



Dr.WEB

Enterprise Security Suite

Managing UNIX Internet Gateways



© **Doctor Web, 2024. All rights reserved**

This document is intended for information and reference purposes regarding the Dr.Web software discussed herein. This document is not a basis for exhaustive conclusions about the presence or absence of any functional and/or technical features in Dr.Web software and cannot be used to determine whether Dr.Web software meets any requirements, technical specifications and/or parameters, and other third-party documents.

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

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 Internet Gateways
Version 13.0
Administrator Manual
7/11/2024

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	5
1.1. About This Manual	5
1.2. Conventions and Abbreviations	6
2. Dr.Web Enterprise Security Suite	8
2.1. About This Product	8
2.2. Protection of Linux Workstations	9
3. Dr.Web for UNIX Internet Gateways	11
3.1. Dr.Web for UNIX Internet Gateways Functions	11
3.2. Dr.Web for UNIX Internet Gateways Components	12
3.3. Dr.Web for UNIX Internet Gateways Operation Modes	13
3.4. Dr.Web for UNIX Internet Gateways Configuration	17
3.4.1. Dr.Web Agent for UNIX Settings	18
3.4.2. Dr.Web ICAPD Settings	19
3.4.3. SpIDer Gate Settings	23
3.4.4. File Checker Settings	25
3.4.5. Scanning Engine Settings	25
3.4.6. Dr.Web ConfigD Settings	26
4. Appendix A. Rules for Traffic Monitoring	28
5. Appendix B. Technical Support	50



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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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.
<i>Anti-virus network</i>	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:

- BRE—Basic Regular Expressions,
- CSV—Comma-Separated Values,
- ERE—Extended Regular Expressions,
- GUS—Dr.Web Global Update System,
- 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,
- OS—Operating System,
- PCRE—Perl Compatible Regular Expressions,



- PDF—Portable Document Format,
- SNI—Server Name Indication,
- SSL—Secure Socket Layers,
- TCP—Transmission Control Protocol,
- TLS—Transport Layer Security,
- URL—Uniform Resource Locator,
- 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*.

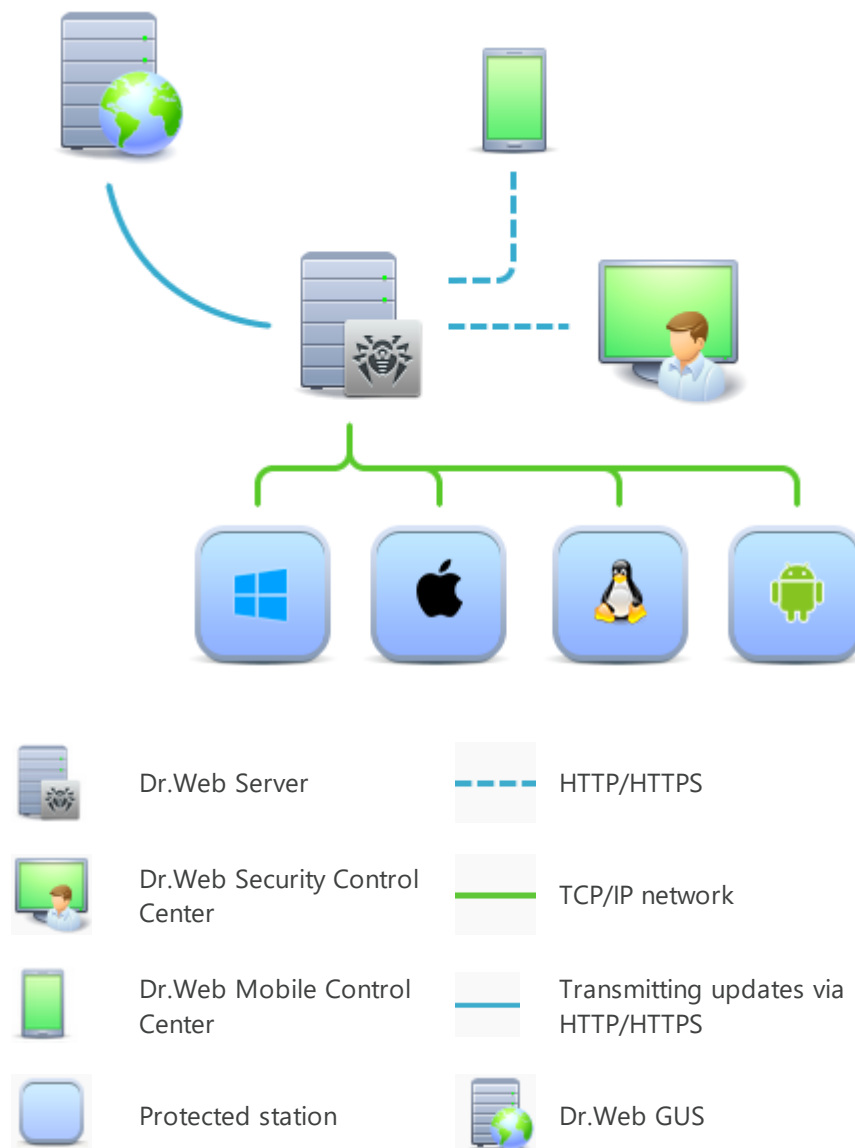


Figure 1. The logical structure of the anti-virus network

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 Linux Workstations

Protection of UNIX Internet Gateways 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 for UNIX Internet Gateways

3.1. Dr.Web for UNIX Internet Gateways Functions

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

Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways:

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. **Analyzing data transmitted to the internet.** Not only user requests are monitored (i.e. attempts to connect to a web server and upload a file to it), but also data sent by web servers in response to user requests. To analyze requests and return data, the program connects via the ICAP protocol as an external filter to a proxy server processing HTTP connections of local network users. Moreover, using the SpIDer Gate component, it is possible to utilize barrier functions that prevent receiving and sending infected files by a public web server of the organization (*this option is available only for GNU/Linux*). To restrict access to unwanted websites, the product uses an automatically updated database of web resources separated into categories, which is bundled with Dr.Web for UNIX Internet



Gateways, and white and black lists created by the system administrator manually. The product also makes a request to the Dr.Web Cloud service to check whether an internet resource is marked as malicious by other Dr.Web products.

