Dr.WEB

Enterprise Security Suite

Managing Unix File Servers

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 the property of their respective owners.

Disclaimer

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

Dr.Web Enterprise Security Suite. Managing Unix File Servers
Version 13.0
Administrator Manual
12/26/2024

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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

1. Introduction

1.1. About This Manual

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

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

The manual contains the information about centralized configuration of anti-virus software on workstations performed by the anti-virus network administrator via Dr.Web Security Control Center. The manual describes the settings of the Dr.Web Server Security Suite anti-virus solution and features of the centralized management of this software.

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

- The Administrator Manual of the Dr.Web Server Security Suite anti-virus solution contains information about configuring the anti-virus software directly on a station.
- The Administrator Documentation of the anti-virus network protected by Dr.Web Enterprise Security Suite (includes the Administrator Manual, Installation Manual and Appendices) contains general information on installing and configuring the anti-virus network and, particularly, on using Dr.Web Security Control Center.

Before reading these documents make sure that you have the latest version of the manuals. The manuals are constantly updated and the actual version can always be found at the official website of Doctor Web.

1.2. Conventions and Abbreviations

Conventions

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

Convention	Comment
❗	An important note or instruction.
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`/home/user`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

Abbreviations

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

- CSV—Comma-Separated Values,
- GUS—Dr.Web Global Update System,
- HTML—HyperText Markup Language,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- IP—Internet Protocol,
- LAN—Local Area Network,
- LKM—Linux Kernel Module,
- OS—Operating System,
- PDF—Portable Document Format,
- SMB—Server Message Block,
- TCP—Transmission Control Protocol,
- URL—Uniform Resource Locator,

- VFS—Virtual File System,
- XML—Extensible Markup Language.

2. Dr.Web Enterprise Security Suite

2.1. About This Product

Dr.Web Enterprise Security Suite is designed for organization and management of integral and reliable complex anti-virus protection of either internal corporate network, including mobile devices, or home computers of employees.

A combination of computers and mobile devices, on which Dr.Web Enterprise Security Suite cooperating components are installed, represents an integral *anti-virus network*.

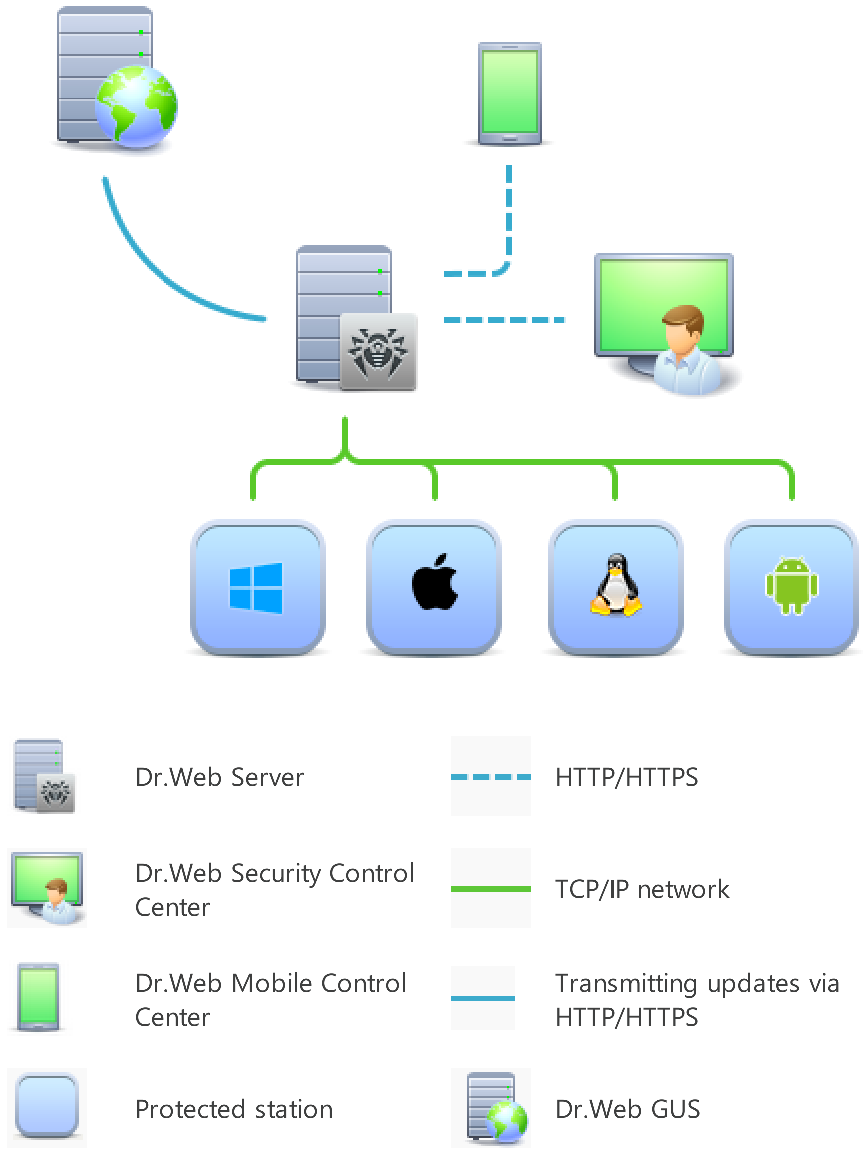
Dr.Web Server
HTTP/HTTPS
Dr.Web Security Control Center
TCP/IP network
Dr.Web Mobile Control Center
Transmitting updates via HTTP/HTTPS
Protected station
Dr.Web GUS

Figure 1. The logical structure of the anti-virus network

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

2.2. Protection of Unix File Servers

Protection of Unix file servers is performed by Dr.Web anti-virus packages.

