



# Dr.WEB

Enterprise Security Suite

## Managing stations under Android



© **Doctor Web, 2018. All rights reserved**

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

### **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 11.0.1**  
**Administrator Manual**  
**9/13/2018**

Doctor Web Head Office  
2-12A, 3rd str. Yamskogo polya  
Moscow, Russia  
125040

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 antivirus 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

<b>Chapter 1. Introduction</b>	<b>5</b>
1.1. About Manual	5
1.2. Conventions	6
<b>Chapter 2. Dr.Web Enterprise Security Suite</b>	<b>7</b>
2.1. About Product	7
2.2. Workstations Protection	8
<b>Chapter 3. Dr.Web for Android</b>	<b>10</b>
3.1. Dr.Web for Android Components	10
3.2. Dr.Web for Android Configuration	11
3.2.1. Dr.Web for Android	12
3.2.2. Scanner	13
3.2.3. SplDer Guard	13
3.2.4. Anti-Spam	14
3.2.5. Anti-Theft	14
3.2.6. Application Filter	15
3.2.7. URL Filter	16
<b>Appendix A. Technical Support</b>	<b>17</b>



## Chapter 1. Introduction

### 1.1. About Manual

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

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

The manual contains the information about centralized configuration of the anti-virus software of workstations which is provided by the anti-virus network administrator via Dr.Web Security Control Center. The manual describes the 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 anti-virus solution contains the information about configuration of the anti-virus software provided on a station directly.
- **Administrator Documentation** of Dr.Web Enterprise Security Suite anti-virus network (includes **Administrator Manual**, **Installation Manual** and **Appendices**) contains the general information on installation and configuration of the anti-virus network and, particularly, on operation with Dr.Web Security Control Center.

Before reading these document, make sure you have the latest version of the manuals. The manuals are constantly updated and the current version can always be found at the official website of Doctor Web 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.
<i>Anti-virus network</i>	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
<b>Save</b>	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
C:\Windows\ C:\Windows\	Names of files and folders, code examples.
<a href="#">Appendix A</a>	Cross-references on the document chapters or internal hyperlinks to web pages.

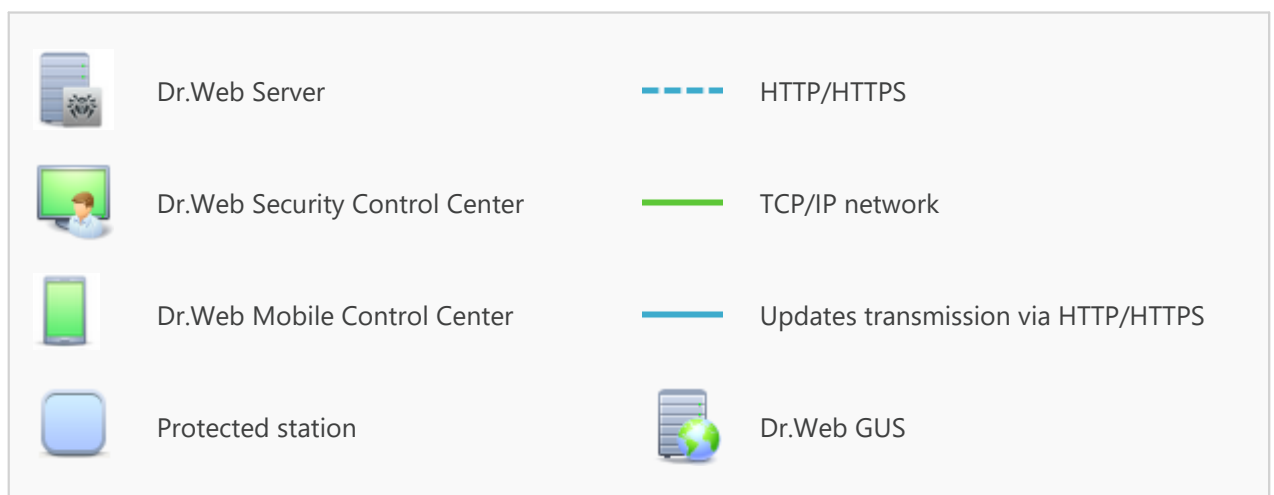
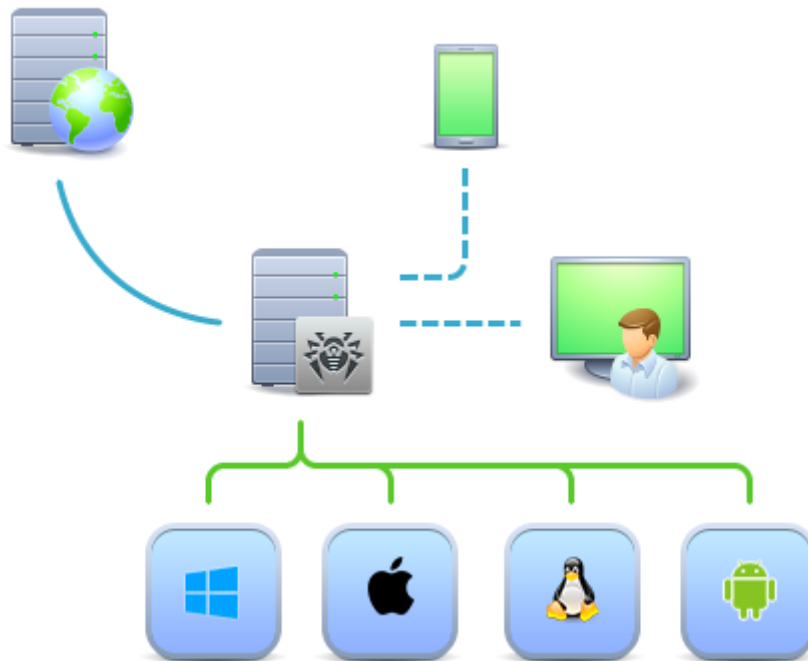


