Dr.WEB

Enterprise Security Suite

Managing Dr.Web for UNIX File Servers

Dr.Web Enterprise Security Suite. Managing Dr.Web for UNIX File Servers
Version 12.0
Administrator Manual
5/25/2021

Doctor Web

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

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

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

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

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

Table of Contents

Chapter 1. Introduction

1.1. About Manual

This manual is a part of 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 UNIX File Servers anti-virus solution and features of centralized configuration of the software.

To get additional information, please refer the following manuals:

- **Administrator Manual** of Dr.Web for UNIX File Servers 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.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`/home/user`	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:

- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- FQDN—Fully Qualified Domain Name,
- FS—File System,
- FTP—File Transfer Protocol,
- HTML—HyperText Markup Language,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- ICAP—Internet Content Adaptation Protocol,
- IP—Internet Protocol,
- LAN—Local Area Network,
- LKM—Linux Kernel Module,
- MBR—Master Boot Record,

- MIME—Multipurpose Internet Mail Extensions,

- OS—Operating System,

- PC—Personal Computer,

- SMB—Server Message Block,

- SSL—Secure Socket Layers,

- TCP—Transmission Control Protocol,

- TLS—Transport Layer Security,

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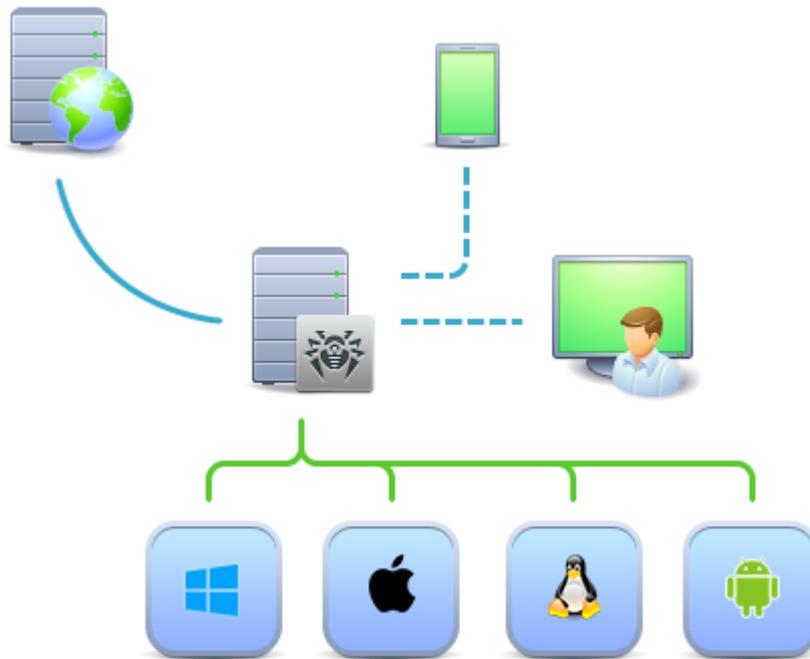
Dr.Web Server		- - - -	HTTP/HTTPS
Dr.Web Security Control Center		———	TCP/IP network
Dr.Web Mobile Control Center		———	Updates transmission via HTTP/HTTPS
Protected station			Dr.Web GUS

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 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 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 UNIX File Servers

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

Dr.Web for UNIX File Servers is an anti-virus solution designed to protect file servers running under UNIX OSes (**GNU/Linux** and **FreeBSD**) from viruses and other types of malicious software, and to prevent distribution of the threats designed for all popular operating systems including mobile platforms.

Dr.Web for UNIX File Servers provides you with the following features:

1. **Detection and neutralization of threats.** Searches for 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).

   Threat detection methods:

   - *Signature analysis*, which allows detection of known threats

   - *Heuristic analysis*, which allows detection of threats that are not present in virus databases

   - *Dr.Web Cloud* service that collects up-to-date information about recent threats and sends it to Dr.Web products.

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

   Scanning at user's request can be performed in two modes: full scan (scan of all file system objects) and custom scan (scan of selected objects: directories or files that satisfy specified criteria). Moreover, the user can start a separate scan of volume boot records and executables that ran processes that are currently active. In the latter case, if a malicious executable is detected, it is neutralized and all processes run by this file are forced to terminate.

2. **Monitoring access to files of**

   - **File system in the OS.** Monitors file events and attempts to run executables. This feature allows to detect and neutralize malware at an attempt to infect the server's file system.

   - **Samba shared directories.** Read and write operations of local and remote users of the file server are monitored. This feature allows to detect and neutralize malware at an attempt to save a malicious program to the file storage, which prevents its distribution over the network.

   - **NSS (Novell Storage Services) volumes.** Monitors write operations of the NSS file storage users. This feature allows to detect and neutralize malware at an attempt to save the malicious program to NSS storage, which prevents its distribution over the network.

