



# Dr.WEB

Enterprise Security Suite

## Managing Dr.Web for Linux



© **Doctor Web, 2021. All rights reserved**

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

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 Dr.Web for Linux**  
**Version 11.0.2**  
**Administrator Manual**  
**5/26/2021**

Doctor Web Head Office

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

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

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

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

## **Doctor Web**

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

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

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

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

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



## Table of Contents

<b>Chapter 1. Introduction</b>	<b>5</b>
1.1. About Manual	5
1.2. Conventions and Abbreviations	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 Linux</b>	<b>10</b>
3.1. Dr.Web for Linux Components	11
3.2. Dr.Web for Linux Configuration	12
3.2.1. Scanner for Workstations Settings	13
3.2.2. SpIDer Guard Settings	15
3.2.3. SpIDer Gate Settings	17
3.2.4. Dr.Web Agent for UNIX Settings	20
3.2.5. File Checker Settings	21
3.2.6. Scanning Engine Settings	22
3.2.7. Dr.Web ConfigD Settings	23
<b>Appendix A. Technical Support</b>	<b>24</b>



## Chapter 1. Introduction

### 1.1. About Manual

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

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

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

To get additional information, please refer the following manuals:

- **User Manual** of Dr.Web for Linux anti-virus solution contains the information about configuration of 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 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 web site of Doctor Web at <https://download.drweb.com/doc/?lng=en>



## 1.2. Conventions and Abbreviations

### 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.
/home/user	Names of files and folders, code examples.
<a href="#">Appendix A</a>	Cross-references on the document chapters or internal hyperlinks to web pages.

### Abbreviations

The following abbreviations will be used in the Manual without further interpretation:

- Dr.Web GUS—Dr.Web Global Update System,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- IP—Internet Protocol,
- LAN—Local Area Network,
- LKM—Linux Kernel Module,
- OS—operating system,
- PC—personal computer,
- TCP—Transmission Control Protocol,
- URL—Uniform Resource Locator.

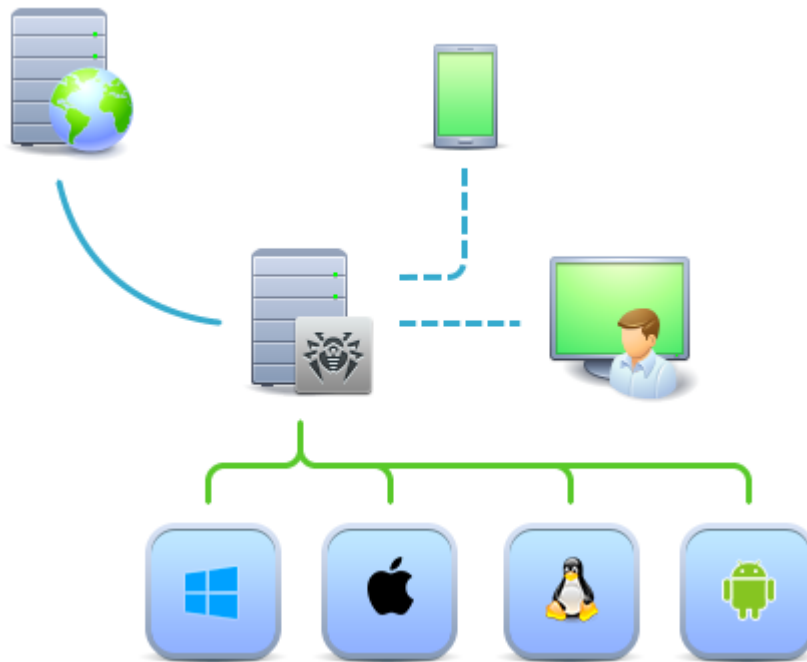


## Chapter 2. Dr.Web Enterprise Security Suite

### 2.1. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either 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*.



	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

#### 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 a computers and mobile devices of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information



via TCP/IP network protocols. Anti-virus software can be installed (and manage them afterwards) on protected stations either via the LAN, or via the Internet.

