Dr.WEB

Enterprise Security Suite

# Managing stations under Android

**Trademarks**

Dr.Web, SpIDer Mail, SpIDer 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 property of their respective owners.

**Disclaimer**

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

**Dr.Web Enterprise Security Suite. Managing stations under Android**
**Version 13.0**
**Administrator Manual**
**2/17/2023**

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 which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web anti-virus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

# Table of Contents

# Chapter 1. Introduction

## 1.1. About Manual

This manual is a part of the documentation package for an anti-virus network administrator. It is intended to provide detailed information on the organization of complex anti-virus protection of corporate computers and mobile devices using Dr.Web Enterprise Security Suite.

The manual is meant for an anti-virus network administrator—an employee of organization who is responsible for the anti-virus protection of workstations and servers of this network.

This manual contains information about centralized configuration of anti-virus software on workstations which is provided by an anti-virus network administrator via Dr.Web Security Control Center. This manual describes settings of Dr.Web for Android anti-virus solution and features of the centralized configuration of the software.

To get additional information, please refer to the following manuals:

- **User Manual** of Dr.Web for Android contains information about configuration of the anti-virus software installed on a station.
- **Administrator Documentation** of Dr.Web Enterprise Security Suite anti-virus network (includes **Administrator Manual**, **Installation Manual** and **Appendices**) contains general information on installation and configuration of the anti-virus network and, particularly, on operating Dr.Web Security Control Center.

Before reading this document, make sure you have the latest version of the manuals. The manuals are constantly updated. You can find the latest version on the official Doctor Web website at https://download.drweb.com/doc/.

## 1.2. Conventions

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

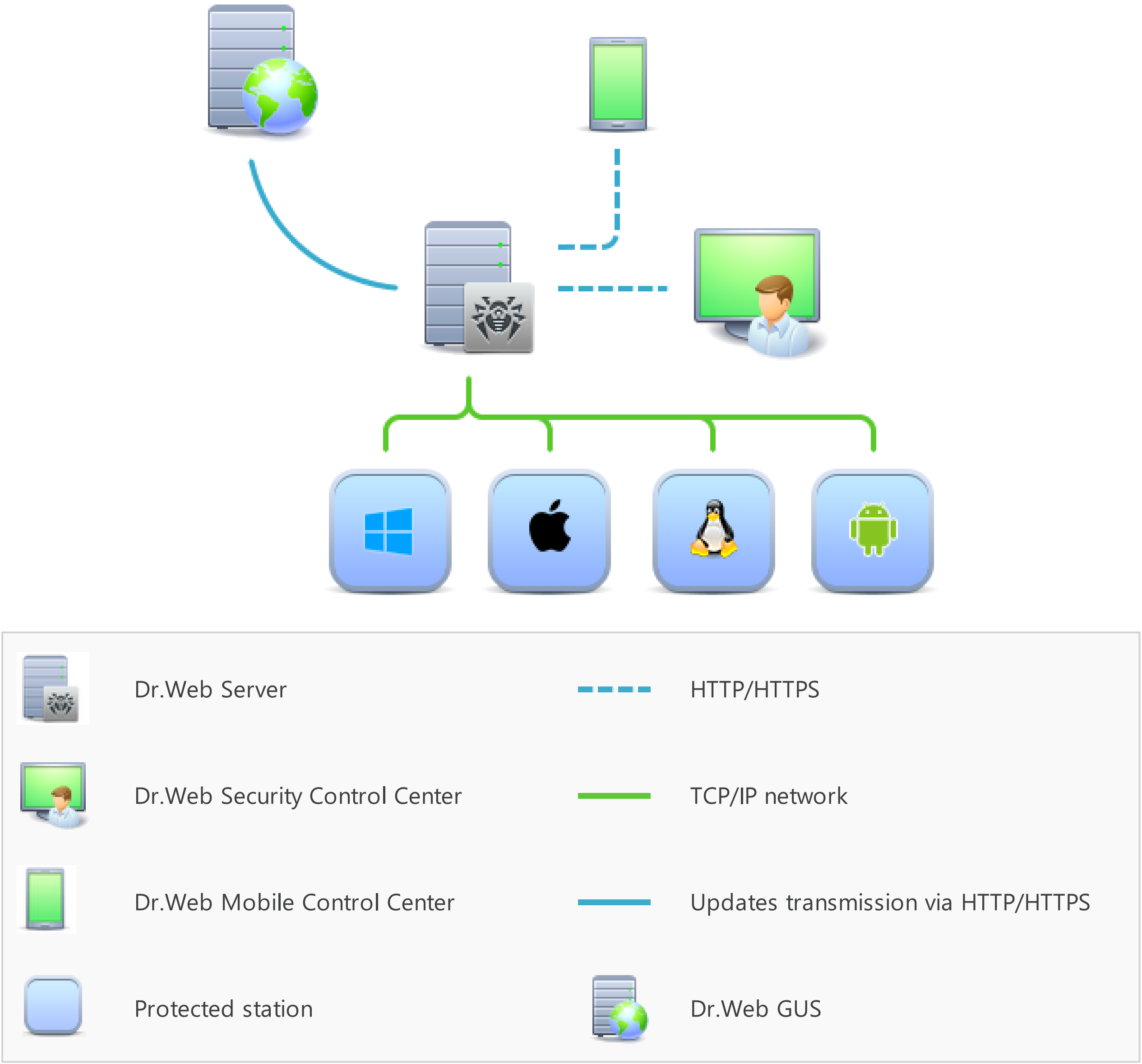
| Convention | Comment |
|---|---|
| (!) | Important note or instruction. |
| ⚠ | Warning about possible errors or important notes to which you should pay special attention. |
| *Anti-virus network* | A new term or an accent on a term in descriptions. |
| *<IP-address>* | Placeholders. |
| **Save** | Names of buttons, windows, menu items and other program interface elements. |
| CTRL | Keyboard keys names. |
| `C:\Windows\` | Names of files and folders, code examples. |
| Appendix A | Cross-references on the document chapters or internal hyperlinks to web pages. |