3.2. Dr.Web for UNIX Internet Gateways Components

For the protection of UNIX Internet Gateways, the following components are provided:

General

Dr.Web ICAPD

An ICAP server analysing requests and traffic which goes via HTTP proxy servers (such as Squid). It prevents transmitting infected files and accessing network hosts covered by the unwanted web resource categories or black lists created by the system administrator. If access to external servers must be forbidden, or transmitted data contains a threat, the component instructs the proxy server to return to the user a special page informing of that it is impossible to access the requested resource or download an infected file.

A core component of Dr.Web for UNIX Internet Gateways. Allows to integrate it with applications using the ICAP protocol (usually this is a protected HTTP proxy server which provides access to the internet for workstations over LAN).

SpIDer Gate

A component for scanning network traffic and URLs. It is designed for scanning for threats all data downloaded to a local host from the network and sent from it to an external network. The component prevents from connecting to network hosts covered by the unwanted categories of web resources and black lists created by the system administrator.



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 for UNIX Internet Gateways for anti-virus scanning.

Auxiliary

Dr.Web Agent for UNIX

An auxiliary component. Used for interaction of Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways with external monitoring systems via the SNMP protocol.

Dr.Web ConfigD

Coordinates operation of all Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways components. Provides the management web interface.

3.3. Dr.Web for UNIX Internet Gateways Operation Modes

The Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways), which ensure anti-virus protection and maintain connection to the centralized protection server.

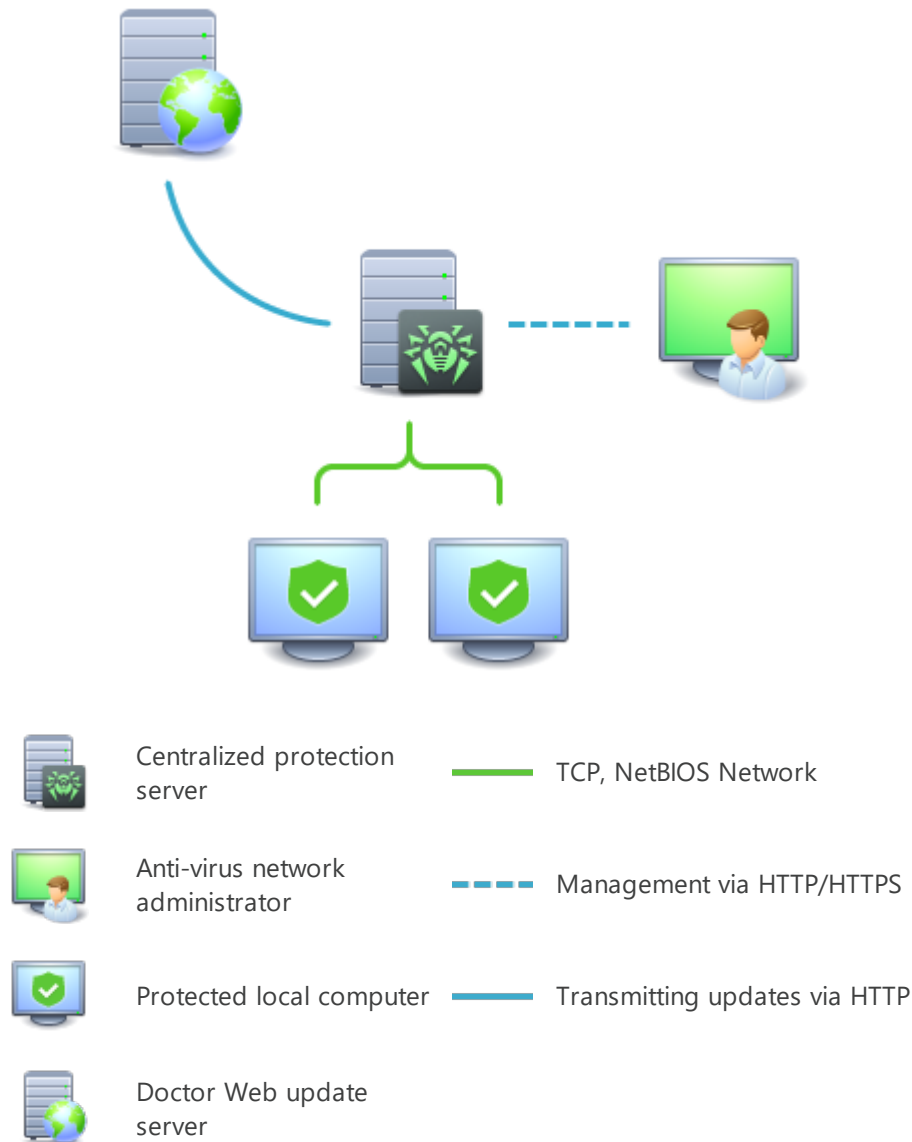


Figure 2. The logical structure of the anti-virus network

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 Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways.

If Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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. Dr.Web Agent for UNIX Settings

3.4.1.1. 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 for UNIX Internet Gateways 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.



3.4.1.2. Configuration

On this page you can specify settings for any of the Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways 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.

3.4.2. Dr.Web ICAPD Settings

3.4.2.1. General Settings

On this page you can manage the following advanced parameters of Dr.Web ICAPD operation on the protected station (internet gateway):

- **Run the component at the start**—select the check box to run the component on the protected internet gateway.
- **Socket for client connections**—a network socket (`<IP address>:<port>`) to be used by ICAP clients (such as Squid) to connect to Dr.Web ICAPD.
- **User**—the name of a UNIX-like OS user with whose rights and privileges the component is run on the protected internet gateway.



If the user name is not specified, the component terminates with an error instantly after an attempt to run it.

- **Log level**—a log verbosity level used for Dr.Web ICAPD message logging.
- **Logging method**—a logging method for Dr.Web ICAPD. 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 ICAPD 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 ICAPD.
 - *Path*—use a separate file to store Dr.Web ICAPD log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.

