



Dr.WEB

Enterprise Security Suite

Managing Dr.Web for UNIX Internet gateways

Жасағаныңды

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Жасағаныңды қорға

Защити созданное

Proteggi ciò che crei

Verteidige, was du erschaffen hast

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

© **Doctor Web, 2016. All rights reserved**

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 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 10.0
Administrator Manual
11/15/2016

Doctor Web Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125040

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

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

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

Doctor Web

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

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

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

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

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



Table of Contents

Chapter 1. Introduction	5
1.2. About Manual	5
1.3. Conventions and Abbreviations	6
Chapter 2. Dr.Web Enterprise Security Suite	8
2.1. About Product	8
2.2. Workstations Protection	9
Chapter 3. Dr.Web for UNIX Internet gateways	11
3.1. Dr.Web for UNIX Internet gateways Components	11
3.2. Dr.Web for UNIX Internet gateways Configutarion	13
3.2.1. Dr.Web ICAPD Settings	14
3.2.2. Logging	14
3.2.3. Anti-virus	15
3.2.4. Proxy	16
3.2.5. Filtering	17
3.2.6. Other	20
3.2.7. Notifications	21
Appendix A. Filtering Rules	22
Request Parameters	23
Logic Expressions	24
Macros	26
Access Rules	27
Proxy Server Settings	29
Appendix B. Technical Support	30



Chapter 1. Introduction

1.2. 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:

- **User 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>



1.3. Conventions and Abbreviations

Conventions

The Manual contains the following conventions:

Symbol	Comment
	Important note or instruction.
	Warning about possible errors or important notes to which you should pay special attention.
<i>Anti-virus net-work</i>	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
C:\Windows\ C:\Windows\	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

Abbreviations

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

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

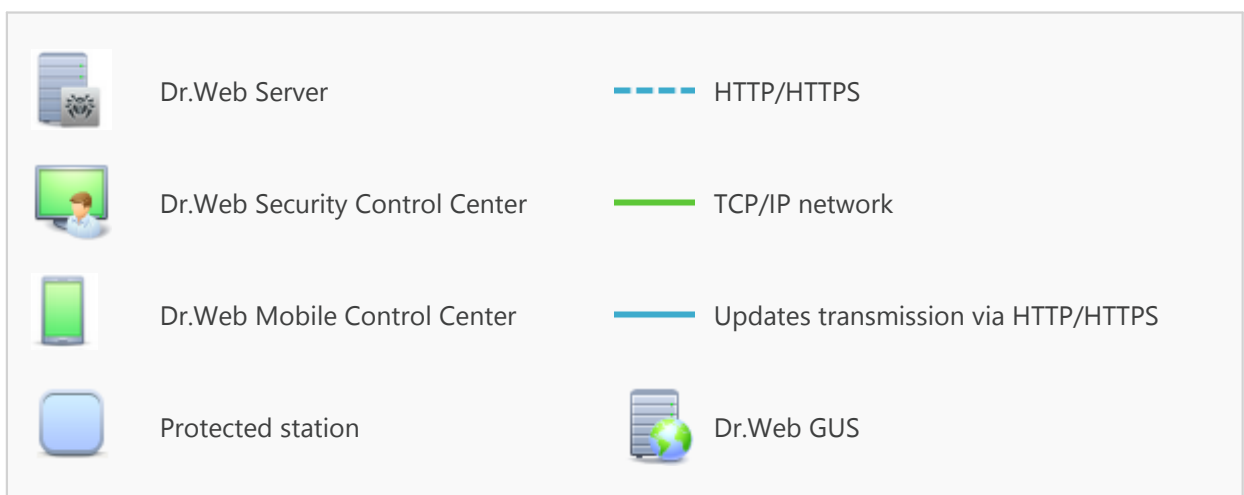
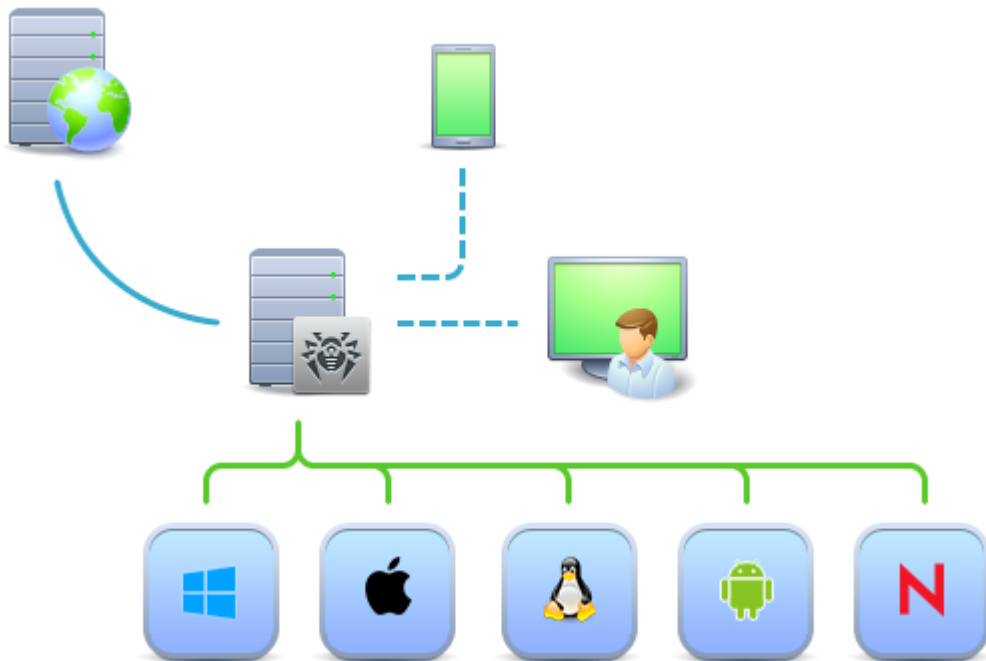