> The term *anti-virus network station* is used to designate a protected device with the anti-virus package installed.
> This term may refer to a PC, a mobile device or 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. The protected stations and the Dr.Web Server communicate via the protocol used in the local network (TCP/IP version 4 or 6).

Installation

Local installation is performed on the protected station directly either by the administrator of this station or by the administrator of the anti-virus network.

> For the detailed description of how to install anti-virus packages on protected stations, refer to the Dr.Web Enterprise Security Suite Installation Manual.

Management

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

- Centralized configuration of the anti-virus package on the protected station via the Security Control Center.

  The administrator can either allow or forbid the users to change the settings of the anti-virus package on the protected station.
- Configuring the schedule for anti-virus scans and other tasks to run on the protected station.
- Getting scan statistics and other information on the operation of the anti-virus components and on the state of the protected station.
- Starting and stopping anti-virus scans, etc. (depending on the functionality of the anti-virus package installed on the protected station).

Updating

Dr.Web Server downloads updates and distributes them to the protected stations connected to it. Thus, optimal protection against threats is implemented, maintained and adjusted automatically regardless of the skills of the administrator of the protected stations.

If a protected station is disconnected from the anti-virus network, the anti-virus package installed on the server uses the local copy of the settings and the anti-virus protection retains its functionality (until the expiration of the user license), but the software is not updated.

3. Dr.Web Server Security Suite

3.1. Dr.Web Server Security Suite Functions

This Manual describes aspects of configuring components of Dr.Web Server Security Suite designed for GNU/Linuxand FreeBSD. The Manual is intended for a person responsible for anti-virus protection and configuration of networks (hereinafter referred to as "Administrator").

Dr.Web Server Security Suite is designed to protect servers running on OSes of GNU/Linux family and FreeBSD from viruses and other types of malicious software, and to prevent distribution of threats designed for different platforms.

Main features of Dr.Web Server Security Suite:

1. **Detection and neutralization of threats.** Scans for malicious programs of all possible types (various viruses, including those that infect mail files and boot records, trojans, mail worms, and so on) and unwanted software (adware, joke programs and dialers).

   Threat detection methods:

   - *signature analysis*—a scan method allowing to detect known threats registered in virus databases;
   - *heuristic analysis*—a set of scan methods allowing to detect threats that are not known yet;
   - *using Dr.Web Cloud* service, which collects up-to-date information about recent threats and sends it to various products of Doctor Web.

   Note that the heuristic analyzer may raise false-positive detections of legitimate software. 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 the Doctor Web anti-virus laboratory.

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

2. **Monitoring access to files:**

   - **File system in the OS.** File events and attempts to run executables are monitored. This feature allows to detect and neutralize malware instantly at attempt of infecting the file system of the server.
   - **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 instantly at attempt of copying a malicious program to the file storage, which prevents its further distribution over the network.
   - **NSS (Novell Storage Services**) volumes**.** Write operations of the NSS file storage users are monitored. This feature allows to detect and neutralize malware instantly at attempt

of copying the malicious program to the NSS storage, which prevents its further 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 Services volumes monitoring is available only for Novell Open Enterprise Server SP2 based on SUSE Linux Enterprise Server 10 SP3 or earlier. For other supported operating systems, the corresponding monitoring components are not included in the distribution.

3. **Reliable isolation of infected or suspicious objects** in a special storage (quarantine) to prevent any harm to the system. When quarantined, objects are renamed according to custom rules and, if necessary, they can be restored to their original location only on demand of the user.

3.2. Dr.Web Server Security Suite Components

For the protection of Unix file servers, the following components are provided:

General

SpIDer Guard (for GNU/Linux version)

A GNU/Linux file system monitor. Operates in a background mode and controls file operations (such as creation, opening, closing, running). Sends requests to File Checker to scan new and modified files, as well as executables upon starting programs.

SpIDer Guard for SMB

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

> The component is supplied only with the distributions designed for GNU/Linux OSes.

Dr.Web ClamD

A component emulating interface of ClamAV® anti-virus product. Enables all applications that support ClamAV® to use Dr.Web Server Security Suite for anti-virus scanning.

Auxiliary

Dr.Web Agent for Unix

An auxiliary component. Used for interaction of Dr.Web Server Security Suite installed on the station with Dr.Web Enterprise Security Suite.

File Checker

Used by the Console Scanner to pass files to the Scanning Engine for scanning and to manage Quarantine on the station.

Network Checker

Used to pass data sent over the network by the components of the software suite to Scanning Engine for scanning. The component is used by all general components.

Scanning Engine

Used by File Checker and Network Checker for anti-virus scan and virus database management.

SNMP Agent

The component is designed for integration of Dr.Web Server Security Suite with external monitoring systems via the SNMP protocol.

Dr.Web ConfigD

Coordinates operation of all Dr.Web Server Security Suite components.