3.4.2.2. Web Filtering



On this page you can manage internet access check options of Dr.Web ICAPD on the protected internet gateway:

- Select the **Block infection sources** check box to block access to websites distributing viruses and other malicious software.
- Select the **Block non-recommended websites** check box to block access to websites that use social engineering techniques to misguide users.
- Select the **Block URLs listed due to a notice from copyright owner** check box to block access to websites due to a notice from copyright owners who have discovered a violation of their rights to intellectual property on the internet.
- To block access to websites from some category of web resources, select the corresponding check boxes carrying names of the categories to be blocked (**Block websites with adult content**, **Block violent websites**, etc.).
- In the **List of advertisement websites** area specify a list of regular expressions to cover URLs associated with advertisement websites. User attempts to follow a URL that matches any expression from the list will be blocked.



Actual usage of the expressions from the list indicated in this parameter depends on the *method* of its usage in the rules for managing access to web sources defined for Dr.Web ICAPD.

The list of default rules guarantees that access to a URL that matches any expressions from this list will always be blocked.

To add a new expression to the list, click  in the corresponding row of the list. To remove an expression from the list, click  in the corresponding row of the list.



3.4.2.3. Exceptions

On this page you can manage exceptions to be made on the protected internet gateway by Dr.Web ICAPD for websites:

- In the section **White list of domains, connections to which are allowed by administrator** specify a list of domains to which the users are allowed to connect, even if these domains are covered by the blocked categories. In addition, users will be allowed to access all sub-domains of the domains indicated in this list.



Actual usage of the domain list indicated in this parameter depends on the *method* of its usage in the management rules of access to web sources defined for Dr.Web ICAPD.



The list of default rules guarantees that access to domains (and their sub-domains) from this list will be granted even if it contains domains from the list of the blocked web source categories. Moreover, this default set of rules guarantees that data downloaded from whitelisted domains *will be checked for threats*.

- In the section **Black list of domains, connections to which are prohibited by administrator** specify a list of domains to which the users are not allowed to connect, even if these domains are not covered by the blocked categories. In addition, users will not be allowed to access all sub-domains of the domains indicated in this list.



Actual usage of the domain list indicated in this parameter depends on the *method* of its usage in the management rules of access to web sources defined for Dr.Web ICAPD.

The list of default rules guarantees that access to domains (and their sub-domains) from this list will be always forbidden. If this domain is simultaneously added to the white and black lists, the default rules guarantee that user access to it will be *blocked*.

To add a new domain to the required list, click  in the corresponding row of the list. To remove a domain from a list, click  in the corresponding row of the list.

3.4.2.4. File Filtering

On this page you can manage options of Dr.Web ICAPD on the protected internet gateway for scanning files and data downloaded from the internet:

- In the **Block files** area, specify types of received unsafe objects to be blocked by Dr.Web ICAPD:
 - **Infected**—the scanned file contains a known virus;
 - **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;
- **Unchecked files**—the file cannot be scanned.
- **Use heuristic analysis**—define how Dr.Web ICAPD uses the heuristic analysis on the protected internet gateway 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 a file by Dr.Web ICAPD on the protected internet gateway. If the value is 0, scan time is not limited.
- In the **Maximum nesting level** area, you can specify settings used by Dr.Web ICAPD for scanning compound files such as archives, mail files, packed objects and other containers (i.e. 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, Dr.Web ICAPD 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 nesting level limit 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 a file being scanned exceeds the specified value, the file will not be scanned.

3.4.2.5. Advanced Settings

On this page you can manage the following advanced parameters of Dr.Web ICAPD operation on the protected station (internet gateway):

- **Use ICAP preview** preview—select the check box to instruct Dr.Web ICAPD to use the ICAP preview mode.
- **Use ICAP 204**—select the check box to allow Dr.Web ICAPD to return response code 204 not only in the ICAP preview mode.
- **Use “early” ICAP** responses—select the check box to allow Dr.Web ICAPD to use the ICAP early response mode, i.e. start sending a response to the client before the entire request has been received from the HTTP proxy server.





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



3.4.2.6. Rules for Traffic Monitoring

On this page you can manage rules for scanning websites and data by Dr.Web ICAPD on the protected internet gateway.

To add a new rule to the list, click  in the corresponding row of the list. To remove a rule from the list, click  in the corresponding row of the list.

For more information about the rules for traffic monitoring, see [Appendix A. Rules for Traffic Monitoring](#).



The rules for traffic monitoring are provided in a shortened form in this document. For the full version, refer to the Administrator Manual for Dr.Web for UNIX Internet Gateways.

3.4.3. SpIDer Gate Settings

3.4.3.1. General Settings

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

- **Run SpIDer Gate**—enable or disable SpIDer Gate on the protected station.
- **Use heuristic analysis**—define how SpIDer Gate uses the heuristic analysis on the protected station to detect unknown threats. The use of 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.

3.4.3.2. Actions

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

- Set the **Scan received files** check box to enable scanning incoming internet traffic (in particular, files downloaded from the internet).
- In the **Block files** and **Additionally block** sections, select types of incoming malicious objects to be blocked by SpIDer Gate.

3.4.3.3. Web Filtering

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

- Select the **Scan URL** check box to block internet resources by categories.



- Select the **Block non-recommended websites** check box to block access to websites that use social engineering techniques to misguide users.
- Select the **Block URLs listed due to a notice from copyright owner** check box to block access to websites due to a notice from copyright owners who have discovered a violation of their rights to intellectual property on the internet.
- In the **Block websites from the following categories** section, choose categories of websites to block access to.
- In the **White list/Black list** sections, add paths to websites to be allowed/blocked:
 - To add a certain website, enter its full domain address (for example, `www.example.com`). Access to all resources of this domain will be defined by this string.

3.4.3.4. Containers

On this page you can manage settings used by SpIDer Gate 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 Gate 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.