# Chapter 2. Dr.Web Enterprise Security Suite

## 2.1. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection of either a local company network including mobile devices, or employees' home computers.

An aggregate of computers and mobile devices, on which Dr.Web Enterprise Security Suite cooperating components are installed, represents a single *anti-virus network*.


Dr.Web Server
HTTP/HTTPS
Dr.Web Security Control Center
TCP/IP network
Dr.Web Mobile Control Center
Updates transmission via HTTP/HTTPS
Protected station
Dr.Web GUS

**Logical structure of the anti-virus network**

Dr.Web Enterprise Security Suite anti-virus network based on a *client-server* architecture. Its components are installed on computers and mobile devices of users and administrators as well as on computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP network protocols. Anti-virus software can be installed on protected stations (that can be managed afterwards) either via LAN or via the Internet.

## 2.2. Workstation Protection

Workstations are protected by the Dr.Web anti-virus packages designed for corresponding operating systems.

> Protected computer with an installed anti-virus package as per its functions in the anti-virus network is called a *workstation* of the anti-virus network. Please note that according to its LAN functions, such computer can be both a workstation or a mobile device and a LAN server.

Anti-virus packages are installed on protected stations and get connected to Dr.Web Server. Each station is included in one or several groups registered on this Server. Stations and the Server communicate through the protocol used in the local network (TCP/IP of version 4 or 6).

### Installation

Local installation of the anti-virus package under Android OS is performed directly on a user’s mobile device. Installation may be implemented either by an administrator or by a user.

> You can find a detailed description of anti-virus package installation procedures on workstations in the Dr.Web Enterprise Security Suite **Installation Manual**.

### Management

When connection with Dr.Web Server is established, an administrator is able to use the following functions implemented by the anti-virus package on a station:

- Centralized configuration of Anti-virus on workstations via the Control Center.

  At this, the administrator can either deny or grant permissions to change the Anti-virus settings on one's own station to users.
- Get scan statistics and other information on anti-virus component operation and on the state of a station.

### Update

Dr.Web Server downloads updates and distributes them to connected stations. Thus, optimal threat protection is implemented, maintained, and adjusted automatically regardless of the workstation users’ computer skills.

A description of the options for updating installation packages with the help of Dr.Web Server version 13.0 is provided in the **Upgrading Dr.Web Agents on Stations under Android OS** section of the Dr.Web Enterprise Security Suite **Installation Manual**.

In case an anti-virus station is disconnected from the anti-virus network, Anti-virus on station uses the local copy of the settings, and the anti-virus protection on a workstation retains its functionality (up to the expiration of the user’s license), but the software is not updated. If a station is allowed to use the *Mobile mode*, after connection with the Server is lost, the virus databases can be updated directly from GUS.