Chapter 2. Dr.Web Enterprise Security Suite

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 stations is included in one or several groups registered on this Server. Stations and Dr.Web Server communicate through the protocol used in the local network (TCP/IP of 4 or 6 version).

Installation

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



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

Management

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

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



Update

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

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



The principle of stations operation in the Mobile mode is described in the **Administrator Manual**.



Chapter 3. Dr.Web for UNIX Internet gateways

This Manual describes management aspects of Dr.Web for UNIX Internet gateways anti-virus software designed for **GNU/Linux**, **FreeBSD** and **Solaris** OSES (**Solaris**—for Intel x86 platform only). The manual is designed for a person responsible for anti-virus protection and security ("Administrator" hereinafter).

Protection of Internet gateways in UNIX systems has the following features:

- Monitoring of all incoming HTTP and FTP traffic to provide virus detection and neutralization. In most cases, viruses are not directly aimed at UNIX systems. For example, through the Internet ordinary Windows viruses are distributed, including macro viruses for **Microsoft Word**, **Excel** and other **Microsoft Office** applications.
- Filtration of access to HTML resources by their MIME type, size and host name.
- Restriction of access to Internet resources according to the black lists that are regularly updated.

Dr.Web for UNIX Internet gateways solution performs all of the tasks mentioned above.

3.1. Dr.Web for UNIX Internet gateways Components

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

Dr.Web ICAPD

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).

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

Provides detection and neutralization of viruses on the local machine including shared directories.

Dr.Web Daemon background monitor (can be managed on station only)

Used by Dr.Web ICAPD component to check files and neutralizes threats, if possible.

Quarantine

Isolates malicious and suspicious objects in the special folder.



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

Dr.Web ICAPD module (`drweb-icapd`) allows integration of all Dr.Web for UNIX Internet gateways components with applications which use the ICAP protocol. This protocol is currently supported by **Squid** and **SafeSquid** proxy servers. Dr.Web ICAPD establishes connection between



Dr.Web Daemon (`drweb-daemon`) and the corresponding proxy server to enable scanning of incoming FTP and HTTP traffic for viruses. It also allows filtering access to HTML resources by both the MIME type and size of downloaded files and the name of the host where these files reside. Moreover, it is possible to restrict access to webpages using regularly updated list of Internet resource categories, and white and black lists defined by the user (administrator of the suite).

Interaction scheme:

1. Client requests an Internet resource (with a HTTP `GET` request).
2. Proxy server requests Dr.Web ICAPD a permission to access the required resource via the ICAP protocol.
3. If access to the requested resource is not forbidden (for example, if the user added the server to the white list, or this server is not included in the user-defined black list and in the list of Internet resource categories, or if the applied rules allow access to the resource), Dr.Web ICAPD allows the HTTP request for the proxy server. Otherwise, Dr.Web ICAPD instructs the proxy server to respond with an HTML page notifying that access to the requested resource is blocked.
4. If access to the remote server is allowed, the proxy server connects to it, receives response and then, via the ICAP protocol, transmits the received content to Dr.Web ICAPD for anti-virus scanning.
5. If the user added the remote server to the white list, the received content is not checked and Dr.Web ICAPD instructs the proxy server to transmit the content to the client. Otherwise, Dr.Web ICAPD checks the content with the use of content-filtering rules, and, if the rules instruct to apply a scan action, the content is transmitted to Dr.Web Daemon for anti-virus scanning.
6. According to the scan results, one of the following actions is applied to the requested content:
 - a) `pass`—Dr.Web ICAPD allows the proxy server to return the requested content to the client.
 - b) `report`—Dr.Web ICAPD instructs the proxy server to return generated HTML page notifying that the requested file is rejected.
 - c) `move`—Dr.Web ICAPD moves the received file to Quarantine and instructs the proxy server to return generated HTML page notifying that the requested file is quarantined.
 - d) `truncate`—an empty file is returned to the client.