3.4.3.5. Advanced Settings

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

The following advanced SpIDer Gate settings are available:

- **Log level**—a log verbosity level used for SpIDer Gate message logging.
- **Logging method**—a logging method for SpIDer Gate. 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 Gate 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 Gate.
 - *Path*—use a separate file to store SpIDer Gate log messages. If you choose this method, you must also specify a path to the file in the **Log file** field.



3.4.4. 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.
- **SplDer Guard file monitoring**—log SplDer 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.

3.4.5. 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.

3.4.6. 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 for UNIX Internet Gateways components for interaction with Dr.Web ConfigD.
- **Administrative communication socket path**—a path to a UNIX socket used by Dr.Web for UNIX Internet Gateways 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 for UNIX Internet Gateways 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 for UNIX Internet Gateways 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. Rules for Traffic Monitoring

The rules are represented by such constructions as IF *<condition>* THEN *<action>*. At that, the following tests are specified in the part *<condition>*: “The variable value is (not) set” or “The variable value is (not) included in the specified set”. The part *<action>* contains an ultimate resolution (skip or block traffic), or an action like “Assign the set value to the specified variable” or “Add the set value to the array of values of the specified variable”.

The *<action>* part is executed only if the *<condition>* part evaluates to true. If *<condition>* evaluates to false, the action is not performed, and the program jumps to the next rule. The rules are processed top to bottom until an ultimate resolution is performed. After this, all following rules are ignored.

Rule Format

A rule has the following format:

```
[<condition> [, <condition> [, ...]]] : <action>
```


The conditional part of the rule (before ':') can be absent, in this case the *<action>* part is executed without any condition. If the conditional part of the rule is absent, the ':' separator can be omitted. A comma between conditions in the conditional part performs a role of a conjunction (that is, logical “AND”), and the conditional part evaluates to true only if all its conditions are true. Key words, variable names and configuration parameters are processed case-insensitively in the rules.

Conditions

The following types of conditions can be used in the rules:

Condition	Meaning of the Condition
<i><variable></i> <i><value></i>	The value of the specified variable coincides with the set value. <i>Can be used only for those variables that do not take on a set of values.</i>
<i><variable></i> [not] in <i><set of values></i>	The value of the specified variable is contained in the specified set of values (with “not”—does not match any value from the specified set).
<i><variable></i> [not] match <i><set of values></i>	The value of the specified variable matches any regular expression from the specified set (with “not”—does not match any expression from the specified set).




Condition	Meaning of the Condition
	 <p>Regular expressions are specified using either the <i>POSIX</i> syntax (<i>BRE</i>, <i>ERE</i>) or the <i>Perl</i> syntax (<i>PCRE</i>, <i>PCRE2</i>).</p>
<code><variable> [not] gt <value></code>	<p>The value of the specified variable is (not) greater than the set value.</p> <p><i>Can be used only for those variables that take on a single numerical value.</i></p>
<code><variable> [not] lt <value></code>	<p>The value of the specified variable is (not) less than the set value.</p> <p><i>Can be used only for those variables that take on a single numerical value.</i></p>

*) The optional key word `not` means negation.

The part `<set of values>` to which a variable is compared can be specified in the following ways:

Syntax	Meaning
<code>(<value 1>[, <value 2>[, ...]])</code>	<p>In the parentheses you directly list the set of values to check against (no less than one value). In case there is only one value and the <code>in</code> condition is used, you can omit the parentheses (and you will end up with <code><variable> <value></code>).</p>
<code>"<section> . <parameter>"</code>	<p>The set of values assigned to a certain configuration parameter. The parameter which value (or set of values) is to be checked must be put in quotation marks (the name of the section to which the parameter belongs must also be specified).</p> <p>Lists of parameters that can be used in a condition depend on the component for which the rules are set and are provided below.</p>
<code>file("<file name>")</code>	<p>A list of values is read from a text file <code><file name></code> (one line per a list item, leading and trailing spaces in strings are ignored). A path to the file must be absolute. If the <code><file name></code> contains quotation marks and apostrophes, they must be escaped with a backslash (<code>'\'</code>).</p>



Syntax	Meaning
	<div data-bbox="916 257 1449 1220" style="background-color: #e6f2e6; padding: 10px;"> The file size must not exceed 64 MB. The file contents are read and inserted into the rules once, while loading the configuration file. If the specified file is absent or its size limit is exceeded, error <code>×102</code> will be displayed while loading settings. In case the file contents were changed during the operation of the software suite, in order to apply changes, you should restart Dr.Web for UNIX Internet Gateways after saving the file. The file does not provide a set of values for all variables. For each variable below it is indicated whether you can test its values against a set of values from the file.</div>

If a variable is multiple-valued, the condition `<variable> in <set of values>` is true if the intersection of the set of current values of the specified variable `<variable>` with the indicated set `<set of values>` is not empty. The condition `not in` is true in the opposite case. For example, suppose `X` is a variable which current value is a set with values `a`, `b` and `c`. Then

- `X in (a, b)` is true because values `a` and `b` are present in both sets;
- `X in (a, d, e)` is true because value `a` is present in both sets;
- `X in (d, e)` is false because none of the values of the variable (`a, b, c`) is in the set (`d, e`);
- `X in ()` is false because the set of variable values is not empty;
- `X not in ()` is true, the set of variable values is not empty;
- `X not in (d, e)` is true because none of the values of the variable (`a, b, c`) is in the set (`d, e`);
- `X not in (a, d, e)` is false because value `a` is present in both sets.

For each variable below it is indicated whether it can take on multiple values.



Actions

Actions are separated into *ultimate resolutions* that determine whether to permit passing an object; *modifying resolutions* that do not interrupt testing but determine the action to be applied to a connection or an object being scanned upon the acceptance of a resolution allowing to pass the traffic and *actions that change the values of some variable*, which can be further used when testing conditions.