Operation of stations in the Mobile mode is described in the Dr.Web Enterprise Security Suite **Administrator Manual**.

# Chapter 3. Dr.Web for Android

Dr.Web for Android offers a reliable protection of mobile devices running on the Android™ operating system from various virus threats designed specifically for these devices.

The application employs the most advanced developments and technologies of Doctor Web aimed at detection and neutralization of malicious objects which may represent a threat to device operation and information security.

Dr.Web for Android uses Origins Tracing™ for Android—a unique algorithm for detecting malware designed specially for Android. This algorithm allows detecting new virus families using the knowledge database on previous threats. Origins Tracing for Android™ can identify recompiled viruses, e.g. Android.SMSSend, Android.MobileSpy as well as applications infected by Android.ADRD, Android.Geinimi, Android.DreamExploid. Names of threats detected using Origins Tracing for  Android™ are of the form: Android.VirusName.origin.

## 3.1. Dr.Web for Android Components

For Android OS stations, the following anti-virus components are provided:

*Dr.Web Scanner*

Scans a mobile device at user request and on schedule. Also, remote launch of anti-virus scan on stations from the Control Center is supported.

*SpIDer Guard*

Constantly scans file system in real-time mode. Scans all files as they are saved in a memory of a device.

*Call and SMS filter (Anti-spam)*

Filters incoming phone calls and SMS to block undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

*Anti-theft*

Detects device location or lock its functions in case it has been lost or stolen.

*URL filter*

Protects the user of a mobile device from unwanted Internet sites.

*Firewall (settings are available on a mobile device only)*

Protects a mobile device from external unauthorized access and prevents leak of vital data via the Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

*Security Auditor (settings are available on a mobile device only)*

Analyzes security of mobile device and resolving of detected problems and vulnerabilities.

*Application filter*

Blocks launch of those applications that are not included in the list of allowed by an administrator.

## 3.2. Dr.Web for Android Configuration

**To view or edit the configuration of the anti-virus components on the workstation:**

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. On the hierarchical list on your next step, click the name of an Android OS station or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **Android** subsection, select the necessary component:
   - Dr.Web for Android
   - SpIDer Guard
   - Call and SMS filter
   - Anti-theft
   - Application filter
   - Scanner
   - URL filter
4. A window with the component settings will open.

   Managing settings of anti-virus components via the Control Center differs from managing settings directly via the corresponding components on station:

   - to manage separate parameters, use the options located to the right of the corresponding settings:

     **Reset to initial value**—restore the previous value of a parameter (last saved value).

     **Reset to default value**—set the default value for a parameter.

   - to manage a set of parameters, use the options located on the toolbar:

     **Reset all parameters to initial values**—restore the previous values of all parameters in this section (last saved values).

     **Reset all parameters to default values**—restore the default values of all parameters in this section.

     **Propagate these settings to another object**—copy settings from this section to the settings of another station, group, or several groups and stations.

**Set the inheritance of settings from the primary group**—remove personal settings of a station and set inheritance of the settings in this section from a primary group.

**Copy settings from the primary group and set them as personal**—copy the settings of this section from a primary group and set them for the selected stations. Inheritance is not set, and the station settings are considered to be personal.

**Export settings from this section to the file**—save all settings from this section to a special format file.

**Import settings to this section from the file**—replace all settings in this section with settings from a special format file.

5. After making changes to the settings via the Control Center, click **Save** to accept the changes. The settings will be passed to the selected stations. If the stations were offline when the changes were made, the settings will be passed once the stations reconnect to the Server.

> An administrator may restrict a user from editing station settings (see the **Permissions of Station Users** section in the **Dr.Web Enterprise Security Suite Administrator Manual**). In this case, only an administrator will be able to edit the settings via the Control Center.

## 3.2.1. Dr.Web for Android

Dr.Web for Android general settings and update settings are available in the **Dr.Web for Android** section.

### General

- Select the **Enable sound alerts** check box to enable sound notifications on threats detection, deletion, or moving to quarantine.
- Select the **Display Dr.Web icon in status bar** check box to show the application icon in the status bar when SpIDer Guard is enabled.
- Select the **Track location** check box to allow the Server to receive information on current device location coordinates.

  In the **Period of coordinates transmission** list, select the time period of device current location update. The minimum period is 5 minutes.

> Automatic positioning is available for stations under Android. You can find detailed information on usage and configuration of this feature in the **Automatic positioning for stations under Android** section of **Appendices to Dr.Web Enterprise Security Suite Administrator Manual**.