## 2.2. Workstations Protection

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



Protected computer with installed anti-virus package as per its functions in the anti-virus network is called a *workstation* of anti-virus network. Please note: according to its LAN functions, such computer can be both a workstation or 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 Dr.Web Server communicate through the protocol used in the local network (TCP/IP of 4 or 6 version).

### Installation

The anti-virus package can be installed on a workstation only locally. Local installation is performed directly on a user's computer. Installation may be implemented either by administrator or by user.



Detailed description of anti-virus packages installation procedures on workstations you can find 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 package on workstations via the Control Center.  
At this, administrator can either deny or grant user's permissions to change anti-virus package settings on stations on one's own.
- Configure the schedule for anti-virus scans and other tasks to execute on a station.
- Get scan statistics and other information on anti-virus components operation and on stations state.
- Start and stop anti-virus scans, etc. (depending on installed anti-virus package).





## Update

Dr.Web Server downloads updates and distributes them to connected stations. Thus, optimal threats 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 package 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 bases can be updated directly from the Dr.Web 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 Linux

This Manual describes management aspects of Dr.Web for Linux anti-virus software designed for the **GNU/Linux** OS. The manual is designed for a person responsible for anti-virus protection and security ("Administrator" hereinafter).

Dr.Web for Linux main functions:

1. **Detection and neutralization** of malicious programs (for example, viruses, including those that infect mail files and boot records, Trojans, mail worms) and unwanted software (for example, adware, joke programs, dialers).

The product uses several malware detection methods simultaneously:

- *Signature analysis*, which allows detection of known threats information on which is stored in virus bases
- *Heuristic analysis*, which allows detection of unknown threats
- Dr.Web Cloud service that collects up-to-date information about recent threats and sends it to Dr.Web products.

Note that the heuristics analyzer may raise false alarms. Thus, objects that contain threats detected by the analyzer are considered "suspicious". It is recommended to quarantine such files and send them for analysis to Doctor Web anti-virus laboratory.

File system scanning can be started in two ways: manually on user request and automatically, according to the schedule. There are two modes of scanning: full scan (scan of all file system objects) and custom scan of selected objects (directories or files). Moreover, the user can start a separate scan of volume boot records and executable files that ran currently active processes. In the latter case, if a malicious executable file is detected, it is neutralized and all processes run by this file are forced to terminate.

2. **Monitoring of file reference.** File events and attempts to run executable files are monitored. This feature allows to detect and neutralize malware at its attempt to infect the computer.
3. **Monitoring of access to the Internet.** All attempts to access Internet servers (web servers, mail servers, file servers) are monitored in order to block access to the websites of the unwanted categories, and to prevent the transfer of email messages with infected files, unwanted links or spam. Check of email messages and files downloaded for viruses and other threats from the web is performed on the fly. To restrict access to unwanted websites, Dr.Web for Linux supports a database of web resource categories that is automatically updated, and black and white lists that are edited by the user. Dr.Web Cloud service is also used to check whether the requested web resource is marked malicious by other anti-virus products of Dr.Web.
4. **Reliable isolation of infected or suspicious objects.** Such objects are moved to a special storage, quarantine, to prevent any harm to the system. When moved to quarantine, objects are renamed according to special rules and, if necessary, they can be restored to their original location only on demand.



## 3.1. Dr.Web for Linux Components

For protecting of workstations running under OS **GNU/Linux** family, the following anti-virus components are provided:

### General Components

#### *Scanner for Workstations*

The component which performs scanning of file system objects (files, directories, boot records) and running processes on demand or as scheduled to detect threats.



Note that as the Scanner for Workstations, the GUI version of the Scanner is implied. Dr.Web for Linux contains also the Console Scanner that is used to run scan from a command line. The Control Center does not manage the Console Scanner operating.

#### *SpIDer Guard*

The component which operates in resident mode and monitors file operations (creation, opening, closing, and running of a file). It scans new and modified files or executable files upon a program startup.

#### *SpIDer Gate*

The component which works in resident mode and monitors all network connections.

