



**Dr.WEB®**

**Anti-virus**

**for Microsoft Exchange Server**

## **Administrator Manual**

Defend what you create

**© 2003-2013 Doctor Web. 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, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk 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 for Microsoft Exchange Server**

**Version 6.00.1**

**Administrator Manual**

**19.07.2013**

Doctor Web Head Office  
2-12A, 3rd str. Yamskogo polya  
Moscow, Russia  
125124

Web site: [www.drweb.com](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

<b>Document Conventions and Abbreviations</b>	<b>7</b>
<b>Introduction</b>	<b>9</b>
What is Dr.Web for Microsoft Exchange Server	9
Scanned Objects	11
<b>Licensing</b>	<b>12</b>
License Key File	12
Get Key File	13
License Update	14
<b>Anti-Virus Scanning for Microsoft Exchange Server</b>	<b>15</b>
Virus-Scanning Applications Based on VSAPI	15
Server Roles	16
Transport Agents	18
Principles of Operation of Dr.Web for Microsoft Exchange Server	19
Anti-Virus and Anti-Spam Checking Cycle	19
Quarantine	21
Virus Events Monitoring	21
<b>Installation and Removal</b>	<b>22</b>
System Requirements	23
Compatibility	25
Install Dr.Web for Microsoft Exchange Server	25
Remove Dr.Web for Microsoft Exchange Server	28
<b>Start to Use</b>	<b>29</b>



<b>Start Administrative Console</b>	<b>29</b>
<b>Start Administrator Web Console</b>	<b>31</b>
<b>Administration</b>	<b>33</b>
<b>Groups and Profiles</b>	<b>33</b>
<b>Create and Manage Profiles</b>	<b>34</b>
Profile Priority Level	<b>37</b>
Notifications	<b>37</b>
Scanning	<b>42</b>
Anti-Spam	<b>45</b>
Filtering	<b>48</b>
Accompanying Text	<b>51</b>
<b>Manage Groups of Clients</b>	<b>52</b>
Create Group	<b>53</b>
Form Group	<b>54</b>
<b>Manage Quarantine</b>	<b>58</b>
<b>View Statistics</b>	<b>61</b>
<b>Manage Distribution of Reports</b>	<b>63</b>
<b>Adjust General Settings</b>	<b>69</b>
<b>Update Virus Databases</b>	<b>73</b>
<b>Logging</b>	<b>74</b>
<b>Event Log</b>	<b>74</b>
<b>Installation Program Text Log</b>	<b>75</b>
<b>Text Log</b>	<b>76</b>
<b>Troubleshooting</b>	<b>77</b>
<b>Check Installation</b>	<b>77</b>
<b>Check Updater Functionality</b>	<b>78</b>




<b>Virus Detection Test</b>	<b>79</b>
<b>Spam Detection Test</b>	<b>80</b>
<b>Appendices</b>	<b>81</b>
<b>Appendix A. Updater's Command-Line Parameters</b>	<b>81</b>
<b>Appendix B. Microsoft Exchange Server Anti-Virus Scanning Settings</b>	<b>84</b>
<b>Appendix C. Operation in Central Protection Mode</b>	<b>88</b>
<b>Appendix D. Technical Support</b>	<b>91</b>
<b>Index</b>	<b>92</b>



# Document Conventions and Abbreviations

Depending on the context, **Dr.Web** can mean either the name of the company – **Doctor Web**, or the name of the product – **Dr.Web for Microsoft Exchange Server**.

The following conventions and symbols are used in this document:

Convention	Description
<b>Bold</b>	Names of buttons and other elements of the graphical user interface (GUI), and required user input that must be entered exactly as given in the guide.
<b>Green and bold</b>	Names of Dr.Web products and components.
<u>Green and underlined</u>	Hyperlinks to topics and web pages.
Monospace	Code examples, input to the command line and application output.
<i>Italic</i>	Placeholders which represent information that must be supplied by the user. For command-line input, it indicates parameter values.  In addition, it may indicate a term in position of a definition.
CAPITAL LETTERS	Names of keys and key sequences.
Plus sign («+»)	Indicates a combination of keys. For example, ALT+F1 means to hold down the ALT key while pressing the F1 key.
	A warning about potential errors or any other important comment.



The following abbreviations are used in the manual:

- AD – Active Directory
- CPU – Central Processing Unit
- HTML – Hypertext Mark-up Language
- HTTP – Hypertext Transfer Protocol
- GUI – Graphical User Interface
- OS – operating system
- RAM – Random Access Memory
- SMTP – Simple Mail Transfer Protocol
- SP1, SP2, etc. – Service Packs





# Introduction

Thank you for purchasing **Dr.Web for Microsoft Exchange Server**. This anti-virus product is a powerful tool against threats propagated through e-mail offering a reliable protection for computers and data inside a corporate network and using the most advanced technologies.

This manual is intended to help administrators of large corporate networks to install, adjust and manage **Dr.Web for Microsoft Exchange Server**, and contains information on all the main features of the software and contact details for technical support. Please read the manual through carefully before using the program.

## What is Dr.Web for Microsoft Exchange Server

**Dr.Web for Microsoft Exchange Server** 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. The scanning is carried out in memory buffers but not directly for the file system objects, that speeds up the process.

The important feature is that all incoming messages are processed in an order based on the scanning priority assigned to them. When a new message is located in the Microsoft Exchange Server Information Store, it is treated as a low priority object. As soon as a client attempts to access such message, the latter is reassigned to a high priority list and is processed in the first place. To ensure ultimate protection, outbound messages are processed prior to being passed to the client. Thus, changing of the messages priority provides perfect protection and efficient use of system resources.



**Dr.Web for Microsoft Exchange Server** also checks objects that are already located in the Microsoft Exchange Server Information Store, which considerably increases the scanning efficiency. Besides, 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).

**Dr.Web for Microsoft Exchange Server** 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
- Isolate infected and suspicious objects to **Quarantine**
- Filter e-mail messages according to various criteria
- Add accompanying text to outgoing external messages
- Group clients to simplify their management
- Send notifications on virus events and log them
- Distribute reports on the operation of the plug-in
- Collect statistics
- Automatically update virus databases and components of the plug-in

**Dr.Web for Microsoft Exchange Server** 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.



## Scanned Objects

**Dr.Web for Microsoft Exchange Server** scans incoming and outgoing messages in real-time mode. It checks the following elements of e-mail messages:

- Body of the message
- Attachments (including archived and packed files)
- Embedded OLE objects and messages

**Dr.Web for Microsoft Exchange Server** scans all objects before they are processed by the client part.



# Licensing

The use rights for the purchased product are regulated by the *license key* file.

## License Key File

The license key has the .key extension and contains, among other, the following information:

- Licensed period for the product
- List of components the user is allowed to use (e.g. the anti-spam feature can be enabled only in the «Anti-Virus&Anti-Spam» version)
- other restrictions (e.g. users number limitation for the license)

A *valid* license key file satisfies the following criteria:

- License is not expired
- The license applies to all components of the product
- Integrity of the license key file is not violated

If any of the conditions is violated, the license key file becomes *invalid*, **Dr.Web for Microsoft Exchange Server** stops detecting the malicious programs. License violation is registered in the Windows Event Log and in the text log of plug-in.



The key file has a write-protected format and must not be edited. Editing of the key file makes it invalid. Therefore, it is not recommended to open your key file with a text editor, which may accidentally corrupt it.

---



## Get Key File

You can receive a license key file in one of the following ways:

- By e-mail in an archived attachment
- With the plug-in distribution kit
- On separate media as a separate file with .key extension

The key file should be obtained before installing **Dr.Web for Microsoft Exchange Server**, as the installer requests the path to a key file.

### To acquire a license key file by e-mail

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. The license key file will be sent as an archived attachment to the e-mail address you specified in the registration form.
5. Extract the license key file and copy it to the computer where you plan to install **Dr.Web for Microsoft Exchange Server**.

For demonstrative purposes you may be provided with a *demo license key file*. Demo license allows you to access full functionality of the **Dr. Web for Microsoft Exchange Server** for a short-term period. No support is provided during trial period. On the expiration of the trial license, you will need to purchase a full license to continue working with the product.

To receive a demo license key file by e-mail, fill in the registration form at <http://download.drweb.com/demoreq/>.

To buy a license key file, you can either contact the nearest partner of **Doctor Web** or use the **Doctor Web** web store service at <http://buy.drweb.com/>.



For more information on licensing and types of license key files, visit the **Doctor Web** official web site at <http://www.drweb.com>.

## License Update

When license expires or security of your system is reinforced, you may need to update the license. The new license then should be registered with the product. **Dr.Web for Microsoft Exchange Server** supports hot license update without stopping or reinstalling the plug-in.

### To update the license key file

1. To update the license key file do the following:
  - Replace an old license key file with the new file in the plug-in installation folder (usually, %Program Files%\DrWeb for Exchange).
  - If Exchange server 2007/2010 is used, you need to replace the key file with the new one in the folder of Updater (C:\Program Files(x86)\DrWeb for Exchange\).
2. **Dr.Web for Microsoft Exchange Server** automatically switches to the new license.

For more information on license types, visit the **Doctor Web** official web site at <http://www.drweb.com>.



## Anti-Virus Scanning for Microsoft Exchange Server

The anti-virus plug-in **Dr.Web for Microsoft Exchange Server** supports the VSAPI (the Virus Scanning Application Programming Interface developed by Microsoft for Exchange Servers).

The plug-in checks all e-mail messages received by the Exchange Server (which include incoming, outgoing and internal messages) for viruses and spam (the anti-spam feature is available with the «Anti-Virus&Anti-Spam» license and only for e-mails received by the server via SMTP).

**Dr.Web for Microsoft Exchange Server** also supports such concepts of Exchange 2007/2010 organization as [server roles](#) and [transport agents](#) and can be installed on the servers with different roles, while the scanning for viruses and spam can be performed on the level of transport agents as well as on the level of VSAPI supporting component.

## Virus-Scanning Applications Based on VSAPI

VSAPI-based anti-virus solutions for Exchange Servers check all e-mail messages received by the server before they are delivered to the clients. Viruses are searched in three modes:

- Proactive
- On-demand
- Background



### Proactive scanning

All e-mail messages received by the Exchange Server are queued to be checked by the anti-virus plug-in. All messages in the queue receive the same low priority. If this priority doesn't change then the check proceeds on the «first in, first out» (FIFO) basis.

### On-demand scanning

If the priority assigned to the message changes to the high one, that occurs in case a mail client tries to access the message, then it would be processed earlier, because the queue is treated by several threads. The initial low priority of incoming messages guaranties that their check would not interfere the processing of high priority messages.

Proactive and on-demand scanning processes ensure checking all the messages passing the server, the priority system allowing to optimize the server load and clients' waiting time.

### Background scanning

In the background scanning mode, messages located in the Information Store are checked, thus the viruses that have passed to the Store before the installation of **Dr.Web for Microsoft Exchange Server** and the previously unknown viruses in the messages checked before the last updating of virus databases can be detected. The Exchange administrator can start this mode by means of a set of registry keys.

For more information on the settings of anti-virus scanning based on VSAPI see [Appendix B](#).

## Server Roles

Exchange Server 2007/2010 can be installed in different configurations determining the server operation modes and functionality. For this purpose, the server roles are specified during the deployment.





Exchange Server 2007/2010 includes 5 server roles: Mailbox Server, Client Access Server, Hub Transport Server, Unified Messaging Server and Edge Transport Server. Three of them support anti-virus and anti-spam scanning – Edge Transport, Hub Transport and Mailbox:

1. **Mailbox Server** provides the main services, hosts mailbox and public folder databases and allows to perform the anti-virus scanning via VSAPI.
2. **Hub Transport Server** routes mail within the Exchange organization, allows to apply security policies to the messages and check them for viruses and spam.
3. **Edge Transport Server** is a standalone server situated in the demilitarized zone (DMZ) that doesn't access to the internal organization resources (except one-way synchronization with Active Directory for the purposes of Hub Transport Servers topology registration), that allows to provide anti-virus and anti-spam protection.

