



# Dr.WEB

Enterprise Security Suite

## Managing Dr.Web for UNIX Internet Gateways



© Doctor Web, 2021. All rights reserved

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

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

## **Trademarks**

Dr.Web, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA and the Dr.WEB logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

## **Disclaimer**

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

**Dr.Web Enterprise Security Suite. Managing Dr.Web for UNIX Internet Gateways**  
**Version 11.0.2**  
**Administrator Manual**  
**5/28/2021**

Doctor Web Head Office

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

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

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

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

## **Doctor Web**

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

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

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

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

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



# Table of Contents

<b>Chapter 1. Introduction</b>	<b>5</b>
1.1. About Manual	5
1.2. Conventions and Abbreviations	6
<b>Chapter 2. Dr.Web Enterprise Security Suite</b>	<b>8</b>
2.1. About Product	8
2.2. Workstations Protection	9
<b>Chapter 3. Dr.Web for UNIX Internet Gateways</b>	<b>11</b>
3.1. Dr.Web for UNIX Internet Gateways Components	12
3.2. Dr.Web for UNIX Internet Gateways Configuration	14
3.2.1. Dr.Web ICAPD Settings	15
3.2.2. SpIDer Gate Settings	18
3.2.3. Dr.Web Agent for UNIX Settings	21
3.2.4. File Checker Settings	22
3.2.5. Scanning Engine Settings	23
3.2.6. Dr.Web ConfigD Settings	24
<b>Appendix A. Traffic Checking Rules</b>	<b>25</b>
<b>Appendix B. Technical Support</b>	<b>37</b>



## Chapter 1. Introduction

### 1.1. About Manual

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

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

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

To get additional information, please refer the following manuals:

- **Administrator Manual** of Dr.Web for UNIX Internet Gateways anti-virus solution contains the information about configuration of anti-virus software provided on a station directly.
- **Administrator Documentation** of Dr.Web Enterprise Security Suite anti-virus network (includes **Administrator Manual**, **Installation Manual** and **Appendices**) contains the general information on installation and configuration of anti-virus network and, particularly, on operation with Dr.Web Security Control Center.



Before reading these document make sure you have the latest version of the manuals. The manuals are constantly updated and the current version can always be found at the official web site of Doctor Web at <https://download.drweb.com/doc/?lng=en>



## 1.2. Conventions and Abbreviations

### Conventions

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

Convention	Comment
	Important note or instruction.
	Warning about possible errors or important notes to which you should pay special attention.
<i>Anti-virus network</i>	A new term or an accent on a term in descriptions.
<code>&lt;IP-address&gt;</code>	Placeholders.
<b>Save</b>	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
<code>/home/user</code>	Names of files and folders, code examples.
<a href="#">Appendix A</a>	Cross-references on the document chapters or internal hyperlinks to web pages.

### Abbreviations

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

- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- FQDN—Fully Qualified Domain Name,
- FTP—File Transfer Protocol,
- HTML—HyperText Markup Language,
- HTTP—HyperText Transfer Protocol,
- HTTPS—Hypertext Transfer Protocol Secure,
- ICAP—Internet Content Adaptation Protocol,
- IP—Internet Protocol,
- LAN—Local Area Network,
- MIME—Multipurpose Internet Mail Extensions,
- OS—Operating System,
- PC—Personal Computer,