- It checks whether the requested URL falls into the unwanted category of web resources or in the user's black list, and, if so, blocks access to the resource.
- Blocks transfer of email messages if they contain malicious objects or unwanted links.
- The component also sends Scanner tasks to scan files downloaded from the Internet (from servers whose access is not restricted) and blocks their download if they contain threats.

Additionally, if it has the permission from the user, the component sends URL to Dr.Web Cloud service for a check.

#### *Console Scanner*

The component which performs scanning of the file system objects, running processes and remote hosts on demand from the command-line OS interface.

### Auxiliary Components

#### *Dr.Web Agent for UNIX*

The component is used for interaction between Dr.Web for Linux installed on the station and Dr.Web Enterprise Security Suite.



### File Checker

The component is used by Scanner for Workstations, Console Scanner, SplDer Guard and SplDer Gate for file checking and managing of Quarantine.

### Scanning Engine

The component is used for anti-virus scan and virus databases managing.

### Dr.Web ConfigD

The component that coordinates operation of all Dr.Web for Linux components.

### Quarantine

Isolates malicious and suspicious objects in the special directory.



Description of how to manage Quarantine via the Control Center you can find in the **Administrator Manual**.

Dr.Web for Linux installed on the station can also include other auxiliary components not specified in the list above.

## 3.2. Dr.Web for Linux 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 **Linux** OS or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **UNIX** subsection, select the necessary component.
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 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 primary group and set them as a personal**—copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered as a 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 **Administrator Manual**). At this, only administrator will be able to edit settings via the Control Center.

## 3.2.1. Scanner for Workstations Settings

The **Scanner for Workstations** page consists of the following sections, containing the corresponding parameters of Dr.Web for Linux operation:

- [General](#)—general settings of Scanner for Workstations
- [Actions](#)—setting actions on threats detected by Scanner for Workstations
- [Excluded paths](#)—paths to be excluded from the file check by Scanner for Workstations.

### 3.2.1.1. General

On this page you can manage the following parameters of Scanner for Workstations on the protected station:

- **Scanning time of one element**—restrictions on time spent on scanning of one file by Scanner for Workstations. If the value is 0, scan time is not limited.

### 3.2.1.2. Actions

On this page you can specify parameters that Scanner for Workstations is use for file checking on the protected station.

Scanner for Workstations can react to the following events:

- **Infected**—scanned file contains a known virus



- **Suspicious**—scanned file marked as *suspicious*
- **Adware**—scanned file contains an adware
- **Dialers**—scanned file contains a dialer
- **Jokes**—scanned file contains a joke program
- **Riskware**—scanned file contains a riskware
- **Hacktools**—scanned file contains a hacktool.

For these events, the following actions are allowed:

- *Cure, move to quarantine if not cured*—instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- *Cure, delete if not cured*—instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- *Move to quarantine*—this action moves a detected threat to the Quarantine that is isolated from the rest of the system.
- *Delete*—It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- *Report*—notify user on a detected threat.

Also the following advanced parameters are presented:

- **Automatically apply actions to threats**—if the check box is cleared, Scanner for Workstations only notifies the user on threat detection and user must determine the necessary action for the file.
- **Archives**—instructs Scanner for Workstations to scan the contents of archives. If the check box is cleared, the archive file structure are scanned by Scanner for Workstations anyway, but enclosed files are excluded from scans.
- **Email files**—instructs Scanner for Workstations to scan the contents of email files (email messages, mailboxes, etc.). If the check box is cleared, the email file structure are scanned by Scanner for Workstations anyway, but enclosed files are excluded from scans.

### 3.2.1.3. Excluded paths

On this page you can specify list of the paths to files and/or to directories on the protected station that are skipped by Scanner for Workstations during the file system scan.

Paths to be excluded are specified in the **Excluded paths** field (one path per line).

To add new path to the list, click . To delete some path from the list, click  in the corresponding line of the list.