**Dr.Web for Microsoft Exchange Server** can be installed on the server with any of these roles or their combinations.

### Anti-virus protection for different server roles

Edge Transport Server is deployed in the organization's perimeter network and routes messages coming to and from the Exchange organization. That is why the anti-virus protection on this level is significant. As the check for viruses and spam is performed by **Dr.Web for Microsoft Exchange Server** on the transport level, you need to register only program's transport agents during the installation.

To increase the efficiency of protection, the anti-virus application **Dr. Web for Microsoft Exchange Server** can be deployed also on the Hub Transport Server and perform the scanning for viruses and spam on the transport level.



Mailbox Server operates with Exchange Information Stores and provide the anti-virus check only via VSAPI, therefore the installation of **Dr. Web for Microsoft Exchange Server** on this server allows to protect the objects that are not transferred via transport and are not protected from viruses on the transport level, e.g. the public folders, sent messages and calendar events.

## Transport Agents

The concept of Exchange 2007/2010 organization bases on modified SMTP events structure. The messages are processed on the stages of SMTP-transport by transport agents that perform different functions.

When a message comes to the server, it is transferred through the SMTP-transport network, and on each SMTP-event several transport agents can be registered. Transport agents can access to the the messages and perform specific actions on them. Each transport agent performs its own check and transmit the message to the next agent. So, transport agents can react on the events related to the receiving of the message and its further routing.

There are two different types of transport agents:

- **SMTP Receive Agent** – allows to react on the events of message receiving.
- **Routing Agent** – allows to react on the events of message routing.

Exchange Server 2007/2010 allows to set the priority to transport agents and manage the order of agents applied to the messages. Therefore, the sequence of transport agents is defined not only by the order of the events, but also by their priorities within the same SMTP-event.

Transport agents allow to implement special software into the Exchange Server for e-mail processing, anti-virus and anti-spam check.



## Principles of Operation of Dr.Web for Microsoft Exchange Server

All **Dr.Web** anti-virus solutions use the following general components that provide the protection of all operating systems and platforms: the virus scanning engine **drweb32.dll** and regularly updated virus database files (with the **.vdb** extension) which store virus records that contain information about the viruses and other malware.

The anti-virus and anti-spam solution **Dr.Web for Microsoft Exchange Server** is based on the VSAPI and integrates **Dr.Web** technologies in the e-mail processing and storing process on Exchange Servers.

The product has a convenient graphical user interface to facilitate management of scanning settings and check results monitoring. For more information about the settings, see [Administration](#).

## Anti-Virus and Anti-Spam Checking Cycle

After a notification that a new message has been received by the server, the message is processed in the following three stages:

1. **Spam check** (performed in case you have the «Anti-Virus&Anti-Spam» license and only for the e-mails received by the server via SMTP, adjusted on the [Anti-Spam](#) section).

In the first place the addresses of the recipients and senders are analysed against the black and white lists, which are specified on the [Settings](#) section. Then the anti-spam filter **Vade Retro** checks the message body and issues a decision that determines the grade of possibility that this message is spam. If the message is spam, the administrator or other persons are notified of the event (in case of corresponding settings on the [Notifications](#) section), the message is handled according to the action set by the administrator for this spam category on the [Anti-Spam](#) section.



2. **Application of filtering rules** (adjusted on the [Filtering](#) section).
  - A. Anti-distribution rules (restriction of distribution lists). You can set rules to limit the number of recipients for the messages (or the messages with attachments). These rules are applied to the senders and allow sending only for the messages, the number of recipients of which doesn't exceed the specified maximum value.
  - B. Attached files filtering rules. You can set rules to remove certain types of attachments: by the extension, file name mask or maximum file size.

Provided that one of the set rules applies, the message (or the attachment) is removed, and (if it is set on the [Notifications](#) section) the administrator or other persons are notified about the event. In case an attached file is deleted it is replaced by a text file with a message that the attachment was deleted. The message template and the file name of such message are also set on the [Filtering](#) section.

3. **Virus check** (adjusted on the [Scanning](#) section).

Messages that have successfully passed the previous stages of checking (or have been passed according to the settings of the **Dr.Web** plug-in) are submitted to be analyzed for malicious code occurrence. If an item (an attachment or message body) contains malicious code, the anti-virus attempts to cure the item. If the heuristic analyzer is enabled in the settings, it implements the detection of the objects containing modified or unknown malicious code and assigns the **Suspicious** category to such objects.

Based on the scan results the items receive the categories (e.g. **Not Cured, Suspicious, Bad, Cured**) and then are treated based on such conclusion. Messages with infected objects receive a text file attachment with information about the detected infection and the actions applied to such objects.

Cured and uninfected items are passed to the server with the respective mark. Not cured, bad and suspicious objects are processed according to the settings on the [Scanning](#) section.



The administrator may be notified of all types of virus events if it is set on the [Notifications](#) section.

## Quarantine

To not cured, bad and suspicious objects the **Quarantine attachment** action may be applied. The objects of such types will be placed in a database serving as a quarantine, that blocks the executing of the objects' code by all system applications. You can receive information about quarantined objects on the [Quarantine](#) section.

## Virus Events Monitoring

To provide the administrator and/or other interested persons with information about the events, monitored by **Dr.Web for Microsoft Exchange Server**, administrator may adjust the event notification system that comprises the following features:

- [Mail Notifications](#). The administrator, as well as message recipients and senders may be notified in the event the message contained cured, not cured, filtered, bad objects and/or was spam (every event and notification recipient is optional).
- [Event Log](#). Such events as server's reception of messages that contained objects which had been cured, not cured, filtered or categorized as bad objects or spam can be logged (logging every event is optional). To see these events use the Windows **Event Viewer** -> **Application** utility.
- [Reports](#). The reports about selected types of virus events may be sent to a predetermined list of recipients by e-mail.
- [Statistics](#). It gives the possibility to view the information about a number of objects checked since the installation of **Dr.Web for Microsoft Exchange Server** or the last cleaning of statistics data. Besides, the list of messages processed by the application and that contained viruses or were spam, as well as the filtered messages, is also available in this section (the Incidents tab).



# Installation and Removal

The **Dr.Web for Microsoft Exchange Server** software is distributed as a ZIP-archived folder containing the installation file **drweb-exchange-20002003-en.msi** and **drweb-exchange-20072010-en.msi** for different versions of Exchange server.

Extract the installation file to a folder on the local drive of the Exchange server.



For proper installation and removal of **Dr.Web for Microsoft Exchange Server** the user must be added to the Domain Users group and the local administrators group on the computer where Microsoft Exchange Server is installed.

If you are using the Windows Terminal Services component, it is recommended to use the **Add or Remove programs** utility to install and uninstall the **Dr.Web for Microsoft Exchange Server** software.

In case you're reinstalling the application and the server operates under load, it is recommended to firstly stop the following services:

- Microsoft Exchange Information Store
- Inetinfo
- Dr.Web Core Services for MSP
- Dr.Web Core Services for MSP Attendant

On completion the installation you need to start Microsoft Exchange Information Store service manually, all other services will start automatically.



## System Requirements

This section provides system requirements for installation and proper operation of **Dr.Web for Microsoft Exchange Server** on your computer.

### Hardware requirements

Specification	Requirement	
	in case Microsoft Exchange Server 2000/2003 is used	in case Microsoft Exchange Server 2007/2010 is used
CPU	Pentium 133 MHz (733 MHz recommended)	One of the following processors: <ul style="list-style-type: none"><li>• Intel processor that supports Intel 64 architecture</li><li>• AMD processor that supports the AMD64 platform</li></ul>
RAM	256 MB or more (512 MB recommended)	2 GB
Disk space	280 MB	265 MB
Monitor	VGA-compatible monitor	



## Operating system and software requirements

Specification	Requirement	
	in case Microsoft Exchange 2000/2003 is used	in case Microsoft Exchange 2007/2010 is used
Operating system	One of the following: <ul style="list-style-type: none"><li>• Microsoft® Windows® 2000 Server or Advanced Server with SP4</li><li>• Microsoft® Windows Server® 2003 Standard, Enterprise or Datacenter edition with SP1 or higher</li></ul>	One of the following: <ul style="list-style-type: none"><li>• Microsoft® Windows Server® 2003 R2 x64 with SP2</li><li>• Microsoft® Windows Server® 2008 x64</li><li>• Microsoft® Windows Server® 2008 R2</li></ul>
File system	NTFS or FAT32	NTFS
Exchange software	Microsoft® Exchange Server 2000/2003 Standard or Enterprise edition	Microsoft® Exchange Server 2007 x64 with SP1 or Microsoft® Exchange Server 2010 x64
Additional software	Microsoft® Windows Installer 3.1 or higher	
	Microsoft .NET Framework 3.5 (for correct operation of <b>Administrator Web Console</b> )	



If Exchange Server 2000/2003 is used, to install **Dr.Web for Microsoft Exchange Server** under Windows 2000, Internet Explorer 6 is required.





## Compatibility

Before installation of **Dr.Web for Microsoft Exchange Server** please review the following information on product compatibility:

1. **Dr.Web for Microsoft Exchange Server** of version 6.00.1 is compatible only with **Dr.Web** products of version 6.
2. **Dr.Web for Microsoft Exchange Server** is not compatible with other anti-virus software. Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have an earlier version of **Dr.Web for Microsoft Exchange Server** or other anti-virus software installed then it is necessary to uninstall it using the installation file or standard tools of the OS (cm. [Remove Dr.Web for Microsoft Exchange Server](#)).

## Install Dr.Web for Microsoft Exchange Server

### Before installation it is strongly recommended:

- To install all critical updates released by Microsoft for the OS version used on your computer (available on the company's updating website at <http://windowsupdate.microsoft.com>).
- To check the file system with the system utilities and remove the detected defects.
- To close all active applications.



---

If you're installing version 6.00.1 of **Dr.Web for Microsoft Exchange Server** and want to save the profiles settings from the previous application version, export the program settings to a configuration file before uninstalling it. You can import the settings from this file to use them with the new version of application. To save settings, right-click the name of the server in the [Console](#) or [Web Console](#) tree and select the corresponding item.

---



## To install Dr.Web for Microsoft Exchange Server

1. Run the installation file **drweb-exchange-20002003-en.msi** or **drweb-exchange-20072010-en.msi** depending on the Exchange server version you are using. The InstallShield Wizard will open on the first window of the installation process. Click **Next** to continue.
2. A window with the text of the License Agreement will open. To continue installation you should read and accept the license by selecting **I accept the terms in the license agreement**. Click **Next**.
3. Choose the type of installation by selecting **Complete** or **Custom**. Click **Next**.
4. If you chose **Custom** installation then a window for selecting the components you wish to be installed will open. Make the necessary changes and click **Next**. If you chose **Complete** then just move on to the next step.
5. Depending on whether **Dr.Web Agent** is installed in the system, you proceed with one of the following steps:
  - in case **Dr.Web Agent** is not installed and plug-in is going to operate in the standalone mode, specify the path to a valid key file in the **License key file** window.



If you do not have a valid key file then click **Get key file** to go to the license key file request page on the **Doctor Web** web site at <http://www.drweb.com>.

---

- if **Dr.Web Agent** is installed in the system, the plug-in installation continues in the central protection mode which does not require a specific license key file for **Dr.Web for Microsoft Exchange Server**. The license key file registered in the anti-virus network for the specified station will be received by **Dr.Web Agent** from **Dr.Web Control Center**. For detailed information on the central protection mode, see [Appendix C](#).

Click **Next**.



6. Specify the User Principal Name (UPN) and password of the user account which will be used for sending the notifications. The specified user must have the mailbox on the Exchange server.



The specified account must have local system administrator rights.

---

Click **Next**.

7. Specify the e-mail address of the server administrator. Notifications will be sent to this address. Click **Next**.
8. If you are re-installing **Dr.Web for Microsoft Exchange Server** and the database of the previous installation is found, you can delete it by selecting the corresponding check box. If Microsoft Exchange 2000/2003 is used, you can also enable the transport scanning.
9. Click **Install** to begin installation of **Dr.Web for Microsoft Exchange Server** on your computer. By default, program files are copied to C:\Program Files\DrWeb for Exchange.
10. Further actions of the InstallShield Wizard do not require user interference. Once the installation is complete, click **Finish**.



