify connection settings received from the anti-virus network administrator or from your Dr.Web Anti-virus service provider.

1. Make sure your device is connected to the network.
2. On the **Settings** screen (see [Figure 34](#)), select **Administration**.
If Dr.Web Anti-theft is enabled on your device, enter your Dr.Web account password.
3. Select the **Dr.Web Agent** check box.




The **Dr.Web Agent** check box is selected by default in the Dr.Web versions that have been received from the anti-virus network administrator of your company or from the Dr.Web Anti-virus service provider.

4. When you enable the centralized protection mode, the application restores settings of your last connection.

However, if the [configuration file](#) is stored on your device, the configuration settings from this file are used. To use another settings, for example, from your installation package, [reset connection settings](#).

If you are connecting to the server for the first time or connection settings are changed, enter the following settings:

- IP address of the centralized protection server.
- Additional authentication settings: ID (assigned to your device for registration) and a password. These settings are saved automatically, so it is not required to enter them again the next time you are connecting to the server. If you want to connect to the server as a newbie, tap **Menu**  and select **Connect as a newbie**.

5. Tap **Connect**.

Connecting using configuration file

The `install.cfg` file received from the anti-virus network administrator or your Dr.Web Anti-virus service provider contains settings to connect to the centralized protection server.




1. Make sure your device is connected to the network.
2. Place the `install.cfg` file to the root folder or any of the folders at the first nesting level of the internal device memory.
3. On the settings screen (see [Figure 34](#)), tap **Administration**.
If Dr.Web Anti-theft is enabled on your device, enter Dr.Web account password to open **Administration**.
4. Select the **Dr.Web Agent** check box.
If the file is downloaded to the device, fields for entering the connection settings will be filled in automatically.



The **Dr.Web Agent** check box is selected by default in the Dr.Web versions that have been received from the anti-virus network administrator of your company or from the Dr.Web Anti-virus service provider. As the application is installed, it starts to search the configuration file and tries to connect to the server. If the file is not found or it contains incorrect connection settings, clear the **Dr.Web Agent** check box and select it again, then enter the settings [manually](#) or use the configuration file with correct settings.

5. Tap **Connect**.

Resetting connection settings

1. Tap **Menu**  on the connection settings entering screen.
2. Tap **Reset connection settings**.

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

Connection errors

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

License (subscription) has expired. Contact your anti-virus network administrator in order to get a license or extend your Dr.Web Anti-virus service subscription.

Subscription is blocked. Contact your Dr.Web Anti-virus service provider in order to enable your subscription.

Running Dr.Web for Android is not allowed by the server. The error occurs if your service plan does not support the use of Dr.Web for Android, or running Dr.Web for Android is disabled by the anti-virus network administrator.



10.2. Administration

If Application filter configuration is enabled on the centralized protection server, you can select applications that will be available on your device.

You can allow or restrict launch of both system and user applications. System applications are located at the top of the list and, by default, are marked as available. User applications are located lower in the list.

To configure Application filter

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



Application launch settings specified on the user device will be applied only if Application filter is enabled for this device on the centralized protection server.

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

10.3. Switching to Standalone Mode

To use the Dr.Web standalone operation mode, open settings screen (see [Figure 34](#)) and tap **Administration** section. Then clear the **Dr.Web Agent** check box.

When the standalone mode is on, all anti-virus settings are restored to their previous or default values. You can once again access all features of Dr.Web.

To operate in the standalone mode, a valid personal [license](#) is required. The license received from centralized protection server cannot be used in this mode. If necessary, you can [purchase](#) or [renew](#) a personal license.



11. Dr.Web on Android TV

The following options are available on the Dr.Web main screen (see [Figure 36](#)):

- [Events](#)
- [Scanner](#)
- [Firewall](#)
- [Security Auditor](#)
- [Miscellaneous](#)

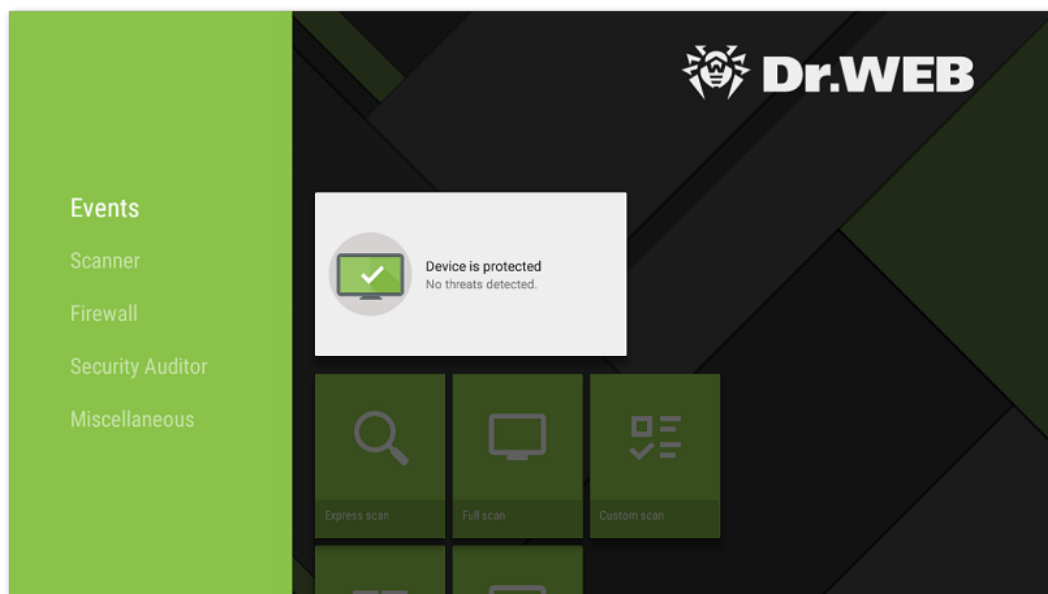


Figure 36. Dr.Web on Android TV

Features of Dr.Web on Android TV



On devices running Android TV, the centralized protection mode is not available.

Permissions

When you launch the application for the first time, you will be prompted to provide the following [permissions](#):

- Access your photos, media and files on your device.
- Access your contacts.

Allow the application to access the required data.



On devices with Android 11.0 or later, the app also requests the permission to access all files.

To allow access to all files

1. In the permission request window, tap the **Go to Settings** button.
2. On the Dr.Web system settings screen, select **Permissions**.
3. Select **Files and media**.
4. Select the **Allow all the time** option.
5. In the dialog window, tap **Allow**.

Interface

- It is not possible to create a [widget](#).
- [Notification bar](#) is unavailable.

11.1. Events on Android TV

The **Events** bar displays current device protection status.

- The green icon indicates that the device is protected. No additional actions are required.
- The yellow icon indicates that Dr.Web has detected issues, for example, a missing license or a vulnerability. To learn more about the detected issues and to eliminate them, select the status bar.
- The red icon indicates that Dr.Web has detected suspicious changes in system area or threats. To open check results and neutralize the threats, select the status bar.

If Dr.Web has detected multiple events that require your attention, select the status bar to open the **Events** screen, which will display all important events.

11.2. Anti-Virus Protection on Android TV

- [SpIDer Guard](#) checks your file system in real time.
- [Dr.Web Scanner](#) allows you to scan your device for threats manually.
- On the [Check results](#) screen, you can select actions to neutralize the detected security threats.

11.2.1. Real-Time SpIDer Guard Protection on Android TV

Enabling real-time protection

When you open Dr.Web for the first time, the constant protection is enabled automatically after you accept the License Agreement. SpIDer Guard keeps protecting the device file system even



if you close the application. If SplDer Guard detects a suspicious change in system area or a threat, the alerting notification appears at the bottom part of the screen.

Configuration

To enable, disable, or configure SplDer Guard, open the Dr.Web main screen and select **Miscellaneous** > **Settings** > **SplDer Guard** (see [Dr.Web Settings on Android TV](#) section).

Statistics

The application registers the events related to the SplDer Guard operation: enabling/disabling SplDer Guard, threat detections, and check results of the device storage and installed applications. SplDer Guard statistics appear in the **Actions** section of the **Statistics** tab and are sorted by date (see [Statistics](#) section).

11.2.2. Dr.Web Scanner on Android TV

Dr.Web Scanner scans files on your device upon your request. It performs express or full check of the whole file system or scans critical files and folders only.

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

Scanning

To scan the system, on the Dr.Web main screen, select **Scanner** (see [Figure 37](#)) and then select one of the following actions:

- To check installed applications, select **Express scan**.
- To scan all the files in the system, select **Full scan**.
- To scan only critical files and folders, select **Custom scan** and then select an object you want to scan.

To scan the whole folder, select the **Scan folder** option. To go up a level, select **Up**.

If your device is rooted, you can also scan `/sbin` and `/data` folders located in the root directory.

After the scanning is finished, the following information is shown:

- Number of scanned objects.
- Number of detected threats.
- Start time.
- Scan time.

To open check results, select **OK**.

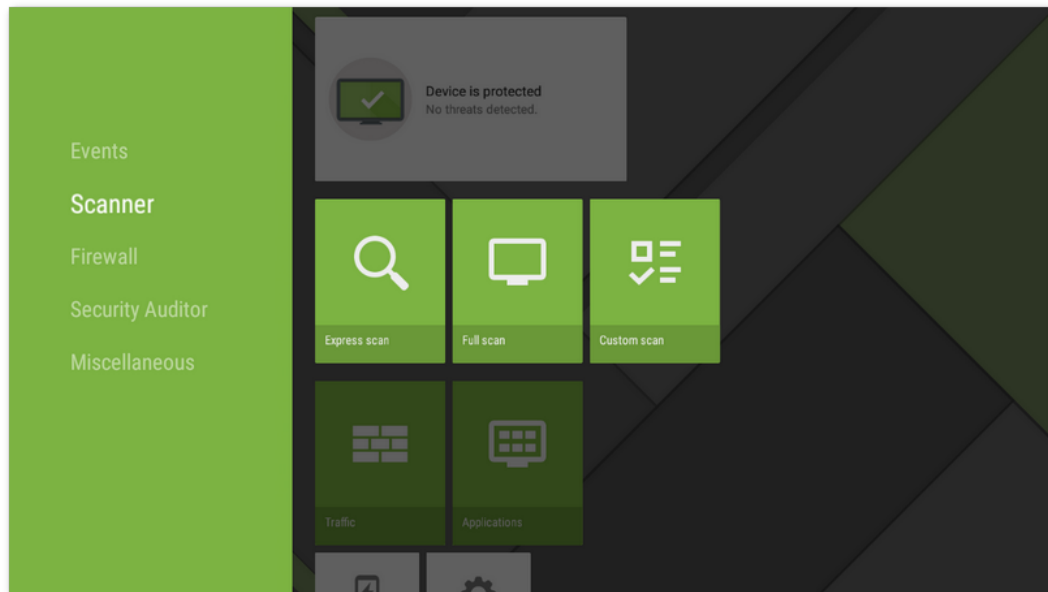


Figure 37. Dr.Web Scanner

Dr.Web Scanner settings

To access Dr.Web Scanner settings, open the Dr.Web main screen and select **Miscellaneous** > **Settings** > **Scanner** (see section [Dr.Web Settings on Android TV](#)).