The same actions (except for moving to Quarantine) can be specified in content-filtering rules. Thus, you can instruct Dr.Web ICAPD to pass content of certain types (e.g. streaming video) without scanning, or, on the contrary, to reject it unconditionally. For that purpose, enable and configure the *ICAP preview* mode.

For information on how to setup **Squid** and **SafeSquid** proxy servers for interaction with Dr.Web ICAPD, see the Dr.Web for UNIX Internet gateways Administrator Manual.












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 UNIX OS (**Linux**, **Solaris** or **FreeBSD**) or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in one of the **UNIX** subsections: **Linux**, **Solaris** or **FreeBSD**, select the Dr.Web ICAPD 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.



3.2.1. Dr.Web ICAPD Settings

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

- [Logging](#)—parameters of logging on the protected server.
- [Anti-virus](#)—settings of scan files downloaded from Internet.
- [Proxy](#)—settings of interaction with protected proxy HTTP server (for example, **Squid**).
- [Filtering](#)—conditions of restriction access to websites and filtering of data downloaded from Internet.
- [Other](#)—some additional settings.
- [Notifications](#)—settings of sending notifications to administrator.

3.2.2. Logging

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

- **Log file**—name of the log file. You can specify syslog here to enable logging Dr.Web ICAPD messages with the **syslog** system service (in this case, you must also specify **Syslog facility** and **Syslog priority**).
- **Syslog facility**—facility label for logging Dr.Web ICAPD messages with the **syslog** service (if the syslog value is specified in the **Log file** field).
- **Syslog priority**—verbosity level for logging Dr.Web ICAPD messages with the **syslog** service (if the syslog value is specified in the **Log file** field).
- **Logging level**—general verbosity level of the log. The value is a sum of an arbitrary set that can consist of the following values:
 - 0—output information on errors and detected viruses
 - 1—output information at the Info level: on checked clean files and other service information
 - 2—output general messages
 - 4—output results of chunk analysis
 - 8—output extended messages on chunks
 - 16—output activity log of the syntax analyzer
 - 32—output other debugging messages

For example, the value 18, which is a sum of the following values: $0 + 2 + 16$, enables logging of information on errors and detected viruses (0) as well as logging of general messages (2) and messages of syntax analyzer (16).

Thus, maximum detailed output of information that includes output of all data is enabled by parameter value equals to 63. Please note that -1 disables logging.



- **Maximum log size**—maximum size of the log file. Each time Dr.Web ICAPD starts, size of the log file is checked. If it is greater than the specified value, log file is overwritten. Set this parameter value to 0 to disable check of log file size at startup.

3.2.3. Anti-virus

On this page you can specify parameters that Dr.Web for UNIX Internet gateways uses for checking of Internet connections through the protected station.

Actions

Defines the list of file checking events and reactions of Dr.Web ICAPD on them. The term file means here any data transferred from client to server (for example, the HTTP POST request) or data received as a server answer (for example, stream of data returned on the HTTP GET request).

Dr.Web ICAPD can react to the following events:

- **Incurable**— the **Cure** action failed for the detected threat
- **Suspicious**—scanned file marked as suspicious
- **Infected**—scanned file contains a known virus
- **Adware**—scanned file contains an adware
- **Dialers**—scanned file contains a dialer
- **Joke programs**—scanned file contains a joke program
- **Riskware**—scanned file contains a riskware
- **Hacktools**—scanned file contains a hacktool
- **Action applied to unchecked archives**—scanned file is an archive that cannot be checked (for example, protected by a password, with too big size after unpacking, etc.)
- **Action upon Dr.Web Daemon error**—Dr.Web Daemon failed during checking a file
- **Skipped files**—file skipped by Dr.Web Daemon because it cannot be check (password protected of corrupter archive, symbolic link, file of non-standard format and etc.)
- **Action upon license error**—file cannot be checked due to license error on the station (for example, license expired).

