Dr.WEB

Light for Android

User manual

Dr.Web Light for Android
Version 12.2
User manual
4/16/2024

Doctor Web Head Office

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

Website: https://www.drweb.com/

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

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

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

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

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

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

Table of Contents

1. Introduction 5
   1.1. Dr.Web Features 6
2. System Requirements 7
3. Installing Dr.Web 8
4. Updating and Uninstalling Dr.Web 9
5. Getting Started 10
   5.1. License Agreement 10
   5.2. Permissions 10
   5.3. Interface 11
   5.4. Notifications 13
   5.5. Widget 14
6. Dr.Web Components 16
   6.1. Anti-Virus Protection 16
      6.1.1. Dr.Web Scanner: On-Demand Scan 16
      6.1.2. Scan Results 19
         6.1.2.1. Threats in System Applications 19
         6.1.2.2. Changes in System Area 19
      6.1.3. Device Lockers 23
   6.2. Virus Databases 24
   6.3. Statistics 25
   6.4. Quarantine 27
   6.5. Help Your Buddy 29
7. Settings 32
   7.1. General Settings 33
   7.2. Reset Settings 34

Keyword Index 35

1. Introduction

Dr.Web Light protects mobile devices running the Android™ operating system from various virus threats designed specifically for these devices.

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

Dr.Web Light uses Dr.Web Mobile Engine SDK—a set of tools that can be used in the development of high security software for the Android platform. Due to a variety of threat detecting methods, it provides protection from both known and new threats for mobile platforms.

About this manual

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

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

Convention	Comment
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`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 Features

Dr.Web Light performs the following features:

- Monitors your file system in real time (downloaded files, installed apps, etc.).
- Scans the entire file system or selected files and folders on your demand.
- Scans archives.
- Monitors changes in system area.
- Quarantines threats or completely removes them from your device.
- Unlocks your device if it is locked by ransomware.
- Helps unlock your buddy's device.
- Downloads Dr.Web virus database updates from the Internet.
- Gathers statistics on detected threats and performed actions; keeps the app log.

Dr.Web Light also works in Multi-Window mode that allows you to launch several applications in separate windows. This mode can be used only on Samsung Galaxy S III or later version and Samsung Galaxy Note 2 or later version.

2. System Requirements

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

Parameter	Requirement
Operating system	Android version 4.4–14.0
CPU	x86/x86-64/ARMv7/ARMv8
Free RAM	At least 512 MB
Free space on device	At least 35 MB (for data storage)
Screen resolution	At least 800×480
Other	Internet connection (for virus database updates)

Please note that correct operation of Dr.Web Light is not guaranteed on devices with custom ROMs and on rooted devices.

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

3. Installing Dr.Web

Installation from Google Play

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

- You have a Google account.
- You have logged in 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 Light in the list of applications and tap **Install**.

   

   If your device does not meet the system requirements, Dr.Web Light will not be displayed in the list of applications in Google Play.

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

Installation from Xiaomi GetApps

Before installing Dr.Web from Xiaomi GetApps, make sure that:

- You have a Xiaomi account.
- You have logged in your Xiaomi 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 Xiaomi GetApps, find Dr.Web Light in the list of applications and tap **Get**.

   

   If your device does not meet the system requirements, Dr.Web Light will not be displayed in the list of applications in Xiaomi GetApps.

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

4. Updating and Uninstalling Dr.Web

Updating Dr.Web

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

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

Uninstalling Dr.Web

To uninstall Dr.Web

1. In your device settings, tap **Applications** or **Application manager**.
2. Select **Dr.Web Light** and then 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 memory of your device.

On devices with Android 11 or later, logs are saved in `Download/DrWeb`.

5. Getting Started

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

5.1. 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. The full version of Dr.Web has the option to opt out of sending the statistics.

5.2. Permissions

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

After you install Dr.Web Light and accept the License Agreement, grant the app the necessary permissions. Dr.Web Light requires the following mandatory permissions:

- On devices with Android 10.0 or earlier: access to your photos, media, and files.
- On devices with Android 11.0 or later: access to all files.

If you don't grant the mandatory permissions, Dr.Web Light will not function. The permission request will be displayed every time you open the app until you grant the permissions by following the instructions provided below or shown on the request screen.

On devices with Android 13.0 or later, Dr.Web Light requires the permission to send you notifications. Dr.Web Light needs this permission to use the notification bar for displaying messages about the device security status. If the permission is not granted, Dr.Web Light cannot notify you about detected threats and the need to scan suspicious files until you open the app.

If you decline the mandatory permission request, you will be prompted to go to the device 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 then select **Permissions**.
  2. Select **Files and media** or **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 Light

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

5.3. Interface

Main screen

When you open the app for the first time, you see the status bar, information on the full version of the app, the Dr.Web Scanner menu, as well as the Dr.Web navigation panel (see Figure 1).