> Note that the function of file system monitoring is available only for the operating systems of the **GNU/Linux** family, and the function of **Novell Storage Service** volumes monitoring is available only for the **Novell Open Enterprise Server** SP2 based on the **SUSE Linux Enterprise Server** 10 SP3 or above. For other supported operating systems, the corresponding monitoring components are not included in the distribution.

3.1. Dr.Web for UNIX File Servers Components

For UNIX file servers protection, the following anti-virus components are provided:

General Components

*SpIDer Guard (for **GNU/Linux**)*

A file system monitor. Operates in background mode and controls file operations (such as creation, opening, closing, running) in **GNU/Linux** file systems. It sends to *File Checker* requests to scan new or changed files as well as executables of programs when they are run.

SpIDer Guard for SMB

A **Samba** shared directories monitor. Operates in background mode and monitors file system operations (such as creation, opening, closing, read and write operations) in the directories selected as the **Samba** server's file storages. Sends content of new or modified files for scanning to *File Checker*. Integration with the file server is performed via VFS SMB modules that operate on **Samba** server side.

SpIDer Guard for NSS

A NSS (**Novell Storage Services**) volumes monitor. Operates in background mode and controls file system operations (such as creation, opening, closing and write operations) on NSS volumes that are mounted on the file system. Sends new or modified files for scanning to *File Checker*.

Dr.Web Console Scanner (can be managed on station only)

Provides detection and neutralisation of viruses on the local machine. Managed via the console command line.

Dr.Web ClamD

Component emulating interface of the anti-virus daemon **clamd**, which is a component of **ClamAV**® anti-virus. Allows all applications that support **ClamAV**® to transparently use Dr.Web for UNIX File Servers for anti-virus scanning.

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**.

Auxiliary Components

Dr.Web Agent for UNIX

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

File Checker

The component is used by *Console Scanner* for checking files in *Scanning Engine* and for managing *Quarantine*.

Network Checker

The component is used to send data to the *Scanning Engine* for actual scanning. It is used by general components to check data transmitted over the network.

Scanning Engine

The component is used by *File Checker* and *Network Checker* for anti-virus scan and virus databases managing.

SNMP Agent

The component is designed for integration of Dr.Web for UNIX File Servers with external monitoring systems over the SNMP protocol.

Dr.Web ConfigD

The component that coordinates operation of all Dr.Web for UNIX File Servers components.

Dr.Web CloudD

The component that sends the following information to the *Dr.Web Cloud* service: visited URLs and information about the scanned files, to check them for threats not yet described in virus databases.

Dr.Web HTTPD (can be managed on station only)

Web server for managing Dr.Web for UNIX File Servers components. It provides the management web interface for product installed on the station.

3.2. Dr.Web for UNIX File Servers 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 required OS (**Linux**, **Solaris** or **FreeBSD**) 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 ale to edit settings via the Control Center.

3.2.1. 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 UNIX File Servers 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.

3.2.1.1. 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.

3.2.1.2. 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.

3.2.1.3. 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.

3.2.1.4. 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.

3.2.1.5. 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.

3.2.2. SpIDer Guard for SMB Settings

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

- General—general SpIDer Guard for SMB settings
- Actions—actions on detection of threats by SpIDer Guard for SMB
- Containers—settings of scanning of compound files (archives, email files, etc.)

- Scanning paths—settings of exclusions of files and directories from monitoring
- Shared directories—individual settings of monitoring shared directories by SpIDer Guard for SMB
- Additional—additional SpIDer Guard for SMB settings.

3.2.2.1. General

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

- **Run the component at the start**—enables or disables SpIDer Guard for SMB on the protected station.
- **Use heuristic analysis**—instructs SpIDer Guard for SMB 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 monitoring but improves its reliability.
- **Maximum checked file cache size**—defines size of the cache that is used by SpIDer Guard for SMB for temporarily storing the results of files scan.
- **Scanning time of one element**—restrictions on maximal time spent on scanning of one file by SpIDer Guard for SMB 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 for SMB is use to check files in shared directories on the protected station.

- **Create file with the blocking reason**—set the checkbox to instruct SpIDer Guard for SMB to create near a blocked file a special text file. The created text file describes the reason why the object was blocked.
- **Block access to the file upon the scanning error**—set the checkbox in order to SpIDer Guard for SMB block access to a file in a shared directory if an attempt to cure it resulted in an error.
- **Delay before the application of action**—specify a delay time between the moment when a threat is detected and the moment when SpIDer Guard for SMB applies the action specified for this threat type. During this time period, the file is blocked.

SpIDer Guard for SMB can react to the following events:

- **Infected**—scanned file contains a known virus
- **Suspicious**—scanned file marked as *suspicious*
- **Incurable**—scanned file contains a threat that cannot be neutralized by *Cure* action.
- **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*—instructs to restore the original state of the object before infection. 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.
- *Block*—block for users access to the infected file.