## Remove Dr.Web for Microsoft Exchange Server

### To uninstall Dr.Web for Microsoft Exchange Server

1. Run the installation file **drweb-exchange-20002003-en.msi** or **drweb-exchange-20072010-en.msi** depending on the Exchange server version you are using. The InstallShield Wizard will open on the first window of the installation process. Click **Next**.



Alternatively you can use the **Add or Remove programs** utility on the Windows Control Panel.

---

2. Select **Remove** and click **Next**.
3. In the opened window, click **Remove**.
4. Once removal is complete, click **Close**.



## Start to Use

This chapter contains information on how to start the [Administrative Console](#) and the [Administrator Web Console](#) to configure the plug-in operation.

## Start Administrative Console

Operation of **Dr.Web for Microsoft Exchange Server** can be configured by means of the **Administrative Console** (see [Figure 1](#)).

### To launch the Administrative Console

1. Click **Start** on the Windows toolbar and select **All Programs**.
2. Select **Doctor Web** -> **DrWeb for Microsoft Exchange** -> **Dr.Web for Exchange Administrative Console**.

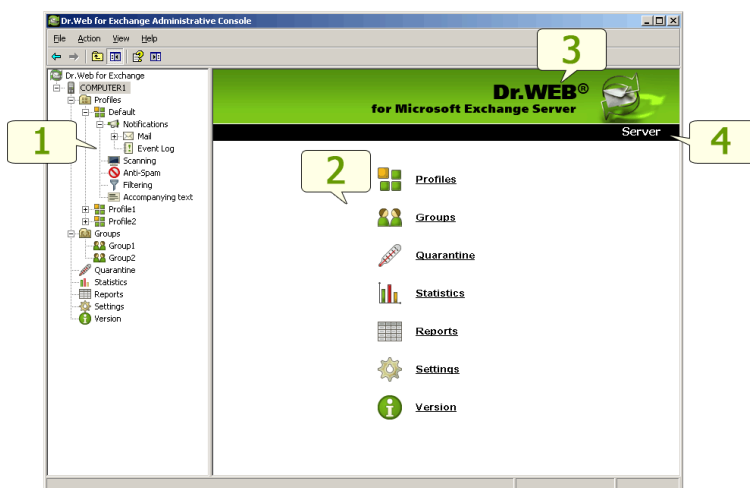


---

Alternatively, the **Administrative Console** can be opened by double-clicking the executable file of the Console (**drwexch.msc**) which is by default located in the C:\Program Files\DrWeb for Exchange folder.

---

By default, the **Administrative Console** opens on the last section you have previously worked with.



**Figure 1. Administrative Console**

The **Administrative Console** consists of two parts:

1. Console tree, which is used for navigation between different sections of the program settings.
2. Details pane, which represents the working area where the settings of the currently selected section are displayed and can be adjusted.

At the top of the details pane the **Dr.Web for Microsoft Exchange Server** name and logo (3) and the name of the current section (4) are located.



All your current **Dr.Web for Microsoft Exchange Server** settings can be saved to a special configuration file and loaded from it in case you will have to reinstall the plug-in or use your settings on another computer. For this right-click the name of the server in the Console tree (e.g. **COMPUTER1** on the illustration above) and select the corresponding item.



## Start Administrator Web Console



For correct operation of **Administrator Web Console** use one of the following browsers:

- Internet Explorer 8 or higher
- Mozilla Firefox 3.5 or higher

To launch **Administrator Web Console** (see [Figure 2](#)) do one of the following actions:

- If **Dr.Web for Microsoft Exchange Server** operates in the central protection mode, you can launch **Administrator Web Console** from **Dr.Web Control Center**;
- If the program operates in the standalone mode and Microsoft Exchange Server 2000/2003 is installed, in an Internet browser open the following page:

```
http://<Exchange Server address>/DrWebAccess/
```

or

```
http://<Exchange Server address>/DrWebAccess/  
DrWebForExchange.aspx,
```

where *<Exchange Server address>* is the IP-address of the Exchange server.

- If the program operates in the standalone mode and Microsoft Exchange Server 2007/2010 is installed, in an Internet browser open the following page:

```
https://<Exchange Server address>/DrWebAccess/
```

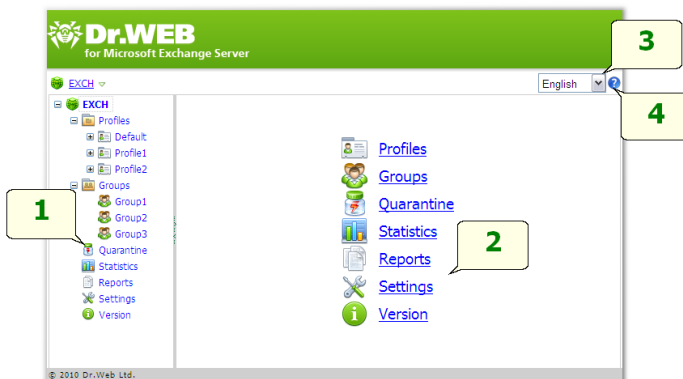
or

```
https://<Exchange Server address>/DrWebAccess/  
DrWebForExchange.aspx,
```

where *<Exchange Server address>* is the IP-address of the Exchange server.



To access to the web console page, you need to enter the administrator login and password.



**Figure 2. Administrator Web Console**

The **Administrator Web Console** consists of two parts:

1. Web Console tree (1).
2. Details pane (2).

At the top of the details pane the **Administrator Web Console** language changing option (3) is located. You can select English or Russian language.

To the right of the language option the option which opens the help on the web-console (4) is located.





# Administration

This chapter contains information on the structure of **Dr.Web for Microsoft Exchange Server** and performing all the administrative tasks required to ensure the ultimate protection for your Exchange environment.

## Groups and Profiles

To simplify management of your Exchange environment **Dr.Web for Microsoft Exchange Server** provides the ability to form groups of clients and assign profiles to them. A profile is a set of adjustable message processing settings which determine the manner of protection of your Exchange environment. The settings of a profile can be found in the **Profiles** section of the Console/Web Console tree and are divided into the following subsections:

- [Notifications](#) – this section allows you to set up notifications which can be used to keep the administrator and other users informed about various events (e.g. detection of infected or suspicious messages, attempts to cure them, filtering of messages, etc.).
- [Scanning](#) – this section allows you to control the operation of your main virus-detection component.
- [Anti-Spam](#) – this section allows you to adjust the operation of the **Anti-Spam** component (settings in this section can be enabled only with the «Anti-Virus&Anti-Spam» version of **Dr.Web for Microsoft Exchange Server**, i.e. if you have an appropriate license key file (see [License Key File](#))).
- [Filtering](#) – this section allows you to create filtering rules for e-mail messages.
- [Accompanying Text](#) – this section allows you to arrange adding text to all outbound e-mail messages.

For more information on creating and managing profiles, please refer to [Creating and Managing Profiles](#).

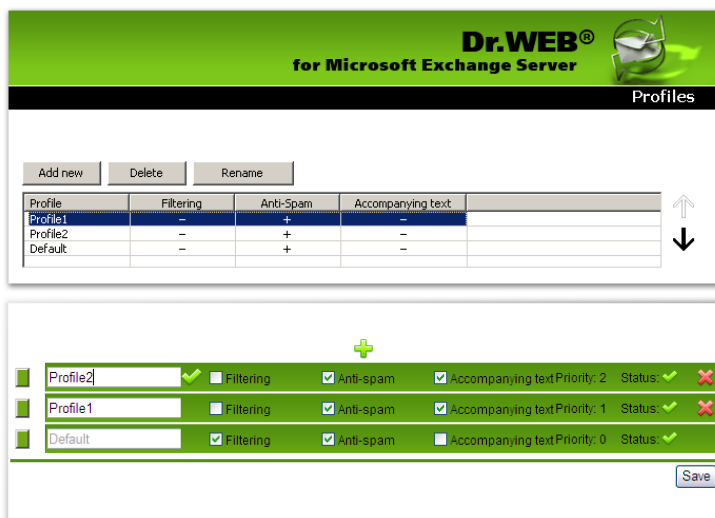


Any profile can be assigned to a certain group of clients. These groups are formed in the **Groups** section of the Console tree (see [Managing Groups of Clients](#)).

## Create and Manage Profiles

During installation of **Dr.Web for Microsoft Exchange Server** the **Default** profile, which cannot be renamed or deleted, is created automatically. This profile will remain active for all Exchange clients as long as you do not create a new profile and assign it to a certain group. When you create a new profile, it has current settings of the **Default** profile.

To manage the existing profiles and create the new ones the **Profiles** pane is used. To open it select **Profiles** in the Console/Web Console tree (see [Figures 3, 4](#)).



**Figures 3 and 4. Profiles pane**

For each profile the information on its settings and priority is displayed in the list.



## To create a new profile

- Click **Add new** or the  button above the list of available profiles on the **Profiles** pane.




Alternatively, if you are using **Administrative Console**, to create a new profile, you can right-click **Profiles** in the Console tree and select **Add profile** (see illustration below).




A new profile named **Profile1** will be created and will appear under **Profiles** in the Console tree. If this name is already used, it will be named **Profile2** and so on.

## To change the name of a profile

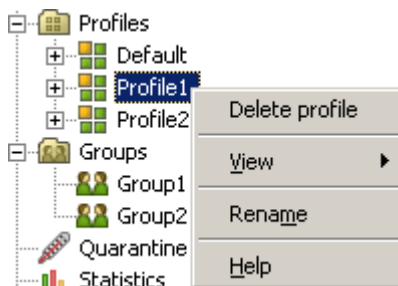
- If you are using **Administrative Console**, select the profile on the **Profiles** pane and click **Rename**.
- If **Administrator Web Console** is used, enter the new name of the profile into the corresponding text field and then click the **Rename** button .

## To delete a profile

- Select it on the **Profiles** pane and click **Delete** or the  button.



Alternatively, if you are using **Administrative Console**, to rename or delete a profile, you can right-click it in the Console tree and select the corresponding item (see illustration below).



By default, a new profile has the same settings as those specified for the **Default** profile.

### To change profile settings



- Click the name of the profile in the Console tree and select the necessary settings section: [Notifications](#), [Scanning](#), [Anti-Spam](#), [Filtering](#) or [Accompanying Text](#).



## Profile Priority Level

Each profile has a certain priority level set by the administrator. If a client is a member of several groups with different profiles, then the profile with the highest priority will be applied when processing messages sent to or by this client.

The priority level is adjusted on the **Profiles** pane by moving profiles up and down the list:

- If you are using **Administrative Console**, use the buttons  and  to move the profile.
- If you are using **Administrator Web Console**, use the button to the left of the profile's name to drag a profile to a new position.

The higher a profile is on the list, the higher is its priority.



The **Default** profile always has the lowest priority level and cannot be moved higher than the lowest position in the list.

---

## Notifications

Notifications are used to keep the administrator and other users informed about various events (e.g. detection of infected or suspicious objects, attempts to cure them, filtering of messages, etc.). There are two notification methods: notifications via mail and logging of events.



By default, events logging is enabled for all types of events, and mail notifications are sent to the administrator on all events except spam.

---



## To configure mail notifications

1. Click **Mail** on the **Notifications** pane or **Mail** under **Notifications** in the Console/Web Console tree.
2. On the **Mail** pane, click the type of object for which you wish to adjust notifications (**Cured**, **Not Cured**, **Spam**, **Filtered**, **Suspicious** or **Bad**).
3. A pane for editing parameters of notifications for the selected type of objects will open (see [Figures 5, 6](#)).