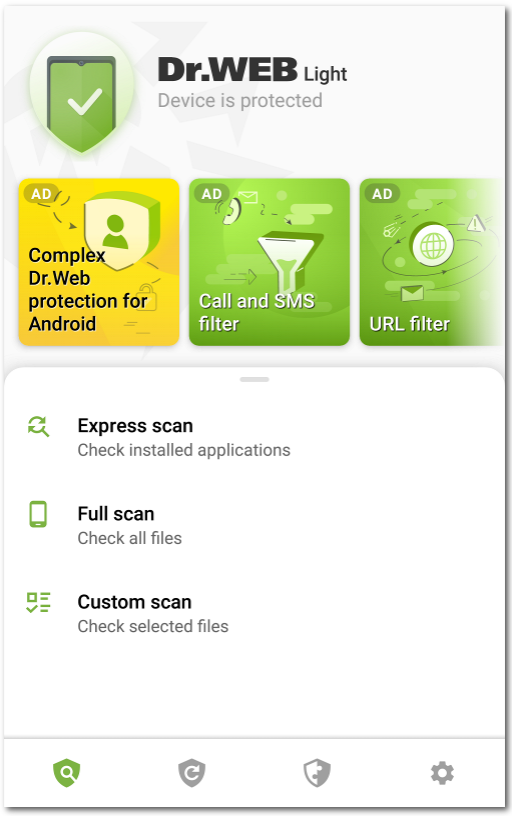

Figure 1. Dr.Web main screen

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 2).

Figure 2. 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. new files have been detected on the device or the virus databases require an update. Tap the panel to start a custom scan of the device.

Information on the full app version

Below the status bar, there are slides introducing the main features of the full version of the app. The slides allow you to learn more about the full version of the app, Dr.Web Security Space for Android, and download it from Google Play.

Tap the first slide to open the Dr.Web Security Space for Android page in Google Play. Tap any of the subsequent slides to learn about the features offered by a component of Dr.Web Security Space for Android. The **More** button on the slide allows you to open the Dr.Web Security Space for Android page on the Doctor Web website. Swipe left to move to the next slide.

Navigation panel

In the bottom part of the screen, there is the Dr.Web navigation panel, which allows you to switch between the app component tabs.

- The Scanner tab allows you to scan your device on demand. Three scan types are available: full scan, express scan, and custom scan.
- The Virus databases tab informs you on the current virus database status and allows you to update the virus databases manually.
- The **Tools** tab includes the following components:
  - Statistics displays statistics on the detected threats and performed actions.
  - Quarantine allows you to view and process quarantined objects.
  - Help Your Buddy helps unlock your buddy's device locked by Dr.Web Anti-theft.
- The Settings tab allows you to manage Dr.Web component and app settings.

5.4. 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. In your device settings, you can manage behavior for each notification category separately. 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	Notifications about threats detected by Dr.Web Scanner.
Anti-virus protection status	If the notification bar is disabled, this category contains the following notifications: • **Device is protected**. Shown if a scan is not being performed by Dr.Web Scanner. • Notification about the Dr.Web Scanner scan type. Shown if an express, full, or custom scan is in progress. If the notification bar is enabled and a scan has been started, a message about the ongoing scan is shown on the notification bar.
Notifications from buddies	Notifications received from your buddies.
Other	• **Permissions required**. Shown when opening the application if access to photos, media, and files has been denied.
Group notifications	This category does not contain any specific notifications but it allows you to group all Dr.Web notifications in one extendable notification.

Notification bar

The Dr.Web notification bar (see Figure 3) notifies of suspicious changes in the system area, as well as potential threats.

The notification bar displays a protection status indicator:  —on devices with Android 11.0 and earlier,  —on devices with Android 12.0 and later. If Dr.Web detects new files on the device or suspicious changes in the system area, the indicator turns yellow. If Dr.Web detects threats, the indicator turns red.

Figure 3. Notification bar on Android 11.0 (left) and Android 12.0 (right)

To enable the Dr.Web notification bar

1. Tap on the Dr.Web navigation panel.
2. Tap **General settings**.
3. Enable the **Notification bar** option.

> On Android 5.0 and 5.1, if Dr.Web detects suspicious changes in 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.

The notification bar allows you to:

- Open the Dr.Web main screen when the indicator is green and the current protection status is **Device is protected**. Tap the indicator.
- Start a custom scan when the indicator is yellow and the current protection status is **Scan your device**. Tap the indicator.
- Open the scan results when the icon is red and the current protection status is **Resolve issues**. Tap the indicator.
- Review the information on Dr.Web Security Space for Android and download it for free trial use for 14 days. Tap **Full version**.

