Dr.WEB

Enterprise Security Suite

Managing stations under macOS

Trademarks

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 stations under macOS
Version 12.0
Administrator Manual
4/1/2019

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

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 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

1.1. About Manual

The manual gives instructions on the centralized configuration of the Dr.Web for macOS antivirus software. Administrator Manual is a part of the documentation package of the antivirus network that provides information on the organization of the complex antivirus protection of corporate computers and mobile devices using Dr.Web Enterprise Security Suite.

The manual is aimed at antivirus network administrators, employees of the organization who are responsible for the antivirus protection of workstations and servers of the corporate network.

The manual provides information on the centralized configuration of the antivirus software of workstations running macOS. Antivirus network administrator manages workstation settings via the Dr.Web Control Center.

Additional information

- **Dr.Web for macOS User Manual** provides information on configuration of the antivirus software directly on the station.
- **Administrator Documentation** of Dr.Web Enterprise Security Suite antivirus network (including **Administrator Manual**, **Installation Manual** and **Appendices**) provides general information on installation and configuration of the antivirus network, and on operation with the Dr.Web Control Center.

You can find the latest versions of manuals on the Doctor Web website.

1.2. Conventions and Abbreviations

Conventions

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

Convention	Comment
❗	Important note or instruction.
⚠	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`/Volumes/Macintosh HD/`	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 are used in the Manual:

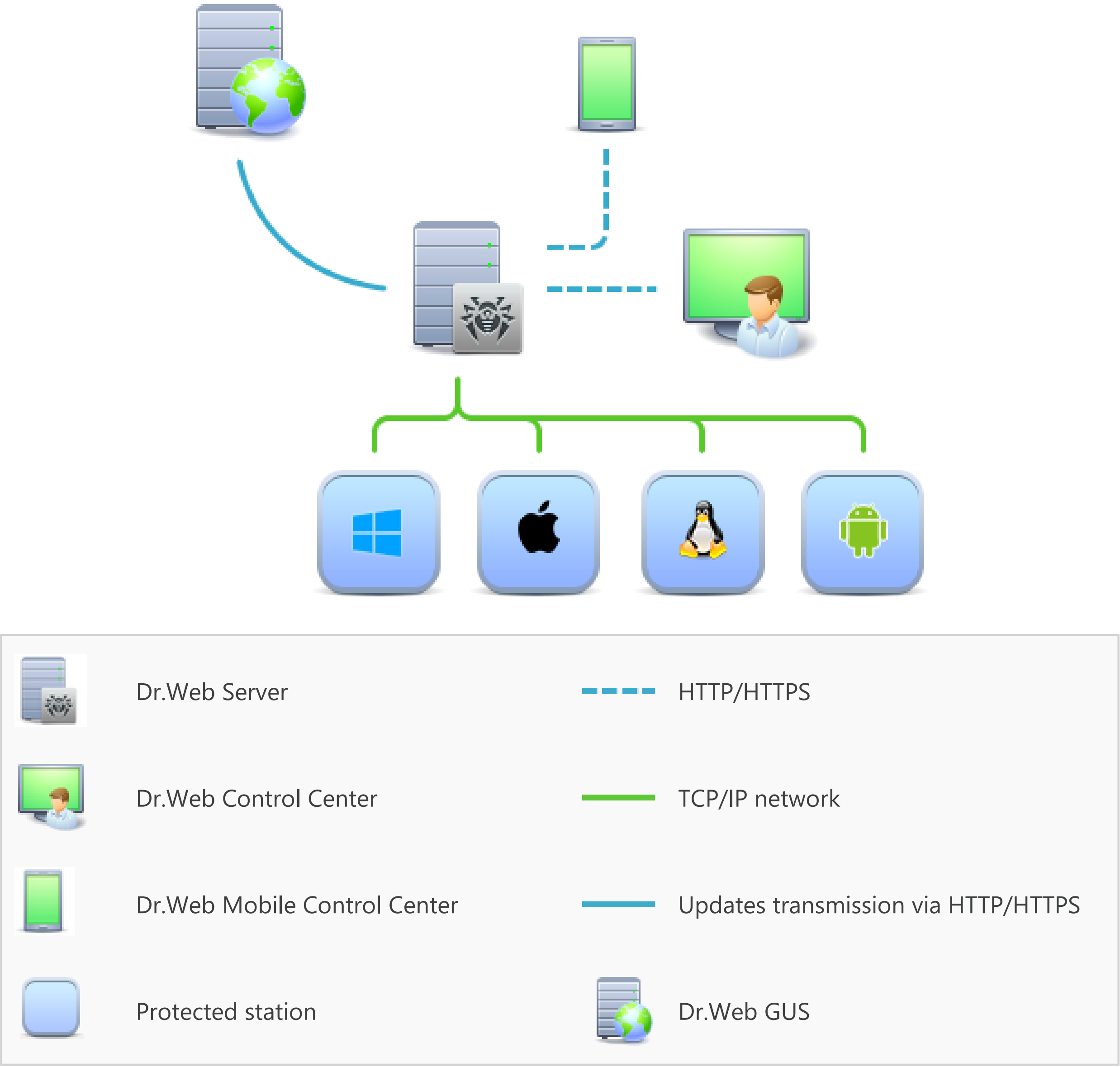
- Dr.Web GUS—Dr.Web Global Update System,
- OS—operating system.