## 3.2.2. SpIDer Guard Settings



SpIDer Guard, the file system monitor, can operate in one of the following modes:

- **FANOTIFY**—using the **fanotify** monitoring interface (not all **GNU/Linux**-based OSes support **fanotify**)
- **LKM**—using the loadable **Linux** kernel module (compatible with any **GNU/Linux**-based OS with kernel 2.6.x and newer)

By default, the file system monitor automatically chooses the appropriate operation mode according to the environment. If SpIDer Guard cannot be started, build and install a loadable kernel module by using the supplied source codes.

The **SpIDer Guard** page consists of the following sections, containing the corresponding parameters of Dr.Web for Linux operation:

- **General**—general SpIDer Guard settings
- **Actions**—actions on detection of threats by SpIDer Guard
- **Containers**—settings of scanning of compound files (archives, email files, etc.)
- **Scanning paths**—settings of exclusions of files and directories from monitoring
- **Additional**—additional SpIDer Guard settings.

### 3.2.2.1. General

On this page you can manage the following parameters of SpIDer Guard on the protected station:

- **Enable SpIDer Guard for Linux**—enables or disables SpIDer Guard on the protected station.
- **Use heuristic analysis**—instructs SpIDer Guard to use the heuristic analysis on the protected station during checking of the files "on the fly". Note that heuristic analysis may slow down the file system monitoring but improves its reliability.
- **Scanning time of one element**—restrictions on maximal time spent on scanning of one file by SpIDer Guard on the station. If the value is 0, scan time is not limited.

### 3.2.2.2. Actions

On this page you can specify parameters that SpIDer Guard is use for file checking on the protected station.

SpIDer Guard can react to the following events:

- **Infected**—scanned file contains a known virus
- **Suspicious**—scanned file marked as *suspicious*
- **Adware**—scanned file contains an adware
- **Dialers**—scanned file contains a dialer



- **Jokes**—scanned file contains a joke program
- **Riskware**—scanned file contains a riskware
- **Hacktools**—scanned file contains a hacktool.

For these events, the following actions are allowed:

- *Cure, move to quarantine if not cured*—instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- *Cure, delete if not cured*—instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- *Move to quarantine*—this action moves a detected threat to the Quarantine that is isolated from the rest of the system.
- *Delete*—It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- *Report*—notify user on a detected threat.

### 3.2.2.3. Containers

On this page you can specify settings which SpIDer Guard is used for checking compound files (containers) of the following types: archives, mail files (email messages, mailboxes), packed objects and other containers (i.e. compound files that are not classified as archives, mail files or packed objects).

For each of the types you can specify in the corresponding field the maximum nesting level. The objects that are nested into container deeper than the specified level are skipped during scanning the container by SpIDer Guard. For example, if you want scan the contents of the archives which are nested into archives, specify the maximum nesting level not less than 2. To disable scanning of nested objects, specify 0 as the maximum nesting level for the corresponding type of containers.

Note that increasing of maximum nesting level slows down the file system monitoring.

The **Maximum compression ratio** field allows you to specify maximum compression ratio (as a ratio of size of compressed file to its original) for compressed files. If compression ratio of a file is greater than the maximum allowed, the file is skipped during the check.

### 3.2.2.4. Scanning paths

On this page you can manage the list of paths to files and directories on a protected station that are checked or are skipped by SpIDer Guard under monitoring of the file system.







The excluded (skipped) paths are specified in the **Excluded paths** field (one path per line). Files and directories which are included into the excluded paths, are skipped by SpIDer Guard during the file system monitoring.

The excluded (trusted) processes are specified in the **Excluded processes** field (one process per line). All actions with files which are initiated by any of the processes (programs) from this list are not under control of SpIDer Guard. For each process to be excluded it is necessary to specify the full (absolute) executable path on the protected station.

The paths to be checked on a protected station are specified in the **Scanned paths** field (one path per line). Note that the monitor will control only files and directories which are included into the paths from this list and not included into the paths from the **Excluded paths** list.

To add new path to any list, click  in the corresponding line. To delete some path from any list, click  in the corresponding line of the list.