To view the protection status, current and recommended actions on devices with Android 12.0 and later, tap .

5.5. Widget

Dr.Web Light widget allows you to control the protection status of your device. You can add the widget to your Home screen.

To add the Dr.Web widget

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

The widget displays the current protection status (see Figure 4).

- The standard green widget indicates that no treat has been detected. No additional actions are required.

- The widget with a yellow icon indicates that new files or apps have been detected on the device. Tap the widget to scan the new objects.
- The widget with a red icon indicates that a threat has been detected. Tap the widget to open the scan results and select actions for the detected threats.

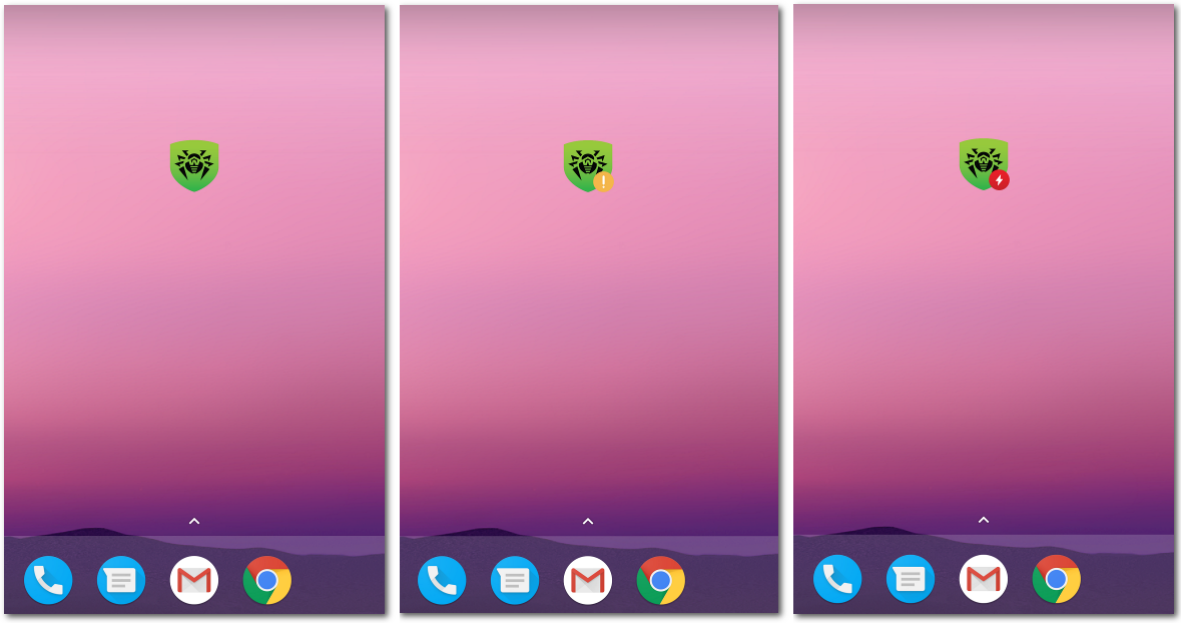

Figure 4. Dr.Web Widget

6. Dr.Web Components

You can navigate to a Dr.Web component by means of the navigation panel in the bottom part of the screen.

- Scanner: allows you to scan your device on demand. Three scan types are available: full scan, express scan, and custom scan.
- Virus databases: informs you on the current virus database status and allows you to update virus databases manually.
- Statistics: displays statistics of the detected threats and performed actions.
- Quarantine: allows you to view and process quarantined objects.
- Help Your Buddy: helps unlock your buddy's device locked by Dr.Web Anti-theft.
- Settings: allows you to manage Dr.Web component and app settings.

6.1. Anti-Virus Protection

- Dr.Web Scanner allows you to scan your device for threats.
- On the Scan results screen, you can select actions to neutralize the detected security threats.

6.1.1. 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. Usually, the express scan is sufficient for this purpose.