The screenshot shows the 'Dr.WEB® for Microsoft Exchange Server' configuration window. The title bar is green with the Dr.Web logo and a green envelope icon. Below the title bar is a black navigation bar with three tabs: 'Administrator' (selected), 'Sender', and 'Recipient'. To the right of the tabs is the text 'Cured messages'. The main content area is white. At the top, there is a checkbox labeled 'Send mail notifications to the administrator' which is checked. Below this, there is a section titled 'Adjust the structure of mail notifications for the administrator'. This section contains three input fields: 'Subject:' with the text 'Dr.Web for Exchange has detected a virus!', 'Body:' with a text area containing 'Dr.Web for Exchange has detected that %ObjectType% is infected with a virus. The %ObjectType% is now %State%. %NewLine%File name:' and a 'Macro...' button to its right, and 'Recipients:' with the text 'Administrator@EXCHSRV-WORK.com'. At the bottom right of the window is a 'Save' button.



**Administrator**

☒ Send notifications to administrator by mail

Configure notification settings for administrator

Subject: Dr.Web for Exchange detected a virus!

Macros: ObjectType

Body: Dr.Web for Exchange detected a virus in %ObjectType%. %  
ObjectType% %State% %NewLine% File name: %File Name% %NewLine%  
Viruses% %NewLine% Message subject: %Message subject% %NewLine% From: %  
MessageSender% %NewLine% To: %MessageRecipients% %NewLine% Carbon  
Copy Recipients: %Carbon Copy Recipients%

Recipient: administrator@exchsnv-work.com

**Sender**

**Recipient**

**Figures 5 and 6. Configure notifications pane**

Using the three tabs/sections on the details pane, you can configure the notifications to administrator, sender and recipient of messages.

4. By selecting the **Send mail notifications to ...** option, you can enable/disable sending notifications on the selected types of objects to the different recipients. The following parameters of the notification message can be configured:
  - Subject of the notification message
  - Body of the notification template. You can use macros while editing the text (e.g. %FileName% adds the name of the file to the text)
  - E-mail addresses of the recipients of notifications
5. When you are done, click **Save**.



## To configure events logging

1. Click **Event Log** on the **Notifications** pane or **Event Log** under **Notifications** in the Console/Web Console tree.
2. To enable logging for any type of objects, select **Enable** against the corresponding object type (e.g. in [Figures 7, 8](#) the event log notifications are enabled for **Not Cured**, **Filtered**, **Suspicious** and **Bad** e-mails and disabled for **Cured** and **Spam**).

**Dr.WEB®**  
for Microsoft Exchange Server

**Event Log**

**Cured**

☐ Enable  
Message body: File %FileName% was infected with a virus and has been %State% by Dr. Web for Exchange%NewLine%%Viruses%%NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

**Not Cured**

☒ Enable  
Message body: File %FileName% was infected with a virus and has been %State% by Dr. Web for Exchange%NewLine%%Viruses%%NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

**Spam**

☐ Enable  
Message body: Dr. Web for Exchange detected spam. %NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

**Filtered**

☒ Enable  
Message body: Dr. Web for Exchange has filtered %ObjectType%. The %ObjectType% is now deleted. %NewLine%File name: %FileName%%NewLine%Filtering details: %FilteringDetails%%NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

**Suspicious objects**

☒ Enable  
Message body: Dr. Web for Exchange has detected that %ObjectType% is suspicious. The %ObjectType% is now %State%. %NewLine%File name: %FileName%%NewLine%Viruses%%NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

**Bad objects**

☒ Enable  
Message body: File %FileName% was bad and has been %State% by Dr. Web for Exchange%NewLine%%Viruses%%NewLine%Message subject: %MessageSubject%%NewLine%Sent from: %MessageSender%%NewLine%Recipients: %MessageRecipients%%NewLine%Carbon Copy Recipients: %CarbonCopyRecipients%

Save





**Cured**

Macros:

☐ Enable

Message text:

**Not Cured**

Macros:

☒ Enable

Message text:

**Spam**

Macros:

☐ Enable

Message text:

**Filtered**

Macros:

☒ Enable

Message text:

**Suspicious**

**Bad**

**Figures 7 and 8. Events log pane**

3. In the **Message body** field, you can edit the predefined notification template for the log entry if necessary. You can use macros while editing the text.
4. When you are done, click **Save**.



## Scanning

The scanning process is adjusted in the **Scanning** section of the profile settings. Changes in this section affect the types of checked objects and therefore they determine the protection level. On the other part, increasing of the number of identified objects' types leads to decrease in server performance.

### To adjust the settings of the scanning process

1. Click **Scanning** under the desired profile in the Console/Web Console tree. The **Scanning** pane will open (see [Figures 9, 10](#)).

The screenshot shows the 'Scanning' configuration window for Dr.Web for Microsoft Exchange Server. The window has a green header with the product name and a 'Scanning' tab. The settings are organized into several sections:

- Enable heuristic analysis:** A checked checkbox.
- Check archives:** A checked checkbox.
- Timeout:** A text box containing '10000' with 'ms' as the unit.
- Treat crypted archives as bad objects:** An unchecked checkbox.
- Scan for:** A section with two columns of checkboxes:
  - Left column: ☐ Riskware, ☐ Dialers, ☐ Hacktools.
  - Right column: ☐ Adware, ☐ Jokes.
- Select action:** A section with two dropdown menus:
  - For incurable and bad objects: 'Delete attachment'.
  - For suspicious objects: 'Quarantine attachment'.
- Attach the following file to infected messages:** A section with:
  - File name suffix:** A text box containing '\_infected.txt'.
  - Text:** A text area containing the message: 'File %FileName% was infected with a virus and has been %State% by Dr.Web for Exchange%NewLine%%Viruses%'. To the right of the text area is a 'Macro...' button.

A 'Save' button is located at the bottom right of the window.



☒ Enable heuristic analysis      Timeout: 10000ms  
☒ Check archives      ☐ Process encrypted archives as bad objects

Scan for

☒ Riskware      ☐ Adware  
☐ Dialers      ☒ Jokes  
☐ Hacktools

Select action

For not cured and bad objects: Delete attachment      For suspicious objects: Move to quarantine

Attach the following file to infected messages

File name suffix: \_infected.txt      Macros: ObjectType      Insert

Text: Infected file %FileName% was %State% by Dr.Web for Exchange%NewLine%%Viruses%

Save

**Figures 9 and 10. Scanning pane**

- By default, the heuristic analyzer and scanning of archives in attachments are enabled. This gives a high level of protection at the expense of the server performance. To disable these features, clear the **Enable heuristic analysis** and **Check archives** options at the top of the **Scanning** pane.



It is not recommended to disable the heuristic analyzer and scanning of archives in attachments as it considerably decreases the protection level of the server.

The **Timeout** field allows to specify the timeout for scanning of a single file. If this timeout is exceeded during the scanning, the file is considered as bad object. By default, the timeout is set to 10000 ms. If necessary, you can change this value.

The **Process encrypted archives as bad objects** option defines whether encrypted archives should be ignored by the scanner or treated by the plug-in as bad objects.

- In the **Scan for** group box below, select the types of objects to check messages for.



4. In the **Select Action** section below, use the drop-down lists to choose the actions for incurable, bad and suspicious objects. You can choose from the following:
- **Block in mailbox** – means that the message will be blocked in the mailbox on the server.
  - **Delete attachment** – means that the message body will be passed through and the attachment will be deleted.
  - **Quarantine attachment** – means that the message body will be passed through and the attachment will be sent to the quarantine (see [Managing the Quarantine](#)).
  - **Request to delete** – means that **Dr.Web for Microsoft Exchange Server** will request the server to delete the message (result will depend on the settings of the Exchange server).
  - **Pass through** – means that such objects will be passed on to the recipient(s) untouched (available only for suspicious objects).



By default, for incurable and bad objects the action **Delete attachment** is set and **Quarantine attachment** is set for suspicious objects.

---

5. In the **Attach the following file to infected messages** group box, you can change the name suffix for the text file which will be attached to an infected e-mail message after the assigned action is performed over it. In the **Text** field below, you can edit the text of the attached text file template, if necessary. You can add macros from the **Macro** list while editing the text.
6. When you finish configuring scanning process, click **Save**.



## Anti-Spam

The **Anti-spam** is configured in the **Anti-Spam** section of the profile settings and it is available only with the «Anti-Virus&Anti-Spam» version of **Dr.Web for Microsoft Exchange Server**. If your key file supports the **Anti-spam** component then spam filtering should be enabled by default, i.e. the **Enable** check box at the top of the **Anti-Spam** pane should be selected.



If all the settings in the **Anti-Spam** section are disabled, it is likely that your license key file does not support the **Anti-spam** component (see [License Key File](#)). To check whether the **Anti-spam** component is supported you can open the key file (**C:\Program Files\DrWeb for Exchange\drweb32.key**) with a text editor and look for the value of the parameter `SpamFilter`. If `SpamFilter=Yes`, then your license supports the **Anti-spam** component, if `SpamFilter=No`, then this component is not supported.

Any editing of the key file makes it invalid!

The **Anti-spam** component analyzes the contents of e-mail messages and defines whether it is spam or not according to the spam-rate value summed up from various criteria.

### To configure the settings of the Anti-Spam component

1. Click **Anti-spam** under one of the profiles in the Console/Web Console tree. The Anti-spam settings pane will open (see [Figures 11, 12](#)).



**Dr.WEB®**  
для Microsoft Exchange Server

**Spam**


☒ Enable

☐ Add predefined SMTP headers


Subject prefix:

Predefined spam recipient:


**Certainly spam**

 Action:  ☐ Add prefix to subject

**Probably spam**

 Action:  ☒ Add prefix to subject

**Unlikely spam**

 Action:  ☐ Add prefix to subject

☒ Enable Anti-spam

☐ Add predefined SMTP headers

Subject prefix:

Predefined spam recipient:

**Certainly spam**

Action:  ☐ Add prefix to subject

**Probably spam**

Action:  ☒ Add prefix to subject

**Unlikely spam**

Action:  ☐ Add prefix to subject

**Figures 11 and 12. Anti-spam settings pane**

2. To disable spam filtering, clear the **Enable** check box. Once the check box is cleared, all parameters become unavailable for editing. Select the check box to enable spam filtering.



3. Select **Add predefined SMTP headers**, if you want preselected headers to be added to e-mail messages. The following headers will be added:

```
X-AntiVirus: Checked by Dr.Web [plugin:
6.00.00.201101170, scanner: 6.0.12080.3,
engine: 5.0.3300.2, virus records:
1821073, updated: 18.01.2011]
```

```
X-DrWeb-SpamRate: 100
```

```
X-DrWeb-SpamReason: 1 random string(s)
(100)
```

```
X-DrWeb-SpamState: Yes
```

```
X-DrWeb-SpamVersion: 1.310.07
```

4. In the **Subject prefix** field, you can change the prefix which will be added to the subjects of e-mail messages which are considered spam. The default prefix is **\*\*\* SPAM \*\*\***.
5. In the **Predefined spam recipient** field, you can specify the e-mail address to redirect the spam messages of the categories, the action **Send to predefined spam recipient** is selected for.
6. In the fields below, you can define the program actions for three categories of messages based on the probability level of their being spam (**Certainly spam**, **Probably spam** or **Unlikely spam**). To do this, select one of the following actions for each category:
  - **Delete message** – means that the message will be deleted.
  - **Move to Junk E-mail folder** – means that the message will be moved to a special folder Junk E-mail and stored there for further consideration. This folder is supported by Microsoft Junk E-mail Filtering system.
  - **Send to predefined spam recipient** – means that the message will be sent to the e-mail address specified in the **Predefined spam recipient** field.
  - **Pass through** – means that the message will be passed through to the recipient.
  - **Reject message** – means that the message will not be delivered to the recipient and will be rejected by the server.



7. If you want to add the prefix (specified in the **Subject prefix** field) to the subject of a certain category of messages, select **Add prefix to subject** against the corresponding category.
8. When you finish setting up the **Anti-spam** component, click **Save**.

## Filtering

Filtering is adjusted in the **Filtering** section of the profile settings. Filters are applied to e-mail messages according to certain rules which can be added by the administrator. These rules determine the conditions for the filtering by the properties of attachments, and you can also prevent mass mailing by using the anti-distribution rules.

