Managing Dr.Web for Linux

Жасағаның
دافع عن إبداعاتك
Защити созданное
Defend what you create
Protégez votre univers
Verteidige, was du erschaffen hast
Захисти створене
保护您创建的一切
Защити созданное
Proteggi ciò che crei
Защити созданное
Жасағанының қорға
Verteidige, was du erschaffen hast
Proteggi ciò che crei
Захисти створене
Defend what you create
脅威からの保護を提供します
Protégez votre univers
Proteggi ciò che crei
Захисти створене
دافع عن إبداعاتك
脅威からの保護を提供します
Defend what you create
Жасағанының қорға
دافع عن إبداعاتك
دافع عن إبداعاتك
Protégez votre univers
保护您创建的一切
Защити созданное
脅威からの保護を提供します
Захисти створене
Verteidige, was du erschaffen hast

Dr.Web Enterprise Security Suite. Managing Dr.Web for Linux
Version 10.00.1
Administrator Manual
2/14/2017

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: http://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

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 Manual contains the following conventions:

Symbol	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.
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.

Abbreviations

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

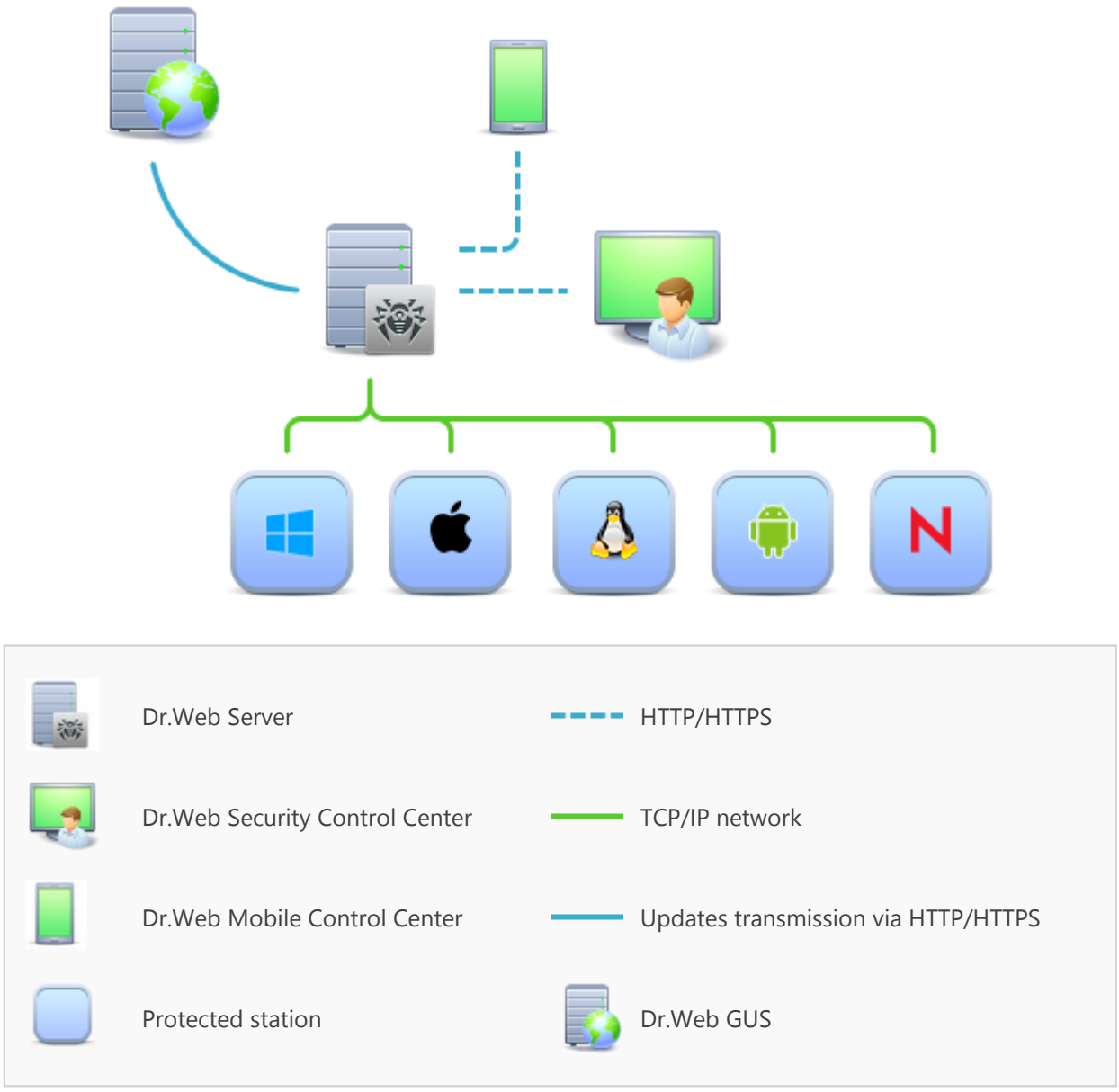
- Dr.Web GUS—Dr.Web Global Update System,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- IP—Internet Protocol,
- LAN—Local Area Network,
- LKM—Linux Kernel Module,
- OS—operating system,
- PC—personal computer,
- TCP—Transmission Control Protocol,
- URL—Uniform Resource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