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

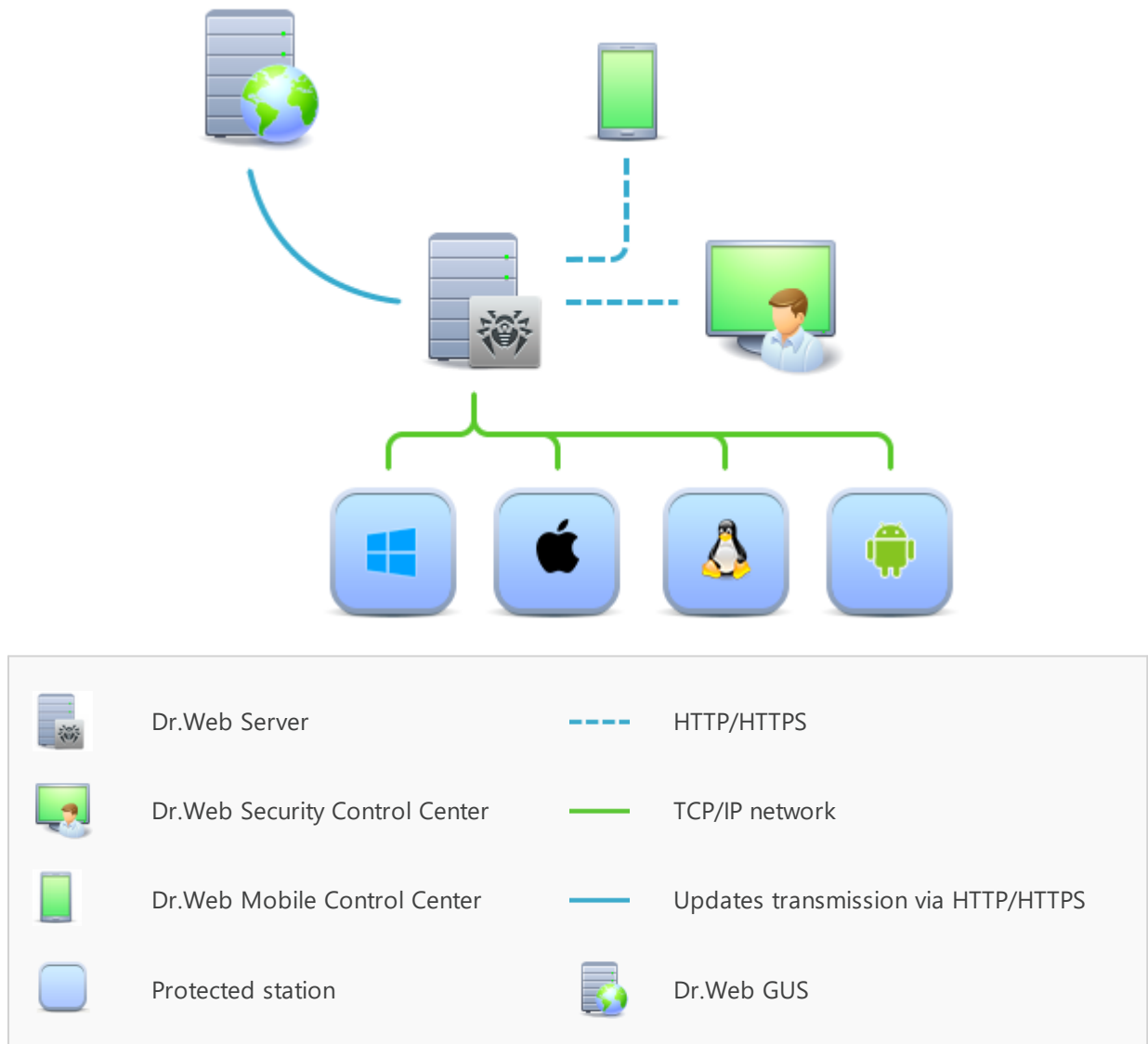


## Chapter 2. Dr.Web Enterprise Security Suite

### 2.1. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either local company network including mobile devices, or home computers of employers.

An aggregate of computers and mobile devices on which Dr.Web Enterprise Security Suite co-operating components are installed, represents a single *anti-virus network*.



#### The logical structure of the anti-virus network

Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on a computers and mobile devices of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information





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

## 2.2. Workstations Protection

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



Protected computer with installed anti-virus package as per its functions in the anti-virus network is called a *workstation* of anti-virus network. Please note: according to its LAN functions, such computer can be both a workstation or mobile device and a LAN server.

Anti-virus packages are installed on protected stations and get connected to Dr.Web Server. Each station is included in one or several groups registered on this Server. Stations and Dr.Web Server communicate through the protocol used in the local network (TCP/IP of 4 or 6 version).

### Installation

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



Detailed description of anti-virus packages installation procedures on workstations you can find in the Dr.Web Enterprise Security Suite **Installation Manual**.

### Management

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

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



## Update

Dr.Web Server downloads updates and distributes them to connected stations. Thus, optimal threats protection is implemented, maintained and adjusted automatically regardless of workstation users' computer skills.

