Dr.WEB

Enterprise Security Suite

Managing Microsoft Exchange Server

Dr.Web Enterprise Security Suite. Managing Microsoft Exchange Server
Version 13.0
Administrator Manual
10/10/2023

Doctor Web Head Office

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

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

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

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

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

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 Microsoft Exchange Server 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 Microsoft Exchange Server 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/.

1.2. Conventions and Abbreviations

Conventions

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

Convention	Comment
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

Abbreviations

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

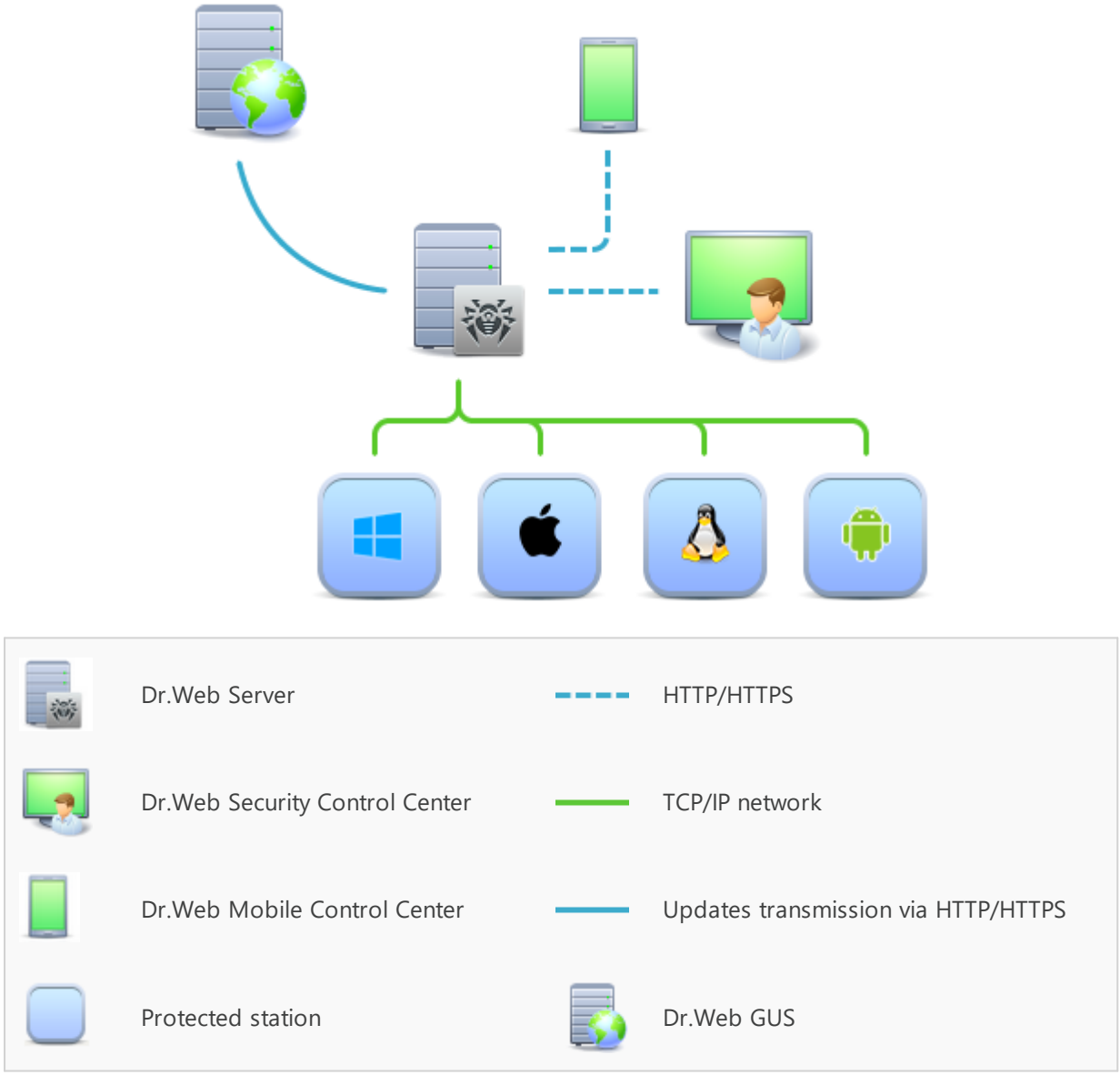
- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- LAN—Local Area Network,
- NAP—Network Access Protection,
- OS—Operating System.