Ultimate Resolutions

Resolution	Description (Meaning)
General Resolutions	
PASS	Skip traffic (allow connection creation, send the object to the recipient). The following rules (if there are any) are not applied.
BLOCK as <i><reason></i>	<p>Block traffic (deny connection creation, send the object to the recipient). The following rules (if there are any) are not applied.</p> <p>Blocking <i><reason></i> is logged. The same reason is used to define a browser notification to be shown to the user. Two standard reasons can be used as <i><reason></i> for blocking:</p> <ul style="list-style-type: none">• <code>BlackList</code>—the data is blocked because it has been blacklisted by the user.• <code>_match</code>—blocking occurs because a web resource or file containing a threat belongs to the category that triggers rule execution (for conditions <code>*_category in (...)</code>). The <code>_match</code> variable contains a list of blocked categories for which a match has been achieved.
Specific Resolutions for Mail Processing Rules	
REJECT [" <i><description></i> "]	<p>Reject a message (prevent its receiving or sending).</p> <p>While working with data transferred via SMTP protocol, form response code SMTP 541 (class of permanent errors). If an optional parameter <i><description></i> is indicated, it will be used as a response. When scanning an email message received from MTA via the Spamd/Rspamd interface, <i><description></i> will be used as the value of the header <i>Message</i>, which is added to the email after the message with scanning results.</p>
TEMPFAIL [" <i><description></i> "]	<p>Return a "temporary failure" error to the sender.</p> <p>If the data is transmitted via the SMTP protocol, return the response with code SMTP 451 (temporary failure). The <i><description></i> parameter is optional; it is used as the text of the response if it is set.</p>



Resolution	Description (Meaning)
	When scanning a message received from MTA via Spamd/Rspamd interface, <i><description></i> will be used as a value of the <i>Message</i> header added to the message after informing about scanning results.
DISCARD	Discard the message, i.e. accept it without returning the error code to the sender and delete it instead of passing to the recipient.

Modifying Resolutions

The modifying resolutions do not interrupt testing against the rules; they define actions to be applied to the data being tested upon the receipt of the *PASS* resolution.

Resolution	Description (Meaning)
REPACK [<i><reason></i>]	<p>Repack a message, i.e. create (on the basis of a predefined template) a new message including the content of the old one and some text informing the recipient about the threats. The unwanted message is cut and placed in a password-protected archive. The archive is added to the message and sent to the recipient as an attachment. Scanning the message is continued until the <i>PASS</i> resolution is achieved. The following predefined repack templates are available:</p> <ol style="list-style-type: none">1) the message is considered spam;2) the message contains one or more threats;3) the message contains one or more malicious or unwanted URLs;4) violation of the security policies established by the administrator. <p><i><reason></i> is logged as a reason for repacking. The same reason is used to define one of four templates to be used for generating a notification message to the recipient. As a <i><reason></i> for <i>REPACK</i>, the following reasons can be used:</p> <ul style="list-style-type: none">• as <i>_match</i>—the message is repacked because it is considered spam or contains a link to a web resource or a file with a threat covered by the category which triggered the rule (conditions <i>*_category in (...)</i>). The <i>_match</i> variable stores the list of unwanted categories that were matched. Template 1, 2 or 3 is chosen for repacking depending upon what has been detected in the message:• if the message has been considered spam, template 1 is chosen;• if at least one threat has been detected, template 2 is chosen;• if at least one malicious or unwanted URL has been detected, template 3 is chosen;



Resolution	Description (Meaning)
	<ul style="list-style-type: none"> if no threats have been detected, template 4 is chosen; “text message”—the message has been repacked in accordance with the settings defined by the administrator, and the text can contain any message from the administrator. Example: <i>REPACK "Virus found!"</i>. Template 4 is chosen for repacking.
<pre>ADD_HEADER("<Name>", "<Value>")</pre>	<p>Add the header <i><Name></i> with the value <i><Value></i> and continue scanning the message until the <i>PASS</i> resolution is achieved. Example: <i>ADD_HEADER ("X-SPAM", "Virus found!")</i>.</p> <p>The value is converted to ASCII in accordance with RFC 2047.</p>
<pre>CHANGE_HEADER("<Name>", "<Value>" _value [+ "<Value>" _value [+ ...]])</pre>	<p>Change the value of the first detected header titled <i><Name></i>. The new value is the concatenation of values after the comma separated by the + sign. Each value can be represented either by a string literal put in quotation marks or by the specific variable <i>_value</i> which takes on the original value of the header being modified. Scanning the message is continued until the <i>PASS</i> resolution is achieved. Example:</p> <pre>CHANGE_HEADER("Subject", "[SPAM] ' + _value + ' (do not read!)")</pre>

Aspects of processing resolutions:

- BLOCK as *BlackList* is always processed as “*is included in a black list*” (irrespective of the condition specified in the rule with this resolution).
- BLOCK as *_match*, if *match* is not empty, is processed as “*belongs to the _match category(-ies)*”.
- BLOCK as *_match*, if *match* is empty, is processed as “*is included in a black list*” (irrespective of the condition specified in the rule with this resolution).
- If all rules have been run through, and none of the rules with a resolution has been triggered (or the rules do not have resolutions), this is equivalent to applying the *PASS* action.

Changing the value of a variable

To change a variable value, the following instruction is used:

```
SET <variable> = ([<value 1>[, <value 2>[, ...]])
```

If nothing is enclosed in parentheses, the list of variable values is cleared. If there is only one value, the brackets must be omitted, that is, the following syntax must be used:

```
SET <variable> = <value>
```



Variables used in the rules

When indicating variables in the rules, the character case is ignored. Multi-word variables can be named with or without an underscore to separate words. Thus, records `variable_name`, `VariableName`, and `variablename` represent the same variable. In this section, all variables contain the underscore (that is, the `variable_name` spelling variant is used).