In case an anti-virus station is disconnected from the anti-virus network, anti-virus package on station uses the local copy of the settings and the anti-virus protection on a workstation retains its functionality (up to the expiry of the user's license), but the software is not updated. If a station is allowed to use the *Mobile mode*, after connection with the Server is lost, the virus bases can be updated directly from the Dr.Web GUS.



The principle of stations operation in the Mobile mode is described in the Dr.Web Enterprise Security Suite **Administrator Manual**.



## Chapter 3. Dr.Web for UNIX Internet Gateways

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

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

Dr.Web for UNIX Internet Gateways provides you with the following features:

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

Threat detection methods:

- *Signature analysis*, which allows detection of known threats
- *Heuristic analysis*, which allows detection of threats that are not present in virus databases
- *Dr.Web Cloud* service that collects up-to-date information about recent threats and sends it to Dr.Web products.

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

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

2. **Analyzing data transmitted to the Internet.** Not only user requests are monitored (i.e. attempts to connect to the web server and to transmit any file to it), but also data sent in response to users' request. To analyze requests and sent data, the program connects via ICAP protocol as an external filter to the proxy server, processing HTTP connections of the local network users. Moreover, using the SpIDer Gate component, it is possible to perform barrier functions, which prevents receiving and transmitting infected files by the public server of the organization (*this option is available only for GNU/Linux*). To restrict access to unwanted websites, the product uses automatically updated databases of web resource categories, which are supplied together with Dr.Web for UNIX Internet Gateways; and white and black lists created by the system administrator manually. The product also refers to Dr.Web Cloud service to check for the information whether the Internet resource is marked as malicious by other Dr.Web.



## 3.1. Dr.Web for UNIX Internet Gateways Components

For UNIX Internet gateways protection, the following anti-virus components are provided:

### General Components

#### *Dr.Web ICAPD*

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

Core component of Dr.Web for UNIX Internet Gateways program complex. Allows to integrate it with HTTP/FTP-proxy server using ICAP protocol (usually this is server under protection that provides access to the Internet for LAN workstations).

#### *SpIDer Gate*

The component which works in resident mode and monitors all network connections. Provides protection for a company's public web server.

- It checks whether the requested URL falls into the unwanted category of web resources or in the user's black list, and, if so, blocks access to the resource.
- Also it checks files uploading from the Internet to server under protection and blocks their uploading if they contain threats.

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

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

#### *Dr.Web ClamD*

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

#### *Quarantine*

Isolates malicious and suspicious objects in the special folder.



Files on the workstation can be quarantined by Console Scanner only.

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



## Auxiliary Components

### *Dr.Web Agent for UNIX*

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

### *File Checker*

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

### *Network Checker*

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

### *Scanning Engine*

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

### *SNMP Agent*

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

### *Dr.Web ConfigD*

The component that coordinates operation of all Dr.Web for UNIX Internet Gateways components.

### *Dr.Web CloudD*

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

### *Dr.Web LookupD*

Component retrieving data from external data sources (directory services, such as **Active Directory**) using LDAP protocol. The data are used in rules of traffic monitoring.

### *Dr.Web HTTPD*

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












## 3.2. Dr.Web for UNIX Internet Gateways Configuration

**To view or edit the configuration of the anti-virus components on the workstation:**

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list of the opened window, click the name of a station under required OS (**Linux**, **Solaris** or **FreeBSD**) or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **UNIX** subsection, select the necessary component.
4. A window with the component settings will be opened.

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

- to manage separate parameters, use the options located on the right from corresponding settings:
    -  **Reset to initial value**—restore the value that parameter had before editing (last saved value).
    -  **Reset to default value**—set the default value for a parameter.
  - to manage a set of parameters, use the options located on the toolbar:
    -  **Reset all parameters to initial values**—restore the values that all parameters in this section had before current editing (last saved values).
    -  **Reset all parameters to default values**—restore default values of all parameters in this section.
    -  **Propagate these settings to another object**—copy settings from this section to settings of other station, group or several groups and stations.
    -  **Set inheritance of settings from primary group**—remove personal settings of a station and set inheritance of settings in this section from a primary group.
    -  **Copy settings from primary group and set them as a personal**—copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered as a personal.
    -  **Export settings from this section to the file**—save all settings from this section to a file of a special format.
    -  **Import settings to this section from the file**—replace all settings in this section with settings from the file of a special format.
5. After settings changes were made via the Control Center, click **Save** to accept the changes. The settings will be passed to the stations. If the stations were offline when changes are made, the settings will be passed when stations connect to the Server.