### To configure messages filtering

1. Select **Enable filtering** at the top of the **Filtering** pane. This makes the parameters in the section available for editing.
2. In the **File name suffix** field, you can edit the default suffix for the name of the file attached to a filtered message if necessary.
3. In the **Body** field, you can edit the text of the attached file. You can add macros from the **Macro** list while editing the text.

In the bottom of the **Filtering** pane, the list of rules is located. By default, it is empty.

### To create a new rule

- If you are using **Administrative Console**, click **Add rule** under the list to create a new rule. This will open the **Rule** window (see [Figure 13](#)), where you can select the desired type of rule and specify a corresponding value for it.

Type	Value	Description
Extension:		

**Figure 13. Rule editing window**





- If you are using **Administrator Web Console**, select the type of the filter and click **Create** (see [Figure 14](#)).

Filter	Value	Description
<a href="#">Update</a> <a href="#">Cancel</a>	* .exe	Filter1
<a href="#">Edit</a> <a href="#">Delete</a>	Maximum file size	

Mask

**Figure 14. Editing filtering rules**

The following rule types are available:

- **Extension** – means that **Dr.Web for Microsoft Exchange Server** will filter e-mail messages with attachments of specified types (in the **Value** field, specify the file format, e.g. `exe`, `com`, `dll`, etc.).
- **Mask** – means that e-mail messages with attachments which contain the text specified in the **Value** field in their names will be filtered (the mask should contain the file name and extension).



You can use the wildcard characters «\*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value.

- **Max file size** – means that e-mail messages with attachments of certain size or bigger will be filtered (the size is specified in bytes).
- The **Max recipients** and **Max recipients with attachments** types determine the maximum number of receivers allowed for an e-mail message.

First three types of rules are used to block attachments received by the members of a group with currently edited profile by certain criteria. For example, if you create an **Extension** type rule and specify `exe` in the **Value** field then any `exe` files attached to e-mail messages will be blocked on the server and the messages themselves will be passed on to their receivers with a notification text file attached. The template of such text files can be edited in the **Body** field of the **Filtering** pane. The name of the attached text file will include the name of the attachment and a suffix which is specified in the **File name suffix** field (e.g. by default, when an e-mail message with the attachment `filename.ext` is filtered,



the name of the text file attached to the message will be as follows: `filename.ext_filtered.txt`).

The last two types of rules are used to set up anti-distribution for your Exchange environment. These rules are applied to the members of a group with indicated profile as to the senders. When creating a rule, select **Max recipients** or **Max recipients with attachments** in the **Type** drop-down list and enter the maximum number of receivers in the **Value** field. Messages sent to a number of recipients equal to or less than the specified value will be delivered. Otherwise (in case the number of recipients is greater than the specified value) messages and attachments will be deleted and a notification on this event will be sent to the administrator.

### To edit or delete an existing rule

- If you are using **Administrative Console**, select the rule and click **Edit** or **Delete** under the list.
- If you are using **Administrator Web Console**, to edit a rule, click **Edit** to the left of its filter type, then modify the parameters values and click **Update** to save changes. To delete a rule, click **Delete** to the left of the rule you want to delete.

When you finish creating and/or editing rules, click **Save**.



## Accompanying Text

In the **Accompanying Text** section (see [Figures 15, 16](#)), you can configure the additional text to be included into outgoing external messages. Select **Enable** at the top to enable adding such text.

The **Accompanying Text** pane has two fields. In the first one you can enter HTML code (for messages sent in HTML format) and in the second one you can enter plain text (for messages sent in Plain Text format). See illustration below for examples.

The screenshot shows the 'Accompanying text' configuration window for Dr.Web for Microsoft Exchange Server. The window has a green header with the product name and a logo. Below the header, there is a section titled 'Parameters' with a green underline. Inside this section, there are two text input fields. The first field is labeled 'HTML:' and contains the following code: 

```
<html>
<head meta http-equiv="Content-Type" content="text/html;
charset=windows-1251" ></head>
<body>
This message has been checked by Dr. Web for Microsoft Exchange Server <br>
With best regards, My Company (c) <br>
</body>
</html>
```

 The second field is labeled 'Plain text:' and contains the following text: 

```
---
This message has been checked by Dr. Web for Microsoft Exchange Server
With best regards, My Company (c)
```

 At the bottom right of the window, there is a 'Save' button.



☒ Enable

Plain text:

---  
This message has been checked by Dr.Web for Microsoft Exchange Server  
With best regards, My Company (c)

HTML:

---  
This message has been checked by Dr.Web for Microsoft Exchange Server  
With best regards, My Company (c)

Save

**Figures 15 and 16. Configure accompanying text**

When you finish setting up the accompanying text, click **Save**.



An accompanying text is included only into the e-mail messages sent from the server protected by **Dr.Web for Microsoft Exchange Server** to another server.


## Manage Groups of Clients

By default, **Dr.Web for Microsoft Exchange Server** applies the parameters of the **Default** profile to all users. If you want to apply parameters of a different profile to certain users (see [Creating and Managing Profiles](#) for more information), join such users in a group and assign the profile to it. Thus you can divide all the Exchange clients into different groups, each of them with its own set of protection parameters.



## Create Group

### To create a new group

1. In the Console/Web Console tree, select **Groups**.
2. On the **Groups** pane, click **Add new** or the  button above the list of available groups.




Alternatively, if you are using **Administrative Console**, to create a new group, you can right-click **Groups** in the Console tree and then click **Add group** on the context menu (see illustration below).




A new group named **Group1** will be created and it will appear under **Groups** in the Console tree. If this name already exists, it will be named **Group2** and so on.

### To change the name of a group

- If you are using **Administrative Console**, select the group on the **Groups** pane and click **Rename**.
- If you are using **Administrator Web Console**, enter the new name into the corresponding field, then click the

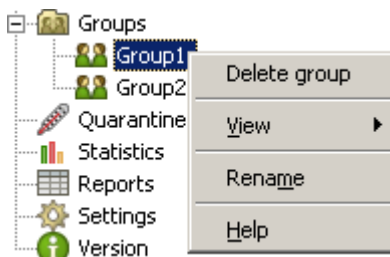
**Update** button  that will appear next to the text field.

### To delete a group

- Select it on the **Groups** pane and click **Delete** or the  button.



Alternatively, if you are using **Administrative Console**, to rename or delete a group, you can right-click it in the Console tree and then click the corresponding item on the context menu (see illustration below).



## To configure group settings

- Click the name of the group in the Console/Web Console tree.

In the **Group name** field you can edit the name of the group if necessary and in the **Profile** drop-down list you can select the profile you want to use for this group. In the **Type** field of the group's pane, you can select the type determining the forming of this group. There are two types of forming Exchange user groups available: **Active Directory Groups Set** and **Filters Set** (see [Forming a Group](#) for details).

When finish creating and/or editing the groups, click **Save**.

## Form Group

For each group you can set up the necessary parameters. To determine the manner of forming the group, choose one of the values in the drop-down list **Type**. Two types of forming Exchange user groups are available: **Active Directory Groups Set** and **Filters Set**.

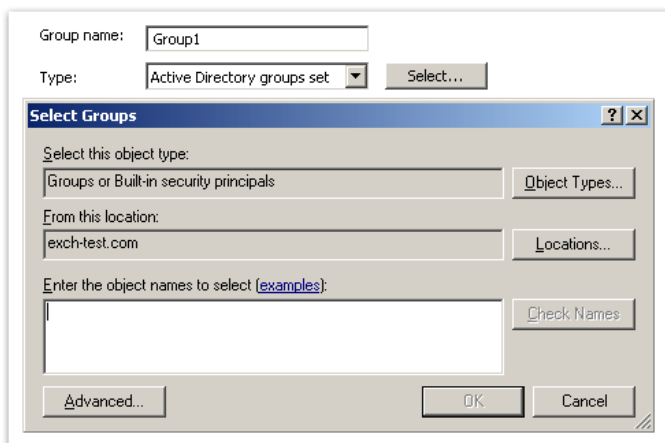


## Active Directory Groups Set

If you select the **Active Directory Groups Set** type in the group's settings, the Exchange user group must consist of AD groups.

### To create a group which contains the Active Directory groups of clients

- If you are using **Administrative Console**, specify the names of AD groups in the **Parameters** field of the group's settings or choose the AD groups via the **Select Groups** window, which opens when you click **Select** (see [Figure 17](#)).



**Figure 17. Select Groups window**

In the **Select groups** window select the type of object and its location, enter its name and click **OK**. If an AD group with the specified name exists, it will be added to the Exchange group and will appear in the **Parameters** field of the group's settings.



You can use the advanced settings to search the AD groups. Click **Advanced** to access to the advanced settings. To find a group, select the type of object and its location, specify a partial or exact name in the corresponding fields and click **Find Now**. Groups complying with the specified search parameters will appear in the **Search results** table in the bottom. Select the necessary group (s) and click **OK**.



You can leave the **Name** field blank to see a list of all the objects of the selected type in the selected location.

- If you are using **Administrator Web Console**, specify the Active Directory groups that you want to add to the edited group of Exchange clients by selecting them from the **Parameters** list. Click **Insert** to add the selected group (see [Figure 18](#)).

Group: Group1

Profile: Profile2

Type: Active Directory groups set

Parameters: DnsAdmins

Insert

testers  
DnsAdmins

Save

**Figure 18. Create Active Directory group**





## Filters Set

If you select the **Filters Set** type, the Exchange user group must be formed by specifying a range of e-mail addresses in the **Parameters** field (see [Figures 19, 20](#)).

Group name:

Type:

Parameters:

user3@mycompany.com

user5@mycompany.com

user7@mycompany.com

Group: Group1

Profile:

Type:

Parameters:

user1@mycompany.com

user2@mycompany.com

user5@mycompany.com

**Figures 19 and 20. Create groups by specifying addresses of clients**



You can use the wildcard characters «\*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value.



The **Quarantine** is operated by a service database which also stores information on various incidents (see [Viewing the Statistics](#)). When the **Quarantine attachment** action is applied to an e-mail message (see the [Scanning](#) section), its attachment is sent to that database and information about it is added to the list in the bottom of the **Quarantine** pane (see [Figures 21, 22](#)).

Administrator Manual



<input type="checkbox"/>	Date/Time	Virus name	Sender	Subject	Recipients	File name
<input type="checkbox"/>	04.10.2010 14:56:53	Trojan.PWS.Lineage	Administrator@EXCHSRV-WORK.com	Test Message From X ML Config #1	Administrator@EXCHSRV-WORK.com	cannotcure.exe
<input type="checkbox"/>	04.10.2010 14:56:54	Trojan.PWS.Lineage	Administrator@EXCHSRV-WORK.com	Test Message From X ML Config #2	Administrator@EXCHSRV-WORK.com	cannotcure.exe
<input type="checkbox"/>	04.10.2010 14:56:55	Trojan.PWS.Lineage	Administrator@EXCHSRV-WORK.com	Test Message From X ML Config #3	Administrator@EXCHSRV-WORK.com	cannotcure.exe
<input type="checkbox"/>	04.10.2010 14:56:56	Trojan.PWS.Lineage	Administrator@EXCHSRV-WORK.com	Test Message From X ML Config #4	Administrator@EXCHSRV-WORK.com	cannotcure.exe
<input type="checkbox"/>	04.10.2010 14:56:58	Trojan.PWS.Lineage	Administrator@EXCHSRV-WORK.com	Test Message From X ML Config #5	Administrator@EXCHSRV-WORK.com	cannotcure.exe

Refresh Scan Delete Copy

Cleaning

Clear records older than  day(s)

Automatically clear records older than  day(s)

Save

**Figures 21 and 22. Quarantine**



For each object in **Quarantine** the following information is displayed:

- Date and time of moving to **Quarantine**
- Name of the virus
- E-mail of the sender of the message which contained the infected object
- Subject of the message which contained the infected object
- E-mail addresses of the recipients of the message with infected attachment
- Name of the infected file

If Administrative Console is used, in the **Filtering** group box, you can set one or several filters according to certain criteria to customize the way information about the objects moved to **Quarantine** is displayed.