General variables

Variable	Description	Can be used in	
		conditional part	action part (SET)
<code>protocol</code>	<p>Network protocol type used by the connection.</p> <p><i>The variable can take on a set of values.</i></p> <p>Allowed values: HTTP, SMTP, IMAP, and POP3.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• The variable value is defined only if SSL/TLS is not used or it was allowed to unwrap SSL.• There is no point in specifying any other value besides HTTP in Dr.Web ICAPD rules—the protocol can be represented only by HTTP.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>protocol in (HTTP, SMTP) protocol in (POP3) protocol in file("/etc/file")</pre>	Yes	No
<code>sni_host</code>	<p>Host SNI (address) to which the connection is established via SSL/TLS.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• If SSL is not used, the variable value is not set, the condition evaluates to false.• There is no point in using it in Dr.Web ICAPD rules (this component does not process SSL, so the condition always evaluates to false).	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<ul style="list-style-type: none">• A set of values for checking a variable value can be read from a file.• You can use this variable together with the <code>proc</code> variable (see below). <p>Examples:</p> <pre>sni_host not in ('vk.com', 'ya.ru') sni_host in "LinuxFirewall.BlackList" sni_host in file("/etc/file")</pre>		
<code>sni_category</code>	<p>The list of categories (<i>AdultContent</i>, and so on) to which the host (identified by SNI) belongs according to databases of web resources; the connection to the host is established via SSL/TLS.</p> <p><i>The variable can take on a set of values.</i></p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• If SSL is not used, the variable value is not set, the condition evaluates to false.• There is no point in using it in Dr.Web ICAPD rules (this component does not process SSL, so the condition always evaluates to false).• For rules used by Dr.Web ICAPD, the condition with <code>not in</code> will be <i>true</i>, even if the host does not belong to any of the predetermined categories ("safe" host) according to the scanning results.• If databases of web resource categories are not installed, the variable must not be used in the rules (an attempt to check if the condition is true in the rule will cause error <code>x112</code>).• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>sni_category not in (AdultContent, Chats) sni_category in "LinuxFirewall.BlockCategory" sni_category in (FreeEmail)</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<code>sni_category not in file("/etc/file")</code>		
<code>url</code>	<p>URL requested by the client. Can be compared with a specified string or a regular expression.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Can be used only in rules for Dr.Web ICAPD.• You can use Dr.Web LookupD to check the value of this variable.• A set of values for checking a variable value can be read from a file.• You can use this variable together with the <code>proc</code> variable (see below). <p>Examples:</p> <pre>url match ("drweb.com", "example\..*", "aaa.ru/") url match "ICAPD.Adlist" url not match LDAP@BadURLs url match file("/etc/file")</pre>	Yes	No
<code>url_host</code>	<p>URL or host to which the connection is established.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• The variable value is defined only if SSL/TLS is not used or it was allowed to unwrap SSL.• You can use Dr.Web LookupD to check the value of this variable.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>url_host in ('vk.com', 'ya.ru') url_host not in "ICAPD.Whitelist" url_host in LDAP@hosts url_host not in file("/etc/file")</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
<code>url_category</code>	<p>The list of categories to which the URL or the host to which the connection is established belongs (based on the database of web resources or the Dr.Web CloudD response).</p> <p><i>The variable can take on a set of values.</i></p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• The variable value is defined only if SSL/TLS is not used or it was allowed to unwrap SSL.• For rules used by Dr.Web ICAPD, the condition with <code>not in</code> will be <i>true</i>, even if the URL or the host does not belong to any of the predetermined categories ("safe" URL or host) according to the scanning results.• If databases of web resource categories are not installed, the variable must not be used in the rules (an attempt to check if the condition is true in the rule will cause error <code>x112</code>).• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>url_category not in (AdultContent, Chats) url_category in "LinuxFirewall.BlockCategory" url_category in (FreeEmail) url_category in file("/etc/file")</pre>	Yes	No
<code>threat_category</code>	<p>The list of categories to which the threat belongs, which is found in the transferred data (according to information from virus databases).</p> <p><i>The variable can take on a set of values.</i></p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• The variable value is defined only if SSL/TLS is not used or it was allowed to unwrap SSL.	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<ul style="list-style-type: none">For rules used by Dr.Web ICAPD, the condition with <code>not in</code> will be <i>true</i>, even if the URL or the host does not belong to any of the predetermined categories ("safe" URL or host) according to the scanning results.A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>threat_category in "LinuxFirewall.BlockThreat" threat_category not in (Joke) threat_category in file("/etc/file")</pre>		
<code>user</code>	<p>The name of the user with whose privileges the process that is sending (or receiving) traffic has been started.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">In Dr.Web ICAPD rules, it is appropriate to use the name of the user who has authenticated on the proxy server (if the proxy server supports authentication). If the proxy server does not support user authentication, the variable has an empty value.You can use Dr.Web LookupD to check the value of this variable.If you need to find out whether a user belongs to a certain user group, use an LDAP or Active Directory data source that returns a list of groups. The request must also comprise the condition of comparing the user group name and the required one (use the following format: <code><type of the LookupD source>@<source of groups>@<required group></code>). Requests to Active Directory (<code>AD@</code>) return only lists of groups, therefore for these requests it is mandatory to use the <code>@<required group></code> part.A set of values for checking a variable value can be read from a file.	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p>Examples:</p> <pre>user in ('user1', 'user2') user in AD@Winusergroups@Admins user in LDAP@AllowedUsers user not in file("/etc/file")</pre>		
src_ip	<p>The IP address of the host establishing the connection.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• You can use Dr.Web LookupD to check the value of this variable.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>src_ip not in (127.0.0.1, 10.20.30.41, 198.126.10.0/24) src_ip in LDAP@AllowedAddresses src_ip not in file("/etc/file")</pre>	Yes	No
proc	<p>The process establishing the connection (the full executable path).</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• There is no point in using it in Dr.Web ICAPD rules (this component does not have any information about processes, so the condition always evaluates to false).• A set of values for checking a variable value can be read from a file.• You can use this variable together with <code>sni_host</code>, <code>url</code>, and <code>dst_address</code> (see below). <p>Examples:</p> <pre>proc in ('/usr/bin/ls') proc not in ('/home/user/myapp', '/bin/bin1') proc in</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<code>"LinuxFirewall.ExcludedProc"</code> <code>proc in file("/etc/file")</code>		
<code>direction</code>	<p>Connection traffic type.</p> <p>Allowed values: <code>request</code> (client request), <code>response</code> (server response).</p> <p><i>This variable cannot take multiple values; conditions of the <code>match</code> and <code>in type</code> cannot be applied.</i></p> <p>Examples:</p> <pre>direction request direction not response</pre>	Yes	No
<code>divert</code>	<p>Connection direction.</p> <p>Allowed values: <code>input</code> (incoming—created or initiated from outside the local host), <code>output</code> (outgoing—created or initiated on the local host).</p> <p><i>This variable cannot take multiple values; conditions of the <code>match</code> and <code>in type</code> cannot be applied.</i></p> <p>Examples:</p> <pre>divert input divert not output</pre>	Yes	No
<code>content_type</code>	<p>MIME type of data transferred during connection.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Can be defined only if SSL/TLS is not used or it was allowed to unwrap SSL.• The expression <code>"*/*"</code> matches data of any MIME type and HTTP responses without the <code>Content-Type</code> header.• You can use Dr.Web LookupD to check the value of this variable.• A set of values for checking a variable value can be read from a file.	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p>Examples:</p> <pre>content_type in ("multipart/byteranges", "application/octet-stream") content_type not in ("text/*", "image/*") content_type not in ("audio/*") content_type in ("*/") content_type in LDAP@BlockedContent content_type not in file("/etc/file")</pre>		
(<i>proc</i> , < <i>variable</i> >)	<p>Network activity of the process, where <i>proc</i> is the full process executable path (see above), and <<i>variable</i>> defines a type of the activity and can take on one of the following values:</p> <ul style="list-style-type: none"> • <i>sni_host</i>—host SNI (address) to which the connection is established via SSL/TLS (see above); • <i>url</i>—URL requested by a client (see above); • <i>dst_address</i>—network address (<<i>IP address</i>>:<<i>port</i>>) at which the process establishes the connection. <p>Usage Aspects:</p> <ul style="list-style-type: none"> • Used only with the condition <code>match ({<Proc_reg>, <Var_reg> [, ...]}, where <Proc_reg> is a regular expression for <i>proc</i>, and <Var_reg> is a regular expression for <<i>variable</i>>.</code> • There is no point in using it in Dr.Web ICAPD rules (this component does not have any information about processes, so the condition always evaluates to false). <p>Examples:</p> <pre>(proc, url) match ({"usr/bin/wget", "www\.\ya\.*"}) (proc, dst_address) match</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<pre>{{"/usr/bin/*.*", "192\.168\.1\.\d+:12345"}}</pre>		
<code>unwrap_ssl</code>	<p>Whether the traffic transferred via SSL/TLS is unwrapped.</p> <p>Allowed values: <code>true</code>, <code>false</code>.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• The variable always has a value, that is, the SET <code>unwrap_ssl = ()</code> instruction is invalid.• The variable cannot be used in conditions and is necessary only to control SSL unwrapping (for example, to display a webpage containing notification about blocking triggered by our side).• There is no point in using it in Dr.Web ICAPD rules (this component does not process SSL, changing the variable value does not influence rule processing). <p>Examples:</p> <pre>SET unwrap_ssl = TRUE set Unwrap_SSL = false</pre>	No	Yes
<code>http_templates_dir</code>	<p>A path to the directory where the notification page template on blocking an HTTP request or response is stored.</p> <p>If the path starts with <code>/</code>, it is an absolute path; if it starts with any other symbol, it is a relative path. In the latter case the root is specified in the <code>TemplatesDir</code> parameter.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Useful only for the HTTP(S) protocol. <p>Examples:</p> <pre>SET http_templates_dir = "/etc/mytemplates" set http_templates_dir = "templates_for_my_site"</pre>	No	Yes