## Chapter 2. Dr.Web Enterprise Security Suite

### 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 home computers of employers.

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



**The logical structure of the anti-virus network**



Dr.Web Enterprise Security Suite anti-virus network has 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 the LAN, or via the Internet.

## 2.2. Workstations Protection

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



Protected computer with 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 4 or 6 version).

### Installation

Local installation of 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 detailed description of the anti-virus packages installation procedures on workstations in the Dr.Web Enterprise Security Suite **Installation Manual**.

### Management

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

- Centralized configuration of Anti-virus on workstations via the Control Center.  
At this, administrator can either deny or grant user's permissions to change Anti-virus settings on stations on one's own.
- Get scan statistics and other information on anti-virus components operation and on stations state.





## Update

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

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 expiry 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 the GUS.



The principle of stations operation 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 the mobile devices working under the Android™ operating system as well as TV sets, media players and game consoles working under Android TV™ platform 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 the device operation and information security.

Dr.Web for Android uses Origins Tracing™ for Android—the unique algorithm to detect 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 the recompiled viruses, e.g. Android.SMSSend, Android.MobileSpy, as well as the applications infected by Android.ADRD, Android.Geinimi, Android.DreamExploit. The names of the threats detected using Origins Tracing for Android are Android.VirusName.origin.

### 3.1. Dr.Web for Android Components

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

#### *Dr.Web Scanner, Dr.Web Agent Scanner*

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

#### *SpIDer Guard*

The constant file system scan in the real-time mode. The check of all files as they are saved in the memory of the device.

#### *Call and SMS filter*

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

#### *Anti-theft*

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

#### *URL filter*

URL filter allows to protect user of the mobile device from unsolicited Internet sites.

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

Protects the 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)*

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

*Application filter*

Blocks the launch on a mobile device of those applications that are not included in the list of allowed by 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. In the hierarchical list of the opened window, click the name of a station under Android OS 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](#)
- [Scanner](#)
- [SplDer Guard](#)
- [Anti-Spam](#)
- [Anti-Theft](#)
- [Application Filter](#)
- [URL Filter](#)


4. A window with the component settings will be opened.

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 on the right from the corresponding settings:
  - ➔ **Reset to initial value**—restore the value that parameter had before editing (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 values that all parameters in this section had before current editing (last saved values).
  - ⚙️ **Reset all parameters to default values**—restore default values of all parameters in this section.
  - 🔄 **Propagate these settings to another object**—copy settings from this section to settings of other station, group or several groups and stations.