Administrator may forbid editing settings on station for a user (see the **Permissions of Station Users** section in the **Administrator Manual**). At this, only administrator will be able to edit settings via the Control Center.



### 3.2.1. Dr.Web ICAPD Settings

The **Dr.Web ICAPD** page contains the following parameters of Dr.Web for UNIX Internet Gateways operation:

- [General](#)—general parameters of the component.
- [Additional](#)—additional and advanced parameters of the component.
- [Web filtering](#)—settings of URL checking and websites access restriction.
- [Exclusions](#)—settings of exclusions of conditions of URL checking and websites access restriction.
- [File Filter](#)—settings of checking files and data downloaded from the Internet.
- [Traffic Checking Rules](#)—settings of traffic checking rules.

#### 3.2.1.1. General

On this page you can manage the following options of Dr.Web ICAPD on the protected workstation (Internet gateway):

- **Run the component at the start**—set the checkbox to run the component on the protected Internet gateway.
- **Socket for client connections**—determines a network socket (*<IP address>:<port>*) which should be used by ICAP clients (such as **Squid**) for connection to Dr.Web ICAPD.
- **User**—determines under which user name the component should be run (the component takes rights and privileges of specified user).



When a user name is not specified, the component operation terminates with an error after the starting up.

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



### 3.2.1.2. Additional

On this page you can manage the following additional options of Dr.Web ICAPD on the protected workstation (Internet gateway):

- **Use ICAP preview**—set the checkbox to instruct Dr.Web ICAPD to use the ICAP preview mode.
- **Use ICAP 204**—set the checkbox to instruct Dr.Web ICAPD to return the response code 204 not only in the ICAP preview mode.
- **Use “early” ICAP responses**—set the checkbox to instruct Dr.Web ICAPD to use the ICAP’s early response mode, i.e. is allowed to start sending an “early” response to the client before the entire request has been received from the HTTP proxy server.



It is recommended that you do not change default values of these parameters, unless it is necessary.

### 3.2.1.3. Web filtering



On this page you can manage Internet access check options of Dr.Web ICAPD on the protected workstation (Internet gateway):

- Set the **Block infection sources** checkbox to restrict access to websites containing viruses and other malicious software.
- Set the **Block non-recommended websites** checkbox to restrict access to websites that are not recommended for user visiting (these websites use phishing, social engineering and other fraud ways).
- Set the **Block URLs listed due to a notice from copyright owner** checkbox to restrict access to the websites due to a notice from copyright owner who has found out the violation of rights to the intellectual property in the Internet.
- To restrict access to websites from pre-defined category of web-resources set the corresponding checkbox (**Block websites with adult content**, **Block violent websites**, etc.).
- In **List of advertisement websites** section specify a list of regular expressions that detect URLs associated with advertisement websites. Attempts of the users to follow the any URL matched to 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 management rules of access to web sources defined for Dr.Web ICAPD.

The list of default rules guarantees that access to URL matched to any of expressions from this list will be always forbidden.

To add new regular expression to the list, click  near the corresponding list item. To remove some expression from the list, click  near the corresponding list item.





### 3.2.1.4. Exclusions

On this page you can manage exclusions for restriction by Dr.Web ICAPD access to the web-sites:

- **White list of domains, connections to which are allowed by administrator**—in this part, specify the list of domains allowed for connection for users, even if these domains are included into blocked categories. In addition, user access will be allowed to all sub-domains of 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 provided even if it contains domains from the list of blocked web source categories. Besides, this default set of rules guarantees that data downloaded from the white list domains *will be checked for threats*.

- **Black list of domains, connections to which are prohibited by administrator**—in this part, specify the list of domains forbidden for connection for users, even if these domains are not included into blocked categories. In addition, user access will be forbidden to all sub-domains of 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 required list, click  near the corresponding list item. To remove some domain from a list, click  near the corresponding list item.