Statistics

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

11.2.3. Check Results on Android TV

How to open check results

If [SpIDer Guard](#) detects a suspicious change in system area or a threat, it will show a notification. To open check results, on the Dr.Web main screen, select **Events**.

To open the [Dr.Web Scanner](#) check results, select **OK**.

Neutralizing Threats

On the **Check results** screen, you can review the list of threats and changes in the system area. For each object, its type and name are specified, as well as the icon of the recommended option for the object.



Objects are marked in different colors depending on the degree of danger. Listed below are the threat types in decreasing danger order:

1. Malware.
2. Riskware.
3. Hacktool program.
4. Adware.
5. [Changes in the system area](#):
 - New files in system area.
 - Change of system files.
 - Deletion of system files.
6. Joke program.

To view the file path, select the object. For threats that are detected in apps, the app package name is also specified.

Neutralizing all threats

To delete all threats

- In the top-right corner of the **Check results** screen, select **Menu** > **Delete all**.

To move all threats to the quarantine

- In the top-right corner of the **Check results** screen, select **Menu** > **All to quarantine**.

Neutralizing one threat at a time

Each object has its own set of available options. To expand the option list, select the object. Recommended options are placed first. Select one of the options:



Cure to cure the infected application.

The option is available for some [threats in system applications](#) if root access is enabled on the device.



Delete to delete the threat from your device.

In some cases, Dr.Web cannot delete applications that use Android accessibility features. If Dr.Web does not delete the app after you select the **Delete** option, reboot to safe mode and delete the app manually. If access to accessibility features has been granted to Dr.Web, the app will be deleted automatically once you select the **Delete** option.

The option is not available for [threats in system applications](#) in the following cases:

- If root access is not allowed on your device.
- If the application cannot be safely deleted.



- If a threat modification is detected. To identify if the app does pose a threat, report a false positive.



Move to quarantine to move the threat to an isolated folder (see [Quarantine](#)).

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



Ignore to temporarily leave the change in the system area or the threat as it is.



Send to laboratory or **False positive** to send the file to the Doctor Web anti-virus laboratory for analysis. The analysis will show if there is a threat or it is a false positive. If it is a false positive error, it will be fixed. To receive the analysis results, enter your email address.

If the file is sent to the laboratory successfully, the **Ignore** option is automatically applied to the object.

The **Send to laboratory** option is available only for added or changed executable files in the system area: .jar, .odex, .so, APK, ELF files, etc.

The **False positive** option is available only for threat modifications and for threats detected in the system area.



More on the Internet to view the detected object description on the Doctor Web website.

11.3. Dr.Web Firewall on Android TV

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

Certain aspects of Dr.Web Firewall operation

Dr.Web Firewall is based on the VPN for Android technology, so it does not require root access on the device. However, the VPN for Android technology sets a number of limitations:

- Only one app can use VPN at a time. As a result, before enabling VPN, the app prompts you to provide it the corresponding permission. If you give the permission, the app starts using VPN, but it also blocks access to VPN for other apps. Dr.Web Firewall requests the VPN permission the first time you enable the component and at every device reboot. It can also request the permission after VPN requests from other apps. VPN is shared between the apps over time. Dr.Web Firewall can operate only when it gets the full rights to use VPN.
- Enabling Dr.Web Firewall can result in inability to connect the device on which Dr.Web Firewall runs to other devices directly using Wi-Fi or a local network. It depends on the device model and the apps which are used to establish a connection between devices.
- When Dr.Web Firewall is enabled, you cannot use your device as a Wi-Fi access point.



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



To enable Dr.Web Firewall

1. On the Dr.Web main screen, select **Firewall** (see [Figure 38](#)).
2. Do one of the following:
 - Use the toggle button to the right of the **Log** panel.
 - Select **Traffic** or **Log** and tap **Enable**.

By default, Dr.Web Firewall is disabled. Dr.Web requests a permission to set up a VPN connection. You need to grant the permission in order for Dr.Web Firewall to function.



If another app gets the rights to use VPN during the operation of Dr.Web Firewall, the component will be disabled. You will be notified on it.

If you use a restricted profile (guest profile) on your device, Dr.Web Firewall is disabled.



Figure 38. Dr.Web Firewall on Android TV

11.3.1. Managing Network Activity on Android TV


Information on the activity of network connections is provided on the **Traffic** screen. Two tabs are available on the screen: **Active apps** and **All apps** (see [Figure 39](#)).

Active apps tab

The tab displays a real-time list of active connections initiated by apps installed on the device.

The following information is provided on every app on the **Active apps** tab:



- Total amount of incoming and outgoing traffic used by established connections.
- [Access to data transmission over Wi-Fi.](#)
- User settings. Icons of apps with a changed access to data transmission are marked with the  icon.

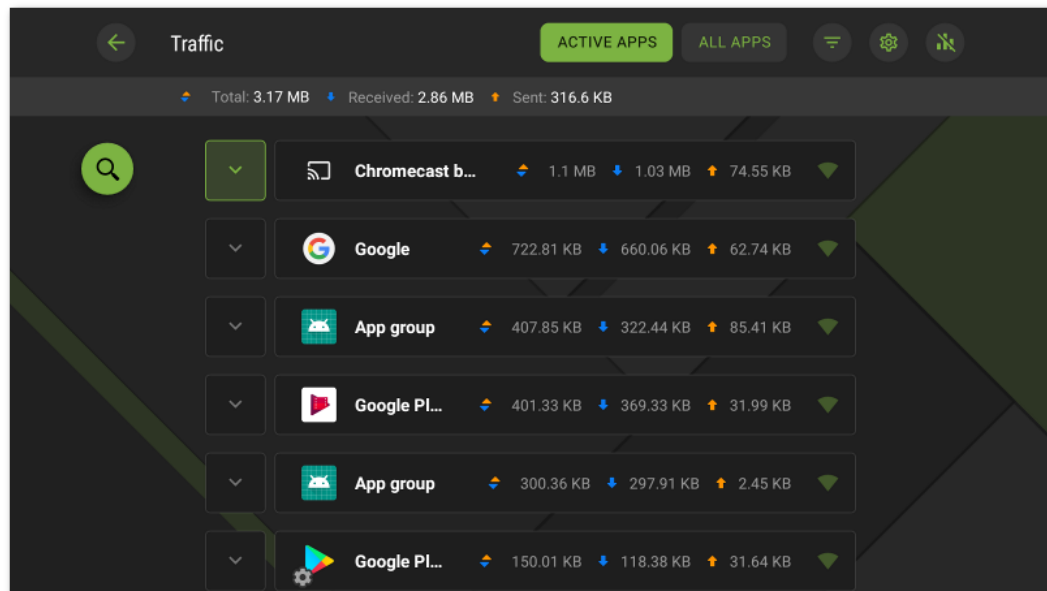







Figure 39. Active apps tab

App connections

Tap the  icon to the left of the name of an app to see detailed information on connections established by the app:

- list of established connections;
- total amount of incoming and outgoing traffic used by each of the established connections;
- connection rule:
 -  allowing,
 -  blocking,
 -  redirecting,
 -  not set.

Tap the connection row to go to the [Connection](#) screen.


All apps tab

To view information on the internet traffic of apps installed on your device, as well as to configure connection rules for them, open the **All apps** tab.




On the **All apps** tab, you can review the total amount of data transferred over networks and the amount of sent and received data. You can view the list of apps (and app groups) as well as the amount of spent traffic for each of them.

The following information is provided on every app on the **All apps** tab:

- Total amount of incoming and outgoing traffic used by established connections.
- [Access to data transmission over Wi-Fi](#).
- User settings. Icons of applications with a changed access to data transmission are marked with the  icon.


App filtering and sorting

To filter or sort the list of apps, tap the  icon in the top-right corner of the screen and select the options:

- Display apps with no traffic;
- Sort:
 - highest traffic first—apps with the highest traffic will be at the top of the list;
 - lowest traffic first—apps with the lowest traffic will be at the top of the list;
 - A to Z;
 - Z to A.

By default, apps are sorted by traffic (apps with the highest traffic are at the top of the list), apps with no traffic are displayed. To restore the default list view, tap **Reset** on the **Filter** screen.

Search

To quickly navigate to a certain app, use the search by app name function. Tap the  icon on the left side of the screen and enter your query in the search field.

Settings

To manage settings for all apps, on the **Traffic** screen, tap  in the top-right corner of the screen.

The following settings are available:

- **Use IPv6.** Allows you to enable or disable the use of IPv6 in parallel with IPv4.
- **Allow DNS over TCP.** Allows you to enable or disable the use of the DNS over TCP protocol for DNS query redirection and the hiding of domain names.




The use of the DNS over TCP protocol may prevent domain names from being displayed on some Firewall screens.

The setting works on devices which support this protocol type. The setting is disabled by default.

- **Block connections for new apps.** Allows you to block access to networks for apps installed after enabling the setting. The setting is enabled by default.
- **Block connections for all apps.** Allows you to block access to networks for all apps installed on the device. If the access is [granted](#) to one app, the setting will be disabled.
- **Store rules and statistics after deleting apps.** Allows you to store data of apps removed from your device for the selected period of time: one week, month, or year.