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

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

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

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

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



Administrator may forbid editing settings on station for a user (see the **Permissions of Station Users** section in the Dr.Web Enterprise Security Suite **Administrator Manual**). At this, only administrator will be able to edit 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

- Set the **Enable sound alerts** check box to enable sound notifications on threats detection, deletion or moving to quarantine.
- Set the **Display Dr.Web icon** check box to show the application sign in the status bar when SplDer Guard is enabled.
- Set the **Track location** check box to allow the Server to receive the 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 the usage and configuration of this function in the **Automatic positioning for stations under Android** section of **Appendices** to Dr.Web Enterprise Security Suite **Administrator Manual**.

#### Updates

- Set the **Update virus databases over Wi-Fi only** check box to disable the 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 the use of mobile networks by other application and device functions.

- Set the **Check for new version** check box to enable the check 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. 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

- Set the **Check archives** check box to enable check of files in archives. By default, the archives check is disabled. Enabling the check of archives may influence the system performance and increase the battery power consumption. Anyway, disabling the archives check does not decrease the protection level because Dr.Web Scanner checks all Android installation files (.apk) regardless of the value of this parameter.

#### Additional

- Set/clear the **Check for Adware** and **Check for Riskware** check boxes to enable/disable detection of adware and riskware (including hacktools and jokes).

### 3.2.3. SpIDer Guard

SpIDer Guard performs constant real-time scanning of the file system, checks all files in the device memory as they are modified or saved, thereby protecting the system against security threats.

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

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



### 3.2.4. Anti-Spam

Call and SMS filtering allows 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 **Anti-Spam** section.

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

- **Accept all.** Filtering is disabled and all the incoming calls and SMS are accepted.
- **Block all.** All the incoming calls and SMS are blocked.
- **Enterprise black list.** Incoming calls and SMS from the contacts included into 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 setting this check box.


- **Enterprise white list.** Incoming calls and SMS from the contacts included into 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 setting this check box.

### 3.2.5. Anti-Theft

Dr.Web Anti-theft allows to detect the device location or lock 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). The password will be used to manage all functions of Dr.Web Anti-theft. If necessary, you can make the characters visible when entering the password by clicking  to the right of the password field.
- Enable the **Lock after reboot** option to lock your device after it is restarted.
- Enable the **Lock if SIM card is changed** option to lock your device in case the SIM card is changed.
- Enable the **Delete information after 10 password-entry errors** option to completely delete all your personal data from the device after 10 incorrect password enterings.
- Select **Text on lock screen** and enter the text (e.g., you can add your contact information to return your lost device) to specify the text which is displayed on the screen of the locked device.
- To the **Buddies list**, add the phone numbers from which you will be able to send SMS commands without a password. From these numbers you can also send an SMS command to disable Dr.Web Anti-theft and reset its password.
- Enable the **Inform your Buddies about a SIM card change** option to notify your friends about changing the SIM card in your device.



- Enable the **Receive SMS commands without a password** option to allow sending SMS commands from friends without entering the Dr.Web Anti-theft password. Even if the **Receive SMS commands without a password** option is disabled, your friends can send you the #RESETPASSWORD# command without password. This command is used to unlock the device and reset the password for Dr.Web Anti-theft.

### 3.2.6. Application Filter

In the **Application filter** section, you can specify the 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 a user's mobile device.


#### To configure the list of allowed applications

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

After the settings are saved 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 set. Applications are defined by the following parameters:

- Application name
  - Package name
  - Application MD5
3. Settings in the Control Center are not allowed to:
    - Add applications in the allowed list. You can add the application only via the settings of the mobile device.
    - Edit applications parameters in the allowed list.
  4. Settings in the Control Center allows 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 a mobile device.



- b) Allow the same applications for another 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 be opened; select one or several objects to propagate settings and click **Save**.
- c) Disable the Application filter. For this, clear the **Enable applications filter** flag.



Please note that if firstly the **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 a mobile device.

If the filtration goal is not 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.

### 3.2.7. URL Filter

**URL filter** allows to protect users of mobile devices from unsolicited Internet websites. URL-filter allows to block access to the various categories of non-recommended and potentially dangerous websites.

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

#### To block access to websites by categories

1. Enable the **Block categories** option.
2. Select the website categories you want to restrict access to.



In Dr.Web for Android starting from version 10.0.0, the option to block the **Known sources of virus** category is no longer supported. Changing the state of the **Known infection source** flag in the Control Center is ignored and the option is considered as always enabled.

This option can be disabled only by disabling the whole **URL filter** module.





## Appendix A. 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/](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.