For these events, the following actions are allowed:

- **Report**—instead of the requested object, return to the user an HTML page containing notification about detected threat.
- **Move to quarantine**—move malicious file to Quarantine and return to the user an HTML page containing notification about moving detected threat to Quarantine.
- **Truncate**—return to the user the requested file with truncated contents.
- **Ignore**—return to the user the requested file.
- **Cure**—cure the detected threat and return to the user the cured file (if curing is impossible, apply action specified in the **Incurable** field).



The mentioned above actions are applied not to all of the mentioned events. For example, the **Cure** action can be applied only to event **Infected**.

Quarantine

Defines parameters of Quarantine which stores isolated malicious files on the protected station.

- **Quarantine directory**—path to the Quarantine directory containing isolated files on the station.
- **Quarantined file permissions**—access permissions mask for files moved to Quarantine. The mask is set in standard for UNIX three-number form.

Advanced

Defines advanced scan options.

- **Dr.Web Daemon addresses**—list of local sockets on station used by Dr.Web ICAPD for connection with Dr.Web Daemon component for files check. At least one socket must be specified to check files. Addresses in the list are separated by commas.

Examples: `inet:3000@localhost, local:%var_dir/.daemon, pid:/usr/local/drweb/run/drwebd.pid`

If you use Dr.Web Daemon running on a remote (for protected station) machine, the **Use local scan** check box must be cleared. When a socket address or path to PID file of Dr.Web Daemon that performs the local scan is specified first in the list, local scanning will be forced to terminate if connection to this address cannot be established. If this list is empty, Dr.Web ICAPD operates without connection to Dr.Web Daemon and check on viruses is not performed.

- **Heuristic analysis**—defines whether the heuristic analyzer is used for detecting unknown threats. Objects detected by the heuristic analyzer are treated by *suspicious*.
- **Use local scan**—enables or disables the local scan mode. If the checkbox is set, Dr.Web Daemon scans files in the local mode; that is, only paths to the files are transmitted to the component. Otherwise, it receives the content of files for scanning. So, the local schedule can be used only if Dr.Web Daemon and Dr.Web ICAPD are operating on the same host.

3.2.4. Proxy

On this page you can setup interaction between Dr.Web ICAPD and HTTP proxy server (such as **Squid**) to be protected.

- **Port**—number of the port to listen by Dr.Web ICAPD waiting for connections from proxy server. Note that this value must be equal to corresponding value, specified for the used HTTP proxy server.
- **Hostname**—IP address or host name where Dr.Web ICAPD operates. Note that this value must be equal to corresponding value, specified for the used HTTP proxy server.



- **Keep connections alive**—enables maintenance of permanent connection with the proxy server when waiting for requests.
- **Use preview mode**—enables the *ICAP preview* mode. If the proxy server does not work correctly in this mode, disable this option (clear the checkbox).
- **Allowed clients**—list of paths to text files, separated by commas. The specified files contain IP addresses or host names, for which access to Dr.Web ICAPD via the ICAP protocol is allowed. If the list is empty or the specified files do not contain any address, access to Dr.Web ICAPD is allowed for all clients.

3.2.5. Filtering

On this page you can setup the rules that are used by Dr.Web ICAPD for blocking of webpages for users as well as define rules for filtering files depending on them type and size.

Content

The section contains the settings of blocking access to different categories of webpages. Also it contains paths to all used user-defined white and black lists of webresources.

Blocking access to websites

The several **Block (Block adult content, etc.)** checkboxes allow you to enable or to disable blocking access to websites of the corresponding categories. If blocking is enabled, on the access attempt the user will receive a special HTML page containing notification that access to a website is blocked.



Note that one Internet resource can be included in several categories. In this case, access to this resource is blocked if at least one category is active. If it is necessary to allow access to such a resource, deactivate all categories where it is included. Also you can create the rules that grant access to it depending on some conditions.

Managing of black and white lists

Dr.Web ICAPD uses access control lists which contain addresses of Internet resources, access to which is blocked or allowed. Apart from the list of Internet resource categories, that are distributed with Dr.Web ICAPD and updated automatically by Doctor Web company, the administrator can create and configure unlimited number of user-defined lists.

You can create both black and white access control lists. User-defined black lists block access and white lists allow access to certain websites.

User-defined white lists can be of the following types:

- *Trusted white list (WhiteHosts)*. All content from the specified hosts is passed without scanning for viruses.



- *Permissive white list (WhiteDWS)*. Users can access the specified hosts regardless whether or not they match a category of Internet resource categories list; however, access to the hosts is forbidden if they are specified in a user-defined black list.