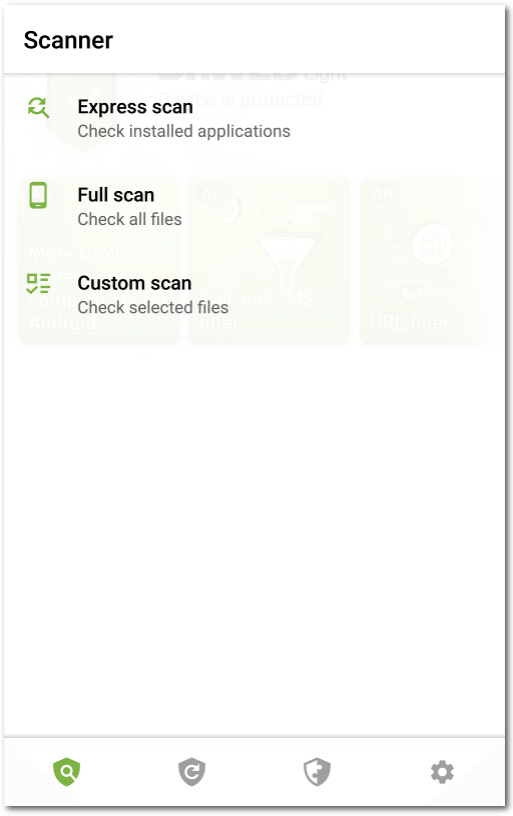

Figure 5. Dr.Web Scanner

Scanning

To scan the system, on the Dr.Web navigation panel, tap , then on the **Scanner** screen (see Figure 5) select one of the following actions:

- To scan only the installed applications, select **Express scan**.
- To scan all the files, select **Full scan**.
- To scan only selected files and folders, select **Custom scan**, select the objects from the list (see Figure 6). To select all objects in the current location, use the check box at the top right. Then tap **Scan**.

> On devices with Android 11.0 or later, the `/Android/data` and `/Android/obb` folders are system-protected and thus cannot be scanned.

If Dr.Web Scanner detects threats, the indicator in the center of the screen turns red. Tap the indicator or the number of detected threats to open scan results (see Figure 7) and neutralize threats. If you switch to another screen or application, you can open scan results by tapping the icon on the notification bar.

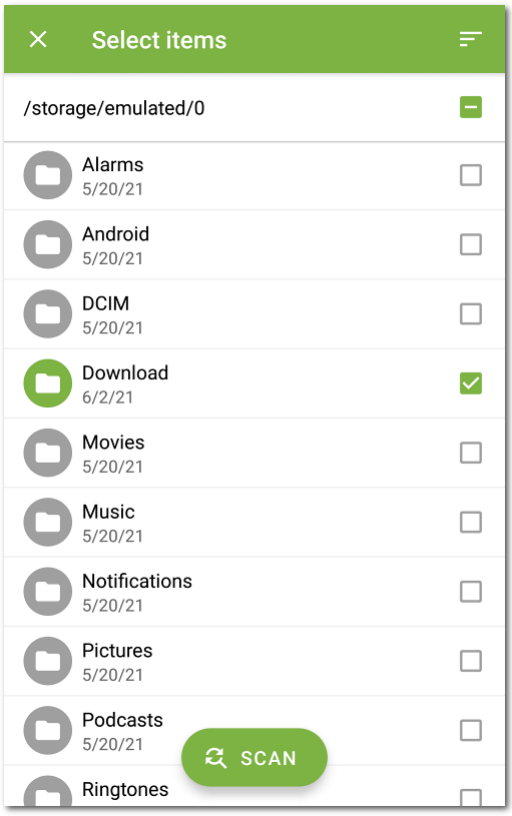

Figure 6. Custom scan

Sending suspicious files to Doctor Web anti-virus laboratory

You can submit suspicious ZIP archives (files with the `.jar` and `.apk` extensions) presumably containing viruses, `.odex`, `.dex`, `.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 6), 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 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 monitor changes in the system area, select the **System area** and **Any files in system area** check boxes. If the setting is enabled, the component monitors changes (addition, modification, and deletion of files) and notifies only on deletion of any files as well as addition and modification of executable files: `.jar`, `.odex`, `.so`, APK, ELF files, etc.
- To enable/disable detection of files that might threaten your device, select the corresponding check boxes:
  - Suspicious objects,
  - Adware,
  - Dialers,
  - Joke programs,
  - Riskware,
  - Hacktool programs,
  - Exploitable software.

Statistics

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

6.1.2. Scan Results

If Dr.Web Scanner detects threats, the following will 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 at the top of the screen.
- A red indicator on the scan screen.

To open scan results, tap the cross in the top-left corner of the scan screen, or the indicator in the notification or on the status bar.