### 3.2.1.5. File Filter

On this page you can manage options of Dr.Web ICAPD on the protected workstation (Internet gateway) for checking files and data downloaded from the Internet:

- In **Block files** part, specify types of the received unsafe objects that must be blocked by Dr.Web ICAPD.
  - **Infected**—scanned file contains a known virus
  - **Suspicious**—scanned file marked as *suspicious*
  - **Adware**—scanned file contains an adware
  - **Dialers**—scanned file contains a dialer
  - **Jokes**—scanned file contains a joke program



- **Riskware**—scanned file contains a riskware
- **Hacktools**—scanned file contains a hacktool
- **Unchecked files**—the file cannot be scanned.
- **Use heuristic analysis**—instructs Dr.Web ICAPD to use the heuristic analysis on the protected station to detect unknown threats. Note that heuristic analysis may slow down the file system monitoring but improves its reliability.
- **Scanning time of one element**—restrictions on maximal time spent on scanning of one file by Dr.Web ICAPD on the Internet gateway. If the value is 0, scan time is not limited.
- In Maximum nesting level part, you can specify settings which Dr.Web ICAPD is used for checking compound files (containers) of the following types: archives, mail files (email messages, mailboxes), packed objects and other containers (i.e. compound files that are not classified as archives, mail files or packed objects).



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

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

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

### 3.2.1.6. Traffic Checking Rules

On this page you can manage traffic checking rules for Dr.Web ICAPD on the protected workstation (Internet gateway).

To add new rule in the list, click  near the corresponding list item. To delete some rule from the list, click  near the corresponding list item.

For more information about the traffic checking rules see [Appendix A. Traffic Checking Rules](#).

### 3.2.2. SpIDer Gate Settings

The **SpIDer Gate** section consists of the following sections, containing the corresponding parameters of Dr.Web for UNIX Internet Gateways operation:

- [General](#)—general SpIDer Gate settings
- [Actions](#)—actions on detection of threats by SpIDer Gate
- [Web filtering](#)—settings of web traffic check and control of access to Internet resources by SpIDer Gate
- [Containers](#)—settings of scanning of compound files (archives, email files, etc.)



- [Additional](#)—additional SplDer Gate settings.

### 3.2.2.1. General

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

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

### 3.2.2.2. Actions

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

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

### 3.2.2.3. Web filtering

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

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



`ample.test.com`, `test.com/example`, `test.example222.com` and other similar websites will be defined by this string.

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

### 3.2.2.4. Containers

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

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

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

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

### 3.2.2.5. Additional

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

The following advanced SplDer Gate settings are available:

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



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

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

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

#### 3.2.3.1. General

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

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



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



### 3.2.3.2. 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).

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

Please note that:

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



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

### 3.2.4. File Checker Settings

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

The following parameters are available:

- **Maximum checked file cache size**—defines size of the cache that is used by File Checker for temporarily storing the results of files scan.
- **Cache validity period**—defines the duration of a time period when File Checker does not rescans the file, if its scan result is available in the cache.
- **Log level**—defines the log verbosity level that is used for File Checker messages logging.
- **Logging method**—defines the logging method for File Checker. The following values are allowed:



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

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

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



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

### 3.2.5. Scanning Engine Settings

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

The following parameters are available:

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



- *Syslog*—use the **syslog** system service for Scanning Engine messages logging. If you specify this method, you must also specify the value of **Syslog facility** parameter. It defines the label (or subsystem) which is used by **syslog** to save messages from Scanning Engine.
- *Path*—use the specified file to store Scanning Engine log messages. If you specify this method, you must also specify a path to the file in the **Log file** field.



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

### 3.2.6. Dr.Web ConfigD Settings

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

The following parameters are available:

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



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





## Appendix A. Traffic Checking Rules

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

The *<action>* part of the rule is executed, only if the *<condition>* part evaluates to true. If the *<condition>* part evaluates to false, the action is not performed, and the program jumps to the next rule. The rules are considered downwardly until any of the ultimate resolutions is performed. After this, all lower rules are ignored.

### Rule Format

Format of the rule production

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


The conditional part of the rule (before ' : ') can be missing, in this case the *<action>* part is executed without any condition. If the conditional part of the rule is missing, the ' : ' separator can be omitted. The comma between conditions in the conditional part performs a role of a logical conjunction (that is, "and"), and the conditional part elevates to true, only if all its conditions are true. In the rules the register is not important for the key words, names of variables and configuration parameters.