Dr.Web CloudD

A component receiving information from the cloud service about whether visited URLs and transferred files are dangerous.

Dr.Web HTTPD

A web server for managing Dr.Web Server Security Suite components. Provides the management web interface.

3.3. Dr.Web Server Security Suite Operation Modes

The Dr.Web Server Security Suite anti-virus solution can operate both in a standalone mode and as a part of a corporate or private *anti-virus network* managed by a *centralized protection server*. Such operation mode is called *centralized protection mode*. Operation in this mode does not require installation of additional software or Dr.Web Server Security Suite re-installation or uninstallation.

- In a *standalone mode*, the protected computer is not connected to the anti-virus network and its operation is managed locally. In this mode, configuration and license key files are located on local disks and Dr.Web Server Security Suite is fully controlled from the protected computer. Updates of virus databases are received from Doctor Web update servers.

- In the *centralized protection mode*, protection of the computer is managed by the centralized protection server. In this mode, some functions and settings of Dr.Web Server Security Suite can be adjusted or locked in accordance with the general (corporate) anti-virus protection policy implemented on the anti-virus network. A custom license key file received from a selected centralized protection server to which Dr.Web Server Security Suite is connected is used on the computer in this mode. A license or demo key file stored on the local computer, if any, is not used. The information about Dr.Web Server Security Suite operation, including statistics on virus events, is sent to the centralized protection server. Updates of virus databases are also received from the centralized protection server.
- In the *mobile mode*, Dr.Web Server Security Suite receives updates from Doctor Web update servers, but uses settings stored locally and a custom license key file that were received from the centralized protection server. You can switch to this mode only if it is allowed in the centralized protection server settings.

Centralized Protection Concept

Doctor Web solutions for managing centralized protection use a client-server model (see the figure below).

Corporate computers or computers of users of an IT service provider are protected by *local anti-virus components* (in this case, of Dr.Web Server Security Suite), which ensure anti-virus protection and maintain connection to the centralized protection server.

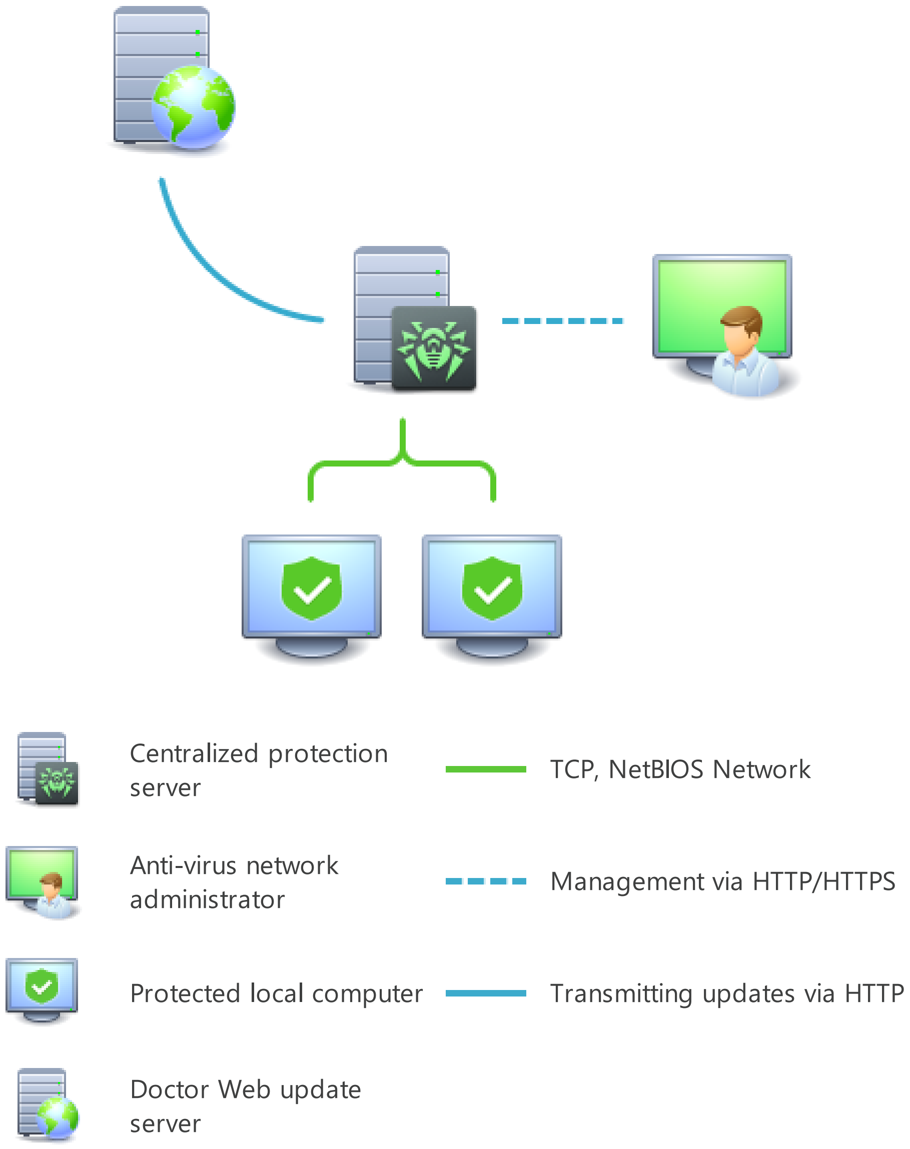
Centralized protection server
TCP, NetBIOS Network
Anti-virus network administrator
Management via HTTP/HTTPS
Protected local computer
Transmitting updates via HTTP
Doctor Web update server

Figure 2. The logical structure of the anti-virus network

Local computers are updated and configured from the *centralized protection server*. The entire stream of instructions, data and statistics in the anti-virus network passes the centralized protection server. The volume of traffic between protected computers and the centralized protection server can be significant, therefore an option for traffic compression is provided. Using encryption while transmitting data prevents leak of sensitive data or substitution of software downloaded to protected computers.