### 3.2.2.5. Additional

On this page you can specify some advanced SpIDer Guard settings on the protected station.

The following advanced SpIDer Guard settings are available:

- **Operation mode**—defines one of the operation modes for SpIDer Guard on the station: via the Linux kernel module (LKM); using the **fanotify** system service; in auto mode, when the suitable operation mode detected automatically. It is recommended to specify the *AUTO* value.
- **Log level**—defines the log verbosity level that is used for SpIDer Guard messages logging.
- **Logging method**—defines the logging method for SpIDer Guard. The following values are allowed:
  - *Auto*—use the logging method which is defined in Dr.Web ConfigD settings for all components of the solution.
  - *Syslog*—use the **syslog** system service for SpIDer Guard messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from SpIDer Guard.
  - *Path*—use the specified file to store SpIDer Guard log messages. If you select this method, you must also specify a path to the file in the **Log file** field.

### 3.2.3. SpIDer Gate Settings

The **SpIDer Gate** page consists of the following sections, containing the corresponding parameters of Dr.Web for Linux operation:

- [General](#)—general SpIDer Gate settings
- [Actions](#)—actions on detection of threats by SpIDer Gate



- [Web filtering](#)—settings of web traffic check and control of access to Internet resources by SpIDer Gate
- [Containers](#)—settings of scanning of compound files (archives, email files, etc.)
- [Additional](#)—additional SpIDer Gate settings.

### 3.2.3.1. General

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- **Enable SpIDer Gate**—enables or disables SpIDer Gate on the protected station.
- **Use heuristic analysis**—instructs SpIDer Gate to use the heuristic analysis on the protected station to detect unknown threats. Note that heuristic analysis may slow down the file system monitoring but improves its reliability.
- **Scanning time of one element**—restrictions on maximal time spent on scanning of one file by SpIDer Gate on the station. If the value is 0, scan time is not limited.

### 3.2.3.2. Actions

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- Set the **Scan received files** checkbox to enable check of incoming (downloaded from Internet) files.
- In the **Block files** and **Additionally block** sections, select types of incoming malicious objects which will be blocked by SpIDer Gate (**Infected**, **Suspicious**, etc.).

### 3.2.3.3. Web filtering

On this page you can manage the following parameters of SpIDer Gate on the protected station:

- Set the **Scan URL** flag to enable check of Internet resources by categories.
- Set the **Block non-recommended websites** flag to deny access to the websites that use social engineering techniques to misguide users.
- Set the **Block URLs listed due to a notice from copyright owner** flag to deny access to the websites due to a notice from copyright owner who has found out the violation of rights to the intellectual property in the Internet.
- In the **Block websites from the following categories** section select the categories of websites (**Adult content**, **Violence**, etc.) you need to block access to.
- In the **White list/Black list** sections add the paths to the websites you need to allow/restrict access to:
  - To add a certain website, enter its full domain address (for example, `www.example.com`). Access to all web pages located on this domain will be defined by this string.



- To configure access to websites with similar names, enter the common part of their domain names. For example, if you enter `example`, the access to the `example.com`, `example.test.com`, `test.com/example`, `test.example222.com` and other similar websites will be defined by this string.
- To configure access to websites within a particular domain, enter the domain name with a period ". ". In this case, the access to all web pages located on this domain will be defined by this string. If specifying domain name, you use a forward slash "/", the substring before the "/" is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter `example.com/test`, SpIDer Gate will configure access to web pages such as `example.com/test11`, `template.example.com/test22`, etc.

### 3.2.3.4. Containers

On this page you can specify settings which SpIDer Gate is used for checking compound files (containers) of the following types: archives, mail files (email messages, mailboxes), packed objects and other containers (i.e. compound files that are not classified as archives, mail files or packed objects).

For each of the types you can specify in the corresponding field the maximum nesting level. The objects that are nested into container deeper than the specified level are skipped during scanning the container by SpIDer Gate. For example, if you want scan the contents of the archives which are nested into archives, specify the maximum nesting level not less than 2. To disable scanning of nested objects, specify 0 as the maximum nesting level for the corresponding type of containers.