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

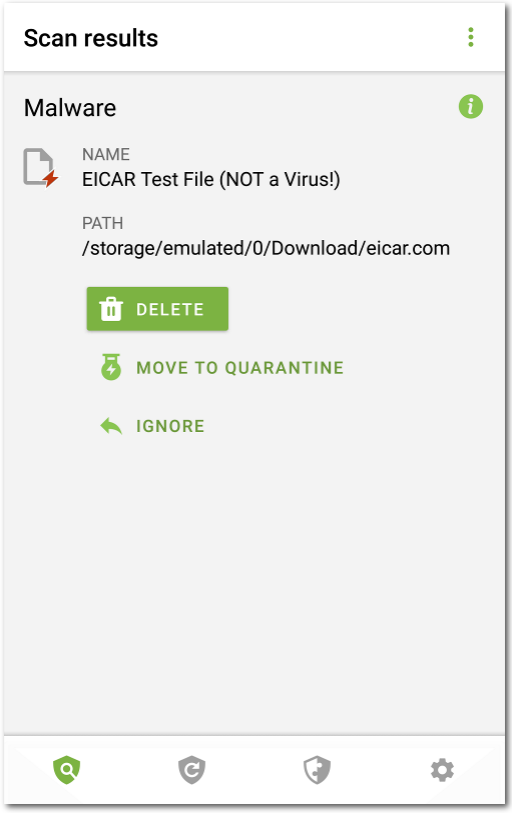

Figure 7. Scan results

Neutralizing Threats

On the **Scan results** screen, you can review the list of threats and changes in the system area. For each object, its type and name are specified.

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. Modification. On the **Check Results** object type shows as **Malware**, but the color key differs.
3. Suspicious object.
4. Adware.

5. Dialer.
6. Joke program.
7. Riskware.
8. Hacktool program.
9. Exploitable software.

The least degree of danger is assigned to changes in the system area:

- New files in system area.
- Change of system files.
- Deletion of system files.

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

If an archive containing multiple threats is detected, you can view the full list of all threats in the archive by tapping **Expand**.

Threats in archives are detected only when the Files in archives option is active.

Neutralizing all threats

To delete all threats

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

To move all threats to the quarantine

- In the top-right corner of the **Scan 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:

Delete to delete the threat from your device.

In some cases, Dr.Web cannot delete applications that use accessibility features of Android. If Dr.Web does not delete the app after you select the **Delete** option, reboot to safe mode and delete the app manually.

The option is not available for threats in system applications.

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.

6.1.2.1. 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 in the full version of Dr.Web 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**.

6.1.2.2. 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.

You can enable system area checking in the Scanner settings. If the component detects suspicious changes in the system area, it notifies you about it after the scan.

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 Dr.Web Scanner 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: APK, ELF, JAR, ODEX, SO files, etc.).
- More on the Internet.

The component 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.

6.1.3. Device Lockers

Dr.Web Light 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 Light 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, you can use Dr.Web Light 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 Light 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 Light 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.

6.2. Virus Databases

Dr.Web Light 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

The virus databases are updated via the internet several times a day automatically. If the virus databases have not been updated for more than 24 hours (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. Tap on the navigation panel.
2. In the pop-up window, you will see the virus database update status and when the virus databases were last updated. If the last update happened more than 24 hours ago, you should update virus databases manually.

To start the update

1. Tap on the navigation panel.
2. Tap **Update**.

> It is recommended to update virus databases as soon as you install the application. This will allow Dr.Web Light 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.

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. Tap on the navigation panel (see Figure 12).
2. Select **Virus databases**.
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.

6.3. Statistics

Dr.Web Light compiles statistics on detected threats and application actions.

To view the application statistics, tap the icon on the navigation panel and select **Statistics**.

Viewing statistics

The **Statistics** tab contains two information sections (see Figure 8):

- **Total**. Contains information on the total number of scanned files, detected and neutralized threats.
- **Events**. Contains information on Dr.Web Scanner scan results, virus database update status, detected threats and actions performed on them.

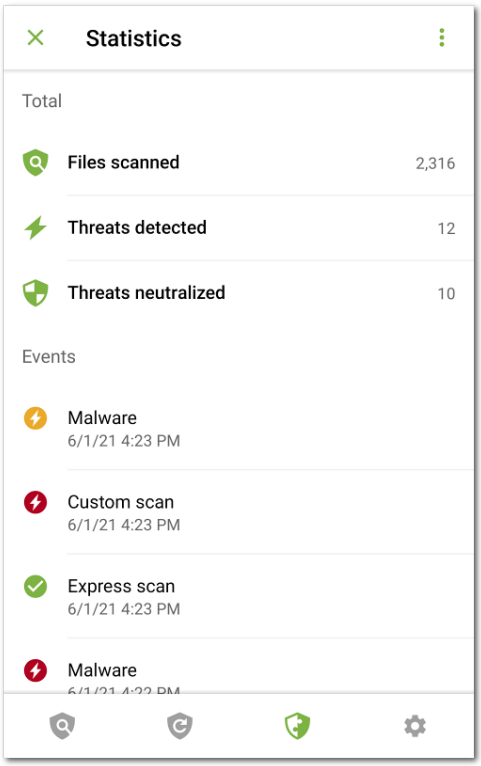

Figure 8. Statistics

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 for further analysis if you experience problems while using the application.