All necessary updates are downloaded to the centralized protection server from Doctor Web update servers.

Changes in the configuration of local anti-virus components and command transfer are performed by anti-virus network administrators using the centralized protection server. The administrators manage configuration of the centralized protection server and topology of the anti-virus network (for example, they validate connection of a local station to the network) and configure operation of individual local anti-virus components when necessary.

> Local anti-virus components are not compatible with anti-virus products of other companies or Dr.Web anti-virus solutions if the latter do not support operation in the centralized protection mode (for example, Dr.Web for UNIX File Servers version 5.0). Installation of two anti-virus programs on the same computer can cause a system crash and loss of important data.

> Dr.Web Server Security Suite version 11.1 operating in the centralized protection mode is compatible with Dr.Web Enterprise Security Suite of versions 11, 12, 13 and 13.0.1.

The centralized protection mode allows exporting and saving Dr.Web Server Security Suite operation reports using the centralized protection center. Reports can be exported and saved in the following formats: HTML, CSV, PDF, and XML.

Connecting to the Centralized Protection Server

Dr.Web Server Security Suite can be connected to the centralized protection server of the anti-virus network using the `esconnect` command of the `drweb-ctl` command-line management tool.

> To verify the centralized protection server, the certificate corresponding to the unique public key of the server is used. By default, Dr.Web ES Agent, a centralized protection agent, will not allow you to connect to the server unless you specify a file of the certificate of the server to which the connection is being established. The certificate file must first be obtained from the administrator of the anti-virus network served by the server to which you want to connect Dr.Web Server Security Suite.

If Dr.Web Server Security Suite is connected to the centralized protection server, you can switch the product to the mobile mode or switch it back to the centralized protection mode. Switching the mobile mode on or off is accomplished using the `MobileMode` configuration parameter of the Dr.Web ES Agent component.

> Dr.Web Server Security Suite can switch to the mobile mode only if it is allowed in the settings on the centralized protection server in use.

Disconnecting from Centralized Protection Server

Dr.Web Server Security Suite can be disconnected from the centralized protection server of the anti-virus network using the `esdisconnect` command of the `drweb-ctl` command-line management tool.

3.4. Dr.Web Server Security Suite Configuration

To view or edit the settings of the anti-virus components on a workstation:

1. Choose **Anti-virus network** in the main menu of the Control Center.
2. In the hierarchical list of the opened window, click the name of a station under the required OS (GNU/Linux or FreeBSD) or a group comprising such stations.
3. In the **Configuration** section of the opened control menu, in the required OS subsection (GNU/Linux or FreeBSD), choose the necessary component.
4. A window with the anti-virus component settings will open.

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

   - to manage individual parameters, use buttons located on the right from the corresponding settings:

     Reset to initial value—restore a value assigned to the parameter before editing (the latest saved value);

     Reset to default value—reset the parameter to the default value;

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

     Reset all parameters to initial values—restore values assigned to the parameters of this section before editing (the latest saved values);

     Reset all parameters to default values—reset all parameters in this section to default values;

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

     Set inheritance of settings from primary group—remove individual settings of the station and inherit the settings of this section from the primary group.

     Copy settings from primary group and set them as personal—copy the settings of this section from the primary group and set them for the selected stations. In this case inheritance is not set and the settings of the station are considered individual.

     Export settings from this section to the file—save all settings from this section to a file in a specific format.

     Import settings to this section from the file—replace all settings in this section with the settings from the file in the specific format.

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

> The administrator may prevent a user from editing settings on a station (see the section **Permissions of Station Users** in the Administrator Manual). Moreover, only the administrator will be able to edit settings via the Control Center.

3.4.1. SpIDer Guard Settings

3.4.1.1. General Settings

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

- **Enable SpIDer Guard for Linux**—enable or disable SpIDer Guard on the protected station.
- **Use heuristic analysis**—define how SpIDer Guard uses the heuristic analysis on the protected station while scanning files "on-the-fly". The heuristic analysis slows down scanning, but improves its reliability.
- **Scanning time of one element**—set a time limit for scanning one file by SpIDer Guard on the station. If the value is set to *0*, the time period for scanning one file is unlimited.

> The SpIDer Guard file system monitor can operate in one of these two modes:
>
> - `FANOTIFY`—using the `fanotify` system mechanism (not all GNU/Linux OSes support this mode);
> - `LKM`—using the loadable Linux kernel module (can be used in any GNU/Linux OS with kernel 2.6.x and later).
>
> 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 the loadable kernel module on the protected station using the supplied source code.