Clearing statistics, settings and rules for apps

To delete all statistics, settings and rules for all apps

1. On the **Traffic** screen, tap the  icon in the top-right corner.
2. Select the relevant check boxes and tap **Clear**.

11.3.2. Processing App Traffic on Android TV

Dr.Web Firewall filters traffic on the app level and, therefore, controls the access of apps and processes to network resources. To view information on the internet traffic of apps installed on your device, as well as to configure connection rules for them, open the app screen (see [Figure 40](#)).

Two tabs are available on the screen:

- The [Statistics](#) tab allows you to review statistics on traffic use of any app on the device and change the individual app settings.
- The [Rules](#) tab allows you to manage rules for connections established by apps.

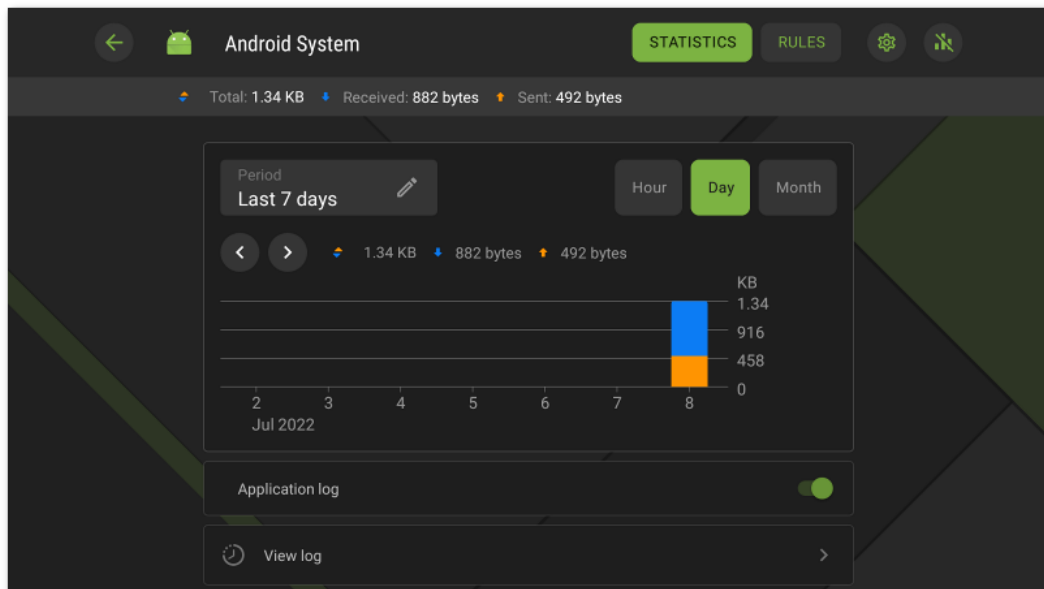


Figure 40. App screen

App group

Some system apps can be combined into an app group. To view the list of apps in a group, on the app screen, tap the counter to the right of the **App group** header.

11.3.2.1. App Statistics and Settings on Android TV

On the **Statistics** tab of the app (app group) traffic screen, you can review the statistics of internet traffic use by this app shown as a graphical diagram (see [Figure 41](#)), as well as change Firewall settings for this app.

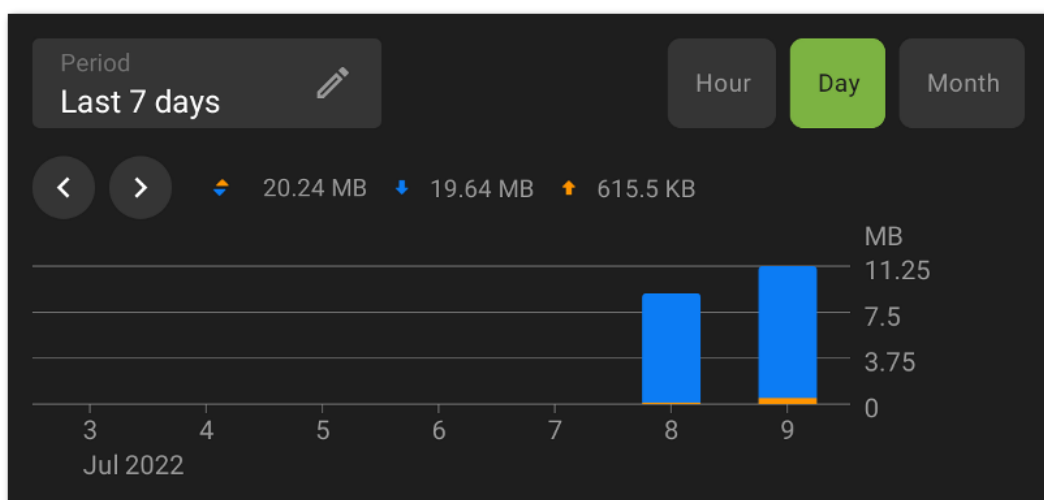


Figure 41. Internet traffic statistics



Internet traffic statistics

Outgoing app traffic is marked with orange on the graph, incoming traffic is marked with blue. The numeric values of the amount of traffic (total, incoming, and outgoing) spent over a specified period of time are shown above the graph.

When reviewing internet traffic statistics, you can do the following:

- Select the period of time over which you want to review the statistics in the field above the diagram. You can review the statistics for the current day, last 7 days, current month, previous month, or specify any other period manually by setting the start and end dates.
- Change the scale of the displayed statistical data within the selected period: hour, day, or month, by using the options above the diagram.

Clearing statistics

- To clear statistics for all apps:
 1. On the **Firewall** screen, select **Traffic**.
 2. On the **Traffic** screen, tap the  icon in the top-right corner.
 3. Select the **App statistics** check box and tap **Clear**.
- To clear statistics for a specific app:
 1. On the **Traffic** screen, select the app to clear the statistics for.
 2. On the app screen, tap the  icon in the top-right corner.
 3. Select the **App statistics** check box and tap **Clear**.



Once you remove an app from the device, its statistics will be cleared automatically within the next 5 minutes.

Application log

Events related to the network activity of apps installed on the device are registered in [application logs](#). Use the toggle button to enable or re-enable the application log. To go to the log, tap **View log**.

App settings

To go to the app (app group) settings, on the **Statistics** tab, tap  in the top-right corner of the screen (see [Figure 40](#)).



Access to data transmission over Wi-Fi

Use this toggle button to block or allow access to data transmission over Wi-Fi for this app. By default, the access is allowed. The access indicator is displayed in the app row on the **Traffic** screen (green indicates that the access is allowed, gray means blocked).

Block all connections not allowed by the rules

To block all connections for an app by default, use the **Block all connections not allowed by the rules** toggle button. With no allowing rules set, the app will be unable to initiate any connections.

An allowing rule for port 53 is automatically added when enabling the **Block all connections not allowed by the rules** setting for this app. This rule (set for the DNS, UDP, or ALL protocols) is mandatory for the functioning of allowing rules with domain names.



To ensure that this setting works as intended in the presence of allowing rules with domain names, disable the use of a private DNS server in your device settings.

Do not control the app



The setting is not available for some system apps.

Dr.Web Firewall is based on the VPN for Android technology. VPN prevents apps from functioning if they use a technology which is incompatible with VPN, e.g. Wi-Fi Direct. This can result in inability to connect your device to other devices. Disabling Firewall completely is not recommended in this case. Instead, disable Dr.Web Firewall control for the app (or app group). To do so, use the **Do not control the app** toggle button.

It is recommended to disable Dr.Web Firewall control only for your trusted apps.

When the option is enabled, Dr.Web Firewall does not control network connections of the app even if you customize traffic settings for it in the Dr.Web Firewall settings. The app traffic is not monitored.

11.3.2.2. Connection Rules on Android TV

App traffic is managed through connections established by apps. You can set up allowing, blocking, or redirecting rules for connections with specified IP addresses and ports for every app installed on the device.



Connections

General information on each connection is shown on the **Connection** screen (see [Figure 42](#)). To go to this screen, do one of the following:

- On the [Active apps](#) tab of the **Traffic** screen, tap the ▼ icon to the left of the name of an app and then tap a connection row.
- In the [Firewall log](#):
 - When events are grouped by date: tap a connection row.
 - When events are grouped by app name: expand the list of app connections by tapping the ▼ icon to the left of the name of an app and then tap a connection row.
- In an [application log](#): expand the list of app connections by tapping the ▼ icon to the right of an event date and then tap a connection row.

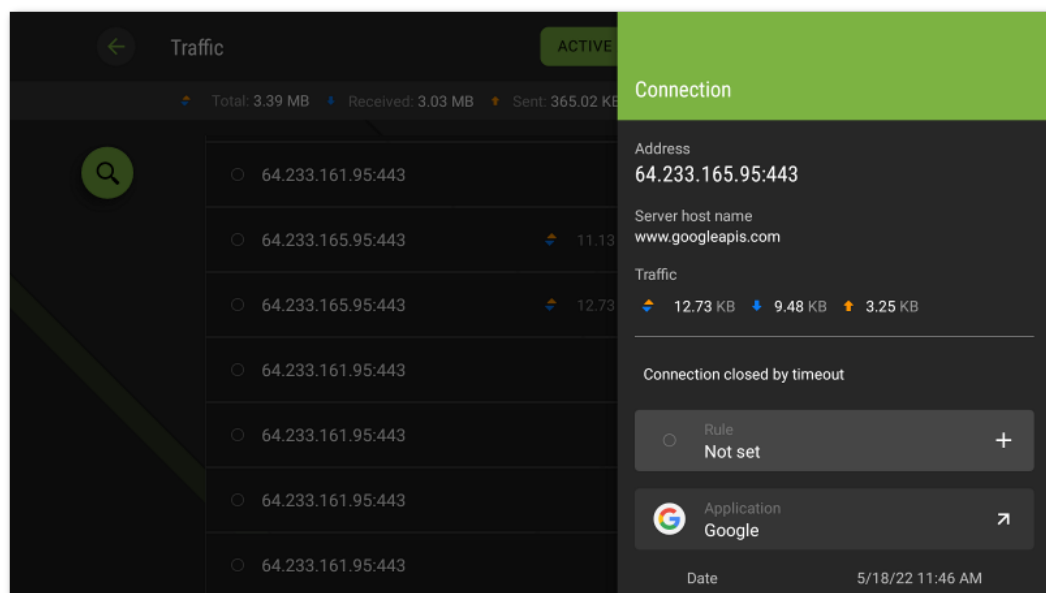


Figure 42. Connection screen

The **Connection** screen contains the following information:

- connection address and port;
- host name (if available);
- amount of incoming and outgoing traffic received or transmitted by the connection;
- connection status;
- connection rule;
- app that established the connection;
- date and time;
- connection type;








- protocol.