### Conditions

The following types of conditions can be use in the conditional part of the rules:

Condition	Meaning of the Condition
<i>&lt;variable&gt; &lt;value &gt;</i>	The value of the specified variable coincides with the set value.  <i>Can be used only for those variables that can contain a set of values simultaneously.</i>
<i>&lt;variable&gt; [not] in &lt;set of values&gt;</i>	The value of the specified variable is contained in the specified set of values ( <i>for not—does not match any value from the specified set</i> ).
<i>&lt;variable&gt; [not] match &lt;set of values&gt;</i>	The value of the specified variable matches any regular expression listed in the specified set ( <i>for not—does not match any expression from the specified set</i> ).





Condition	Meaning of the Condition
	<div> 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>).</div>
<code>&lt;variable&gt; [not] gt &lt;value&gt;</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 can have a single value.</i></p>
<code>&lt;variable&gt; [not] lt &lt;value&gt;</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 can have a single value.</i></p>

\*) An optional key word `not` means negation.

Part *<set of values>* to which a variable is compared can be specified in the following ways:

Syntax	Meaning
<code>(&lt;value 1&gt;[, &lt;value 2&gt;[, ...]])</code>	<p>In the parentheses you directly list the set of values to check against (not 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 a case <code>&lt;variable&gt; &lt;value&gt;</code>).</p>
<code>"&lt;section&gt;.&lt;parameter&gt;"</code>	<p>The set of values currently assigned to a certain configuration parameter; where between the quotation marks you should specify the name of a configuration parameter whose value (or set of values) must be checked (note that you also need to specify the name of the section to which the parameter belongs).</p> <p>The lists of the parameters that can be used as conditions depend on the component for which the rules are set. The lists are provided below.</p>
<code>file("&lt;file name&gt;")</code>	<p>List of values is read from the text file <code>&lt;file name&gt;</code> (one file string—one list element, leading and trailing spaces in strings are ignored). A path to the file must be absolute. If a <code>&lt;file name&gt;</code> contains quotes and apostrophes, they must be escaped: <code>'\'</code>.</p>



Syntax	Meaning
	<div>The file size must not exceed 64 MB.</div> <div>The file contents are read and inserted into the rules once, during Dr.Web for UNIX Internet Gateways is starting up. If there is no file or the file size is exceeded, an error x102 appears.</div> <div>In case the file contents are changed during the process, in order to apply all changes, you should restart Dr.Web for UNIX Internet Gateways after the changes are saved.</div> <div>A set of values from the file is not available for all variables. Whether you can use a variable to scan its value by using a set of values from the file is indicated below.</div>
<code>&lt;type_of_LOOKUP_request&gt;@&lt;tag&gt;[@&lt;value&gt;]</code>	<p>A set of values is requested via Dr.Web LookupD from an external data source (LDAP, ActiveDirectory), where <code>&lt;LOOKUP_request_type&gt;</code> is the type of the data source used (LDAP or AD); <code>&lt;tag&gt;</code> is a section name describing the connection that is used to sample the data, and <code>&lt;value&gt;</code> (optional) is a value that must be contained in the set of values retrieved from the data source.</p> <div>Values from Dr.Web LookupD are not available for all variables. Also, the condition <code>&lt;scanning&gt;</code> cannot be applied to all variables. Whether you can use a variable to scan its value by using Dr.Web LookupD is indicated below.</div>



## Actions

The actions can be divided into *ultimate* resolutions, defining whether the traffic is blocked or allowed and *actions that change the value of a variable*, which can be used to check the downward conditions.

### Ultimate Resolutions

Resolution	Description (Meaning)
<b>Common Resolutions</b>	
PASS	<p>Skip traffic (allow creating connection). The downward rules (if there are any) are ignored.</p> <p>For the rules of mail processing, there is merit in a command that allows a message to be transmitted to a recipient after all collected changes have been applied to it (i. e. all executed actions <code>REPACK</code>, <code>ADD_HEADER</code>, <code>CHANGE_HEADER</code>, see below).</p>
BLOCK as <i>&lt;reason&gt;</i>	<p>Block traffic (block creating connection). The downwards rules (if there are any) are ignored.</p> <p>A blocking <i>&lt;reason&gt;</i> is recorded in the log. The same reason is used to define a browser notification to be shown to a user. Two standard reasons can be used as <i>&lt;reason&gt;</i> for BLOCK:</p> <ul style="list-style-type: none"><li>• <code>BlackList</code>—the data is blocked because it is included in user's black list.</li><li>• <code>_match</code>—the block happens because a web resource or file containing threat belongs to a category that triggers rule executing (for conditions <code>*_category in (...)</code>). The <code>_match</code> variable contains the list of blocked <a href="#">categories</a> for which the correspondence has been executed.</li></ul>