Chapter 2. Dr.Web Enterprise Security Suite

2.1. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of an integrated and secure complex antivirus protection of either a 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 creates a single *antivirus network*.



The logical structure of the antivirus network

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

2.2. Workstations Protection

Every computer with installed antivirus package according to its functions in the antivirus network is a separate *workstation* of the antivirus network. Workstations are protected by the Dr.Web antivirus packages designed for the corresponding operating systems.

> Protected computer with an installed antivirus package in the is called a workstation of the antivirus network. Please note: according to its LAN functions, such A computer with an installed antivirus package can be both a workstation or a mobile device and a LAN server according to its functions.

Antivirus 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. Data between stations and the Server is transferred via a TCP/IP protocol version 4 or 6 used in a local network.

Installation

Administrators or users install antivirus packages for macOS directly on the station. You can find detailed description of the antivirus packages installation on workstations in the Dr.Web Enterprise Security Suite **Installation Manual**.

Management

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

- Centralized configuration of Dr.Web on workstations via the Control Center.

  At this, administrator can either restrict or grant user's permissions to change settings on stations.
- Configure the schedule for the antivirus scans and other tasks to execute on a station.
- Get scan statistics and other information on antivirus components operation and on stations state.
- Start and stop antivirus scans and etc.

Update

Dr.Web Server downloads updates and distributes them to connected stations. It allows to automatically implement, maintain, and adjust protection regardless of workstation users’ computer skills.

In case an antivirus station is temporarily disconnected from the antivirus network, a local copy of settings is used on the station. Components of the antivirus protection keep operating (up to the expiry of the user’s license). At this, the software is not updated. If a station is allowed to operate in the Mobile mode, when connection with the Server is lost, virus databases are updated directly via 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 macOS

Dr.Web for macOS protects computers running macOS and macOS Server against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

Dr.Web for macOS consists of several protection components responsible for the corresponding functionalities. Scan engine and virus databases are common for all components. Product components are constantly updated. Virus databases, lists of non-recommended websites, and rules for email spam filtration are regularly added with new threat signatures.

Constant update provides an up-to-date level of protection for users’ devices, applications, and data against latest threats. Heuristic analysis methods implemented in the scan engine ensure an additional protection against unknown malicious software.

3.1. Dr.Web for macOS Components

The following antivirus components protect workstations running macOS/macOS Server:

Dr.Web Scanner, Dr.Web Agent Scanner

Scans Mac on user demand and according to the schedule. Remote launch of the antivirus scan of stations from the Control Center.

SpIDer Guard

The constant file system protection in a real-time mode. Monitors all programs and processes launched on Mac. Scans new files on hard drives and files that users open on removable media.

SpIDer Gate

Scans all connections to websites via the HTTP protocol. Neutralizes threats and blocks transferring objects that may pose a threat to computer security. Restricts access to non-recommended websites, known virus sources, and webpages with that violate copyright laws.

Quarantine

Isolates detected malicious and suspicious objects in a special folder.

> You can find how to manage Quarantine via the Control Center in the Dr.Web Enterprise Security Suite **Administrator Manual**.