Variables used in mail processing rules

Variable	Description	Can be used in	
		conditional part	action part (SET)
header	<p>The contents of the message header part.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Used for comparison of the header part with the list of specified templates (regular expressions are used).• Any header provided in the message can be checked.• The comparison is case-insensitive; Unicode can be used.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>header match ("subject: sp.m", "From: sales.*@.*") Header not match ("Subject: .*buy.*") header match file("/etc/file")</pre>	Yes	No
body	<p>Text content of the message body</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Used for comparison of the message body with the list of specified templates (regular expressions are used).• Any text part of the message can be checked.• The comparison is case-insensitive; Unicode can be used.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>body match ("e.ternit[y]") body not match file("/etc/file")</pre>	Yes	No
body_part_header	<p>Headers of message body parts (MIME part).</p>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p>Usage Aspects:</p> <ul style="list-style-type: none">• Used for comparison of headers in message body sections with the list of specified templates (regular expressions are used).• Headers of any part of the message body can be checked.• The comparison is case-insensitive; Unicode can be used.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>body_part_header match ('Content-Disposition: attachment; .*filename="virus.exe"') BodyPartHeader not match ("Content-Disposition: attachment; .*") body_part_header match file("/etc/file")</pre>		
attachment_name	<p>Names of files attached to the message</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Used for comparison of names of files (<i>Content-Disposition: attachment</i>) attached to the message with a list of specified templates (regular expressions are used).• The comparison is case-insensitive; Unicode can be used.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>attachment_name match ("\.ex.\$", "\.js\$", "^virus.*") attachment_name not match ("\.txt\$", "\.rtf\$") attachment_name not match file("/etc/file")</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
<code>total_spam_score</code>	<p>The normalized spam score of the message (from 0 to 1) received from Dr.Web ASE.</p> <p>The spam score received from Dr.Web ASE is normalized according to the following rules:</p> <ol style="list-style-type: none">0 or less spam points—0.0;100 points—0.8;1000 and more spam points—1.0. <p>The normalized spam score increases within the specified intervals.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">The variable is numerical, always has one value and can be used only in conditions with <code>lt</code> and <code>gt</code>.If Dr.Web ASE is not installed, messages are not scanned for spam, and the <code>total_spam_score</code> variable cannot be used in rules (an attempt to check if a condition in a rule is true will cause the “<i>Dr.Web ASE is unavailable</i>” error). <p>Examples:</p> <pre>total_spam_score gt 0.32 total_spam_score gt 0.5, total_spam_score lt 0.95</pre>	Yes	No
<code>smtp_mail_from</code>	<p>Address of the sender sent within the SMTP session with the <code>MAIL FROM</code> command.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">Used for comparison of the name of a sender indicated within the SMTP session with a list of specified templates (regular expressions are used).Comparison is case-insensitive.This variable cannot be used in rules of the <i>Spamd</i> interface: this protocol does	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p>not provide information about the message sender.</p> <ul style="list-style-type: none">• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>smtp_mail_from match ("^john@.*", ".*@domain.com\$") smtp_mail_from not match ("^user@domain.com\$") smtp_mail_from match file("/etc/file")</pre>		
smtp_rcpt_to	<p>List of addresses of the message recipients sent within the SMTP session with the RCPT TO command.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">• Used for comparison of recipient names indicated within the SMTP session with a list of specified templates (regular expressions are used).• Comparison is case-insensitive.• This variable cannot be used in rules of the <i>Spamd</i> interface: this protocol does not provide information about the message recipient.• If there is <i>all</i> before <i>match</i>, the condition with this variable will be true only in case <i>all values from the list match</i> the indicated templates.• A set of values for checking a variable value can be read from a file. <p>Examples:</p> <pre>smtp_rcpt_to match ("^user1@domain.com\$", ".*@domain2.com\$") smtp_rcpt_to all match ("^john@.*", ".*@domain.com\$") smtp_rcpt_to match file("/etc/file")</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
maild_templates_dir	<p>A path to the template used for repacking messages.</p> <p>If the path starts with /, it is an absolute path; if it starts with any other symbol, it is a relative path. In the latter case the root is specified in the <code>TemplatesDir</code> parameter.</p> <p>Usage Aspects:</p> <ul style="list-style-type: none">Useful only for mail protocols (<i>POP3</i>, <i>IMAP</i>, and <i>SMTP</i>) and MTA interfaces (<i>Milter</i>, <i>Spamd</i>, and <i>Rspamd</i>). <p>Examples:</p> <pre>SET maild_templates_dir = "/etc/my_mail_templates" set MaildTemplatesDir = "templates_for_my_MTA"</pre>	No	Yes