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*.



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. Microsoft Exchange Servers Protection

Microsoft Exchange servers are protected by Dr.Web anti-virus packages.

Anti-virus packages are installed on protected servers and get connected to Dr.Web Server. Each server may be included in one or several groups registered on this Server. Microsoft Exchange servers and Dr.Web Server communicate via the protocol used in the local network (TCP/IP of 4 or 6 version).

Installation

Anti-virus package is installed on a server locally. Installation is implemented by administrator.

Management

When connection with Dr.Web Server is established, administrator is able to configure the Anti-virus on servers via the Control Center:

Update

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

In case a server is disconnected from the anti-virus network, the plug-in uses the local copy of settings and the anti-virus protection on a workstation retains its functionality (up to the expiry of the user's license). If Mobile mode is allowed at the anti-virus network node, after connection with the Server is lost, only the virus bases can be updated using the direct connection to the GUS servers. The plug-in software is not updated.

The principle of operation in the Mobile mode is described in the Dr.Web Enterprise Security Suite administrator manual, Mobile mode settings are described in the Dr.Web Agent for Windows user guide.

Chapter 3. Managing Dr.Web for Microsoft Exchange Server

3.1. Dr.Web for Microsoft Exchange Server

Enterprise Security Suite is an anti-virus plug-in designed to protect corporate mail systems against viruses and spam. It flexibly integrates into the system and processes each message and attachment dispatched to the server. All the messages are scanned before they are processed by the client part.

Enterprise Security Suite can perform the following functions:

- Scan all incoming and outgoing messages in real-time mode.
- Filter and block spam, use manually compiled black and white lists of addresses (if the anti-spam module is installed).
- Isolate infected and suspicious objects to quarantine.
- Filter email messages according to various criteria.
- Group clients to simplify their management.
- Log virus events in OS log and support an internal event database **cmstracedb**.
- Collect statistics.
- Support the common application settings on a distributed system of firewalls, including those organized in clusters.
- Automatically update virus databases and components of the plug-in.

To facilitate working with the plug-in, it is launched fully automatically (at system startup) and uses convenient update procedures (once added to the Windows Task Scheduler).

Enterprise Security Suite uses virus databases which are constantly supplemented with new records to assure up-to-date protection. Also, a heuristic analyzer is used for additional protection against unknown viruses.

The plug-in operates on the Dr.Web CMS (Central Management Service), which supports the central configuration of application settings and components and remote administration via protected protocol HTTPS. Dr.Web CMS features an internal web server Dr.Web CMS Web Console with client authentication, thus, only the authorized administrators can access the application settings.

The interaction between the components and their configuration is based on internal service protocols operating over TCP. Such service protocols allow Dr.Web CMS to connect the application components with the managing service database **cmsdb** and with the internal event database **cmstracedb** located in the plug-in installation folder and based on the SQLite database.

The interaction between the components and Dr.Web CMS platform is carried out in the following way:

1. The application component connects to Dr.Web CMS service via the service protocol over TCP on its start (if it is a service) or on its loading (if it a library).
2. Dr.Web CMS registers the application connection and creates a data structure related to the corresponding application component in the **cmsdb** database.
3. Dr.Web CMS controls the operation of the application component by constantly monitoring the TCP session and the service messages exchange with the component.
4. In case the component state changes, Dr.Web CMS modifies the corresponding variables in **cmsdb** database.

Dr.Web CMS services installed on different servers can be organized in a hierarchy tree by the administrator, to support replication of parameters of **cmsdb** database with the **Shared** attribute of the application working with Dr.Web CMS. The parameters are copied from the main server to the sub-server one, thus, the servers tree parameters can be configured on the main host.

3.2. Dr.Web for Microsoft Exchange Server 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 Windows OS or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **Plug-ins** subsection, select **Dr.Web for Microsoft Exchange Server**.
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.

Inherit settings from policy or parent group—remove personal settings of a station and inherit settings from a policy or parent group.