Note the following features of user-defined lists:

- If a host is included in a *trusted white list*, access to it is controlled as usual: the host is checked whether it is included in an active category of Internet resource categories list in compliance with the rules and then—whether it is included in a user-defined black list.
- If a host is included in a user-defined black list, access to this host is blocked unconditionally; that is, you cannot create a redefining rule that allows access to such a resource. Moreover, user-defined black lists take precedence over user-defined permissive white lists, that is, if a host is added both to a user-defined white list and to a user-defined black list, access to this host is blocked.

Parameters:

- **DWS files directory**—path to the directory with files of Internet resource categories list used by Dr.Web ICAPD on the protected station.
- **White lists for content filtering**—permissive user-defined white list. The parameter value is a list of paths to text files on the station, separated by commas. The specified files contain hosts which content is not to be checked for matching a black list category. However, the content is to be scanned for viruses. The parameter is necessary to allow access to those websites which are blocked due to being included in a black list.
- **User black lists**—user-defined black list. The parameter value is a list of paths to text files on the station, separated by commas. The specified files contain hosts access to web sites on which is to be blocked.
- **White lists for anti-virus scanning**—trusted user-defined white list. The parameter value is a list of paths to text files on the station, separated by commas. The specified files contain hosts which content is not to be scanned for viruses. However, the content is to be checked for matching a black list. Please note, this parameter only disables anti-virus check of files received from this hosts but does not allow the access to the hosts.

MIME Filtering

The section contains the only one editable multi-line field **MIME filtering rules**. In this field, you can specify rules of anti-virus checking of the transferred data depending on MIME type and size.

Text in the field is always starting with the line `MimeStart` and ending with the line `MimeEnd`. Between these lines you should specify the rules of content filtering, one rule per one line.



Content filtering requires the proxy server to support the *ICAP preview* mode. Moreover, ensure that the **Use preview mode** checkbox is set on the **Proxy** page.



Filtering rules are specified as follows (elements are separated by the space sign):

```
<MIME type> <action1> <size> <action2>
```

where

- *<MIME type>*—it is a MIME type of content, for example:
 - ***—file of any type
 - *application*—executables, archives, MS Office and PDF documents, etc.
 - *audio*—audio files (mp3, wav, wma, etc.)
 - *image*—images (gif, jpg, png, svg, etc.)
 - *message*—messages between web servers and clients
 - *multipart*—containers (mail files, packed files)
 - *text*—text or source code (html, xml, css, etc.)
 - *video*—video files (mpeg-1, mp4, wma)
 - *model*—3D models files.

You can specify either a family of MIME types or a concrete type (for example, *video* indicates any video files, *video/mpeg*—only file of MPEG type).

The rule specified for the nearest matching MIME type is applied to an object. Thus, the rule specified for files of any type "***" is applied only if no other rule matching the object MIME type is found.

- *<action1>*—action (*scan*, *pass*, *reject*) that is applied if the object size of this MIME type is not greater than the specified *<size>* value.
- *<size>*—threshold size. If the object size of this MIME type is not greater than this threshold, *<action1>* is applied; otherwise *<action2>* is applied.
- *<action2>*—action (*scan*, *pass*, *reject*) that is applied if the object size is greater than the specified *<size>* value.

If the key value *all* is specified as the size, only the first action (*<action1>*) is applied to all objects of this MIME type not depending on their size. In this case, it is not required to specify *<action2>*.

The following actions are allowed:

- *scan*—send the file for anti-virus scanning
- *pass*—pass the file to the user without scanning
- *reject*—reject the file and return another object. This action must be specified with a switch that defines what data is returned to the user:
 - *-report*—return an HTML page notifying the user that the file is blocked
 - *-trunc*—return a requested file truncated to zero length (empty file).



Note that the `reject` action must not be specified without a switch.

The order in which filtering rules are specified is indifferent.

Definitions

The section contains the only one editable multi-line field **Definitions**. In this field, you can specify your own macros that can be used in rules which allow or block access to websites depending on some conditions. The macros are specified in the `[def]` section.

Rules

The section contains the only one editable multi-line field **Access rules**. In this field, you can specify your own rules which allow or block access to websites depending on some conditions. The rules are specified in the `[match]` section.



For details on macros and rules, refer to [Appendix A](#).

3.2.6. Other

On this page you can specify some other (additional) settings for Dr.Web ICAPD:

- **Notification templates**—path to directory on the station containing templates for HTML pages generation. These pages are returned to the user in case restriction access to websites or instead of downloading malicious files.
- **PID file**—path to Dr.Web ICAPD PID file with information on the PID, UNIX socket or port number (depending on what is used for interaction) that is saved on the Dr.Web ICAPD startup.
- **Maximum size of memory block**—maximum size of the memory block which can be allocated by Dr.Web ICAPD at a time. If random access memory is enough, this parameter value can be increased for better performance.
- **Write timeout**—timeout for a sockets of Dr.Web ICAPD to wait for data to be received, in seconds. When at least one byte is received/sent, the waiting counter is reset. If 0 is specified, the wait time is unlimited. The parameter manages the connections established by Dr.Web ICAPD, not only with a web proxy but with Dr.Web Daemon as well.
- **User**—user whose privileges are used by Dr.Web ICAPD.
- **Cache**—path to the directory where temporary files of Dr.Web ICAPD are created and stored.