3.2. Dr.Web for macOS Configuration

To view or edit the configuration of protection 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 macOS/macOS Server or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **macOS** subsection, select the necessary protection component:
   - Scanner for workstations/Scanner for servers
   - SpIDer Guard for workstations/SpIDer Guard for servers
   - SpIDer Gate for workstations/SpIDer Gate for servers

   A window with the component settings will be opened.
4. Configure component settings.

   Note that managing component settings via the Control Center differs from managing component settings directly on the station:
   - to manage separate parameters, use the options located on the right from the corresponding settings:

     Reset to initial value—restore the last saved value for a parameter.

     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 last saved values for all parameters in this section.

     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 the inheritance of settings from the parent group—remove personal settings of a station and set inheritance of settings in this section from a primary group.

     Copy settings from the parent group and set them as personal—copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered 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. Click **Save**.

   The settings will be passed to the stations. If the stations are offline when changes are made, the settings will be passed when stations connect to the Server next time.

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

3.2.1. Scanner

Dr.Web Scanner runs an express or full scan of the whole file system or scans critical files and folders only.

Dr.Web Scanner settings for computers running macOS are available in the **Scanner for workstations** section, for macOS Server—in the **Scanner for servers** section.

General

- Enable the **Check archives** option to scan files in archives.
- Enable the **Check email files** option to scan email files.
- In the **Scanning time of one element** field, specify the maximum time for scanning a file. Value 0 means that the time to scan one file is unlimited.

⚠ Scanning the contents of archives and email files and increasing the time for scanning a single file may slow down the computer and increase the overall scanning time.

Actions

In this section, you can configure actions that Dr.Web will apply to threats detected by Scanner. The actions are set separately for each type of malicious and suspicious objects. These actions vary for different object types.

Possible actions

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

  The action is available only for the objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects, such as email files and file containers.

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

  The action is available only for the objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects, such as email files and file containers.

- **Move to quarantine**. Moves a detected threat to a special folder isolated from the rest of the system.
- **Delete**. Deletes the object that poses a threat.

  It is the most effective way to remove all types of threats.
- **Ignore**. Skips the object without any actions. Notifications are not displayed.

> The default settings are optimal for most cases. Do not change them unnecessarily.

Excluded paths

In this section, specify paths to files and folders that will be excluded from scanning by Dr.Web Scanner.

3.2.2. SpIDer Guard

The file system monitor SpIDer Guard scans all the files that users open or change in real time. SpIDer Guard also monitors programs and processes launched on Mac.

SpIDer Guard settings for computers running macOS are available in the **SpIDer Guard for workstations** section, for macOS Server—in the **SpIDer Guard for servers** section.

General

- Enable the **Use heuristic analysis** option to use heuristic analysis for detecting unknown threats.
- Use the **Enable SpIDer Guard for macOS** (for servers—**Enable SpIDer Guard for macOS Server**) option to enable the constant antivirus protection of the file system.
- In the **Scanning time of one element** field, specify the maximum time for scanning a file. Value 0 means that time to scan one file is unlimited.

> Increasing the time for scanning a single file may slow down the computer and increase the overall scanning time.

Actions

In this section, you can configure actions that Dr.Web will apply to threats detected by SpIDer Guard The actions are set separately for each type of malicious and suspicious objects. These actions vary for different object types.

Possible actions

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

  The action is available only for the objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects, such as email files and file containers.
- **Cure, delete if not cured**. Restores the original state of the object before infection. If the object is incurable or the attempt of curing fails, the object is deleted.

  The action is available only for the objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects, such as email files and file containers.
- **Move to quarantine**. Moves a detected threat to a special folder isolated from the rest of the system.
- **Delete**. Deletes the object that poses a threat.

  It is the most effective way to remove all types of threats.
- **Ignore**. Skips the object without any actions. Notifications are not displayed.

> The default settings are optimal for most cases. Do not change them unnecessarily.

Containers

In this section, you can specify the maximum nesting level for containers. If the nesting level is higher than the specified value, the container will be ignored during the scan. Value 0 means that nested objects will not be scanned.

In the **Maximum compression ratio** field, specify the maximum compression ratio for compressed objects (a ratio of source object size to compressed size). If compression ratio of an object is greater than the specified value, the object will be ignored when scanning.