Connection rules are displayed on the [Rules](#) tab of the app screen.

Connection rules

Creating rules

To create a new connection rule

1. For connections without rules:
 - On the **Connection** screen, tap the  icon to the right of the **Rule** section.
For any connection:
 - On the app screen, open the **Rules** tab and tap the  icon on the left side of the screen.
2. On the next screen, select the rule type:
 -  allowing,
 -  blocking,
 -  redirecting.
3. Check the IP address/host name. If the address is not specified, enter a valid IP address (in the a.b.c.d format for IPv4 addresses or [a:b:c:d:e:f:g:h] for IPv6), an IP address range (in the a1.b1.c1.d1-a2.b2.c2.d2 or [a1:b1:c1:d1:e1:f1:g1:h1]-[a2:b2:c2:d2:e2:f2:g2:h2] format), or a network (in the a.b.c.0/n format, where n is a number from 1 to 32). If you are creating a redirecting rule, enter the redirection address in the field below. You can specify a host name instead of an address.
4. Tap **More** for the additional **Protocol** setting to choose a network protocol for the connection.
5. Tap **Save**.

Icons of apps with set connection rules are marked with the  icon.

Viewing rules

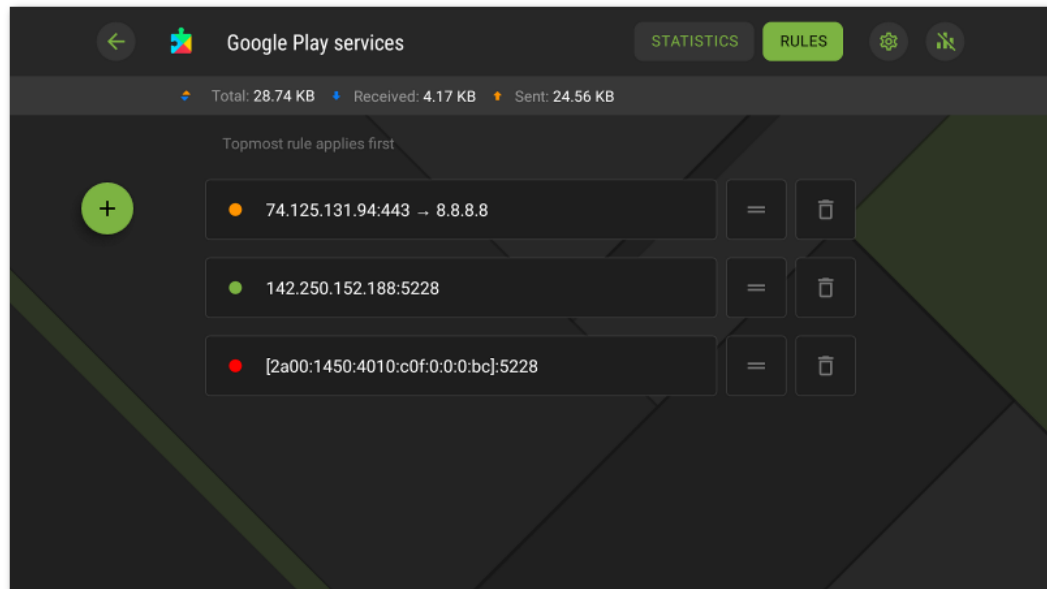


Figure 43. Rules tab

To view all connection rules of an app

- Go to the app screen and open the **Rules** tab (see [Figure 43](#)).


The tab contains the list of all rules set for the app, in the order of their execution.

To change the order of rule execution

- Tap and hold the **=** icon next to the rule you want to move, then drag the rule to the desired position on the list.

Editing rules


To edit an existing rule

1. Do one of the following:
 - On the **Connection** screen, tap the  icon to the right of the rule.
 - On the app screen, open the **Rules** tab and tap the rule row.
2. Make changes.
3. Tap **Save**.




Deleting rules


To delete a rule

- On the rule editing screen:
 1. Tap **Delete rule**.
 2. On your next step, tap **Delete**.
- On the **Rules** tab of the app screen:
 1. Tap the  icon to the right of the rule.
 2. On your next step, tap **Delete**.

To delete all rules for a certain app

1. On the app screen, open the **Rules** tab and tap the  icon in the top-right corner of the screen.
2. On your next step, select the **App rules** check box and tap **Clear**.

To delete all rules for all apps

1. On the **Firewall** screen, select **Traffic**.
2. On the **Traffic** screen, tap the  icon in the top-right corner of the screen.
3. On your next step, select the **App settings and rules** check box and tap **Clear**.

Block all connections not allowed by the rules

You can block all connections except for those allowed by rules for an app by using the [corresponding toggle button](#) on the app settings screen.

11.3.2.3. Application Log on Android TV

Each application log contains a list of events related to network connections of a certain app installed on your device.

To enable application logging

1. On the **Traffic** screen, select an app.
2. On the app screen, use the **Application log** toggle button.

To open an application log

1. On the **Traffic** tab, select an app from the list.
2. On the app screen, tap **View log**.



Viewing an application log


All events related to the app are grouped by date. To open the list of events for a certain date, select the date from the list.

You can review the following information for each event:

- connection address and port;
- used up traffic;
- connection rule:
 - ● allowing,
 - ● blocking,
 - ● redirecting,
 - ○ not set.

Tap the connection row to go to the [Connection](#) screen and set up rules.

To clear an application log

1. On the **Application log** screen, tap the  icon in the top-right corner.
2. Tap **Clear**.

To disable application logging

1. On the **Traffic** screen, select an app.
2. On the app screen, use the **Application log** toggle button.

11.3.3. Dr.Web Firewall Log on Android TV

To open the list of all events related to the operation of Dr.Web Firewall, on the **Firewall** screen, select **Log**.

You can review the following information for each event in the Firewall log (see [Figure 44](#)):

- name of the app;
- connection address and port (as well as the redirection address if such a rule is set);
- used up traffic;
- event date and time;
- connection rule.

When an event is tapped, the [Connection](#) screen opens.

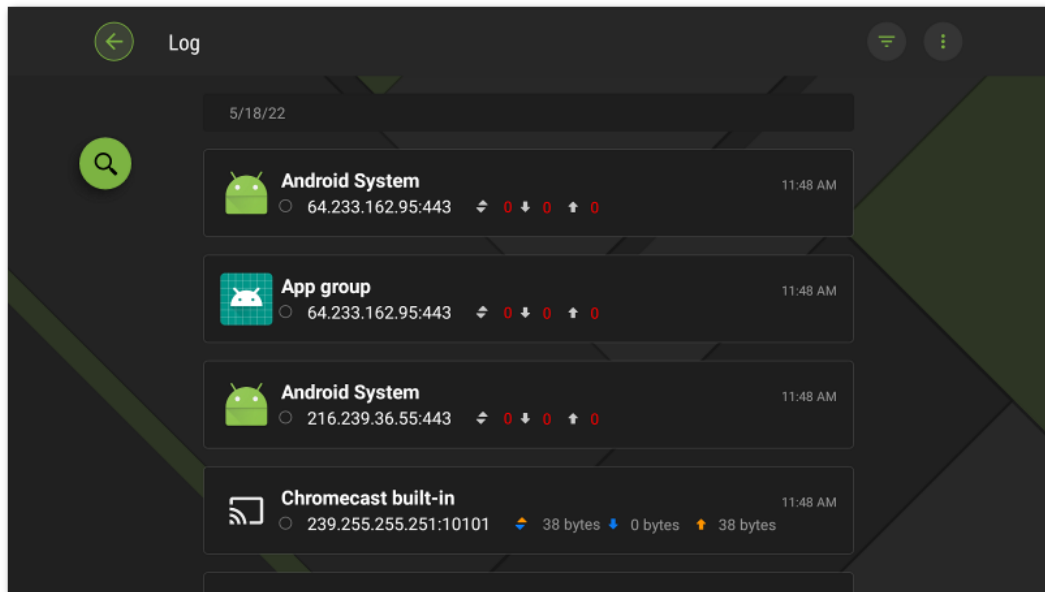



Figure 44. Dr.Web Firewall log

To filter or sort events in the Firewall log


1. Tap the  icon in the top-right corner of the **Log** screen.
2. Select the options:
 - Sort:
 - newest on top—newest events at the top of the log;
 - oldest on top—oldest events at the top of the log;
 - A to Z;
 - Z to A.
 - Display connections:
 - established,
 - reset,
 - redirected,
 - with errors.

By default, events are sorted by date (newest events are at the top of the log), all connections are displayed. To restore the default log view, tap **Reset** on the **Filter** screen.


You can group events by app for easier log navigation.




To group events by app

- On the **Log** screen, tap  in the top-right corner and use the **Group by app name** toggle button.

To search through the Firewall log

- Tap the  icon on the left side of the screen and enter your query in the search field.


To clear the Firewall log

1. On the **Log** screen, tap  in the top-right corner and select the **Clear log** option.
2. Confirm the action by tapping **Clear**.

Maximum log size

By default, the maximum size for the log file is set to 5 MB.

To change the maximum size for the log:

1. On the **Log** screen, tap  in the top-right corner and select the **Maximum log size** option.
2. On the next screen, change the value and tap **Save**.



The maximum log file size must exceed 0 MB.

11.4. Security Auditor on Android TV

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

Dr.Web detects the following security problems:

- [Vulnerabilities](#).
- [System settings](#) that affect device security.
- [Hidden device administrators](#).
- [Applications exploiting Fake ID vulnerability](#).



To open the list of the detected problems (see [Figure 45](#)), select **Security Auditor** on the Dr.Web main screen.