Copy settings from policy or parent group and set them as a personal—copy settings of this section from a policy or parent group and set them for selected stations. Inheritance is not set and stations settings considered as a personal.

Export settings from this section to the file—save all settings from this section to a file of a special format.

Import settings to this section from the file—replace all settings in this section with settings from the file of a special format.

5. After settings changes were made via the Control Center, click **Save** to accept the changes. The settings will be passed to the stations. If the stations were offline when changes are made, the settings will be passed when stations connect to the Server.

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

3.2.1. Configuring General Settings

On **General** tab you can configure **Dr.Web for Microsoft Exchange Server** plug-in:

- **Use heuristic analysis** option allows Dr.Web for Microsoft Exchange Server to detect suspicious objects that are most likely infected with the unknown viruses. The option is enabled by default. If this option is disabled, only the signature analysis is used for scanning;
- **Check archives** is intended for anti-virus scanning of archive attachments on MS Exchange Server. The option is enabled by default. If this option is disabled, archives are not checked;
- **Check installation packages** is intended for anti-virus scanning of installation packages on MS Exchange Server. The option is enabled by default. If this option is disabled, installation packages are not checked;
- **Treat crypted archives as bad objects** option is intended for scanning the archives that are password-protected, as damaged archives. The option is enabled by default. If this option is disabled, password-protected archives are checked normally.

As the workstation is connected, on **General** tab the additional field is displayed. It contains the link to administrative console for plug-in managing and appears in the following format: **URL of Dr.Web administrator console** <*address*>, where <*address*> is the network address of the administrative console.

This field is only displayed in case of workstation personal settings. In the case of propagated settings or group settings, this field is not displayed.

Malware group contains the following options:

- **Adware**

- **Dialers**
- **Hacktools**
- **Jokes**
- **Riskware**

The options of **Malware** group are disabled by default. To check the required malware groups, activate the corresponding options.

Actions groups contains the following options:

- **Infected**. This option is intended to perform an appropriate action on an object, identified by the plug-in as infected. The following actions are available:
  - **Move to quarantine**
  - **Delete**
  - **Archive**
- **Suspicious**. This option is intended to perform an appropriate action on an object, identified by the plug-in as suspicious. The following actions are available:
  - **Move to quarantine**
  - **Delete**
  - **Ignore**
  - **Archive**

After configuring the options and actions, click **Save** right upper of the workspace of the plug-in configuration page.

3.2.2. Configuring Anti-spam Parameters

On the **Antispam** tab, you can configure anti-spam settings for **Dr.Web for Microsoft Exchange Server**. To access anti-spam settings check the **Enable anti-spam** option.

Mark as spam group contains the following settings:

- **Email campaigns and advertising email**
- **Suspected spear-phishing attacks**
- **Social network messages**
- **Transactional emails**
- **Messages in Asian languages**

By default, options from **Mark as spam** group are disabled. Enable the corresponding options to move the groups of messages into spam.

Actions group contains the following settings:

- **Certainly spam**. This option is intended for performing an appropriate action on the object, defined as spam by the plug-in. The following actions are available:

- **Ignore**. With this action selected, the message, defined as spam, is passed to the mail client as usual, that is, without performing any action.
- **Add a prefix to headers of spam messages**. With this action selected, the subject of the message, defined as spam, contains the prefix defined in **Prefix** field.
- **Block**. With this action selected, the message, defined as spam, is blocked by the plug-in.
- **Redirect**. With this action selected, the message, defined as spam, is forwarded to the email address, specified in **Redirection address** field.
- **Move to junk**. With this action selected, the message, defined as spam, a **X-MS-Exchange-Organization-SCL** header is added, together with the message distrust index score. This header is recognized by Microsoft mail clients and Microsoft Exchange Server. If the score is between 4 and 7, the clients move such message to the **Junk** folder.