3.2.2.3. Containers

On this page you can specify settings which SpIDer Guard for SMB 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 SMB. 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 for SMB under monitoring of the file system.

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

The paths to be checked in the shared directory 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. Shared directories

On this page you can specify some individual parameters for monitoring separate **Samba** shared directories by SpIDer Guard.

Each shared directory in this case must have a unique tag value. The tag value is specified in the **Samba** configuration file. To associate individual monitoring parameters with the certain shared directory, specify the corresponding tag value in the **Shared directory tag** field.

To add individual monitoring parameters for a shared directory, click ![+] in the list of shared directories. To delete individual monitoring parameters for a some shared directory, click ![−] in the corresponding item of shared directories.

> For a shared directory that does not have individual monitoring parameters, the common monitoring parameters are applied. These parameters are defined on the corresponding pages (**Actions**, **Containers**, **Scanning paths**, etc.).

In the shared directory section with the tag you can specify individual values for some of monitoring parameters. To do that, select a required parameter in **Shared directory settings** list, then specify required value of the parameter in the **Settings parameter** field.

To add new individual monitoring parameter in the list of individual settings for the shared directory, click ![+] in the corresponding list item. To delete any individual monitoring parameter for the shared directory, click ![−] in the corresponding list item.

3.2.2.6. Additional

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

The following advanced SpIDer Guard for SMB settings are available:

- **Virtual root directory**—defines the path to the root directory of the SMB file storage (can be redefined by the file server with the help of the **chroot** restriction). Used as a prefix inserted at the beginning of all paths to files and directories residing in the file server's storage and describes the path relative to the root of the local file system.
- **Path to the socket file**—defines the path to the socket file which enables interaction between SpIDer Guard for SMB and VFS SMB modules. The path is always relative and is a supplement for the path specified as the **Virtual root directory** parameter value.
- **Log level**—defines the log verbosity level that is used for SpIDer Guard for SMB messages logging.

- **Logging method**—defines the logging method for SpIDer Guard for SMB. 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 for SMB 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 for SMB.

  - *Path*—use the specified file to store SpIDer Guard for SMB 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 Guard for NSS Settings

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

- General—general SpIDer Guard for NSS settings
- Actions—actions on detection of threats by SpIDer Guard for NSS
- 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 for NSS settings.

3.2.3.1. General

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

- **Run the component at the start**—enables or disables SpIDer Guard for NSS on the protected station.
- **Use heuristic analysis**—instructs SpIDer Guard for NSS 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 NSS volumes monitoring but improves its reliability.
- **Scanning time of one element**—restrictions on maximal time spent on scanning of one file by SpIDer Guard for NSS on the station. If the value is *0*, scan time is not limited.

3.2.3.2. Actions

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

SpIDer Guard for NSS can react to the following events:

- **Infected**—scanned file contains a known virus
- **Suspicious**—scanned file marked as *suspicious*

- **Incurable**—scanned file contains a threat that cannot be neutralized by *Cure* action.
- **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
- **Actions in case of error**—file cannot be scanned or the scan raised an error.

For these events, the following actions are allowed:

- *Cure*—instructs to restore the original state of the object before infection. 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.

3.2.3.3. Containers

On this page you can specify settings which SpIDer Guard for NSS 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 NSS. 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.

3.2.3.4. 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 for NSS 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 for NSS during the file system monitoring.

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.

3.2.3.5. Additional

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

The following advanced SpIDer Guard for NSS settings are available:

- **NSS volumes mounting point**—defines the path to the file system directory where NSS file system volumes are mounted.
- **Protected NSS volumes**—defines the list of names of NSS file system volumes mounted on **NSS volumes mounting point** and protected by the suite. If no value is specified, all volumes in **NSS volumes mounting point** must be protected.

  To add new volume in the list list, click ➕ in the corresponding line of the list. To delete some volume from the list, click ➖ in the corresponding line of the list.
- **Log level**—defines the log verbosity level that is used for SpIDer Guard for NSS messages logging.
- **Logging method**—defines the logging method for SpIDer Guard for NSS. 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 for NSS 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 for NSS 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 UNIX File Servers operation:

- General – Dr.Web Agent for UNIX settings.

- Configuration – editor of settings for all the Dr.Web for UNIX File Servers 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 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 UNIX File Servers 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 rescan 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
- **SpIDer Guard file monitoring**—save SpIDer 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 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 UNIX File Servers components.

- **Administrative communication socket path**—path to internal UNIX socket that is used for interaction with Dr.Web ConfigD by Dr.Web for UNIX File Servers components operating with superuser privileges.

- **Temporary files directory**—path to the directory with temporary files saved by Dr.Web for UNIX File Servers 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 UNIX File Servers 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/.
- 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.