Categories of unwanted websites and threats

1. Categories of unwanted websites (for `sni_category` and `url_category` variables)

Convention	Website category
<i>InfectionSource</i>	Websites containing malicious software ("infection sources").
<i>NotRecommended</i>	Fraudulent websites (that use "social engineering") visiting which is not recommended.
<i>AdultContent</i>	Websites that contain pornographic or erotic materials, dating sites, and so on.
<i>Violence</i>	Websites that encourage violence or contain materials about various fatal accidents, and so on.
<i>Weapons</i>	Websites that describe weapons and explosives or provide information on their manufacturing, and so on.
<i>Gambling</i>	Websites that provide access to gambling, online casinos, auctions, including sites for placing bets, and so on.
<i>Drugs</i>	Websites that promote use, production or distribution of drugs, and so on.



Convention	Website category
<i>ObsceneLanguage</i>	Websites that contain the obscene language (in section titles, articles, and so on).
<i>Chats</i>	Websites that offer a real-time exchange of text messages.
<i>Terrorism</i>	Websites that contain aggressive and propaganda materials or description of terrorist attacks, and so on.
<i>FreeEmail</i>	Websites that offer the possibility of free registration of an email box.
<i>SocialNetworks</i>	Various social networking services: general, professional, corporate, interest-based; special dating websites.
<i>DueToCopyrightNotice</i>	Websites, links to which are defined by copyright holders of some copyrighted work (movies, music, and so on).
<i>OnlineGames</i>	Websites that provide access to games using the permanent internet connection.
<i>Anonymizers</i>	Websites that allow the user to hide personal information and providing access to blocked websites.
<i>CryptocurrencyMiningPool</i>	Websites that provide access to common services for cryptocurrency mining.
<i>Jobs</i>	Job search websites.

The names of the parameters that control blocking (see below) can be used as the values of the `sni_category` and `url_category` variables.

2. Threat categories (for the `threat_category` variable)

Convention	Threat categories
<i>KnownVirus</i>	Known threat (virus).
<i>VirusModification</i>	Modification of the known threat (virus).
<i>UnknownVirus</i>	Unknown threat, suspicious object.
<i>Adware</i>	Adware.
<i>Dialer</i>	Dialer.
<i>Joke</i>	Joke program.
<i>Riskware</i>	Riskware.
<i>Hacktool</i>	Hacktool.



The names of the parameters that control blocking (see below) can be used as the value of the `threat_category` variable.

Configuration parameters that can be used in rule conditions

Parameters used in the Dr.Web ICAPD component rules (indicated with the `ICAPD.` prefix):

Parameter	Description and Usage Example
Whitelist	White list contains a list of domains, access to which is allowed, even if these domains are included in the database of categories. Examples: <pre>url_host not in "ICAPD.Whitelist" : Block as BlackList</pre>
Blacklist	Black list contains a list of domains, access to which is blocked by the user (or the administrator). Examples: <pre>url_host in "ICAPD.Blacklist" : Block as BlackList</pre>
Adlist	Advertisement list. Contains a list of regular expressions that describe advertising websites. The list is defined by the user (or the administrator). Examples: <pre>url match "ICAPD.Adlist" : Block as BlackList</pre>
BlockCategory	"Meta-parameter": its value is a list of names of those web resource categories (<i>Chats</i> , <i>AdultContent</i> , and so on) for which the corresponding <code>Block*</code> parameters in the <code>[ICAPD.]</code> section are set to <code>Yes</code> . Examples: <pre>url_category in "ICAPD.BlockCategory" : Block as _match</pre>
BlockThreat	"Meta-parameter": its value is a list of names of those threat types (<i>KnownVirus</i> , <i>Joke</i> , and so on) for which the corresponding <code>Block*</code> parameters in the <code>[ICAPD.]</code> section are set to <code>Yes</code> . Examples: <pre>threat_category in "ICAPD.BlockThreat" : BLOCK as _match</pre>



5. Appendix B. 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/>.