3.4.1.2. Actions

On this page you can manage anti-virus protection parameters used by SpIDer Guard to scan files.

SpIDer Guard can react to the following threats:

- **Infected**—the scanned file contains a known threat;
- **Suspicious**—the scanned file has been marked as *suspicious*;
- **Adware**—the scanned file contains adware;
- **Dialers**—the scanned file contains a dialer;
- **Jokes**—the scanned file contains a joke program;
- **Riskware**—the scanned file contains riskware;
- **Hacktools**—the scanned file contains a hacktool.

Available actions:

- **Cure, move to quarantine if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is quarantined.

This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).

- **Cure, delete if not cured**—restore the state of the object before the infection. If the object is incurable or the attempt of curing fails, the object is deleted.

  This action is available only for the objects infected with a known virus that can be cured except for trojans and infected files within compound objects (archives, email files or file containers).
- **Delete**—delete the object that poses a threat.

  This is the most effective way to remove all types of threats.
- **Move to quarantine**—move a detected threat to a special directory isolated from the rest of the system.
- **Report**—notify of a threat without performing other actions.

Default settings are optimal in most cases. Do not change them unless necessary.

Table 1. Actions applied to threats detected by Dr.Web SpIDer Guard

Object	Action				
	Cure, move to quarantine incurable	**Cure, delete incurable**	**Delete**	**Move to quarantine**	**Report**
Infected	+/*	+	+	+	
Suspicious			+	+/*	+
Adware			+	+/*	+
Dialers			+	+/*	+
Jokes			+	+	+/*
Riskware			+	+	+/*
Hacktools			+	+	+/*

Conventions

+	action is enabled for an object of this type
+/*	action is set as default for an object of this type

3.4.1.3. Containers

On this page you can manage settings used by SpIDer Guard for scanning compound files, such as archives, mail files, packed objects and other containers (i.e. the compound files that are not related to any of the types above).

You can specify the nesting level limit for each of the file types in the corresponding field; when this limit is exceeded, SpIDer Guard will not unpack a file of such type during scanning. For example, to scan the contents of the archives that are nested in archives, specify the nesting level limit of no 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 the maximum nesting level slows down scanning.

The **Maximum compression ratio** field allows you to specify the maximum compression ratio (as a compressed/uncompressed file ratio) for objects to be scanned. If the compression ratio of an object to be scanned exceeds the specified value, this object will not be scanned.

3.4.1.4. Scanning Paths

On this page you can manage a list of paths to files and directories on the protected station to be scanned or skipped by SpIDer Guard while monitoring the file system.

Excluded paths are specified in the **Excluded paths** field (one path per line). Files and directories added to the list of the excluded paths are skipped by the SpIDer Guard monitor.

The excluded processes are specified in the **Excluded processes** field (one process per line). All file actions performed by processes (programs) from this list are not monitored by SpIDer Guard. For each process to be excluded it is necessary to specify a full executable path on the protected station.

The paths to be scanned on the protected station are specified in the **Scanned paths** field (one path per line). The SpIDer Guard monitor controls only those files that are added to the scanned paths and does not control those added to the paths from the **Excluded paths** list.

To add a new path to the relevant list, click + in the corresponding row of the list. To remove a path from the list, click − in the corresponding row of the list.

3.4.1.5. Advanced Settings

On this page you can manage advanced SpIDer Guard settings on the protected station (file server).

The following advanced SpIDer Guard settings are available:

- **Operation mode**—set one of the operation modes for SpIDer Guard on the protected station: using the Linux kernel module (LKM), using the fanotify system service, or in an auto mode, when a suitable operation mode is detected automatically. It is recommended to keep the *AUTO* value.

- **Log level**—a log verbosity level used for SpIDer Guard message logging.
- **Logging method**—a logging method for SpIDer Guard. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for SpIDer Guard message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from SpIDer Guard.
  - *Path*—use a separate file to store SpIDer Guard log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.2. SpIDer Guard for SMB Settings

3.4.2.1. General Settings

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

- **Run the component at the start**—enable or disable SpIDer Guard for SMB on the protected station at startup.
- **Use heuristic analysis**—define how SpIDer Guard for SMB uses the heuristic analysis on the protected station while scanning files “on-the-fly”. The heuristic analysis slows down scanning, but improves its reliability.
- **Maximum checked file cache size**—a size of the cache used by SpIDer Guard for SMB to temporarily store file scan results.
- **Scanning time of one element**—set a time limit for scanning one file by SpIDer Guard for SMB on the station. If the value is set to *0*, the time period for scanning one file is unlimited.

3.4.2.2. Actions

On this page you can manage anti-virus protection parameters used by SpIDer Guard for SMB to scan files in shared directories.

- **Create file with the blocking reason**—select this check box to instruct SpIDer Guard for SMB to create a special file describing a blocking reason in a shared directory next to an infected file.
- **Block access to the file upon the scanning error**—select this check box to instruct SpIDer Guard for SMB to block access in a shared directory to those files that could not be scanned.
- **Delay before the application of action**—specify a delay during which the file is blocked after a threat is detected and before SpIDer Guard for SMB applies the action to it (see below).