3.2.7. Notifications

On this page you can specify settings for operation Dr.Web ICAPD with notifications that are sent to the administrator upon any incident on a protected workstations (threat detection, restricted access to a webpage, etc.):

- **Administrator address**—email address of the administrator to send notifications.
- **Notify admin on blocked access**—enables or disables sending notifications to administrator on attempt to download a malicious object.
- **Notify admin on blocking by black lists**—enables or disables sending notifications to administrator on attempt to open a web page blocked due to matching a black list category.
- **Email send command**—a shell command executed to send a notification to administrator. Placeholder %s in the command text is replaced with the **Administrator address** value.
- **Send statistics**—enables or disables sending statistics on detected virus events to Control Center.
- **Delay between notifications**—time period, in seconds, within which notifications on the same event (repeated attempts to open the same forbidden page or downloading of infected file) are not sent to the administrator. If the parameter value is set to 0, notification is sent every time a page is blocked.



Appendix A. Filtering Rules

You can specify individual settings to configure access to Internet resources. For that purpose, you can specify redefining rules.

In the current version of Dr.Web for UNIX Internet gateways, you can redefine the following parameters:

- `BlockAdult`—block access to websites with adult content.
- `BlockViolence`—block access to websites dedicated to violence: contain photos and videos of car accidents, plane crashes, natural disasters, etc.
- `BlockWeapon`—block access to websites dedicated to weapon: contain texts, photos, and videos of weapons (from cold steel to weapons of mass destruction) and information on manufacture of explosives.
- `BlockGamble`—block access to websites dedicated to gamble: to Internet casinos, gambling and bookmaking websites.
- `BlockDrugs`—block access to websites dedicated to drugs: contain information on drug production, distribution, and use.
- `BlockObscenity`—block access to websites with obscene language.
- `BlockChats`—block access to chats.
- `BlockTerrorism`—block access to websites dedicated to terrorism: contain detailed description of terroristic acts, manufacture of explosives, terrorist propaganda materials.
- `BlockEmail`—block access to websites that offer free email registration.
- `BlockSocialNetwork`—block access to social networks: dating websites, business social networking sites, corporate social networks, etc.
- `BlockMalwareLinks`—block access to known infection sources.
- `BlockAll`—block access to all websites.

Access rules are defined in the **Rules** section on the [Filtering](#) page; macros that are used in defined rules, should be specified in the **Definitions** section on this page.

To determine the actual status of accessibility to any website for a user, the following algorithm is used:

1. Dr.Web ICAPD checks whether the requested resource matches any of the pre-defined categories.
2. If the corresponding URL is found in such category (for example, in the Terrorism list), Dr.Web ICAPD defines the access mode for sites of this category. In Control Center, these settings are specified by corresponding flags (in the given example, **Block terrorist websites**) on the **Filtering** page.
3. The value is first searched in the **Rules** section according to the following algorithm:
 - for all request variables, value of the `if` statement expression is calculated
 - if true, the required parameter is searched in the configuration section



- if this parameter is found, its value is returned and the search completes
 - if this parameter is not found or if the `if` statement is false, Dr.Web ICAPD goes to the next `if` statement.
4. If in the **Rules** section none of the rules is matching or does not contain the required parameter, the global parameter value is returned (or default value).

Search of the parameter value is performed until the first match; thus, the first found value is returned (from the configuration blocks of those `if` statements that have `true` expressions).



One Internet resource can be included into several categories of Internet resources as well as in a user-defined black list. In this case, access to this resource is blocked if at least one category is active. If it is necessary to allow access to such resource, deactivate all categories where it is included and exclude it from the user-defined black list.

However, to block access to other resources matching the deactivated black list categories, it is strongly recommended to include check of both URL of allowed resource and client properties (such as IP address) into the condition of an allowing access rule.

Note that if an Internet resource is included in a user-defined black list, access to this resource cannot be allowed by a rule.