## To configure filtering of the list of Quarantine

1. To enable filtering, select the **Filter** check box. This makes the parameters in the section available for editing. You can set one or several filters according to certain criteria to customize the way information about the objects sent to **Quarantine** is displayed.
2. To add a new filter, click the Add button  to the right of filter's parameters.
3. To set a filter, choose the type of criteria in two drop-down lists and enter the desired values in corresponding fields.
4. To delete a filter, click the Delete button  to the right of parameters of the filter you want to delete.
5. Click **Apply** to save changes.

## Manage objects in Quarantine

1. To delete one or more objects from the **Quarantine**, select them in the list and click **Delete**.
2. To save one or more objects moved to **Quarantine** in the file system, select them in the list and click **Copy**.
3. You can recheck the files in **Quarantine** and neutralize the malicious objects after updating the virus databases. To do this, select one or several objects in the list and click **Scan**.
4. To refresh manually the list of **Quarantine**, click **Refresh**.



The **Quarantine** list is updated every time you start the **Administrative Console** or refresh the **Administrator Web Console** page, but if it stays active for a long time, it is recommended to refresh the list manually from time to time.



## To clear the list of Quarantine

1. To delete manually the records older than a certain number of days, in the **Cleaning** group box specify the number of days and click **Delete**.
2. Specify the number of days for automatic deleting of the records older than the specified number of days. By default, the records older than 20 days are deleted automatically.

Click **Save** to save the changes made in the **Quarantine** section.

## View Statistics

Click **Statistics** in the Console/Web Console tree to view the statistics on the operation of **Dr.Web for Microsoft Exchange Server**. There are two tabs/sections on this pane:

- The **Statistics** tab/section displays a table with an overview on the amount of processed objects. You can clear or refresh the statistics by clicking **Clear** or **Refresh**.



Every time an e-mail message is processed by **Dr.Web for Microsoft Exchange Server**, 3 objects are added to the statistics table because the plug-in first checks the message for spam, then performs an anti-virus scan of the message body and its attachment.

- The **Incidents** tab/section displays a list of virus and spam messages processed by **Dr.Web for Microsoft Exchange Server** and those filtered out. It is similar to the list on the **Quarantine** pane (see [Managing the Quarantine](#)) because they use the same database.

In case the **Administrative Console** is used, the list can be sorted according to different criteria by clicking the title of the corresponding column. Moreover, one or several filters can be applied to the list using the group box **Filter** (see [Figure 23](#)).



Sender	Recipients	Subject	State	Date/Time	File name	Virus name
Administrator@EXC HSRV-WORK.com	Administrator@EXC HSRV-WORK.com	Test Message From XML Config #1	перенесен в карантин	04.10.2010 14:56:54	cannotcure.exe	Trojan.PWS.Lineage
Administrator@EXC HSRV-WORK.com	Administrator@EXC HSRV-WORK.com	Test Message From XML Config #2	перенесен в карантин	04.10.2010 14:56:54	cannotcure.exe	Trojan.PWS.Lineage
Administrator@EXC HSRV-WORK.com	Administrator@EXC HSRV-WORK.com	Test Message From XML Config #3	перенесен в карантин	04.10.2010 14:56:56	cannotcure.exe	Trojan.PWS.Lineage

[Export](#)
[Refresh](#)

Cleaning

Clear records older than  [Clean](#)

Automatically clear records older than  day(s)

[Save](#)

### Figures 23 and 24. List of incidents



To manage the list of incidents, the following actions are available:

- To save the list of incidents as a text file, click **Export**.
- To refresh the list of incidents, click **Refresh**.
- To clear the records older than a certain date, in the **Cleaning** group box, specify the date and click **Clean**. By default, the incidents older than 30 days are deleted automatically. You can change the number of days in the corresponding field if necessary.

Click **Save** to save the changes made in the **Incidents** tab/section.

## Manage Distribution of Reports


Click **Reports** in the Console/Web Console tree to set up distribution of reports on the operation of **Dr.Web for Microsoft Exchange Server**. These reports are sent as e-mail attachments to the addresses specified by the administrator.

At the top of the **Reports** pane (see [Figures 25, 26](#)), you can view the list of six available report types:

- All virus incidents
- Incidents by recipients
- Most recent viruses
- Recipients of the maximum number of viruses
- Recipients of the maximum number of spam messages
- Spam count



**Dr.WEB®**  
for Microsoft Exchange Server



Reports

Reports

Report	Header	Recipients	Days	Schedule
<input checked="" type="checkbox"/> All virus incidents	Dr.Web for ...		5	Task not scheduled
<input type="checkbox"/> Incidents by recipients	Dr.Web for ...		5	Task not scheduled
<input checked="" type="checkbox"/> Most recent viruses	Dr.Web for ...		5	Task not scheduled
<input type="checkbox"/> Recipients of the maximum number of spam messages	Dr.Web for ...		5	Task not scheduled
<input checked="" type="checkbox"/> Recipients of the maximum number of viruses	Dr.Web for ...		5	Task not scheduled
<input type="checkbox"/> Spam count	Dr.Web for ...		5	Task not scheduled

Send

Schedule...

Properties

Mail

Subject:

Dr.Web for Microsoft Exchange Report: All virus incidents

Body:

Please find the virus report in the attached file.

Recipients:

Do not send reports older than  day(s)

Save





**Reports**

Report	Subject	Recipients	Days	Schedule
<input type="checkbox"/> All virus incidents	Dr.Web for Microsoft Exchange Report: All virus incidents		5	Task not scheduled
<input checked="" type="checkbox"/> Incidents by recipients	Dr.Web for Microsoft Exchange Report: Incidents by recipients	admin@mycompany.com	5	At 9:00 every day, starting 10/5/2010
<input type="checkbox"/> Most recent viruses	Dr.Web for Microsoft Exchange Report: Most recent viruses		5	Task not scheduled
<input checked="" type="checkbox"/> Recipients of the maximum number of spam messages	Dr.Web for Microsoft Exchange Report: Recipients of the maximum number of spam messages		5	Task not scheduled
<input type="checkbox"/> Recipients of the maximum number of viruses	Dr.Web for Microsoft Exchange Report: Recipients of the maximum number of viruses	admin@mycompany.com	5	Task not scheduled
<input type="checkbox"/> Number of spam messages	Dr.Web for Microsoft Exchange Report: Number of spam messages		5	Task not scheduled

**Properties**

Subject: Dr.Web for Microsoft Exchange Report: Incidents by recipients

Body: Please find the report in the attached file.

Recipient: admin@mycompany.com

Send report for last: 5 day(s)

**Figures 25 and 26. Configure distribution of reports**

By default, all the report types are disabled, not scheduled and no recipients are assigned for them.

### To enable a certain type of reports

1. Select the check box against the corresponding list entry.
2. Edit the subject and body of the message if necessary.
3. Specify the recipient e-mail addresses of the reports of selected type.

You can also set the period (in days) for collecting of information for the report. The events that have taken place before the specified period would not be presented in the report.

You can send reports of the selected types manually at any time by clicking **Send** under the list. Alternatively, you can set up schedules for report types.



## To set up a schedule for a certain report type

1. Select the necessary report type and click **Schedule** below the list. This will open the window with task parameters (see [Figures 27, 28](#)).

The screenshot shows the 'SettingsTask' dialog box with the 'Schedule' tab selected. The dialog has a title bar with a question mark and close button. Inside, there is a list box containing one item: '1. At 9:00 every day, starting 19.12.2008'. To the right of the list box are 'New' and 'Delete' buttons. Below the list box, there are two labels: 'Schedule Task:' and 'Start time:'. Under 'Schedule Task:' is a dropdown menu currently set to 'Daily'. Under 'Start time:' is a time input field set to '9:00' with up/down arrows, and an 'Advanced...' button. Below these is a section titled 'Schedule Task Daily' containing an 'Every' label, a spinner box set to '1', and the text 'day(s)'. At the bottom left, there is a checked checkbox labeled 'Show multiple schedules.'. At the bottom right, there are 'OK' and 'Cancel' buttons.

SettingsTask

Schedule

1. At 9:00 every day, starting 19.12.2008

New Delete

Schedule Task: Start time:

Daily 9:00 Advanced...

Schedule Task Daily

Every 1 day(s)

☒ Show multiple schedules.

OK Cancel



**Figures 27 and 28. Configure schedule for reports distribution**

2. Click **New/Create** to add a new task.



To delete an existing task, select it in the drop-down list and click **Delete**.

3. Select the frequency in the **Schedule Task** drop-down list, the time of day when the report should be sent in the **Start time** entry field and additional schedule conditions below. You can also choose to send reports at system startup, at logon or when the computer has been idle for a certain period of time.
4. If you are using **Administrative Console**, click **Advanced** to adjust some extra parameters if necessary. This will open the **Advanced Schedule Options** window (see [Figure 29](#)).



**Advanced Schedule Options**

Start Date: 19 декабря 2008 г.

☐ End Date:

☐ Repeat task

Every: [ ] [ ]

Until: ☒ Time: [ ]

☐ Duration: [ ] hour(s) [ ] minute(s)

☐ If the task is still running, stop it at this time.

OK Cancel

**Figure 29. Configure advanced task settings**

Make the necessary changes of the additional parameters of the task's schedule and click **OK**.

5. When you finish adjusting the schedule for the report type, click **OK** in the **SettingsTask** window to save the changes made.

Click **Save** to apply the changes when you finish adjusting the necessary report types.



The schedule and parameters are saved only for enabled report types (against which the check box is selected in the report types list).



## Adjust General Settings

The **Settings** section allows you to adjust some general parameters of the program operation. It is divided into three tabs/sections: **Notification protocol**, **Service account** and **Black/White Lists**. In the **Notification protocol** tab/section, you can specify and configure the protocol which is used for sending program notifications and also the server from which the notifications will be sent. In the **Service account** tab/section you can change the parameters of the service account which is used for plug-in administration. In the **Black/White Lists** tab/section you can create and/or edit the black and white lists for **Anti-spam**.

### Notification protocol

You can select and configure one of the following protocols:

- **MAPI**. To use this protocol, specify the administrator e-mail address and password as well as the name of the server to send notifications from.



If Exchange Server 2007/2010 is used, for sending notifications and reports through MAPI protocol, Microsoft Exchange Server MAPI Client and Collaboration Data Objects package available at Microsoft official web site at <http://www.microsoft.com/downloads/details.aspx?FamilyID=E17E7F31-079A-43A9-BFF2-0A110307611E&displaylang=en> is required.

- **SMTP**. To use this protocol, specify the administrator e-mail address and password and also the name of the server and the number of port for sending notifications.
- **HTTP**. To use this protocol, specify the administrator e-mail address and password, the URL address and the Exchange server version.



To check the settings of the selected protocol, you can send a test e-mail. In the **Test selected configuration** group box, specify the parameters of the test message:

- E-mail address of message recipient
- Message subject
- Message text
- Attachment

Click **Send test message** to send the e-mail.

To save the changes, click **Save**.

## Service account

In this tab/section you can enter the service account UPN (User Principal Name) and password. This account might not necessarily belong to administrator.

## Black/White Lists

In the **Black/White Lists** tab/section you can compile lists, which determine the behavior of the **Anti-spam** component with trusted and distrusted e-mail addresses (see [Figures 30, 31](#)).

The screenshot shows the 'Dr.WEB® для Microsoft Exchange Server' settings window. The 'Black/White Lists' tab is selected. At the top, there are tabs for 'Notification protocol', 'Service Account', 'Black/White Lists', and 'Settings'. The 'Black/White Lists' section has a checkbox labeled 'Enable' which is checked. Below this, there are two main columns. The left column is for the 'White List' and the right column is for the 'Black List'. Each column has an 'Add to [List]' button at the top, a list of e-mail addresses in the middle, and a 'Remove from [List]' button at the bottom. The 'White List' contains two entries: 'trusted\_address1@mail.com' and 'trusted\_address2@mail.com'. The 'Black List' contains two entries: 'distrusted\_address@mail.com' and '\*@distrusted\_domain.com'. At the bottom right of the window, there are three buttons: 'Import', 'Export', and 'Save'.