SpIDer Guard for SMB can react to the following threats:

- **Infected**—the scanned file contains a known threat;
- **Suspicious**—the scanned file has been marked as *suspicious*;
- **Incurable**—the scanned file contains a threat that cannot be neutralized with the Cure action;
- **Adware**—the scanned file contains adware;
- **Dialers**—the scanned file contains a dialer;
- **Jokes**—the scanned file contains a joke program;
- **Riskware**—the scanned file contains riskware;
- **Hacktools**—the scanned file contains a hacktool.

Available actions:

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

  This action is available only for objects infected with a known virus that can be cured except for trojans and files within compound objects.
- **Delete**—delete the object that poses a threat.

  This is the most effective way to remove all types of threats.
- **Block**—keep the file in the shared directory, but block user access to it.
- **Move to quarantine**—move a detected threat to a special directory isolated from the rest of the system.
- **Report**—notify of a threat without performing other actions.
- **Ignore**—skip the object without displaying notifications or performing other actions.

Default settings are optimal in most cases. Do not change them unless necessary.

Table 2. Actions applied to threats detected by SpIDer Guard for SMB

Object	Action					
	Cure	Delete	Block	Move to quarantine	Report	Ignore
Infected	+/*	+	+	+		
Suspicious		+	+	+/*	+	+
Incurable		+	+	+/*		
Adware		+	+	+	+	+/*
Dialers		+	+	+	+	+/*
Jokes		+	+	+	+	+/*

Object	**Action**					
	Cure	**Delete**	**Block**	**Move to quarantine**	**Report**	**Ignore**
Riskware		+	+	+	+	+/*
Hacktools		+	+	+	+	+/*

Conventions

+	action is enabled for an object of this type
+/*	action is set as default for an object of this type

3.4.2.3. Containers

On this page you can manage settings used by SpIDer Guard for SMB for scanning compound files, such as archives, mail files, packed objects and other containers (i.e. the compound files that are not related to any of the types above).

You can specify the nesting level limit for each of the file types in the corresponding field; when this limit is exceeded, SpIDer Guard for SMB will not unpack a file of such type during scanning. For example, to scan the contents of the archives that are nested in archives, specify the nesting level limit of no 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 the maximum nesting level slows down scanning.

The **Maximum compression ratio** field allows you to specify the maximum compression ratio (as a compressed/uncompressed file ratio) for objects to be scanned. If the compression ratio of an object to be scanned exceeds the specified value, this object will not be scanned.

3.4.2.4. Scanning Paths

On this page you can manage a list of paths to files and directories on the protected station (file server) to be scanned or skipped by SpIDer Guard for SMB while monitoring the file system.

Excluded paths are specified in the **Excluded paths** field (one path per line). Files and directories added to the list of the excluded paths are skipped by the SpIDer Guard for SMB monitor.

The paths to be scanned on the protected station are specified in the **Scanned paths** field (one path per line). The monitor of SpIDer Guard for SMB will control only those files that are added to the scanned paths and are not added to the paths from the **Excluded paths** list.

To add a new path to the relevant list, click ⊞ in the corresponding row of the list. To remove a path from the list, click ⊟ in the corresponding row of the list.

3.4.2.5. Shared Directories

On this page you can manage individual parameters of SpIDer Guard for SMB for scanning files in various Samba shared directories.

Each shared directory, for the scanning of which individual settings must be applied, is identified with a unique tag specified in Samba server settings. To associate individual scanning settings with a certain directory, specify its tag in the **Shared directory tag** field.

To add individual scanning settings for a new shared directory, click ⊞ in the list of shared directories. To remove individual scanning settings for a shared directory, click ⊟ in the corresponding row of the list of shared directories.

> Common scanning settings are applied to those shared directories that do not have individual scanning settings. The common settings are provided on pages **Actions**, **Containers** and **Scanning paths**.

In the tagged shared directory section you can specify values of scanning parameters individual for such directory. To do that, select a required parameter in the **Shared directory settings** field from a drop-down list, then specify the value of this parameter in the **Settings parameter** field.

To add a new individual scanning parameter to the list, click ⊞ in the corresponding shared directory section. To remove an individual parameter from the list, click ⊟ in the corresponding row of the list of parameters in the shared directory section.

3.4.2.6. Advanced Settings

On this page you can manage advanced SpIDer Guard for SMB settings on the protected station (file server).

The following advanced SpIDer Guard for SMB settings are available:

- **Virtual root directory**—a path to a file system directory used by the Samba server as a virtual root directory (can be redefined using the `chroot` command). Used as a prefix inserted at the beginning of all paths used by the Samba server, including paths to files and directories located in shared directories, and describes a path to them relative to the root of the local file system. If this path is not specified, the path to the file system root (`/`) is used.
- **Path to the socket file**—a path to the socket file which enables interaction with VFS SMB modules. This path is always relative and supplements the path to the virtual root directory.
- **Log level**—a log verbosity level used for SpIDer Guard for SMB message logging.

- **Logging method**—a logging method for SpIDer Guard for SMB. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for SpIDer Guard for SMB message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from SpIDer Guard for SMB.
  - *Path*—use a separate file to store SpIDer Guard for SMB log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.3. SpIDer Guard for NSS Settings

3.4.3.1. General Settings

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

- **Run the component at the start**—enable or disable SpIDer Guard for NSS on the protected station at startup.
- **Use heuristic analysis**—define how SpIDer Guard for NSS uses the heuristic analysis on the protected station while scanning files “on-the-fly”. The heuristic analysis slows down scanning, but improves its reliability.
- **Scanning time of one element**—set a time limit for scanning one file by SpIDer Guard for NSS on the station. If the value is set to *0*, the time period for scanning one file is unlimited.