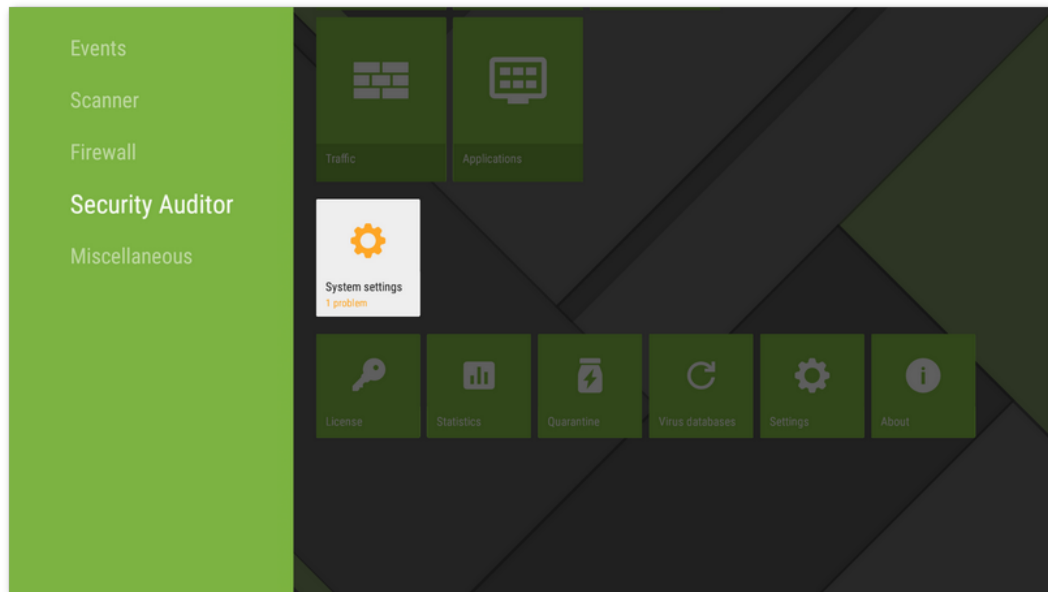


Figure 45. Security Auditor

Vulnerabilities

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

Security Auditor detects the following vulnerabilities in the device system: [BlueBorne](#), [EvilParcel](#), [Extra Field](#), [Fake ID](#), [Janus](#), [ObjectInputStream Serialization](#), [OpenSSLX509Certificate](#), [PendingIntent](#), [SIM Toolkit](#), [Stagefright](#), and [Stagefright 2.0](#).

The vulnerabilities allow adding malicious code to some applications, that may result in performing of dangerous functions by these applications and damage the device.

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.

Root access

The device may become vulnerable to different types of threats if it is rooted, i.e. the procedure of rooting has been performed to attain control (known as root access) over the device system. It results in ability to modify and delete system files, that may potentially damage the device. If you rooted your device yourself, rollback the changes for security reasons. If root access is the



integral feature of your device or you need it for your everyday tasks, be extremely cautious installing applications from the unknown sources.

System settings

Security Auditor detects the following system settings that affects the device security:

- **Debugging enabled.** USB debugging is intended for developers and allows copying data from PC to the device and vice versa, installing the applications on the device, viewing their logs and deleting them in some cases. If you are not a developer and do not use the debug mode, you are recommended to turn this mode off. To open the corresponding device settings section, select **Settings** on the screen with detailed information on the problem.
- **Installation of apps from unknown sources is enabled.** Installing application from unknown sources is one of the main reasons devices running Android get infected. Applications downloaded from elsewhere other than the official market are likely to be unsafe and become a threat to device security. To mitigate risks of installing the unsafe applications, you are recommended to disable application installation from unknown sources. To open the corresponding device settings section, select **Settings** on the screen with detailed information on the problem. You should also scan for viruses all the applications you install on your device. Before scanning, make sure Dr.Web virus databases are up to date.
- **Dr.Web notifications are blocked.** In this case, Dr.Web cannot immediately inform you on detected threats. This compromises security of your device. That is why, you are recommended to enable Dr.Web notifications in the settings of your device.
- **User root certificate installed.** If any user certificates are detected on your device, Security Auditor detects and displays them. Certificates may be used by a third party to monitor your network activity. If you are not aware why these certificates are installed on your device, you are recommended to remove them.

Hidden device administrators

Applications that are activated as device administrators but not shown on the list of administrators on the corresponding section of the device settings cannot be deleted by means of the operation system. Most likely, such applications are potentially harmful for your device.

If you do not know why an application is not displayed in the list of device administrators, you are recommended to delete it from the device. To delete the application, select **Delete** on the screen with the detailed information on the problem related to this application.

Applications exploiting Fake ID vulnerability

If applications exploiting Fake ID vulnerability have been detected on the device, they will be displayed in the separate Security Auditor category. These applications can be malicious, therefore it is recommended to delete them. To delete the application, select **Delete** on the



screen with the detailed information on the problem related to this application, or use standard OS tools.

11.5. Miscellaneous

The **Miscellaneous** screen (see [Figure 46](#)) allows you to open application settings, quarantine and statistics. You can check application version number, license information, such as activation and expiration dates. Also, you can check when virus databases were last updated, and update them manually.

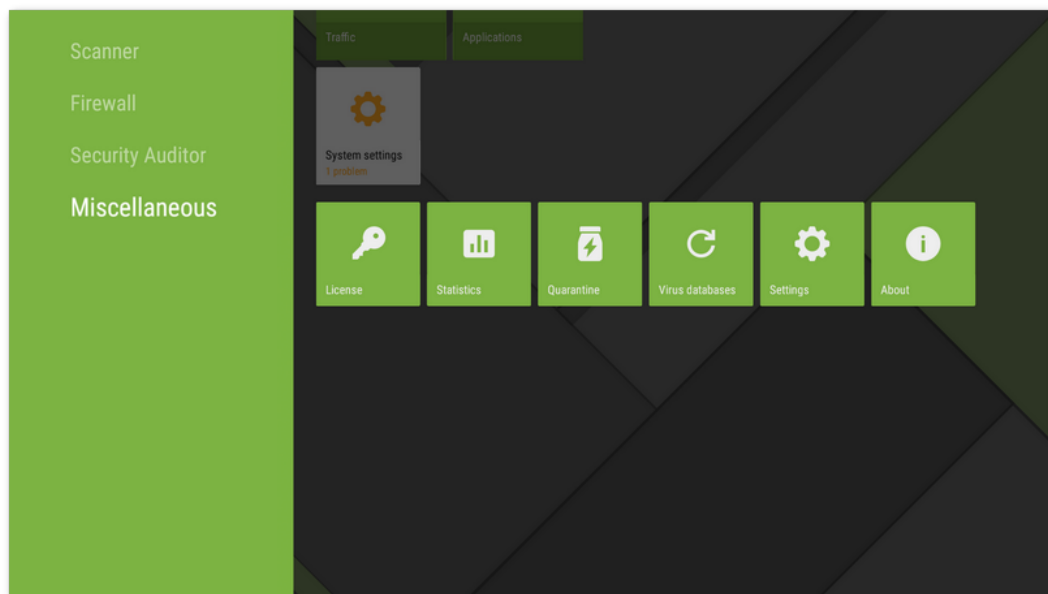


Figure 46. Miscellaneous

License

You can view license activation and expiration dates.

In this window, you can also [buy](#) and [activate](#) a new license.

Statistics

The **Statistics** section contains the information on Dr.Web Scanner check results, enabling and disabling of SpIDer Guard, detected threats and performed actions (see [Statistics](#) section).

Quarantine

Quarantine is a special folder used for isolating and secure storing detected threats (see [Quarantine](#) section).



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 Android 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

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

1. Open the **Virus databases** section.
2. In the opened screen, you will see update status of virus databases, and the date of the last update.

If virus databases are not up to date, you should update them manually. Select **Update** in the right-hand section.



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.

Settings

The **Settings** section allows you to configure anti-virus components, set general application settings, enable and disable sending statistics, and restore default settings (see [Dr.Web Settings on Android TV](#) section).

About

On the **About** screen, you can view application version. It also contains links to Doctor Web official website.

11.5.1. Dr.Web Settings on Android TV

General settings

- **Sound** enables and disables sound notifications on threat detection, deletion or moving to the quarantine. By default, sound notifications are enabled.
- **Send statistics** allows you to enable and disable sending statistics to Doctor Web.



- **Additional options** contains additional settings:
 - **System applications** allows you to enable or disable notifications on [threats in system applications](#) that cannot be safely deleted. This option is disabled by default.

SplDer Guard

- **Files in archives** allows you to enable scanning of files in archives.



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

- **Built-in SD card and removable media** allows you to enable scanning of the built-in SD card and removable media on each mounting. If the setting is enabled, the scan starts every time SplDer Guard is enabled.
- **System area** allows you to monitor [changes in the system area](#). If the setting is enabled, SplDer Guard monitors changes (addition, change, and deletion of files) and notifies only on deletion of any files as well as addition and change of executable files: .jar, .odex, .so, APK, ELF files, etc.
- **Recheck system area** allows you to run a recheck of the system area. SplDer Guard will check previously ignored threats in the system area again.
- **Notifications about system area** allows you to enable notifications on changes of any files in the system area (not only executables).
- **Additional options** allows you to enable and disable detection of adware and riskware (including hacktools and jokes).

Scanner

- **Files in archives** allows you to enable scanning of files in archives.



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

- **Additional options** allows you to enable and disable detection of adware and riskware (including hacktools and jokes).

More

- **Reset settings** allows you to reset settings to default.
- **New app version** (for the version downloaded from the Doctor Web website) allows to check for new versions every time the virus databases get updated. If a new version is available, you will be prompted to download and install it.



12. Technical Support

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

- Download and review the latest manuals and guides at <https://download.drweb.com/doc/>.
- See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
- 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:

- Fill out a web form in the appropriate section at <https://support.drweb.com/>.
- 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/>.



13. Forgot Password?

If you forget your Dr.Web account password, you can reset it:

- [Via email](#). You used this address when creating your Dr.Web account or configuring Dr.Web Anti-theft.
- [Via SMS](#). The option is available only in the app version from the website if the Dr.Web Anti-theft buddy list contains at least one phone number.
- [Via notification](#). The option is available if at least one buddy has confirmed your buddy request in the Dr.Web Security Space app.
- [Via technical support request](#). Our technical support team will be able to help you only after making sure that you are the device owner.