### Updates

- Select the **Update virus databases over Wi-Fi only** check box to disable use of mobile networks for downloading the updates. If no Wi-Fi networks are available, you will be prompted to use 3G or GPRS. Changing this setting does not affect use of mobile networks by other application and device functions.

- Select the **Check for new version** check box to enable checking for a new version availability every time the virus databases are updated. When a new version of the application is available, you will get a standard notification and will be able to download and install a new version.

## 3.2.2. SpIDer Guard

SpIDer Guard constantly scans file system in real-time, checks all files in device memory as they are modified or saved, thereby protecting system against security threats.

SpIDer Guard settings are available in the **SpIDer Guard** section.

- Select/clear the **Enable SpIDer Guard** check box to enable/disable SpIDer Guard. When SpIDer Guard is enabled it protects file system of a device. It remains active even if you close the application.
- Select the **Check archives** check box to enable file scan of archives. By default, scanning of archives is disabled. Enabling the scanning may influence system performance and increase battery power consumption. Anyway, disabling scanning of archives does not decrease protection level because SpIDer Guard scans all Android installation files (.apk) regardless of the value of this parameter.
- Select the **Check SD cards** check box to enable file scan of SD cards on each mounting.
- Select the **Check for Adware** and **Check for Riskware** check boxes to enable detection of adware and riskware (including hacktools and jokes).

## 3.2.3. Call and SMS Filter

Call and SMS filtering allows you to block undesired messages and calls, e.g., advertisements, as well as messages and calls from unknown numbers.

Call and SMS filtering settings are available in the **Call and SMS filter** section.

In the **Current profile** list, select a filtering mode:

- **Accept all**. Filtering is disabled, and all incoming calls and SMS are accepted.
- **Reject all**. All incoming calls and SMS are blocked.
- **Enterprise black list**. Incoming calls and SMS from the contacts on the black list only are rejected.

  In this mode, the **Private numbers blocked** check box is available. You can block incoming calls and SMS from hidden numbers by selecting this check box.
- **Enterprise white list**. Incoming calls and SMS from the contacts on the white list only are accepted.

  In this mode, the **Private numbers allowed** check box is available. You can allow incoming calls and SMS from hidden numbers by selecting this check box.

## 3.2.4. Anti-Theft

Dr.Web Anti-theft detects device location or locks its functions in case it has been lost or stolen.

Dr.Web Anti-theft settings are available in the **Anti-theft** section.

- In the **Password** field, enter a password (the password must contain at least four characters). This is a required field. The password will be used to manage all functions of Dr.Web Anti-theft.
- Select the **Delete information after 10 password-entry errors** check box to completely erase all personal data from the device after 10 failed attempts to enter the password.
- Select the **Lock device** > **After reboot** check box to lock the device after it is restarted.
- Select the **Lock device** > **If SIM card is changed** check box to lock the device in case a SIM card is changed.
- In the **Text on lock screen** field, enter a message text, e.g., contact information to return the lost device.
- In the **Buddies list** field, add phone numbers from which the user will be able to receive SMS commands without a password. The user can also receive an SMS command from these numbers to disable Dr.Web Anti-theft and reset its password.
- Select the **Inform your Buddies about a SIM card change** check box to notify the user's buddies about the change of a SIM card on the device.

The **Anti-theft** section also allows you to remotely unlock a user device.

You can navigate to the Anti-theft settings of a particular station in order to unlock the device in either of the two ways: using the station ID or the QR code shared by the device user.

**To generate the unlock code using the station ID and recovery code**

1. Get the station ID and the recovery code from the device user. The data is displayed on the screen of the locked device.
2. Select the **Anti-virus network** item in the main menu of the Control Center.
3. In the **Anti-virus network** panel, click the ⏷ icon.
4. Enter the station ID in the **Search** filed and click **Apply**.
5. Expand the anti-virus network tree and click the station to see its properties.
6. On the **Station properties** panel in the **Configuration** > **Android** section, click **Anti-theft**.
7. On the station Anti-theft settings page, click **Generate the unlock code**.
8. Enter the recovery code you received from the user in the field in the pop-up window and click **Next**.

**To generate the unlock code using a QR code**

1. Get the QR code displayed on the screen of the locked device from the device user.

2. Select the **Anti-virus network** item in the main menu of the Control Center.
3. Select **General** > **QR code recognition** in the menu on the left.
4. Drag the QR code in the `.png` or `.jpeg` format to the drag-and-drop area or click the area to select the QR code file using the explorer. If the QR code is uploaded successfully, the station ID and recovery code appear below the drag-and-drop area.
5. Click **Generate the unlock code**.