> SpIDer Guard for NSS operates only in the Novell Open Enterprise Server SP2 environment on SUSE Linux Enterprise Server 10 SP3 or later.

3.4.3.2. Actions

On this page you can manage anti-virus protection parameters to be used by SpIDer Guard for NSS for scanning files on a protected NSS volume.

SpIDer Guard for NSS can react to the following threats:

- **Infected**—the scanned file contains a known threat;
- **Suspicious**—the scanned file has been marked as *suspicious*;
- **Incurable**—the scanned file contains a threat that cannot be neutralized with the Cure action;
- **Adware**—the scanned file contains adware;
- **Dialers**—the scanned file contains a dialer;
- **Jokes**—the scanned file contains a joke program;
- **Riskware**—the scanned file contains riskware;

- **Hacktools**—the scanned file contains a hacktool.

Available actions:

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

  This action is available only for objects infected with a known virus that can be cured except for trojans and files within compound objects.
- **Delete**—delete the object that poses a threat.

  This is the most effective way to remove all types of threats.
- **Move to quarantine**—move a detected threat to a special directory isolated from the rest of the system.
- **Report**—notify of a threat without performing other actions.

Default settings are optimal in most cases. Do not change them unless necessary.

Table 3. Actions applied to threats detected by SpIDer Guard for NSS

Object	Action			
	Cure	Delete	Move to quarantine	Report
Infected	+/*	+	+	
Suspicious		+	+/*	+
Incurable		+	+/*	
Adware		+	+	+/*
Dialers		+	+	+/*
Jokes		+	+	+/*
Riskware		+	+	+/*
Hacktools		+	+	+/*

Conventions

+	action is enabled for an object of this type
+/*	action is set as default for an object of this type

3.4.3.3. Containers

On this page you can manage settings used by SpIDer Guard for NSS for scanning compound files, such as archives, mail files, packed objects and other containers (i.e. the compound files that are not related to any of the types above).

You can specify the nesting level limit for each of the file types in the corresponding field; when this limit is exceeded, SpIDer Guard for NSS will not unpack a file of such type during scanning. For example, to scan the contents of the archives that are nested in archives, specify the nesting level limit of no 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 the maximum nesting level slows down scanning.

The **Maximum compression ratio** field allows you to specify the maximum compression ratio (as a compressed/uncompressed file ratio) for objects to be scanned. If the compression ratio of an object to be scanned exceeds the specified value, this object will not be scanned.

3.4.3.4. Scanning Paths

On this page you can manage a list of paths to files and directories on the protected station (file server) to be scanned or skipped by SpIDer Guard for NSS while monitoring the NSS protected volume.

Excluded paths are specified in the **Excluded paths** field (one path per line). Files and directories added to the list of the excluded paths are skipped by the SpIDer Guard for NSS monitor.

The paths to be scanned on the protected volume are specified in the **Scanned paths** field (one path per line). The monitor of SpIDer Guard for NSS will control only those files that are added to the scanned paths and are not added to the paths from the **Excluded paths** list.

To add a new path to the relevant list, click ⊞ in the corresponding row of the list. To remove a path from the list, click ⊟ in the corresponding row of the list.

3.4.3.5. Advanced Settings

On this page you can manage advanced SpIDer Guard for NSS settings on the protected station (file server).

The following advanced SpIDer Guard for NSS settings are available:

- **NSS volumes mounting point**—a path to a file system directory of a file server where protected NSS volumes are mounted.

- **Protected NSS volumes**—a list of names of NSS volumes mounted on a mounting point provided in the parameter above and stated for protection by SpIDer Guard for NSS. If no value is specified for this parameter, all NSS volumes at the mounting point will be protected.

  To add a new volume to the list, click ➕. To remove a volume from the list, click ➖ in the corresponding row of the list.
- **Log level**—a log verbosity level used for SpIDer Guard for NSS message logging.
- **Logging method**—a logging method for SpIDer Guard for NSS. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for SpIDer Guard for NSS message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from SpIDer Guard for NSS.
  - *Path*—use a separate file to store SpIDer Guard for NSS log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.4. Dr.Web Agent for Unix Settings

3.4.4.1. General Settings

On this page you can manage the following settings of the auxiliary component Dr.Web Agent for Unix on the protected station:

- **Collect information about stations**—allow or do not allow Dr.Web Agent for Unix to collect statistics about stations.
- **Period of collecting information about stations**—specify the frequency (in minutes) with which Dr.Web Agent for Unix should send requests to stations to collect information.
- **Statistics sending period**—set the frequency with which Dr.Web Agent for Unix should send statistics to the server.
- **Mobile mode for updates**—set up the mobile mode for updates. The following values are allowed:
  - *Auto*—use the mobile mode, if allowed by the administrator of the Dr.Web Enterprise Security Suite server (fetch updates either from GUS servers by using a local updating component installed on the station, or fetch updates from Dr.Web Enterprise Security Suite, depending on which connection is available and which the quality of which connection is better).
  - *Enable*—use the mobile mode, if allowed by the administrator of the Dr.Web Enterprise Security Suite server (fetch updates from GUS servers using a local updating component installed on the station).
  - *Disable*—do not allow Dr.Web Server Security Suite installed on the station to fetch updates from GUS servers in case of a failure to connect to the Dr.Web Enterprise Security Suite server.