Dr.WEB® для Microsoft Exchange Server			
Notification protocol	Service Account	Black/White Lists	Settings
<input checked="" type="checkbox"/> Enable			
E-Mail <input type="text"/>			
Add to White List		Add to Black List	
e-mail trusted_address1@mail.com trusted_address2@mail.com		e-mail distrusted_address@mail.com *@distrusted_domain.com	
Remove from White List		Remove from Black List	
		Import Export Save	



Notification protocol

Service account

Black/White lists

☒ Enable

E-mail

Add to white list

trusted\_address1@mail.com  
trusted\_address2@mail.com

Add to black list

\*@distrusted\_domain.com  
distrusted\_address@mail.com

Remove from white list

Remove from black list

Import Export

Save

**Figures 30 and 31. Black and white lists**

Select **Enable** to enable the lists. You can add e-mail addresses you trust to the white list. In this case, messages from these addresses will not be checked for spam. If you add an address to the black list, all messages from it will be considered as **Certainly spam**.

To add an e-mail into one of the lists, enter it in the **E-mail** field and click **Add to white List** or **Add to black List**.

To delete an e-mail, select it in the necessary list and then click **Remove from white List** or **Remove from black List**.

You can also use the **Import** and **Export** buttons to save the list into a special file with **.lst** extension or to load the lists from the file and to create or edit the lists manually using a text editor, for example Notepad.



While creating and/or editing the files of black and white lists manually, you need to add prefix to the e-mails: «+» to add the e-mail into the white list, «-» to add the e-mail into the black list, e.g. **+trusted\_address@mail.com** and **-distrusted\_address@mail.com**. The created text file must be saved with **.lst** extension in Unicode format.



You can use the asterisk («\*») to substitute a part of the address (e.g. **\*@domain.org** stands for any address in the **domain.org** domain).

---

Click **Save** when you finish editing the lists.





## Update Virus Databases

An updating task (**DrWeb for Microsoft Exchange Update Task**) is created in the Windows Task Scheduler (the **C:\Windows\Tasks** folder) during installation of **Dr.Web for Microsoft Exchange Server**. The task runs the updating module **DrWebUpW.exe**, which downloads the virus databases and components of the program.

The task can be adjusted by changing its properties (double-click **DrWeb for Microsoft Exchange Update Task**). The operation of the updating module can be adjusted by specifying certain command-line parameters (see [Appendix A](#)) in the **Run** field of the task properties.

### To configure update without using Internet connection

1. Create a folder on your computer's local drive (e.g. C:\MyDocs\DrWebUpdate).
2. Put the components which need to be updated into this folder (you can find the list of components which can be updated in the file **drweb32.lst** located in the C:\Documents and Settings\All Users\Application Data\Doctor Web\Bases\ folder).
3. Add the following command-line parameter to the **Run** field of **DrWeb for Microsoft Exchange Update Task**: **/URL:** *<path to created folder>* (for example, **/URL:"C:\MyDocs\DrWebUpdate"**).



## Logging

**Dr.Web for Microsoft Exchange Server** registers the errors and application events in following logs:

- Windows Event Log
- Text log of the installation program
- Plug-in debug logs

The update information is registered in a separate text file drwebupw.log, that is located in the %alluserprofile%\AppData\Doctor Web\Logs\ folder (see [Checking Updater Functionality](#)).

## Event Log

**Dr.Web for Microsoft Exchange Server** registers the following information in the Windows Event Log:

- Plug-in starts and stops
- License key file parameters including validity, licensed period
- Parameters of the plug-in components including scanner, core, virus databases (information is registered when the plug-in starts or components are updated)
- License invalidity notifications if the license key file is missing, some of the plug-in components are not licensed, license is blocked or license key file is corrupted (information is registered when the plug-in checks the license)
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)
- Information on server's reception of messages that contained objects which had been cured, not cured, filtered or categorized as bad objects or spam (see [Notifications](#)).



### To view Event Log

1. On the Control Panel, double-click **Administrative Tools** and then double-click **Event Viewer**.
2. In the tree view, select **Application**.
3. The application Event Log displays in the right pane. The Source for the plug-in events are the applications Dr.Web ® Engine, Dr.Web Core Service for MSP and Dr.Web Core Services for MSP Attendant.

## Installation Program Text Log

The installation program of **Dr.Web for Microsoft Exchange Server** also keeps a log of the installation process so that it could be viewed later for bug-tracking purposes. The log file is created in the root directory of drive **C:\** and is named **Dr.Web Core Services for MSP.log**. It contains information on the installation of Dr.Web Core Services for MSP and can be deleted after the installation has proved to be successful (see [Check Installation](#)).

The installation program additional logging can be also enabled by running the program installation file with the following parameters: **msiexec /i** *<path to the installation file>* **/lvx\*** *<path to the installation program log>* **CHECK\_MAIL\_LOG=***<path to the additional log>*. In this case two files with more logging details will be created by the specified paths.



## Text Log

On installation of **Dr.Web for Microsoft Exchange Server** the program debug logging is disabled by default. You can enable the debug logging by editing the **HKEY\_LOCAL\_MACHINE\SOFTWARE\Doctor Web\Core Services for MSP\Logging** registry key parameters and setting the value 5 for the **DumpToLog** parameter (by default the value is set to 0, that means, that the debug logging is disabled).

All debug log files are created in the **%alluserprofile%\AppData\Doctor Web\Logs\** folder.



Enabling the plug-in debug logging is recommended only in case it is requested by **Dr.Web Technical Support**. The debug logging may considerably decrease the server performance.

---



# Troubleshooting

To check whether **Dr.Web for Microsoft Exchange Server** is installed and configured properly, use the following tests described in this chapter:

- Application installation check
- Updater check
- Viruses and spam detection capabilities check

## Check Installation

**Dr.Web for Microsoft Exchange Server** must be installed to the following folders:

- C:\Program Files\DrWeb for Exchange
- C:\Documents and Settings\All Users\Application Data\Doctor Web

Besides, if Microsoft Exchange Server 2000/2003 is used, **Dr. Web for Microsoft Exchange Server** must be also installed to the C:\Program Files\Common Files\Doctor Web folder, otherwise, if you are using Microsoft Exchange Server 2007/2010, the program must be installed to the C:\Program Files(x86)\DrWeb for Exchange and C:\Program Files(x86)\Common Files\Doctor Web folders.

Make sure that these folders have been created during installation and contain program files.

After that open the Windows **Event Viewer** and make sure that there are no errors associated with **Dr.Web for Microsoft Exchange Server** in it.

Then check that there are no errors in Dr.Web Core Services for MSP. log, which is created in the root directory of drive C:\ during installation (see [Installing Dr.Web for Microsoft Exchange Server](#)).



Finally, make sure that the following local services are started:

- Dr.Web® Scanning Engine (DrWebEngine)
- Dr.Web Core Services for MSP
- Dr.Web Core Services for MSP Attendant

## Check Updater Functionality

The updating module **DrWebUpW.exe** automatically starts after the installation of **Dr.Web for Microsoft Exchange Server**. It updates the anti-virus engine **drweb32.dll**, the anti-spam engine **vrcpp.dll** and the virus databases.

### To make sure that an update was successful:

1. Depending on the version of the operating system, run the **Tasks** command to open the C:\WINDOWS\Tasks folder or open the Task Scheduler.
2. Check that **DrWeb for Microsoft Exchange Update Task** has been created and it is working correctly (the return code in the **Last Result** field must be 0x0).
3. Open the updater log file **%allusersprofile%\Application Data\Doctor Web\Logs\drwebupw.log** and make sure that there are no errors in it.



## Virus Detection Test

To check the functionality of the plug-in's virus detection capabilities and its default configuration, it is recommended to use the EICAR (European Institute for Computer Antivirus Research) test file. The test script is not a virus, it cannot replicate and does not contain any payload, however, it is recognized by anti-virus software as a virus. You can download the test file from the EICAR website at <http://eicar.org/> or create it yourself.

### To create the EICAR test file:

Open the Notepad text editor and copy the following string to it:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD  
-ANTIVIRUS-TEST-FILE!$H+H*
```

Save the file with a **.com** extension (you can use any name, e.g. **eicar.com**), attach it to an e-mail message and send it to any test e-mail address. The received message should contain an attached text file with the **\_infected.txt** suffix and the following contents:

```
File eicar.com was infected with a virus and  
has been deleted by Dr.Web for Exchange. Virus  
name: EICAR Test File (NOT a Virus!)
```

Also, a mail notification with similar text will be sent to the e-mail address of the administrator specified during installation.



Do not use real viruses to check the functionality of anti-virus software!

---



## Spam Detection Test



The **Anti-Spam** component works only with the «Anti-Virus&Anti-Spam» version of **Dr.Web for Microsoft Exchange Server**, i.e. if you have an appropriate license key file (see [License Key File](#)).

To test the functionality of your **Anti-Spam** component, it is recommended to use an e-mail message with test string.

### To create a test spam message:

Copy the following string to the body of a new e-mail message:

```
Start enjoying the benefits of Generic  
Medicine. Order quickly and easily, and save  
a ton of money. Try them out, they're 100%  
money back guarantee.
```

Send the message to a test e-mail address via SMTP. Then open the Windows **Event Viewer** -> **Application** utility and find the information that **Dr.Web for Microsoft Exchange Server** has detected spam.





## Appendices

### Appendix A. Updater's Command-Line Parameters

Below is a list of command-line parameters which can be added to the Run entry field of the updating task (**C:\Windows\Tasks\ DrWeb for Microsoft Exchange Update Task**) in order to adjust the operation of the updating module.

Parameter	Description
/DBG	Detailed log.
/DIR : <directory>	Change the name of the folder where the updated files are placed; by default, the folder from which the Automatic Updating Utility was launched is used.
/INI : <path>	Use alternative configuration file with the specified name or path.
/NI	Do not use parameters specified in the <b>drweb32.ini</b> configuration file.
/GO	Package operation mode, without dialogs.
/LNG : <filename>	Name of the language resources file (English is used if other is not specified).
/PASS : <user password for HTTP server>	User password for the updating server.
/USER : <user name for HTTP server>	User name for the updating server.
/PPASS : <proxy user password>	User password for the proxy server.
/PUSER : <proxy user name>	User name for the proxy server.



Parameter	Description
/PURL : <proxy address>	Address of the proxy server.
/URL : <URL of the updating server>	Only UNC names are accepted.
/QU	Compulsory close the Automatic Updating Utility after the updating is finished, regardless whether it was successful or not. The success of the updating can be checked via the <b>drwebupw.exe</b> return code, e.g. from the BAT file by the errorlevel variable value: <ul style="list-style-type: none"><li>• 0 = successful</li><li>• other values = unsuccessful</li></ul>
/REG	Launch the updater for registration and to receive the license key file.
/UPD	Regular updating; used together with the /REG parameter to run the updating session itself during the registration.
/RP<file_name> or /RP+<file_name>	Log to a file the name of which is specified in the parameter. If no name is specified log to a file with the default name. If the + character is present the file is appended; if there is no + character a new file is created.
/NR	Do not create a log file.
/SO	Enable sounds (only when errors occur).
/ST	Run the updater in invisible mode ( <i>stealth mode</i> ).
/UA	Download all files specified in the updating list regardless the used OS and the installed components. This mode is designed to receive the full local copy of the <b>Dr.Web</b> server updating area; this mode cannot be used for updating the anti-virus installed on a computer.
/UVB	Update the virus databases and <b>drweb32.dll</b> (the anti-virus engine) only (disables /UA, if it is set).



Parameter	Description
<code>/UPM:&lt;proxy mode&gt;</code>	<p>Mode of using a proxy server; it can have the following values:</p> <ul style="list-style-type: none"><li>• direct – do not use proxy server</li><li>• ieproxy – use system settings</li><li>• userproxy – use settings specified by the user (the <code>/PURL</code>, <code>/PUSER</code> and <code>/PPASS</code> parameters)</li></ul>
<code>/URM:&lt;mode&gt;</code>	<p>Restart after the updating is finished. It can have the following values:</p> <ul style="list-style-type: none"><li>• prompt – prompt whether a reboot is needed after the updating session is finished</li><li>• noprompt – if necessary reboot without prompting</li><li>• force – always reboot (regardless whether it is required after the updating or not)</li><li>• disable – do not reboot</li></ul>



## Appendix B. Microsoft Exchange Server Anti-Virus Scanning Settings

The VSAPI-based anti-virus scanning is adjusted by means of a set of registry keys and involves two following types of settings:

### 1. Global settings

These settings are used by default for all Information Stores on server.

#### On access scanning

Registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]
```

```
"Enabled"=dword:00000001
```

This setting enables the anti-virus check for all Information Stores. The message will be scanned every time it is requested by a client.