Note that increasing of maximum nesting level slows down the file system monitoring.

The **Maximum compression ratio** field allows you to specify maximum compression ratio (as a ratio of size of compressed file to its original) for compressed files. If compression ratio of a file is greater than the maximum allowed, the file is skipped during the check.

### 3.2.3.5. Additional

On this page you can specify some advanced SpIDer Gate settings on the protected station.

The following advanced SpIDer Gate settings are available:

- **Log level**—defines the log verbosity level that is used for SpIDer Gate messages logging.
- **Logging method**—defines the logging method for SpIDer Gate. The following values are allowed:
  - *Auto*—use the logging method which is defined in Dr.Web ConfigD settings for all components of the solution.
  - *Syslog*—use the **syslog** system service for SpIDer Gate messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from SpIDer Gate.



- *Path*—use the specified file to store SplDer Gate log messages. If you select this method, you must also specify a path to the file in the **Log file** field.

### 3.2.4. Dr.Web Agent for UNIX Settings

The **Dr.Web Agent** page consists of the following sections, containing the corresponding parameters of Dr.Web for Linux operation:

- [General](#) – Dr.Web Agent for UNIX settings.
- [Configuration](#) – editor of settings for all the Dr.Web for Linux components.

#### 3.2.4.1. General

On this page you can manage the following parameters of Dr.Web Agent for UNIX on the protected station:

- **Statistics sending period**—defines the time period of sending general statistics from Dr.Web Agent for UNIX to the server.
- **Mobile mode for updates**—allows the workstation to receive updates from GUS if the server is not available. The following values are allowed:
  - *Auto*—instructs to use mobile mode, if allowed by the server, and perform updates both from GUS and from central protection server, depending on which connection is available and which connection quality is higher.
  - *Enable*—instructs to use mobile mode if it is allowed by the server (that is, perform updates from GUS using the updating component installed on the station).
  - *Disable*—instructs not to use mobile mode (updates are always received from the server).
- **Process the discovery requests**—set the flag, to allow Dr.Web Agent for UNIX to receive discovery requests from the server (discovery requests are used by the server to check the structure and state of the anti-virus network).
- **Log level**—defines the log verbosity level that is used for Dr.Web Agent for UNIX messages logging.
- **Logging method**—defines the logging method for Dr.Web Agent for UNIX. The following values are allowed:
  - *Auto*—use the logging method which is defined in Dr.Web ConfigD settings for all components of the solution.
  - *Syslog*—use the **syslog** system service for Dr.Web Agent for UNIX messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from Dr.Web Agent for UNIX.
  - *Path*—use the specified file to store Dr.Web Agent for UNIX log messages. If you select this method, you must also specify a path to the file in the **Log file** field.



Usually, for the parameters of this component the optimal values are specified. Thus, it is not recommended to change them, if it is not necessary.

### 3.2.4.2. Configuration

On this page you can specify settings for any of the Dr.Web for Linux components installed on the station (an `.ini` configuration file format is used).

To specify settings, make the corresponding changes in the **Configuration file `drweb.ini`** field (*ini editor*).

Please note that:

- The *ini editor* shows only the configuration parameters having the values that have been changed on this page.
- Values of the configuration parameters that specified in the editor take precedence over values specified by the component setting pages: if on a settings page is one value of some parameter is specified and the other value for this parameter is specified in the *ini editor* on the **Configuration** page, the value that is specified on the **Configuration** page, will be used on the station. Moreover, if a section of some component is specified in the *ini editor*, for all parameters of the component that are not defined in the section, the default values are applied on the station.
- The context hints are supported by the *ini editor*: to show hint containing list of available parameters (or configuration section names, depending on the context), press CTRL+SPACE.
- You can export contents of the *ini editor* to `.ini` configuration file and import the contents from `.ini` configuration file. To do that click the corresponding icon at the top part of the page (above the *ini editor*).



For a complete list of components on the station that are available for configuration, and for a description of their parameters in the `drweb.ini` configuration file, refer to User manual or Administrator manual of the product installed on the station.