1. On the **Statistics** tab, tap **Menu** and select **Save logs**.
2. The logs are saved in the `DrWeb_Log.txt` and `DrWeb_Err.txt` files located in the `Android/data/com.drweb/files` folder in the internal memory of your device.

On devices with Android 11 or later, logs are saved in `Download/DrWeb`.

6.4. Quarantine

Dr.Web allows you to move detected threats to the quarantine folder, where they are isolated and cannot damage the system (see Figure 9).

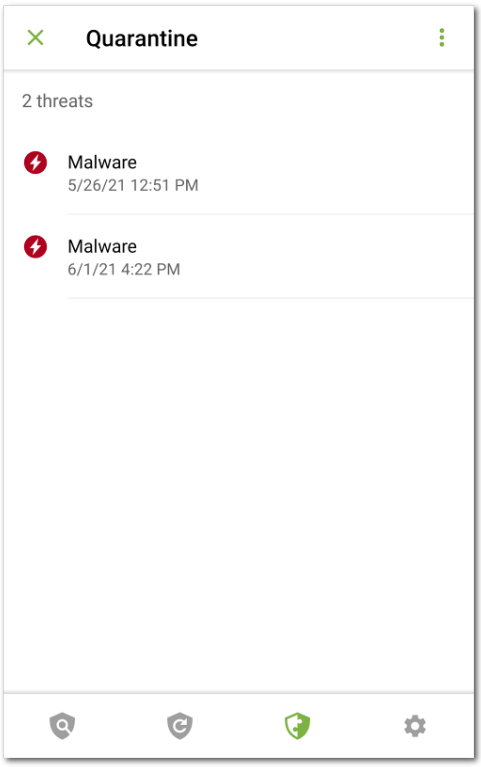

Figure 9. Quarantine

Viewing quarantined files

To view the list of threats moved to quarantine, tap the icon on the navigation panel and select **Quarantine**.

Viewing information on quarantined threats

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

For each threat, the following information is available:

- file name;
- path to the file;

- date and time the threat was quarantined.

You can expand a card containing information on a threat by swiping it up. Swipe the card down to collapse it.

To view the full list of all threats in an archive which contains multiple threats, select it and tap **Expand** in the **Threat** row.

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 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 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 **Delete** 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 **Size**.
3. Tap **OK** to return to the **Quarantine**.

6.5. Help Your Buddy

The **Help Your Buddy** component helps unlock your buddy's device locked by Dr.Web Anti-theft.

What is Dr.Web Anti-theft

Anti-theft is available in Dr.Web Security Space for Android. If the device is lost or stolen, Anti-theft locks it. To unlock the device, a password is needed. If the device owner does not remember the password, you can help them reset the password and unlock the device.

How does Help Your Buddy work

You enable **Help Your Buddy** and enter your email address, then tell it to Dr.Web Security Space for Android users you trust. Dr.Web Security Space for Android users add you as their buddy in Anti-theft. You confirm the buddy requests.

When a buddy needs help in unblocking their device, your buddy sends you a notification. Once you receive the notification, you contact your buddy, ask for the verification code, and send an unblock request. Upon receiving the request, Anti-theft allows your buddy to reset their password. After that your buddy can continue using their device as normal.

Both devices need to be connected to the Internet. Delivery of push notifications can take up to 15 minutes.

To enable Help Your Buddy

1. Tap the  icon on the navigation panel and select **Help Your Buddy**.
2. On the **Help Your Buddy** screen, tap **Enable**.
3. Enter your email address and tap **Continue**.

To add a buddy

1. Share your email address with a user of Dr.Web Security Space for Android so that they could send you a buddy request.
2. Wait for the buddy request notification.
3. Tap the notification to go to the **Help Your Buddy** screen.
4. Tap the row with your buddy's email address.
5. Tap **Confirm** on your buddy's card to confirm the buddy request.

If you decline or do not accept the buddy request, the user cannot request your help with unlocking their device.