- **Probably spam**. This option is intended for performing an appropriate action on the object, defined as probable spam by the plug-in. The following actions are available:
  - **Ignore**. With this action selected, the message, defined as probable spam, is passed to the mail client as usual, that is, without performing any action.
  - **Add a prefix to headers of spam messages**. With this action selected, the subject of the message, defined as probable spam, contains the prefix, defined in **Prefix** field.
  - **Block**. With this action selected, the message, defined as probable spam, is blocked by the plug-in.
  - **Redirect**. With this action selected, the message, defined as probable spam, is forwarded to the email address, specified in **Redirection address** field.
  - **Move to junk**. With this action selected, the message, defined as probable spam, an **X-MS-Exchange-Organization-SCL** header is added, together with the message distrust index score. This header is recognized by Microsoft mail clients and Microsoft Exchange Server. If the score is between 4 and 7, the clients move such message to the Junk folder.
- **Unlikely spam**. This option is intended for performing an appropriate action on the object, defined as unlikely being a spam by the plug-in. The following actions are available:
  - **Ignore**. With this action selected, the message, defined as unlikely being a spam, is passed to the mail client as usual, that is, without performing any action.
  - **Add a prefix to headers of spam messages**. With this action selected, the subject of the message, defined as unlikely being a spam, contains the prefix, defined in **Prefix** field.
  - **Block**. With this action selected, the message, defined as unlikely being a spam, is blocked by the plug-in.
  - **Redirect**. With this action selected, the message, defined as unlikely being a spam, is forwarded to the email address, specified in **Redirection address** field.
  - **Move to junk**. With this action selected, the message, defined as unlikely being a spam, a **X-MS-Exchange-Organization-SCL** header is added, together with the message distrust index score. This header is recognized by Microsoft mail clients and Microsoft Exchange Server. If the score is between 4 and 7, the clients move such message to the **Junk** folder.

- **Redirection address**. This field is intended to specify the email address, where messages, defined as spam, or probable spam, or unlikely being a spam are forwarded. To specify a new address, enter it in this field.
- **Prefix**. This field is intended to specify the prefix for messages, defined as spam, or probable spam, or unlikely being a spam. Default value is: ***SPAM***. To change the prefix, enter the new prefix in this field.

Managing the DNS black list

To access the DNS black list settings, check the **Enable DNS black list** option. In the **Server response time-out (ms)** field specify general request timeout for all the selected DNSBL servers.

You can add a server to the DNS black list by clicking ✚. The **Add server** window opens. Specify the server name and spam score that will be assigned for the message sender's IP address match with the DNSBL entry. In the **Return codes** section specify a return code and the spam score that will be assigned when this return code is matched. Check the **Add to eventlog** option to log the entry with this return code to the Event log, then specify the minimum time interval between two log entries. To add more return codes, click the  button. To delete unneeded return codes, click the  button.

Click **Add** in the upper right of the window to save the changes.

Managing lists of trusted and distrusted email addresses

To access the trusted and distrusted email addresses list settings, check the **Use white and black lists** option.

- **Black list**. To add an address to a black list, enter the address in this field. To add more addresses to a black list, click the  button, the new field appears. To delete unneeded fields of a black list, click the  button.
- **White list**. To add an address to a white list, enter the address in this field. To add more addresses to a black list, click the  button, the new field appears. To delete unneeded fields of a white list, click the  button.

Dump messages group contains the following settings:

- **Dump messages marked as spam** option enables dumping of spam emails. Specify a folder to export dumps of spam emails, in the Export folder field. Dumps of spam emails will be stored in special files with `.txt` extension.
- **Dump messages not marked as spam** option enables dumping of non-spam emails. Specify a folder to export dumps of non-spam emails, in the Export folder field. Dumps of non-spam emails will be stored in special files with `.txt` extension.

After configuring the options and actions, click **Save** in the upper right of the workspace of the plug-in configuration page.

Appendix A. Technical Support

If you have a problem installing or using Doctor Web products, please try the following before contacting technical support:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- See the Frequently Asked Questions section at https://support.drweb.com/show_faq/.
- Browse the official Doctor Web forum at https://forum.drweb.com/.

If you haven't found a solution to your problem, you can request direct assistance from Doctor Web technical support specialists. Please use one of the options below:

- Fill out a web form in the appropriate section at https://support.drweb.com/.
- Call +7 (495) 789-45-86 (for customers in Moscow) or 8-800-333-79-32 (a toll-free line for customers within Russia).

For information on regional and international offices of Doctor Web, please visit the official website at https://company.drweb.com/contacts/offices/.