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 stations 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 **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 **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 are monitored in order to block access to the websites included in the black lists and to categories that marked as unwanted, and to check files on the fly for viruses or other threats. To restrict access to unwanted websites, Dr.Web for Linux supports databases of web resource categories that are automatically updated, and white and black 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. For additional protection, Dr.Web Link Checker is also included. It is an extension for **Google Chrome** and **Mozilla Firefox** browsers which allows to scan the content of downloaded webpages for malicious links and obtrusive advertising as well as to block such downloads automatically.

3.1. Dr.Web for Linux Components

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

Scanner

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

SpIDer Guard

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

SpIDer Gate (can be managed on station only)

The component which works in resident mode and monitors all attempts to access the Internet. It checks whether the requested URL in unwanted category of web resources or in the user's black list, and, if so, blocks access to the resource. The component also sends File Checker tasks to scan files downloaded from the Internet (from web 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.

File Checker

The auxiliary component. It is used by Scanner, SpIDer Guard and SpIDer Gate for file checking and managing of Quarantine.

Scanning Engine

The auxiliary component. It is used by File Checker for managing of virus databases during file checking.

Dr.Web ConfigD

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

Dr.Web Link Checker (can be managed only locally)

This is an extension for **Google Chrome** and **Mozilla Firefox** browsers, which allows to scan the content of downloaded webpages for malicious links and obtrusive advertising as well as to block such downloads automatically.

Quarantine

Isolates malicious and suspicious objects in the special folder.

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

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** → **Linux** subsection, select the necessary component of Dr.Web for Linux.
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.

3.2.1. Scanner Settings

The **Scanner** pare consists of the following sections, containing the corresponding parameters of Scanner operation:

- General—general Scanner settings
- Actions—setting actions on threats detected by Scanner
- Excluded Paths—paths to be excluded from the file check.

3.2.1.1. General

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

- **Executable file path**—executable path for Scanner
- **Scanning timeout**—restrictions on time spent on scanning of one file by Scanner on the station. If the value is 0, scan time is not limited.

3.2.1.2. Actions

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

Scanner 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 dele-

tion 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 only notifies the user on threat detection and user must determine the necessary action for the file.
- **Archives**—instructs Scanner to scan the contents of archives. If the check box is cleared, the archive file structure are scanned by Scanner anyway, but enclosed files are excluded from scans.
- **Email files**—instructs Scanner 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 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 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** pare 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.)
- 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 timeout**—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. 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 **Included 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 processes** 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.
- **Executable file path**—executable path for SpIDer Guard.
- **Logging 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. 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:

- **Executable file path**—executable path for File Checker.
- **Maximum 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 rescan the file, if its scan result is available in the cache.
- **Logging 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

- **SpIDer Guard events**—save SpIDer Guard scan requests
- **File cache changes**—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.

3.2.4. 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:

- **Executable file path**—executable path for Scanning Engine.
- **Fixed socket path**—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.
- **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 termination the suspended scanning processes ("watchdog" timer).
- **Logging 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.

3.2.5. 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 socket file**—path to internal UNIX socket that is used for interaction with Dr.Web ConfigD by Dr.Web for Linux components.
- **Administrative socket file**—path to internal UNIX socket that is used for interaction with Dr.Web ConfigD by Dr.Web for Linux components operating with superuser privileges.
- **Virus-Finding Engine library**—executable path of Dr.Web Virus-Finding Engine that is used for detecting threats.
- **Virus database directory**—path to the directory containing virus databases that are used on the station.
- **Cache directory**—path to the directory with files cached by Dr.Web for Linux components.
- **Temporary files directory**—path to the directory with temporary files saved by Dr.Web for Linux components.
- **PID files and sockets directory**—path to the directory with PID files and UNIX sockets that used for Dr.Web for Linux components interaction.
- **Path to subject black lists**—path to the directory containing database of Internet resource categories that used on the station.
- **Library directory**—path to the directory with auxiliary libraries.
- **Logging 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 http://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at http://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 from in the corresponding section at http://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

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