To change your buddy's name

1. Tap on your buddy's card (see Figure 10).
2. Enter the new name.
3. Tap to save the changes.

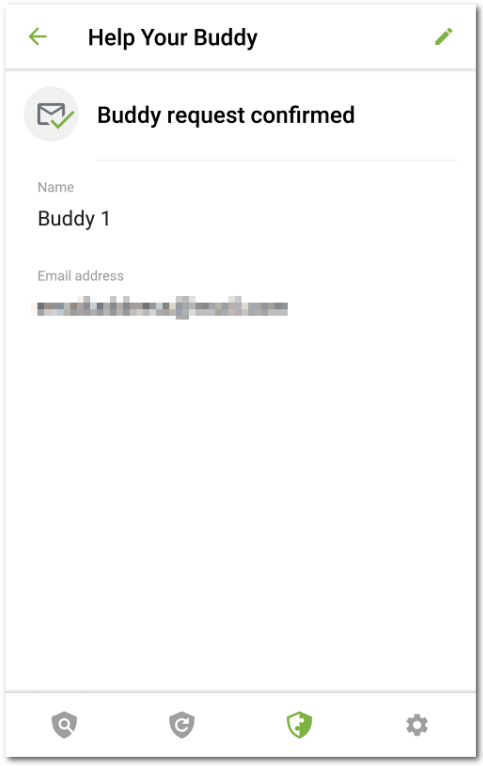

Figure 10. Buddy card

You can edit your buddy's name only. If your buddy's email address has changed or is no longer in use, you can remove your buddy.

To remove a buddy

- Swipe the buddy contact to the left.

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

To unlock your buddy's device

1. Tap the lock notification that you received from your buddy.
2. Contact the buddy. The device could be lost or stolen and someone else could have sent the notification.
3. If your buddy does need help with unlocking their device, get the verification code from the buddy. The verification code is displayed on the lock screen of your buddy's device.

4. Enter the verification code and tap **Unlock** (see Figure 11).

If you ignore or close the lock notification by accident, ask the buddy to send a notification again.

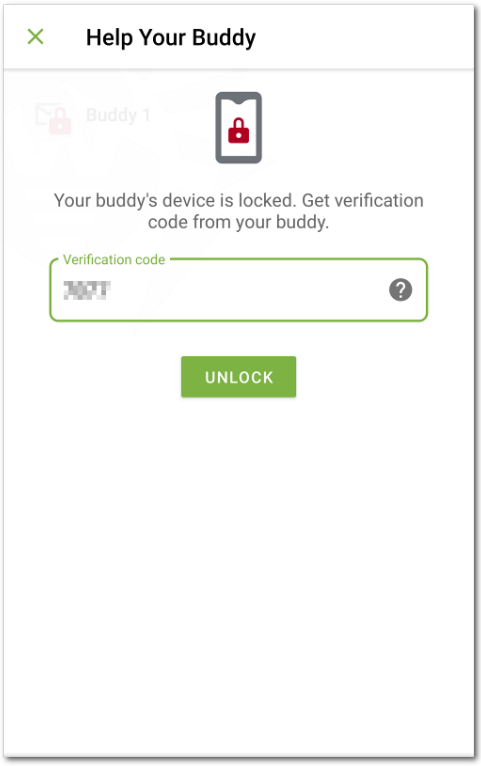

Figure 11. Unlock verification code

To disable Help Your Buddy

1. Tap the icon on the navigation panel and select **Help Your Buddy**.
2. On the **Help Your Buddy** screen, tap **Menu** and select **Disable**.

> When **Help Your Buddy** is disabled, all buddies are removed from your buddy list. Your buddies receive a notification about your declining their buddy request.

7. Settings

To open the settings screen (see Figure 12), tap the icon on the navigation panel.

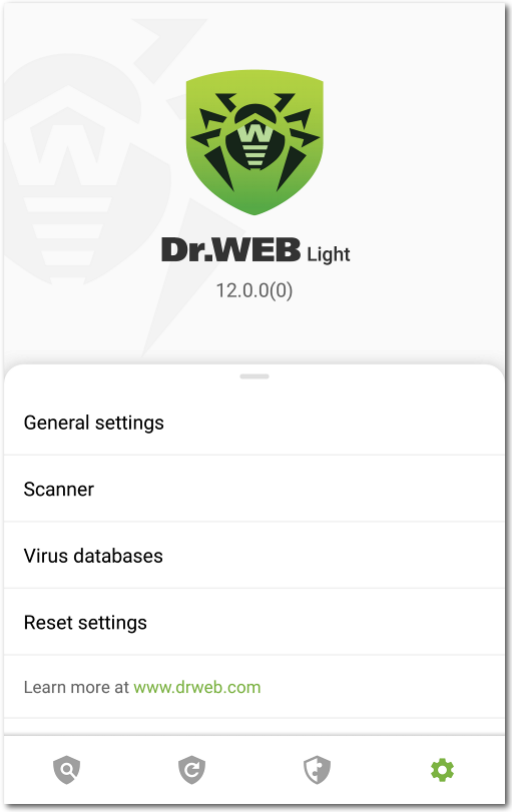

Figure 12. Settings

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

- **General settings**. Allows you to turn on dark mode, configure the notification bar and notifications about threats in the system area, enable and disable sound alerts (see General Settings).
- **Scanner**. Allows you to configure Dr.Web Scanner, which scans your device on your request (see Dr.Web Scanner settings).
- **Virus databases**. Allows you to disable virus database updates over mobile networks (see Virus databases).
- **Reset settings**. Allows you to reset user settings and restore the default configuration (see Reset Settings).
- **Learn more at www.drweb.com**. Allows you to visit the Doctor Web website to view information about the application and other company products.