If Dr.Web operates in the [centralized protection mode](#) and Dr.Web Anti-theft is configured on the server, you will not be able to set a new password in the aforementioned ways. Contact the anti-virus network administrator of your company or the Dr.Web Anti-virus service provider and use a [symbolic or QR recovery code](#).

Reset password via email

On the pane for resetting your password via email (see [Figure 47](#)), the following are shown:

⋮ **Key**. This is a unique character sequence that has been generated for your account.

✉ **Email address**. You used this address when creating your Dr.Web account or configuring Dr.Web Anti-theft.

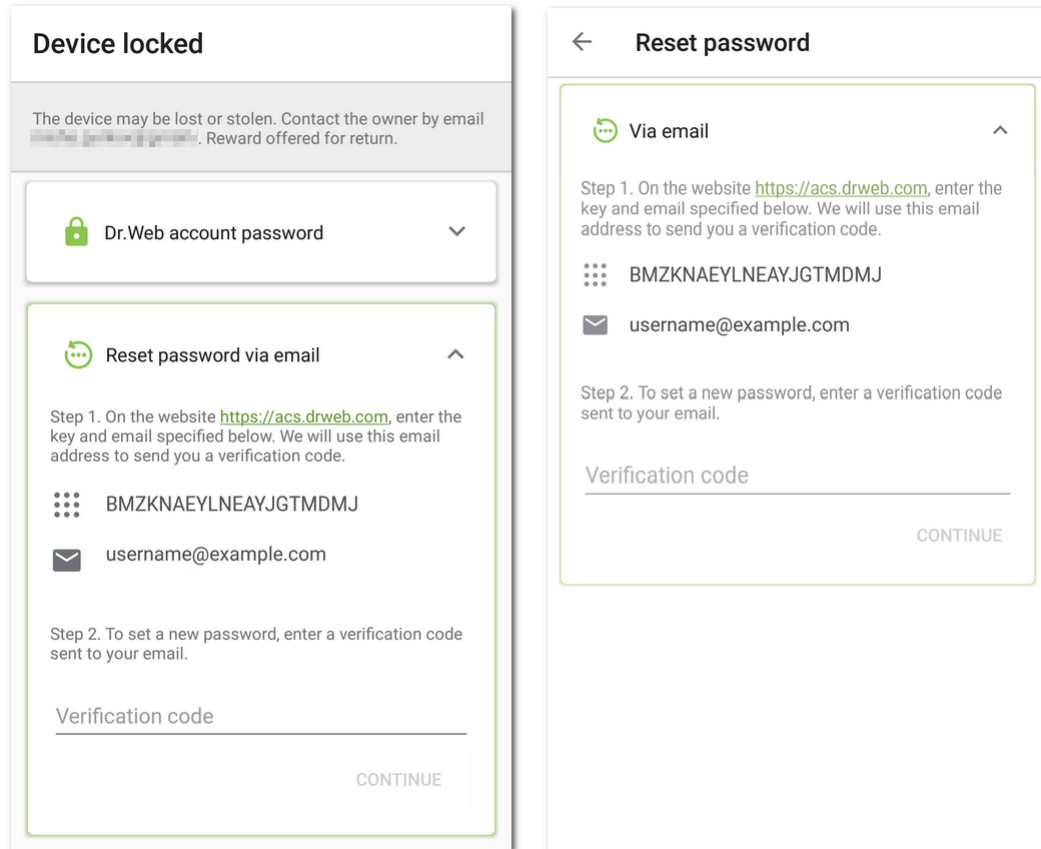


Figure 47. Reset password via email
Locked (left) and unlocked (right) device

To reset your password

1. On a computer or another device, open the Dr.Web account website: <https://acs.drweb.com> (see [Figure 48](#)).



If you use Dr.Web 11.1.3 or earlier, use the Dr.Web Anti-theft website at <https://antitheft.drweb.com/> to reset your password, or update your app to version 12.



The screenshot shows the 'Dr.WEB Account' screen. At the top is a green header with the Dr.Web logo and the word 'Account'. Below the header, there are two input fields: 'Key' and 'Email address'. Below these fields is a button labeled 'Receive code'. At the bottom, there is a paragraph of text explaining the process: 'Enter the key and email address specified on the screen of your device. You will receive an email with a verification code. Use this code to set a new Dr.Web account password. [Learn more...](#)'

Figure 48. Dr.Web Account

2. On this page, enter the key and email address (see [Figure 49](#)) displayed in the Dr.Web app.

The screenshot shows the 'Dr.WEB Account' screen with the input fields filled. The 'Key' field contains the text 'BMZKNAEYLNEAYJGTMDMJ'. The 'Email address' field contains the text 'username@example.com'. The 'Receive code' button is now green. The explanatory text at the bottom remains the same: 'Enter the key and email address specified on the screen of your device. You will receive an email with a verification code. Use this code to set a new Dr.Web account password. [Learn more...](#)'

Figure 49. Entering the key and email address

3. Tap **Receive code**.



If you enter the correct data, a message appears confirming that a verification code has been sent to your email (see [Figure 50](#)).

If you do not receive the email within 10 minutes:

1. Please check your Spam folder.
2. Try entering the data again. You could have entered the wrong key or an email address that is different from the one shown in the Dr.Web app.
3. If after that you do not receive the email, contact the Doctor Web technical support. To do so, tap **Did not receive the email?** (see [Figure 50](#)).

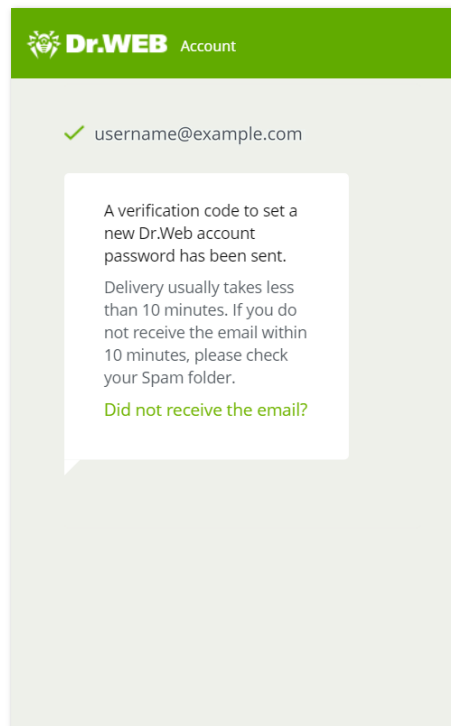


Figure 50. Notification on verification code sending

4. Open the email from the Dr.Web Account service. You will find your verification code there.



5. In the Dr.Web app, enter the verification code in the **Verification code** field (see [Figure 51](#)).

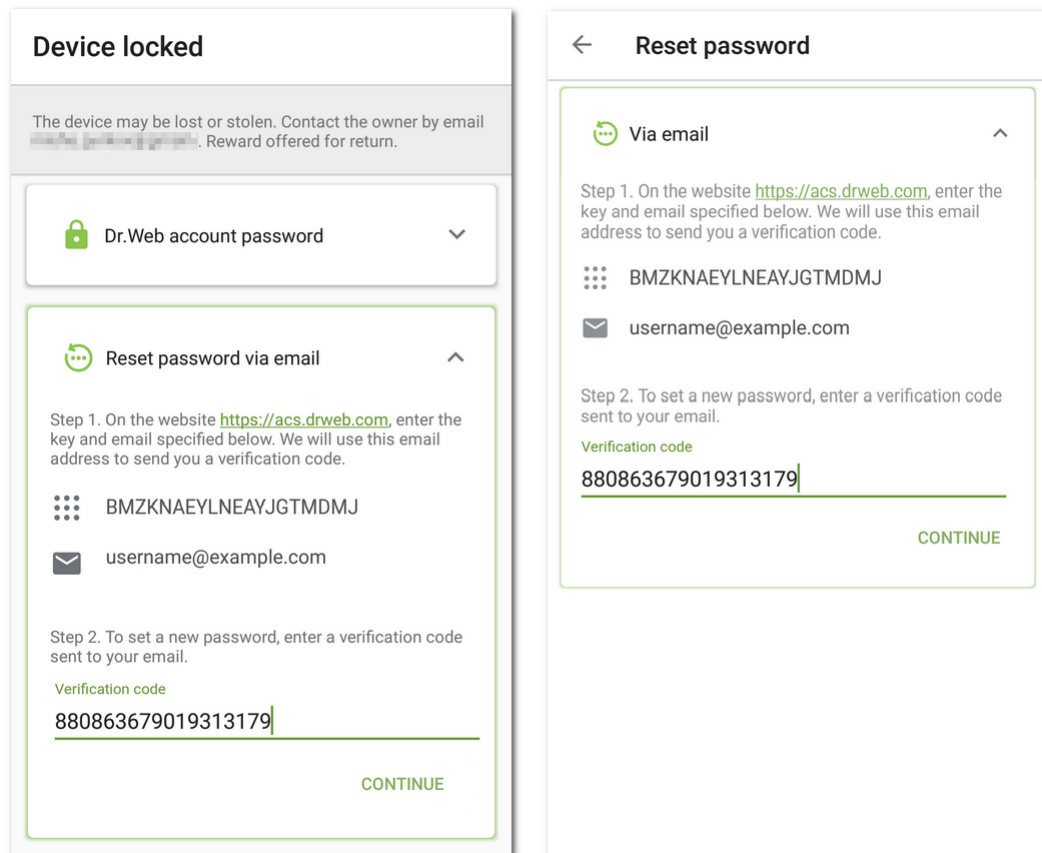




Figure 51. Entering the verification code received via email
Locked (left) and unlocked (right) device

6. Tap **Continue**.
7. On the **Change password** screen, enter a new password. The password must contain at least 4 characters.
- Tap  to the right of the password field to show the password characters. Tap  to hide the characters.
8. Confirm the password and tap **Save**.

Reset password via SMS from a buddy's number

You can reset your password this way if the following conditions are met:

1. Your app version was downloaded from the Doctor Web website.
2. Your device is within the network service area and switched on.
3. Dr.Web Anti-theft is enabled on your device.
4. The Anti-theft [I trust](#) list contains at least one phone number.
5. The phone number the SMS command will be sent from is added to the [I trust](#) list.