After generating the unlock code you can share the code with the user by any means available, including sending the code to the specified email address.

1. Select the **View the unlock code** check box to view the symbolic or QR unlock code. You can copy the symbolic code from the field or by clicking ⧉ to the right of the field. You can also download the QR code in the `.png` format by clicking **Download** under the QR code.
2. Select the **Send the unlock code to email** check box to send the symbolic and QR unlock codes to the specified email address. Enter the address in the required **Email address** field.
3. Click **Done**.

   The status of the email containing the unlock codes will appear at the top of the screen.

Once the user enters or scans the unlock code, the device is unlocked.

## 3.2.5. Application Filter

In the **Application filter** section, you can specify a list of applications, which are allowed to be launched on mobile devices connected to an anti-virus network.

> ⚠ If you use this option, all other applications (except for the system ones) which are not included into the specified list will not be able to run on users' mobile devices.

### To configure the list of allowed applications

> ⓘ Before you specify a list of allowed applications, make sure you checked the **Change Dr.Web Applications Filter** configuration option in the **Permissions** for workstations under Android. Otherwise, the **Administration** option will not display on user's device.

1. On a mobile device connected to the Server, specify the list of allowed applications:
   a) On the main screen of Dr.Web application, tap **Administration**.
   b) Select the applications, which will be available on the device.
   c) Tap **Allow selected**.

   After you save settings on the device, they will be transferred to the Server and saved as this device personal settings.

2. In the Control Center, open the **Application filter** section (see Dr.Web for Android Configuration) for station with personal settings specified at step 1.

   In the **Permitted applications** section, the application list received from the device is displayed. Applications are defined by the following parameters:

   - Application name,
   - Package name,
   - Application MD5.

3. Settings in the Control Center do not allow you to

   - Add applications in the allowed list. You can add applications only via settings of a mobile device.
   - Edit applications parameters in the allowed list.

4. Settings in the Control Center allow you to

   a) Remove applications from the allowed list. For this, click ⊟ next to the corresponding application.

   > ⚠ If you remove all applications from the allowed list but leave the Application filter enabled, none of user applications will be able to run on their mobile device.

   b) Allow the same applications for other mobile device or a group of devices of the anti-virus network. For this, click **Propagate these settings to another object** on the toolbar of this section. The window with the anti-virus network tree will open; select one or several objects to propagate settings and click **Save**.

   c) Disable Application filter. For this, clear the **Enable applications filter** check box.

   > Please note that if firstly Application filter was disabled on a station, you can enable it via the Control Center settings, but you cannot add applications into the allowed list. At this, none of the user applications will be able to run on their mobile device.
   >
   > If you do not intend to forbid all user applications, it is recommended that you start the configuration on a mobile device as it is described in the step 1 of this procedure.

5. After settings changes were made, click **Save**. The settings will be passed to the mobile device.

## 3.2.6. Scanner

Dr.Web Scanner performs express or full scan of the whole file system or scans critical files and folders only.

Dr.Web Scanner settings are available in the **Scanner** section.

### General

Select the **Check archives** check box to enable scanning files in archives. By default, scanning of archives is disabled. Enabling the scanning may influence system performance and increase battery power consumption. Anyway, disabling scanning of archives does not decrease protection level because Dr.Web Scanner scans all Android installation files (`.apk`) regardless if the option is enabled or not.

### Additional

Select the **Check for Adware** and **Check for Riskware** check boxes to enable detection of adware and riskware (including hacktools and jokes).

## 3.2.7. URL Filter

URL filter protects users of mobile devices from unsolicited Internet websites. URL filter allows to restrict access to various categories of non-recommended and potentially dangerous websites.

URL filter settings are available in the **URL filter** section.

**To block access to websites by categories**

1. Select the **Block categories** check box.

   The **Block categories** option enables URL filter on mobile devices. This restricts access to websites that are known as infection sources.

2. Select the website categories you want to restrict access to.

> In Dr.Web for Android starting from version 10.0.0, the **Known infection sources** category is no longer supported. The state of the **Known infection sources** check box in the Control Center is ignored, and the option is considered to be always enabled.
>
> This option can be disabled only by disabling the whole URL filter module.

# Technical Support

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

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

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

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

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