The **Settings** screen also provides information on the app and its manufacturer. The top part of the screen displays the app version below the app name. Swipe the **Settings** menu up to view the additional informational options:

- **Help**. Allows you to learn how to use the app in the Dr.Web Light user manual.
- **Social network icons**. Allow you to visit the Doctor Web company profiles in the corresponding social networks.

7.1. General Settings

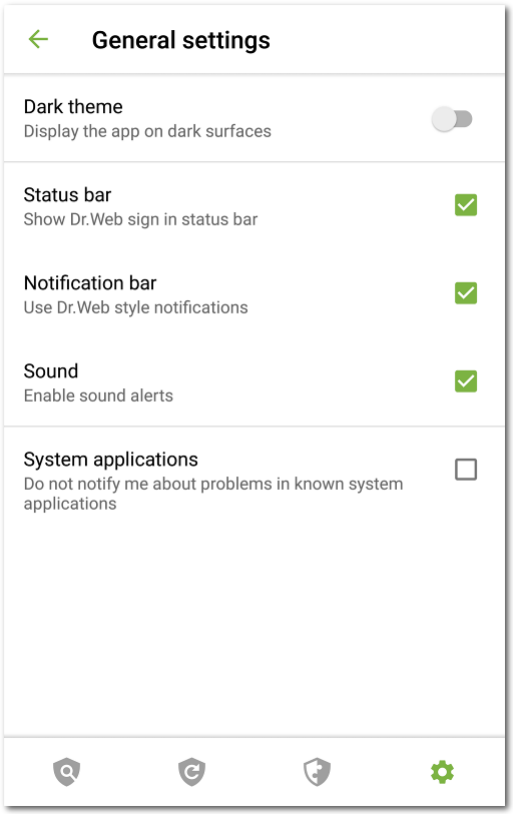

Figure 13. General settings

On the **General settings** screen (see Figure 13), the following options are available:

- **Dark theme**. Allows you to set the dark mode of the application.
- **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.
- **Sound**. Enables and disables sound alerts on threat detection, deletion or moving to quarantine. By default, sound alerts are enabled.

- **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.

7.2. Reset Settings

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

To reset settings

1. Tap **Reset settings** on the settings screen (see Figure 12). Then tap **Reset settings**.
2. Confirm that you want to restore the default settings.

Keyword Index

A

anti-virus laboratory 18
anti-virus protection 16
  check results 19
  device lockers 23
  Dr.Web Scanner 16
  neutralizing multiple threats 21
  neutralizing one threat at a time 21
  ransomware 23
  system applications 22
  system area 23

C

check results 19
components 16
  Dr.Web Scanner 16
custom scan 17

D

detecting threats 19
  system applications 22
  system area 23
device lockers 23
Dr.Web Scanner 16
  custom scan 17
  express scan 17
  full scan 17
  settings 19
  statistics 19

E

express scan 17

F

false positive 18, 22
features 6
full scan 17

G

getting started 10

H

Help Your Buddy 29

I

installation from Google Play 8
installing
  from Google Play 8
interface 11
  main screen 11, 16
  navigation panel 11
  status bar 11, 12
  widget 14

L

License Agreement 10
log
  events 26

M

main screen 11

N

navigation panel 11
neutralizing multiple threats 21
neutralizing one threat at a time 21
neutralizing threats 19
notification bar 13
  settings 33
notifications 13

O

Origins Tracing 5

P

permissions 10
protection status 12

Q

quarantine 27
  size 28

R

ransomware 23
reset settings 32, 34

S

scanning
  custom 17

Keyword Index

scanning
express 17
false positive 18
full 17
sending file to laboratory 18, 22
sending statistics 10, 33
settings 32
general settings 33
notification bar 33
reset 32, 34
sending statistics 33
virus database update 25
sound 33
start to use 10
statistics 25
clearing 26
Dr.Web Scanner 19
saving log 26
viewing 26
status bar 11, 12
system applications 22
system area 23
system requirements 7

T

threats 19
all to quarantine 21
delete 21
delete all 21
device lockers 23
false positive 22
ignore 22
more on the internet 22
move to quarantine 21
quarantine 27
ransomware 23
send to laboratory 22
system applications 22
system area 23

U

uninstalling Dr.Web 9
update
Dr.Web 9
virus databases 24

V

virus databases
manual update 24
update 24
update settings 25

W

widget 14