Request Parameters

Every request sent from a client to the proxy server has a set of unique parameters. You can use these parameters in the rules:

Parameter name	Parameter type	Description
<code>request_url</code>	string	Request URL
<code>request_username</code>	string	Name under which the user authorized on the proxy server. The name is extracted from the <code>X-Client-Username</code> header. If the header is not present, the parameter value is treated as an empty line.
<code>request_ip</code>	IP-address with network mask (CIDR)	IP address of the user who sent a request to the proxy server. The address is extracted from the <code>X-Client-IP</code> header. If the header is not present, the parameter value is treated as undefined.
<code>system_time</code>	time	Current system time (hours and minutes).



The use of the `request_ip` and `request_username` parameters requires the **Squid** HTTP proxy server to be [configured accordingly](#).



Logic Expressions

Logical expressions are operations of function call united by the following operators: `&&` - conjunction (logical AND), `||` - disjunction (logical OR), `!` - negation (logical NOT). To group operations and change their priority, use brackets.



Only `&&`, `||` and `!` operators can be used in a logical expression. Standard mnemonics (`AND`, `OR`, `NOT`) are not allowed.

Syntax of `BOOL_EXPR` logical expressions is as follows:

```
macro_name() | COMPARE |  
(BOOL_EXPR) | !BOOL_EXPR |  
BOOL_EXPR && BOOL_EXPR |  
BOOL_EXPR || BOOL_EXPR
```

Where `macro_name()` is a call of macro with the `macro_name` name, and `COMPARE` is one of the comparison operations listed below. The macro must be defined in the **Definitions** section.

To define the `COMPARE` operation, you can use the following notations:

Notation	Description
<code>string_var</code>	
<code>cidr_var</code>	Parameter of the corresponding type (<code>STRING</code> , <code>CIDR</code> or <code>TIME</code>)
<code>time_var</code>	
<code>TIME</code>	String of the following format: "HH:MM" or "H:MM" (hours, minutes); must be enclosed in quotation marks
<code>STRING</code>	Random string enclosed in quotation marks
<code>REGEX</code>	Regular expression of the <i>POSIX extended</i> format; must be enclosed in quotation marks
<code>FILE_NAME</code>	File path enclosed in quotation marks
<code>CIDR</code>	IPv4 address enclosed in quotation marks (you can specify a network prefix after a stroke character). If the network prefix is not specified, it is treated equal to /32. An empty string "" indicates the special <code>undefined</code> value

The following comparison operations are supported for variables of the `string` type:

Operation	Description
<code>string_var == STRING</code>	Variable matches the string



Operation	Description
<code>string_var != STRING</code>	Variable does not match the string
<code>string_var ~ REGEX</code>	Variable contains the substring that is checked for matching the regular expression (<i>search</i> method is used)
<code>string_var == file:FILE_NAME</code>	Variable matches at least one string in the specified file
<code>string_var ~ file:FILE_NAME</code>	Variable corresponds to at least one regular expression in the specified file

Note that `==` and `~` operations are case insensitive.

The following comparison operations are supported for variables of the `cidr` type:

Operation	Description
<code>cidr_var <<= CIDR</code>	IP address is within the specified network range
<code>cidr_var <<= file:FILE_NAME</code>	IP address is within at least one of the networks listed in the file

If both arguments of the `<<=` operation have the `undefined` value, the operation result is `true`. If only one parameter has the `undefined` value, the operation result is `false`.

The following comparison operations are supported for variables of the `time` type:

Operation	Description
<code>time_var > TIME</code>	Time comparison
<code>time_var >= TIME</code>	
<code>time_var < TIME</code>	
<code>time_var <= TIME</code>	

Every operation has a certain priority relative to other operations. Sorted in descending order, comparison operation priority is as follows:

1. `!` ("logical NOT")
2. `<` ("less than"), `<=` ("less than or equal to"), `>` ("greater than"), `>=` ("greater than or equal to")
3. `==` ("equal to"), `!=` ("not equal to"), `~` ("matches"), `<<=` ("belongs to")
4. `&&` ("logical AND")
5. `||` ("logical OR")

Operations listed in the same line have equal priority and are processed from left to right.



For certain operations, reading of a value array from a file (specified with the `file:` prefix) is available. Lines beginning with the `#` or `;` characters as well as with empty lines are skipped when reading values.



The content of the `file:FILE_NAME` file is read while the configuration file is processed. Thus, after changing content of the file that contains values or a path to such a file, force Dr.Web ICAPD to reread its configuration, for example, by sending the `SIGHUP` signal.

Macros

Macros can be used in any [logical expressions](#); however, each macro must be predefined before use. They are defined in the **Definitions** section on the **Filtering** page. The `[def]` line must precede the macros definition.

Macro definition syntax:

```
macro_name = { BOOL_EXPR }
```

where `BOOL_EXPR` is a [logical expression](#).