Aspects of resolution processing:

- BLOCK as `BlackList`, always processes as *"is included in a black list"* (without considering the condition specified in the rules with this resolution).
- BLOCK as `_match`, if `_match` is not empty, processes as *"belongs to the \_match category"*.
- BLOCK as `_match`, if `_match` is empty, processes as *"is included in a black list"* (without considering the condition specified in the rules with this resolution).
- If all rules have been considered, and none of the rules with resolutions performs (or the rules do not have resolutions), this situation is the same as PASS action.

### Changing Value of a Variable

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



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

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

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

## Variables used in the rules

When indicating variables in the rules, the register of symbols is not considered. The variables with compound names could be saved using underscore for spacing or without it. Thus, records `variable_name`, `VariableName` and `variablename` represent the same variable. In this section, all variables are saved using underscore (i.e. `variable_name`).

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 simultaneously contain a set of values.</i></p> <p><b>Allowed values:</b> HTTP, SMTP, IMAP, POP3.</p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• The variable value can be defined only if SSL/TLS is not used or it was allowed to unwrap SSL.</li><li>• It does not make sense to specify any other value except <code>HTTP</code> for the Dr.Web ICAPD rules: only HTTP can be specified for Dr.Web ICAPD.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>protocol in (HTTP, SMTP) protocol in (POP3) protocol in file("/etc/file")</pre>	Yes	No
<code>url</code>	<p>URL requested by the client. Can be compared with the specified string or with a regular expression.</p>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• Dr.Web LookupD can be used to check the value of this variable.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>url match ("drweb.com", "example\..*", "aaa.ru/") url match "ICAPD.Adlist" url not match LDAP@BadURLs url match file("/etc/file")</pre>		
url_host	<p>URL/host with which the connection is established.</p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• The variable value can be defined only if SSL/TLS is not used or it was allowed to unwrap SSL.</li><li>• Dr.Web LookupD can be used to check the value of this variable.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></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
url_category	<p>The list of <a href="#">categories</a> to which the URL/host belongs. The information is based according to the database of categories or Dr.Web Cloud replies.</p> <p><i>The variable can simultaneously contain a set of values.</i></p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• The variable value can be defined only if SSL/TLS is not used or it was allowed to unwrap SSL.</li></ul>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<ul style="list-style-type: none"><li>For rules used by Dr.Web ICAPD, condition with <code>not in</code> will be <i>true</i>, even if according to the scanning results, URL/host does not belong to any of the predetermined categories ("safe" URL/host).</li><li>If databases of web resource categories are not installed, the variable could not be used in rules (attempts to check if a condition in the rule is true will lead to the error x112).</li><li>A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>url_category not in (AdultContent, Chats) url_category in "LinuxFire- wall.BlockCategory" url_category in (FreeEmail) url_category in file("/etc/file")</pre>		
threat_category	<p>The list of <a href="#">categories</a> to which the threat belongs, which is found in the transferred data (according to information from virus databases).</p> <p><i>The variable can simultaneously contain a set of values.</i></p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>The variable value can be defined only if SSL/TLS is not used or it was allowed to unwrap SSL.</li><li>For rules used by Dr.Web ICAPD, condition with <code>not in</code> will be <i>true</i>, even if according to the scanning results, the object does not contain threats from any of the predetermined categories ("safe" object).</li><li>A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>threat_category in "LinuxFirewall.BlockThreat"</pre>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<pre>threat_category not in (Joke) threat_category in file("/etc/file")</pre>		
user	<p>The name of the user with whose privileges the process that is sending (or receiving) the traffic has been launched.</p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• In the Dr.Web ICAPD rules, the name of that user is implied 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.</li><li>• Dr.Web LookupD can be used to check the value of this variable.</li><li>• If you need to find out whether the user belongs to a certain user group, use an LDAP or an Active Directory data source that returns a list of groups and specify the name of the required group (for which you want to know whether the user is its member or not). Use the following format: <i>&lt;type of the source for LookupD&gt;@&lt;source of groups&gt;@&lt;required group&gt;</i>. Requests to Active Directory (AD@) return only lists of groups, therefore for these requests it is mandatory to use the <i>@&lt;required group&gt;</i> part.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>user in ('user1', 'user2') user in AD@Winusergroups@Admins user in LDAP@AllowedUsers user not in file("/etc/file")</pre>	Yes	No
src_ip	The IP address of a host establishing the connection.	Yes	No





Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• Dr.Web LookupD can be used to check the value of this variable.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></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>		
direction	<p>The type of traffic on the connection.</p> <p><b>Allowed values:</b> request (client request), response (server reply).</p> <p><i>This variable cannot simultaneously contain a set of values; conditions of the match and in type cannot be applied.</i></p> <p><b>Examples:</b></p> <pre>direction request direction not response</pre>	Yes	No
divert	<p>The direction of the connection.</p> <p><b>Allowed values:</b> input (incoming—created/initiated from outside the local host), output (outgoing—created/initiated on the local host).</p> <p><i>This variable cannot simultaneously contain a set of values; conditions of the match and in type cannot be applied.</i></p> <p><b>Examples:</b></p> <pre>divert input divert not output</pre>	Yes	No
content_type	<p>MIME type of data transferred during connection.</p>	Yes	No



Variable	Description	Can be used in	
		conditional part	action part (SET)
	<p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• Can be defined if only SSL/TLS is not used or it was allowed to unwrap SSL.</li><li>• The expression “*/*” matches data of any MIME type and HTTP replies without the header <code>Content-Type</code>.</li><li>• Dr.Web LookupD can be used to check the value of this variable.</li><li>• A set of values for checking a variable value is available from the file.</li></ul> <p><b>Examples:</b></p> <pre>content_type in ("multi-part/byteranges", "application/octet-stream") content_type not in ("text/*", "image/*") content_type not in ("audio/*") content_type in ("*/") content_type in LDAP@B-lockedContent content_type not in file("/etc/file")</pre>		
<code>http_templates_dir</code>	<p>The path to the directory where the notification page template on blocking HTTP request is stored.</p> <p>If the path starts with a / (forward slash), it is an absolute path; if it starts with any other symbol, then it is a relative path. In the latter case it is given relative to the directory specified in the <b>TemplatesDir</b> parameter.</p> <p><b>Usage Aspects:</b></p> <ul style="list-style-type: none"><li>• It is useful only for the HTTP(S) protocol.</li></ul> <p><b>Examples:</b></p> <pre>SET http_templates_dir = "/etc/mytemplates" set http_templates_dir = "templates_for_my_site"</pre>	No	Yes

## Categories of unwanted websites and threats

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

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 containing adult content.
<i>Violence</i>	Websites containing graphic violence.
<i>Weapons</i>	Websites dedicated to weapons.
<i>Gambling</i>	Gambling websites.
<i>Drugs</i>	Websites dedicated to drugs.
<i>ObsceneLanguage</i>	Websites with obscene language.
<i>Chats</i>	Chat websites.
<i>Terrorism</i>	Websites that contain information about terrorism.
<i>FreeEmail</i>	Websites that offer free email registration.
<i>SocialNetworks</i>	Social networking websites.
<i>DueToCopyrightNotice</i>	Websites that were specified by the holders of copyrights pertaining to content or works protected by copyright law (movies, music, etc.).

As values of the variables `sni_category` and `url_category`, it is also possible to use names of the parameters that control blocking (see below).

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.
<i>Riskware</i>	Riskware.



Convention	Threat categories
<i>Hacktool</i>	Hacktool.

As a value of the variable `threat_category`, it is also possible to use names of the parameters that control blocking (see below).

## Configuration parameters that can be used in rule conditions

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

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



## Appendix B. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at <https://download.drweb.com/doc/>.
- Read the frequently asked questions at [https://support.drweb.com/show\\_faq/](https://support.drweb.com/show_faq/).
- Browse the Dr.Web official forum at <https://forum.drweb.com/>.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at <https://support.drweb.com/>.
- Call by phone in Moscow: +7 (495) 789-45-86.

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