### 3.2.5. File Checker Settings

On this page you can manage parameters which are used by File Checker auxiliary component on the protected station.

The following parameters are available:

- **Maximum checked file cache size**—defines size of the cache that is used by File Checker for temporarily storing the results of files scan.
- **Cache validity period**—defines the duration of a time period when File Checker does not rescans the file, if its scan result is available in the cache.



- **Log level**—defines the log verbosity level that is used for File Checker messages logging.
- **Logging method**—defines the logging method for File Checker. The following values are allowed:
  - *Auto*—use the logging method which is defined in Dr.Web ConfigD settings for all components of the solution.
  - *Syslog*—use the **syslog** system service for File Checker messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from File Checker.
  - *Path*—use the specified file to store File Checker log messages. If you specify this method, you must also specify a path to the file in the **Log file** field.

Also, you can choose which additional data will be saved to the log on the *Debug* verbosity level.

- **IPC subsystem**—save IPC messages on component interaction
- **File scanning**—save file scan results
- **SplDer Guard file monitoring**—save SplDer Guard scan requests
- **Checked file cache status**—save the cache state changes.



Usually, for the parameters of this component the optimal values are specified. Thus, it is not recommended to change them, if it is not necessary.

### 3.2.6. Scanning Engine Settings

On this page you can manage parameters which are used by Scanning Engine auxiliary component on the protected station.

The following parameters are available:

- **Path to the socket file of the fixed copy of the component**—path to the special UNIX socket that is used by separate Scanning Engine instance. This instance is running permanently, if the socket is specified, and can be used by external programs for file scan via this socket. If the path is empty, the separated Scanning Engine instance is not running and is not available for external programs. The standard Scanning Engine instance running and terminating automatically, when it necessary for file scanning.
- **Number of scanning processes**—defines the maximum allowed number of child scanning processes that can be running by Scanning Engine during the scanning of files. If you want to change this value, evaluate the number of CPU cores available on the station.
- **Watchdog timer**—defines the duration of a time period which is used by Scanning Engine for automatic detection and termination the suspended scanning processes ("watchdog" timer).
- **Log level**—defines the log verbosity level that is used for Scanning Engine messages logging.



- **Logging method**—defines the logging method for Scanning Engine. The following values are allowed:
  - *Auto*—use the logging method which is defined in Dr.Web ConfigD settings for all components of the solution.
  - *Syslog*—use the **syslog** system service for Scanning Engine messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from Scanning Engine.
  - *Path*—use the specified file to store Scanning Engine log messages. If you specify this method, you must also specify a path to the file in the **Log file** field.



Usually, for the parameters of this component the optimal values are specified. Thus, it is not recommended to change them, if it is not necessary.

### 3.2.7. Dr.Web ConfigD Settings

On this page you can manage parameters which are used by Dr.Web ConfigD auxiliary component on the protected station.

The following parameters are available:

- **Public communication socket path**—path to internal UNIX socket that is used for interaction with Dr.Web ConfigD by Dr.Web for Linux components.
- **Administrative communication socket path**—path to internal UNIX socket that is used for interaction with Dr.Web ConfigD by Dr.Web for Linux components operating with superuser privileges.
- **Temporary files directory**—path to the directory with temporary files saved by Dr.Web for Linux components.
- **Path to the directory with PID files and communication sockets**—path to the directory with PID files and UNIX sockets that used for Dr.Web for Linux components interaction.
- **Log level**—defines the log verbosity level that is used for Dr.Web ConfigD messages logging.
- **Logging method**—defines the logging method for Dr.Web ConfigD. The following values are allowed:
  - *Syslog*—use the **syslog** system service for Dr.Web ConfigD messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from Dr.Web ConfigD.
  - *Path*—use the specified file to store Dr.Web ConfigD log messages. If you specify this method, you must also specify a path to the file in the **Log file** field.



Usually, for the parameters of this component the optimal values are specified. Thus, it is not recommended to change them, if it is not necessary.



## 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.