#### Background scanning

Registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]
```

```
"BackgroundScanning"=dword:00000001
```

This setting enables the background scanning. Background scanning implies creating of a new thread where all the messages from the Store are scanned. Enabling the background scanning may adversely affect the mail server performance.



## Proactive scanning

Registry key:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Services\MSExchangeIS\VirusScan]
```

```
"ProactiveScanning"=dword:00000001
```

This setting enables the proactive scanning. In this case all the messages are checked immediately after they get into the Store. Messages that have passed proactive scanning and have not changed their time stamps aren't checked once more when they are requested by a client.

## Disabling outgoing messages check

Registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\S
ervices\MSExchangeIS\VirusScan
```

```
"TransportExclusion"=reg_dword:00000000
```

This setting allows to disable/enable (by specifying 1 or 0 value respectively) the malware check for outgoing messages when they are picked up by transport system from the Store. This check is enabled by default.

## Configuring the number of threads for VSAPI

The number of threads for VSAPI 2.6 is specified by default in the Exchange Server settings. But you can also configure it manually by creating the ScanningThreads parameter in the registry entry below.

Registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\S
ervices\MSExchangeIS\VirusScan
```

```
"ScanningThreads"=reg_dword
```



This parameter determines the maximum number of threads created for scanning. Changing the value of this parameter affects only on access and proactive scanning. It does not affect the background scanning, which always uses one thread per database.

By default, the value of this parameter is set to  $2 * \text{<number of processors>} + 1$ .

## 2. Database settings

These settings allow to specify the scanning parameters for each mail database on the server. The registry key for these settings is the following:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-Name>\<ID Base>],
```

where <Server-Name> is the name of the server, <ID Base> is the database identifier, e.g. Private-ae39732e-fb7f-426d-98a0-298f3f014c77.

Parameters:

- "VirusScanEnabled"=dword:00000001 – enables the anti-virus scanning of the specified database.
- "VirusScanBackgroundScanning"=dword:00000001 – enables the background scanning of the specified database.
- "VirusScanProactiveScanning"=dword:00000001 – enables the proactive scanning of the specified database.



### 3. SMTP transport scanning

---



The transport scanning settings are available only for Microsoft Exchange Server 2000/2003.

---

Registry key:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\TransportAVAPI\]
```

```
"Enabled"=dword:00000001
```

Transport scanning is disabled by default. You can enable it on the last step of program [installation](#). So, the first anti-virus scanning of the message will be performed on the OnSubmission SMTP event, i.e. on the transport level. Another scanning will be performed in the Exchange Information Store when the message is requested by a client.



## Appendix C. Operation in Central Protection Mode

**Dr.Web for Microsoft Exchange Server** can operate in the central protection mode in a network managed by **Dr.Web Control Center**. Central protection helps automate and simplify configuring and managing information security of computers within logical structures (for example, company computers that access each other from both inside and outside of company's local networks). Protected computers are united in one *anti-virus network* which security is monitored and managed from central server (**Dr.Web Control Center**) by administrators. Connection to centralized anti-virus systems guarantees high level of protection while requiring minimum efforts from end-users.

### Logical Structure of Anti-virus Networks

Solutions for central protection from **Doctor Web** use client-server model (see [Figure 32](#)).

Workstations and servers are protected by *local anti-virus components* (clients; herein, **Dr.Web for Microsoft Exchange Server**) installed on them, which provides for anti-virus protection of remote computers and ensures easy connection to central protection server.

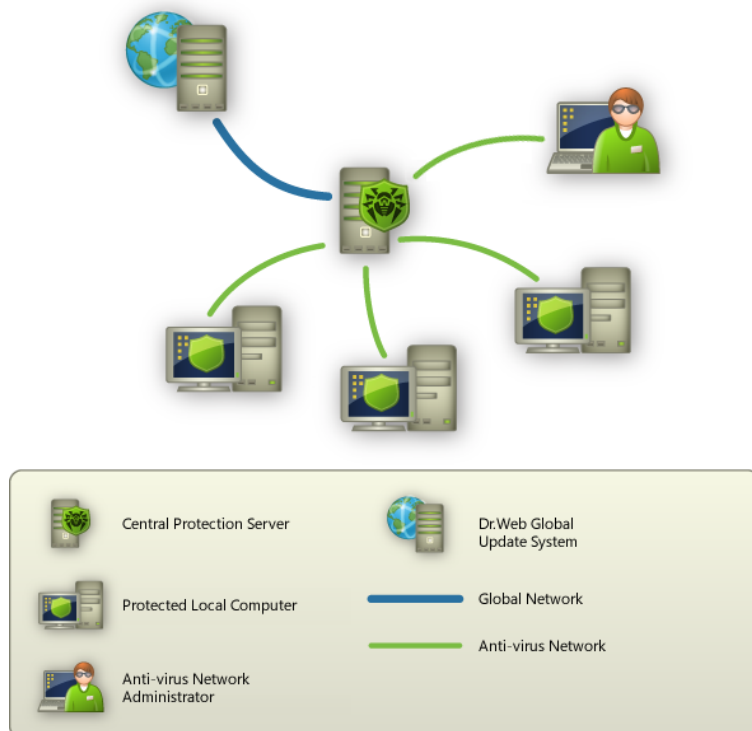
Local computers are updated and configured from *central server*. The stream of instructions, data and statistics in the anti-virus network goes also through the central protection server. The volume of traffic between protected computers and the central server can be quite sizeable, therefore solutions provide options for traffic compression. To prevent leak of sensitive data or substitution of software downloaded onto protected computers, encryption is also supported.

All necessary updates are downloaded to central protection server from **Dr.Web Global Update System** servers.





Local anti-virus components are configured and managed from central protection server according to commands from *anti-virus network administrators*. Administrators manage central protection servers and topology of anti-virus networks (for example, validate connections to central protection server from remote computers) and configure operation of local anti-virus components when necessary.



**Picture 32. Logical structure of anti-virus networks.**



## Operation of Dr.Web for Microsoft Exchange Server in Central Protection Mode

For operation of **Dr.Web for Microsoft Exchange Server** in central protection mode, version 6.00.1 of **Dr.Web Agent** is required to be installed and operate correctly on the same operating system.



The version 6.00.1 of **Dr.Web for Microsoft Exchange Server** is not compatible with **Dr.Web Agent** of versions, other than 6.

**Dr.Web for Microsoft Exchange Server** operating in the central protection mode provides the following possibilities:

- Sending statistics of **Dr.Web for Microsoft Exchange Server** operation. The statistics is displayed in the **Statistics** and **Summary statistics** tables of **Dr.Web Control Center**.
- Sending notifications on detected viruses with information on the infections and performed actions. These events are displayed in the **Infection** table of **Dr.Web Control Center**.
- Virus databases and anti-virus engine updates from **Dr. Web Control Center** repositories. This action allow disabling the standard updater of **Dr.Web for Microsoft Exchange Server**, which starts by default according to a schedule. In this case components update starts from **Dr.Web Control Center** repositories according to its schedule.
- Using a license key file for **Dr.Web for Microsoft Exchange Server** that is registered in the anti-virus network. On **Dr.Web for Microsoft Exchange Server** installation the license key file is received by **Dr.Web Agent** for the specified station.



## Appendix D. Technical Support

Support is available to customers who have purchased a commercial version of Doctor Web products. Visit Doctor Web technical support site at <http://support.drweb.com/>.

If you encounter any issues installing or using company products, take advantage of the following Doctor Web support options:

- Download and review the latest manuals and guides at <http://download.drweb.com/>
- Read the frequently asked questions at <http://support.drweb.com/>
- Look for the answer in Dr.Web knowledge database at <http://wiki.drweb.com/>
- 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 Technical Support by filling in the web-form in the corresponding section of the support site at <http://support.drweb.com/>.

For regional office information, refer to the Doctor Web official website at <http://company.drweb.com/contacts/moscow>.



# Index

## A

- abbreviations 7
- accompanying text 51
- administration 33
- administrative console
  - console tree 29
  - details pane 29
  - launch 29
- administrator web console
  - details pane 31
  - launch 31
  - web console tree 31
- anti-spam
  - configure 45
  - license 45

## B

- background scanning 15
- black list 69

## C

- central protection 88
- check 77
  - cycle 19
  - installation 77
  - spam 45
  - updater 78
- configure
  - accompanying text 51

- anti-spam 45
- filtering 48
- notification protocol 69
- scanning 42
- service account 69
- VSAPI 84

## D

- detection
  - spam 80
  - viruses 79
- document conventions 7
- Dr.Web for Microsoft Exchange Server 9
  - administrative console 29
  - administrator web console 31
  - central protection mode 88
  - functions 9
  - install 22, 25
  - introduction 9
  - logging 74
  - main features 9
  - principles of operation 19
  - remove 22, 28
  - scanned objects 11
  - server roles 15
  - start to use 29
  - statistics 61
  - system requirements 23
  - technical support 91



# Index

Dr.Web for Microsoft Exchange Server  
9  
transport agents 15  
VSAPI 15

## E

EICAR test file 79  
event log 21, 37, 74

## F

filtering  
configure 48  
rules 19, 48

## G

general settings  
black/white lists 69  
notification protocol 69  
service account 69  
get key file 13  
getting started 29  
groups 33, 52  
AD groups 54  
create 53  
form 54  
types 54

## I

incidents  
monitoring 21  
statistics 61

install Dr.Web for Microsoft Exchange  
Server 22, 25  
check 77  
system requirements 23  
installation program 25, 75  
log 75

## K

key file 12, 13  
acquisition 13  
anti-spam support 45  
update 14  
validity 12

## L

license 12  
acquisition 13  
anti-spam 45  
key file 12  
update 14  
validity 12  
licensing 12  
logging 74  
event log 74  
installation program log 75

## M

mail notifications 21  
manage  
black and white lists 69  
groups 52



# Index

manage

- profiles 34
- quarantine 58
- reports 63

## N

- notifications 37
- protocol 69

## O

- on-demand scanning 15
- operation mode 88

## P

- post-installation review 77
- proactive scanning 15
- profiles 33
  - accompanying text 51
  - anti-spam 45
  - create 34
  - manage 34
  - message filtering 48
  - notifications 37
  - priority 37
  - scanning 42

## Q

- quarantine 21, 58

## R

- remove Dr.Web for Microsoft Exchange Server 22, 28
- reports 21
  - schedules 63
  - types 63
- requirements 23

## S

- scanned objects 11
- scanning
  - background scanning 15
  - configure 42
  - on-demand scanning 15
  - proactive scanning 15
- server roles 15, 16
- service account 69
- statistics 21
  - incidents 61
  - view 61
- system requirements 23

## T

- technical support 91
- test
  - spam detection 80
  - virus detection 79
- test spam message 80
- transport agent 18
- transport agents 15



# Index

troubleshooting 77, 79, 80

## U

update

- check module 78

- command-line parameters 81

- license 14

- virus databases 73

updater 73, 81

## V

virus events

- event log 21

- monitoring 21

- notifications 21

- reports 21

- statistics 21, 61

VSAPI 15

- registry keys 84

- settings 84

## W

white list 69

