Dr.WEB

Enterprise Security Suite

Managing stations under OS X

Жасағаны

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

Защити созданное

Жасағаныңды қорға

Verteidige, was du erschaffen hast

Proteggi ciò che crei

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

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 OS X
Version 10.00.1
Administrator Manual
2/14/2017

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Web site: http://www.drweb.com/

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

Refer to the official web site 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

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 OS X 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 OS X 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 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.
Anti-virus network	A new term or an accent on a term in descriptions.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`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:

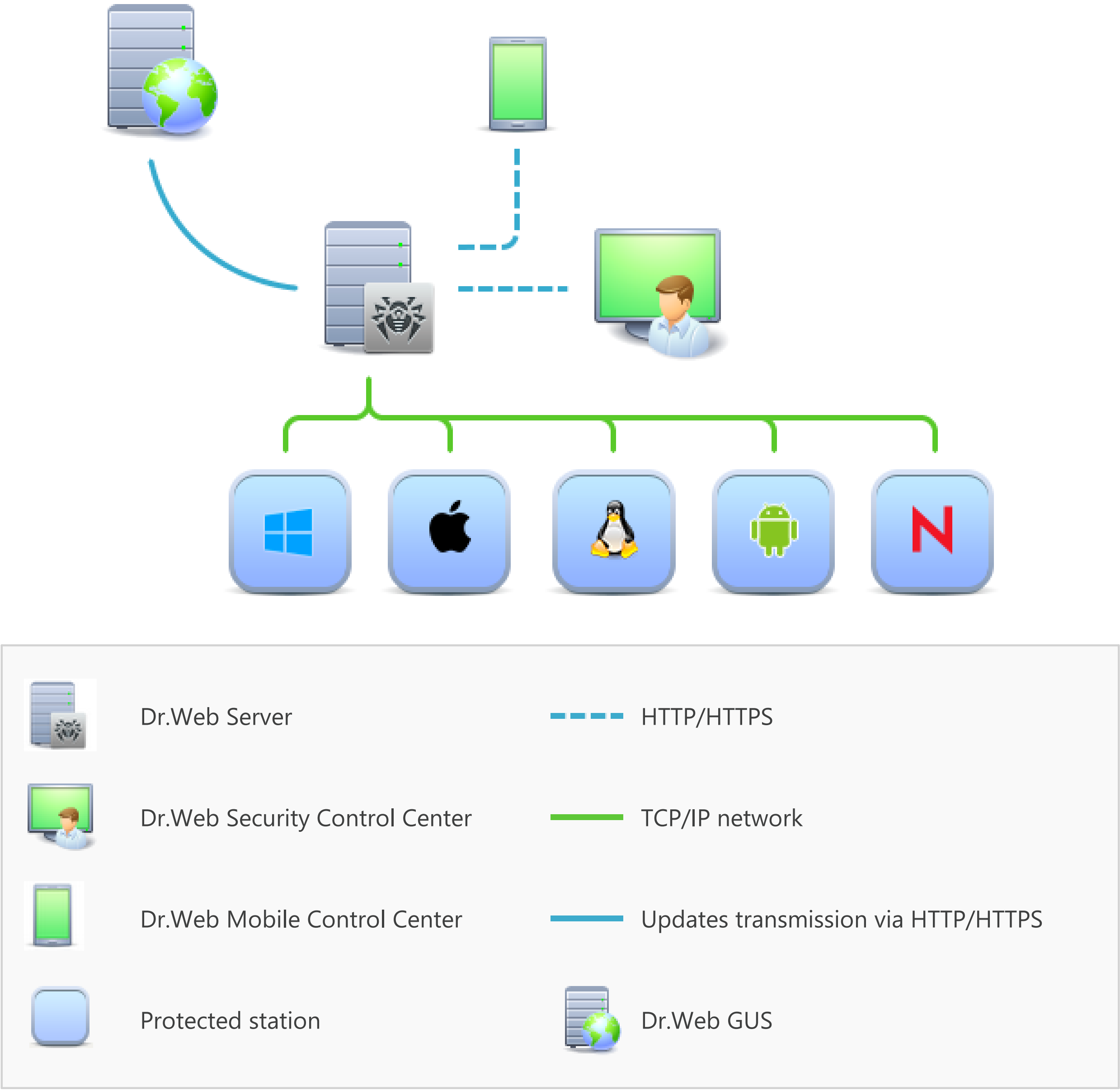
- Dr.Web GUS—Dr.Web Global Update System
- OS—operating system

Chapter 2. Dr.Web Enterprise Security Suite

2.1. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of 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*.


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

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

Local installation of anti-virus package under OS X is performed directly on a station. 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 on workstations via the Control Center.

  At this, administrator can either deny or grant user's permissions to change Anti-virus 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 and etc.

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 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 GUS.

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

Chapter 3. Dr.Web for OS X

Dr.Web for OS X protects computers running OS X and OS X Server from viruses and other types of threats.

The core components of the application (*anti-virus engine* and *virus databases*) are not only extremely effective and resource-sparing but also cross-platform, which allows specialists in Doctor Web to create secure anti-virus solutions for different operating systems. Components of Dr.Web for OS X are constantly updated and virus databases are supplemented with new signatures to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.

3.1. Dr.Web for OS X Components

For the workstations running OS X/OS X Server the following anti-virus components are provided:

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a computer on user demand and according to the schedule. Also the remote launch of anti-virus scan of stations from the Control Center is supported.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

SpIDer Gate (settings are available on a station only)

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

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

3.2. Dr.Web for OS X Configutarion

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 OS X/OS X Server or a group containing such stations.

3. In the **Configuration** section of the opened control menu, in the **MacOS X** subsection, select the necessary component:

   - Scanner for workstations/Scanner for servers
   - SpIDer Guard for workstations/SpIDer Guard for servers

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 ale to edit settings via the Control Center.

3.2.1. Scanner

Dr.Web Scanner performs express or full check of the whole file system or scans the critical files and folders only.

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

General

- Set the **Check archives** flag to enable check of files in archives.
- Set the **Check email files** flag to enable check of email files contents.
- In the **Scanning timeout** field specify the maximum time for scanning one file. Value 0 means that 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, select actions that will be applied automatically to computer threats detected by Dr.Web Scanner depending on their types:

- **Cure, move to quarantine if not cured**. Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- **Cure, delete if not cured**. Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- **Move to quarantine**. This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete**. It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- **Ignore**. No actions are applied to the object. Notifications are not displayed.

The actions selected by default are optimal for most uses. Do not change them unnecessarily.

Excluded paths

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

3.2.2. SpIDer Guard

SpIDer Guard performs constant real-time scanning of the file system, checks files as they are modified or saved, thereby protecting the system against security threats.

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

General

- Set the **Use heuristic analysis** flag to use heuristic analysis for detecting unknown threats.
- Set/clear the **Enable SpIDer Guard for OS X** (for servers—**Enable SpIDer Guard for OS X Server**) flag to enable/disable SpIDer Guard.
- In the **Scanning timeout** 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, select actions that will be applied automatically to computer threats detected by SpIDer Guard depending on their types:

- **Cure, move to quarantine if not cured**. Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- **Cure, delete if not cured**. Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- **Move to quarantine**. This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete**. It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- **Ignore**. No actions are applied to the object. Notifications are not displayed.

The actions selected by default are optimal for most uses. Do not change them unnecessarily.

Containers

In this section, specify the maximum nesting level for containers being checked. If the nesting level is higher than the specified value, the container will be ignored when scanning. Value 0 means that nested objects will not be checked.

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.

Appendix A. 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 from in the corresponding section at http://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.