All macros return a Boolean value, arguments are not supported. In fact, a macro is just a shorthand notation for an logical expression.

Example:

Definition of the `is_localhost` and `local_ip` macros: they are to be `true` if the request was sent from one of the specified IP addresses or from one of the IP addresses listed in the file.

```
[def]
is_localhost = { request_ip <<= "127.0.0.0/8" }

local_ip = {
    request_ip <<= "127.0.0.0/8"
    || request_ip <<= "192.168.0.0/16"
    || request_ip <<= "172.16.0.0/12"
    || request_ip <<= file:"/tmp/icapd/other_local_ips.txt"
}
```

Definition of a `worktime()` macro: if the current system time is between 9:30 and 13:00 or 14:00 and 18:15, the macro is to be `true`.

```
[def]
worktime = {
    (system_time>="9:30" && system_time<="13:00")
    ||
    (system_time>="14:00" && system_time<"18:15")
}
```



Access Rules

The access rules are defined in the **Rules** section on the **Filtering** page. The `[match]` line must precede the rules definition.

The specific `if` operators are user to define the rules.

The `if` operator syntax:

```
if BOOL_EXPR {
    config_block
}
```

where `BOOL_EXPR` is a [logical expression](#), a `config_block` is a list of [parameter](#), to which new values, different from the [global values](#), specified on the **Filtering** page (in the **Content** section), are to be assigned.

Examples

If it is necessary to block access to Internet resources from the **Adult** and **Email** lists during working hours of the local network users, as well as block access from a certain IP address, you can specify the following rule:

```
[match]
if (local_ip() ||
    request_ip <=&= "87.249.57.20") &&
    worktime()
{
    BlockAdult = yes
    BlockEmail = yes
}
```

If you want to block access to Internet resources from the **Terrorism** list during night time (from 23:00 to 8:00) for certain IP addresses, you can specify the following rule:

```
[match]
if (request_ip <=&= "93.185.182.46" ||
    request_ip <=&= "195.98.93.66") &&
    (system_time>="23:00" ||
    system_time<="8:00")
{
    BlockTerrorism = yes
}
```

To prevent Internet access during nonworking time for the "edx" user:

```
[match]
if request_username=="edx" && !worktime()
```



```
{
  BlockAll = yes
}
```

Note that `local_ip()` and `worktime()` macro, used in the examples, must be [predefined](#).

To block access to a certain Internet resource for all users whose name either matches the "john.*" regular expression, or any regular expression specified in the file, or one of the lines in the file, use the following rule:

```
[match]
if (request_username ~ "john.*" ||
    request_username ~ file:"/tmp/icapd/users_re_block.txt"
    || request_username == file:"/tmp/icapd/users_block.txt")
&& (request_url == "http://example.com/mega_music.mp3")
{
  BlockAll = yes
}
```

Note that setting the `BlockAll` parameter value to `No` does not mean enabling access to all resources when the rule is true. In this case, access to a resource is allowed if it is either included in user-defined white list or not included in active black lists (in both blocked categories of Internet resources and user-defined black lists). To manage active categories and user-defined white and black lists, use the **Filtering** page.

If in normal mode access to resources is blocked due to being on the black lists, but it is required to allow access to some of these resources, specify a corresponding rule.

For example, let it be required to allow access to `socialnetwork.com` for users whose IP address is within `192.168.1.1/32` network range, despite this resource being included in **SocialNetwork** and **Chats** active categories:

```
if (request_ip <<= "192.168.1.1/32") && (request_url ~ "socialnet-
work.com")
{
  BlockSocialNetwork = no
  BlockChats = no
}
```

This rule allows access to resources included in **SocialNetwork** and **Chats** active categories only if both of the following conditions are true:

- client's IP address is within the `192.168.1.1/32` range
- the requested URL contains the `socialnetwork.com` substring.

Otherwise, global settings, specified on the **Filtering** page (**Content** section), are applied. Note that if a resource matches several categories, it is required to disable blocking of the resource by all of the categories.



Proxy Server Settings

Usage of the `request_username` and `request_ip` parameters requires additional configuration of the **Squid** proxy server on a protected station. For that purpose, you must edit its configuration file (typically `/usr/local/squid/etc/squid.conf`).

If the following lines are already present in the configuration file, you can uncomment them and adjust the values if necessary. Otherwise, add the lines at the end of the file.

To enable use of `request_ip`:

```
# request_ip
icap_send_client_ip on
```

To enable use of `request_username`:

```
# request_username
icap_send_client_username on
icap_client_username_header X-Client-Username
icap_client_username_encode off
```



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 http://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at <http://forum.drweb.com/>.

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

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

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