6. You know the phone number of the SIM card that is used on your device. The SMS command can only be sent to this number.

If you do not know the number, insert a SIM card with a known number.



If you use two SIM cards on your device, the SMS command can be sent to any of your numbers.

To reset password

1. Send the SMS text message **#RESETPASSWORD#** to your device from a buddy's number.

A list of phone numbers that an SMS command can be sent from is shown on the **Device locked** or **Reset password** screen (see [Figure 52](#)). SMS commands are case-insensitive.

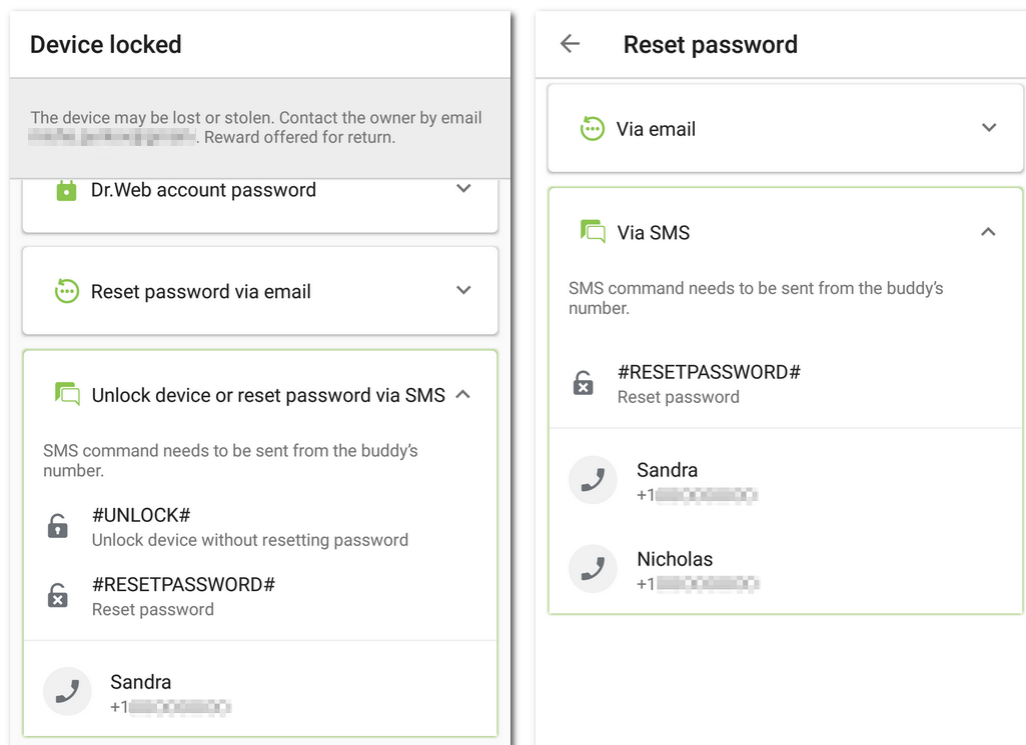


Figure 52. Reset password via SMS from a buddy's number

Locked (left) and unlocked (right) device

2. When the SMS is received, the **Change password** screen appears automatically. Enter a new password. If your device was locked, it will be unlocked.



If your device is locked, you can unlock it without resetting the password. To do so, send the SMS command **#UNLOCK#** to your device.



Reset password via notification

You can reset your password via a notification if the following conditions are met:


- **For your device**

1. The device is turned on and connected to the internet.
2. Dr.Web Anti-theft is enabled.
3. The Anti-theft [I trust](#) list contains at least one email address.

- **For your buddy's device**

- If your device is locked:
 1. Your buddy's device is turned on and connected to the internet.
 2. Dr.Web Security Space or Dr.Web Light is installed on your buddy's device.
 3. The buddy has confirmed your buddy request in the Help Your Buddy component or in Dr.Web Anti-theft. To receive your notification, the components must be enabled.
- If your device is unlocked:
 1. Your buddy's device is turned on and connected to the internet.
 2. Dr.Web Security Space is installed on your buddy's device.
 3. The buddy has confirmed your buddy request in Dr.Web Anti-theft. To receive your notification, the component must be enabled.

To reset your password

1. Send a notification to your buddy. Tap the  icon (see [Figure 53](#)).
2. Pass the verification code specified on the same pane on to your buddy.

Your buddy needs to enter the verification code on their device and send a command to Anti-theft to reset your password.
3. When the command is received, the **Change password** screen appears automatically. Enter a new password. If your device was locked, it will be unlocked.

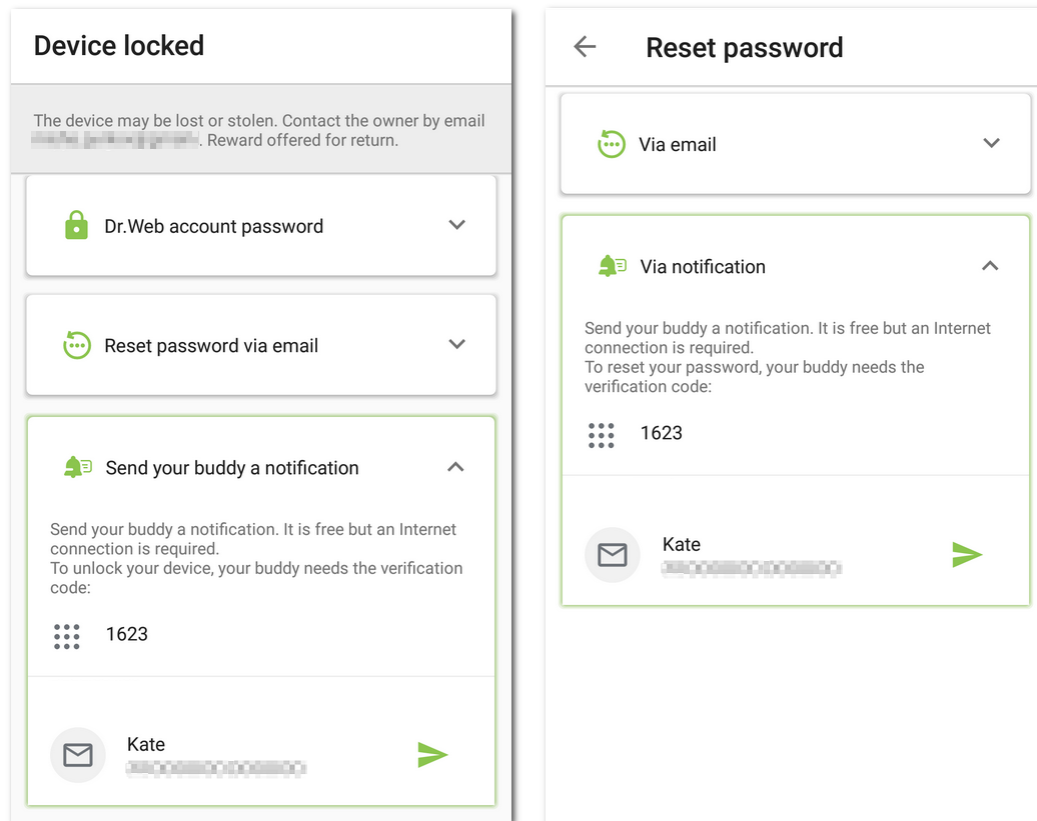


Figure 53. Reset password via notification
Locked (left) and unlocked (right) device

Reset password via technical support request

If you cannot unlock your device or set a new password yourself, send a request to the Dr.Web technical support team:

1. Open the technical support website: <https://support.drweb.com/>.
2. In the **Technical support** section, select the **Dr.Web program operation** option.
3. On the next page, specify your license or order number.
4. On the **Protection for home PCS/MACS** tab, select **Android**.
5. On the next page, fill out all fields.
6. Attach the following files to your request:
 - Photo of the **Device locked** or **Reset password** screen with the distinguishable key and email address (see [Figure 47](#)).
 - If you have your device's original packaging, attach a photo of the packaging with the distinguishable IMEI number (a unique 15-digit identifier of your device) on it.
 - Photo or scanned copy of the receipt for the device.
 - Photo or scanned copy of the completed warranty certificate.



- Documents that prove your Dr.Web license purchase (an email from the online store, a payment document, etc.). If you won your license at the Dr.Web auction, specify your Doctor Web website account login. If you use a demo version, skip this step.





The text in the images should be clearly readable: the technical support specialist has to make sure that you own the device and the Dr.Web license.

7. Tap **Send**.

An email with the link to your request will be sent to the email address that you have specified earlier. On your request page, you will see a verification code.

8. Enter the verification code in the **Verification code** field on the **Device locked** or **Reset password** screen (see [Figure 51](#)). Tap **Continue**.
9. On the **Change password** screen, enter a new password. The password must contain at least 4 characters.

Tap  to the right of the password field to show the password characters. Tap  to hide the characters.

10. Confirm the password and tap **Save**.

Unlock device via request to administrator

If Dr.Web is operating in the centralized protection mode and Dr.Web Anti-theft is configured on the server, you need to contact the anti-virus network administrator of your company or the Dr.Web Anti-virus service provider to unlock your device. You can use one of the two device unlock options:

- Using a QR code:
 1. Contact the anti-virus network administrator of your company or the Dr.Web Anti-virus service provider.
 2. Share the QR code displayed on the **Device locked** screen with the administrator. Tap and hold the QR code to save it to your device. You can also take a photo of the screen with the clearly readable QR recovery code.

The administrator will send you a QR device unlock code.
 3. Make sure you have received the QR unlock code and tap **Continue**.
 4. On the next screen, tap **Scan QR code** and point your device's camera at the QR unlock code you received from the administrator.

If the QR code is recognized successfully, the device will be unlocked.
- Using a symbolic code:
 1. On the **Device locked** screen, tap **Another option**.
 2. Contact the anti-virus network administrator of your company or the Dr.Web Anti-virus service provider.
 3. Share the ID and the recovery code shown on the **Device locked** screen with the administrator.



The administrator will send you a device unlock code.

4. Make sure you have received the unlock code and tap **Continue**.
5. On the next screen, enter the code you received from the administrator in the **Unlock code** field and tap **Unlock**.