Excluded paths

In this section, specify paths to files and folders which will be excluded from scanning by SpIDer Guard.

3.2.3. SpIDer Gate

Internet monitor SpIDer Gate scans HTTP traffic and blocks transferring objects that may pose a threat to computer’s security.

SpIDer Gate restricts access to non-recommended websites, and websites known as infection sources, and webpages that violate copyright laws.

Also, SpIDer Gate allows to restrict access to Internet resources by categories, for example, gambling, weapons, drugs, and so on.

SpIDer Gate settings for computers running macOS are available in the **SpIDer Gate for workstations** section, for macOS Server—in the **SpIDer Gate for servers** section.

General

- Use the **Enable SpIDer Gate** option to enable HTTP-traffic scan.
- Enable the **Use heuristic analysis** option to use heuristic analysis for detecting unknown threats.
- In the **Scanning time of one element** field, specify the maximum time for scanning a file. Value 0 means that time to scan one file is unlimited.

> ⚠ Increasing the time for scanning a single file may slow down the computer and increase the overall scanning time.

Actions

- Enable the **Scan received files** option to scan files received from the Internet for viruses and other threats.
- In the **Block files** and **Additionally block** lists, select types of incoming malicious objects which will be blocked by SpIDer Gate.

Web filtering

- Enable the **Scan URL** option to scan Internet resources by categories.
- Enable the **Block non-recommended websites** option to restrict access to the websites with unreliable content (suspected of phishing, password theft, and so on).
- Enable the **Block URLs listed due to a notice from copyright owner** option to restrict access to the websites with content that infringes copyright (according to the copyright owners of this content). Among such websites are pirated sites, file reference directories, file hosting services, and so on.
- In the **Block websites from the following categories** list, select the categories of websites you need to block access to:

Category	Description
Adult content	Websites that contain pornographic or erotic materials, dating sites, etc.

Category	Description
Violence	Websites that encourage violence or contain materials about various fatal accidents, etc.
Weapons	Websites that describe weapons and explosives or provide information on their manufacturing.
Gambling	Websites that provide access to online games of chance, casinos, auctions, including sites for placing bets, etc.
Drugs	Websites that promote use, production or distribution of drugs, etc.
Obscene language	Websites that contain the obscene language (in titles, articles, etc.).
Chats	Websites that offer a real-time transmission of text messages.
Terrorism	Websites that contain aggressive and propaganda materials or terroristic attacks descriptions, etc.
Email	Websites that offer the possibility of free registration of a web mailbox.
Social networks	Different social networks: general, professional, corporate, interest-based; thematic dating sites.

- In the **White list**/**Black list** sections, add the paths to the websites you need to allow/restrict access to:

  a) To add a certain website, enter its URL (for example, `www.example.com`). This allows access to all webpages located on this website.

  b) To allow access to websites whose URL contains a certain text, enter this text in the input field. For example, if you enter `example`, then the access to `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru`, and others will be granted.

  c) To allow access to websites within a particular domain, enter the domain name with a period (`.`) character, for example, `.com`. This allows access to all webpages located on this domain.

     If the domain name includes a forward slash (`/`), the substring before the slash 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`, such webpages as `example.com/test11`, `template.example.com/test22`, and so on will be processed.

  d) To add certain websites to the exclusions, enter the mask of their names. Masks will be added in the `mask://...` format.

     A mask denotes the common part of object names, at that:

     - The asterisk (*) character replaces any, possibly empty, sequence of characters.
     - The question mark (?) replaces any, including an empty, character (one).

Examples:

- `mask://*.com/` or `.com`—enable opening of all the domain .com websites;
- `mask://mail`—enable opening of all websites whose names contain the word “mail”;
- `mask://???.com`—enable opening of all the domain .com websites, whose names consist of three characters or less.

Your input may be unified. For example: the `http://www.example.com` address will be transformed into `www.example.com`.

Containers

In this section, you can specify the maximum nesting level for containers. If the nesting level is higher than the specified value, the container will be ignored during the scan. Value 0 means that nested objects will not be scanned.

In the **Maximum compression ratio** field, specify the maximum compression ratio for compressed objects (a ratio of source object size to compressed size). If compression ratio of an object is greater than the specified value, the object will be ignored when scanning.

Additional

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

Technical Support

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

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

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

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

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