- **Process discovery requests**—select the check box to allow the agent to receive discovery requests (used to check the structure and state of the anti-virus network) from the Dr.Web Enterprise Security Suite server.
- **Log level**—a log verbosity level used for Dr.Web Agent for Unix message logging.
- **Logging method**—a logging method for Dr.Web Agent for Unix. The following values are allowed:
    - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
    - *Syslog*—use the syslog system service for Dr.Web Agent for Unix message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Dr.Web Agent for Unix.
    - *Path*—use a separate file to store Dr.Web Agent for Unix log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

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

3.4.4.2. Configuration

On this page you can specify settings for any of the Dr.Web Server Security Suite components installed on the station (an `.ini` configuration file format is used). For that, introduce required changes to the **drweb.ini configuration file** field.

Note that:

- The Control Center does not support configuring all existing parameters. To configure Dr.Web Agent for Unix components in depth, use the Dr.Web Server Security Suite configuration editor.
- The settings editor shows only those configuration parameters the values of which have been changed on this page.
- The values of the configuration parameters specified in the editor take precedence over the values specified by component configuration pages: if a value of some parameter is specified on a configuration page and a different value is specified on the **Configuration** page, the value specified on the **Configuration** page will be used for the station. Moreover, undefined configuration parameters take default values for components which sections are provided in the **drweb.ini configuration file** editor.
- The configuration editor supports context help: to show a drop-down list of available parameters (or parameter sections, depending on the context), press CTRL+SPACE.
- You can import and export editor contents as an `.ini` configuration file. To do that, click the corresponding button on the page above the configuration editor.

> ! For the complete list of components on the station that are available for configuration, and

for description of their parameters provided in the `drweb.ini` configuration file, refer to the User manual or the Administrator manual for the product installed on the station.

3.4.5. File Checker Settings

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

The following settings are available:

- **Maximum checked file cache size**—a size of the cache used by File Checker to temporarily store file scan results.
- **Cache validity period**—a time period during which File Checker does not rescan files, if scan results are already available in the cache.
- **Log level**—a log verbosity level used for File Checker message logging.
- **Logging method**—a logging method for File Checker. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for File Checker message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from File Checker.
  - *Path*—use a separate file to store File Checker log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

Moreover, you can choose which additional data will be stored in the log at the *Debug* verbosity level.

- **IPC**—log all inter-process communication (IPC) messages on component interaction.
- **File scanning**—log info about file scans.
- **SpIDer Guard file monitoring**—log SpIDer Guard scan requests.
- **Checked file cache status**—log status information about the cache for scanned files.

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

3.4.6. Scanning Engine Settings

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

The following settings are available:

- **Path to the socket file of the fixed copy of the component**—a path to a Unix socket file of a resident Scanning Engine instance. This socket can be used to scan files by external programs. If the parameter is empty, scanning files is unavailable to external programs, and Scanning Engine runs and terminates automatically, when necessary.
- **Number of scanning processes**—a number of child scanning processes that can be created by Scanning Engine while scanning files. When changing the value of this parameter, take into account the number of CPU cores available on the station.
- **Watchdog timer**—a time period used by Scanning Engine to automatically detect a hang-up of child scanning processes.
- **Log level**—a log verbosity level used for Scanning Engine message logging.
- **Logging method**—a logging method for Scanning Engine. The following values are allowed:
  - *Auto*—use logging parameters defined for all components in Dr.Web ConfigD settings.
  - *Syslog*—use the syslog system service for Scanning Engine message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Scanning Engine.
  - *Path*—use a separate file to store Scanning Engine log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

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

3.4.7. Dr.Web ConfigD Settings

On this page you can manage parameters that are used by the Dr.Web ConfigD auxiliary management component during its operation on the protected station.

The following settings are available:

- **Public communication socket path**—a path to a Unix socket used by Dr.Web Server Security Suite components for interaction with Dr.Web ConfigD.
- **Administrative communication socket path**—a path to a Unix socket used by Dr.Web Server Security Suite components operating with superuser privileges for interaction with Dr.Web ConfigD.
- **Temporary files directory**—a path to a directory with temporary files stored by Dr.Web Server Security Suite components.

- **Path to the directory with PID files and communication sockets**—a path to a directory with PID files and Unix sockets that are used for internal interaction of Dr.Web Server Security Suite components.
- **Log level**—a log verbosity level used for Dr.Web ConfigD message logging.
- **Logging method**—a logging method for Dr.Web ConfigD. The following values are allowed:
    - *Syslog*—use the syslog system service for Dr.Web ConfigD message logging. If you choose this method, you must also specify a value of the **Syslog facility** parameter in the drop-down list. This parameter defines a subsystem (label) to be used by syslog to store messages from Dr.Web ConfigD.
    - *Path*—use a separate file to store Dr.Web ConfigD log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

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

4. Appendix A. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

1. Download and review the latest manuals and guides at https://download.drweb.com/doc/.
2. See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
3. Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

1. Fill out a web form in the appropriate section at https://support.drweb.com/.
2. Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.