If the correct unlock code is entered, the device will be unlocked.

If for some reason you are unable to complete the procedure using either of the device unlock options, tap on **Another option** on the **Device locked** screen to choose the other option.

To reset your password after unlocking the device, contact the anti-virus network administrator of your company or the Dr.Web Anti-virus service provider.



Keyword Index

A

- about 40
- access to data transmission 96
 - on Android TV 145
- account
 - account 41
 - creating 41
 - deleting 42
 - managing 42
 - password 41, 42, 161
- acquiring license 18
- activating license 18
- allowing filter 59
- Android TV
 - anti-virus protection 136
 - app settings 145
 - app traffic 144, 145, 147
 - application log 151
 - check results 138
 - connection rules 147
 - connections 147
 - deleting connection rules 151
 - Dr.Web Firewall 140
 - Dr.Web Firewall log 152
 - Dr.Web Scanner 137
 - events 136
 - Fake ID 156
 - internet traffic statistics 145
 - main screen 135
 - miscellaneous 157
 - network activity 141
 - network connections 141
 - permissions 135
 - root access 155
 - Security Auditor 154
 - security problems 154
 - settings 158
 - SplDer Guard 136
 - system settings 156
 - threats 138
 - user certificates 156
 - vulnerabilities 155
- anti-virus laboratory 50
- anti-virus network 130
- anti-virus protection 44

- check results 51
- device lockers 56
- Dr.Web Scanner 47
- neutralizing multiple threats 53, 139
- neutralizing one threat at a time 53, 139
- on Android TV 136
- ransomware 56
- SplDer Guard 44
- system applications 54
- system area 55
- app settings
 - on Android TV 145
- app traffic on Android TV 144
- application traffic on Android TV 145
- apps
 - active apps 91
 - all apps 94
 - application log 107
 - clearing statistics 100
 - connection rules 102
 - internet traffic 94, 98, 99
 - settings 101
 - statistics 99
 - traffic 91

B

- backup
 - export 128
 - import 128, 129
- black list
 - URL filter 64
- blocked app screen 80
- blocked calls and SMS 61
- blocking access
 - to app 80
 - to app group 80
 - to component 80
 - to website categories 62
 - to websites 62
- blocking filter 58
- buddies 67

C

- Call and SMS filter 57
 - allowing filter 59
 - blocked calls and SMS 61



Keyword Index

- Call and SMS filter 57
 - blocking filter 58
 - centralized protection mode 57
 - editing lists 60
 - permissions 57
- centralized protection mode 130
 - Application filter 134
 - automatic connection 131
 - Call and SMS filter 57
 - configuration file 132
 - connection errors 133
 - Dr.Web Anti-theft 66
 - entering connection settings 132
 - licensing 130
 - notification bar 38
 - reset settings 133
 - switching to standalone mode 134
 - update 131
 - virus database update 127, 128
- check results 51
 - on Android TV 138
- components 44
 - Call and SMS filter 57
 - Dr.Web Anti-theft 65
 - Dr.Web Firewall 89
 - Dr.Web Scanner 47
 - Parental Control 77
 - Security Auditor 109
 - SplDer Guard 44
 - URL filter 62
- configuring
 - Dr.Web Anti-theft 66
- connection rules 102
 - on Android TV 147
- cure 53, 139
- custom scan 48
- D**
- demo license 18
 - activating 19
 - restoring 27
- detecting threats 51
 - system applications 54
 - system area 55
- device lockers 56
- Dr.Web Anti-Theft 65
- buddies 67
- centralized protection mode 66
- commands 72
- configuring 66
- disabling 77
- Dr.Web Anti-theft Locator 75
- enabling 65
- help 67
- lock after restart 71
- lock if SIM card is changed 71
- no SIM mode 72
- notification for buddies 71
- password 66
- push commands 73
- removing data 72
- SIM card replacement 71
- SMS commands 75
- text on the lock screen 70
- trusted SIM cards 70
- Dr.Web Anti-theft Locator 75
- Dr.Web Firewall 89
 - app settings 101
 - app settings on Android TV 145
 - app traffic 91, 94, 99
 - app traffic on Android TV 144, 145, 147
 - application log 107
 - application log on Android TV 151
 - clearing application log 107
 - clearing log 109, 154
 - clearing statistics 100
 - connection rules 102
 - connection rules on Android TV 147
 - connections 102
 - connections on Android TV 147
 - enabling 89
 - floating window 92
 - limiting mobile traffic usage 97
 - log 108
 - log file size 109, 154
 - log on Android TV 152
 - logging 107, 108
 - network activity on Android TV 141
 - network connections on Android TV 141
 - on Android TV 140
 - statistics 99
- Dr.Web Scanner 47



Keyword Index

Dr.Web Scanner 47
 custom scan 48
 express scan 48
 full scan 48
 on Android TV 137
 scan types 47
 settings 47, 50
 statistics 50

E

EICAR test file 44, 46
events on Android TV 136
express scan 48

F

Fake ID
 on Android TV 156
false positive 50, 53, 140
features 9
floating window 91, 92
full scan 48
functions 9

G

getting started 31

I

installation from Google Play 11
installing
 from Doctor Web website 12
 from Google Play 12
 using synchronization software 14
interface 34
 main screen 34, 44
 navigation panel 34
 status bar 34, 35
 widget 39
internet traffic statistics
 on Android TV 145

K

key file 24, 25

L

license 18
 activating 18, 22

 configuring notifications 30
 demo 18, 19
 expiration 30
 for 1 year 20
 for 2 years 20
 key file 22, 24, 25, 28
 lifetime 20
 purchasing 18, 20
 purchasing from Doctor Web website 22
 purchasing from Google Play 20
 renewing 28
 restoring 26
 serial number 22, 24
 subscription 20

License Agreement 31
license key file 24, 25, 28
licensing 18
 centralized protection mode 130
lifetime license 20
lock after restart 71
lock if SIM card is changed 71
log
 application 107
 application log on Android TV 151
 Dr.Web Firewall 108
 Dr.Web Firewall on Android TV 152
 events 122
 Parental Control 86

M

main screen 34
 on Android TV 135
miscellaneous on Android TV 157
mobile internet
 notifications 97
 usage limit 97
My Dr.Web 40

N

navigation panel 34
network activity 90
 on Android TV 141
network connections 90
 floating window 92
 on Android TV 141
neutralizing multiple threats 53, 139



Keyword Index

neutralizing one threat at a time 53, 139
neutralizing threats 51, 138
 Stagefright 55
new password 161
no SIM mode 72
notification bar 36, 37
 centralized protection mode 38
 settings 126
notification for buddies 71
notifications 36
 license expiration 30
 mobile internet 97

O

optimization settings 112
 Asus 113
 Huawei 114
 Meizu 116
 Nokia 117
 OnePlus 117
 Oppo 118
 Samsung 119
 Sony 119
 Xiaomi 120
Origins Tracing 8

P

Parental Control 77
 disabling 78
 enabling 77, 78
 log 86
 settings 85
 training mode 77
password 41
 Dr.Web account 41, 65
password, Dr.Web account 41, 42, 161
permissions 31
 on Android TV 135
personal webpage 40
protection status 35
purchasing license 18, 20
push commands 73

Q

quarantine 123
 size 124

R

ransomware 56
real-time protection 44
registering a serial number 22
 in application 23
 on Doctor Web website 24
removing data 72
renewing license
 from Doctor Web website 28
 from Google Play 29
reset settings 125, 129
restoring license 26
root access 111
 on Android TV 155

S

scanning
 custom 48
 express 48
 false positive 50
 full 48
Security Auditor 109
 Asus 113
 Fake ID vulnerability 112
 hidden device administrators 112, 156
 Huawei 114
 Meizu 116
 Nokia 117
 on Android TV 154
 OnePlus 117
 Oppo 118
 optimization settings 112
 root access 111
 Samsung 119
 Sony 119
 supported browsers 112
 system settings 111
 user certificates 111
 vulnerabilities 110
 Xiaomi 120
security problems 109
 hidden device administrators 156
 on Android TV 154
 root access 111
 user certificates 111



Keyword Index

sending file to laboratory 50, 53, 140

sending statistics 31, 126

settings 125

 backup 128

 general settings 126

 notification bar 126

 on Android TV 158

 reset 125, 129

 sending statistics 126

 SpIDer Guard 45

 system applications 127

 virus database update 128

SIM card replacement 71

SIM cards

 lock if SIM card is changed 71

 no SIM mode 72

 sending SMS if SIM card is changed 71

 trusted 70

SMS commands 75

 sending 76

sound 126

SpIDer Guard 44

 EICAR test file 46

 enabling 44

 on Android TV 136

 settings 44, 45

 statistics 46

 testing 44, 46

Stagefright 55

start to use 31

statistics 121

 app traffic 99

 clearing 122

 Dr.Web Scanner 50

 saving log 122

 SpIDer Guard 46

 viewing 122

status bar 34, 35

subscription

 canceling 27

 pausing 27

 resuming 27

supported browsers 9, 10, 62, 112

switching to standalone mode 134

system applications 54

 settings 127

system area 55

system requirements 10

system settings

 Android TV 156

T

technical support 160

text on the lock screen 70

threats 51

 all to quarantine 53, 139

 cure 53, 139

 delete 53, 139

 delete all 53, 139

 device lockers 56

 false positive 53, 140

 ignore 53, 140

 more on the internet 54, 140

 move to quarantine 53, 140

 on Android TV 138

 quarantine 123

 ransomware 56

 send to laboratory 53, 140

 Stagefright 55

 system applications 54

 system area 55

traffic 98

 apps 99

 current activity 91

 mobile 96, 97

 roaming 96

 statistics 99

 Wi-Fi 96

trusted SIM cards 70

U

uninstall

 Dr.Web 15

uninstalling Dr.Web 16

unlock 161

update

 centralized protection mode 131

 Dr.Web 15

 virus databases 127

URL filter 62

 black list 64

 settings 62



Keyword Index

URL filter 62
 supported browsers 62
 website categories 63
 white list 64
user certificates 111
 on Android TV 156

V

virus database update
 centralized protection mode 127, 128
virus databases
 manual update 127
 update 127
 update settings 128
vulnerabilities
 Android TV 155

W

website categories 63
white list 64
widget 39

