Dr.WEB

for Microsoft Exchange Server

Administrator Manual

Жасағаны

دافع عن إبداعاتك

Защити созданное

Defend what you create

Protégez votre univers

Verteidige, was du erschaffen hast

Захисти створене

保护您创建的一切

Защити созданное

Proteggi ciò che crei

Защити созданное

Жасағаныңды қорға

Verteidige, was du erschaffen hast

Защити созданное

Proteggi ciò che crei

Захисти створене

Defend what you create

脅威からの保護を提供します

Protégez votre univers

Proteggi ciò che crei

Захисти створене

دافع عن إبداعاتك

脅威からの保護を提供します

Defend what you create

Жасағаныңды қорға

دافع عن إبداعاتك

دافع عن إبداعاتك

Protégez votre univers

保护您创建的一切

Защити созданное

脅威からの保護を提供します

Захисти створене

Verteidige, was du erschaffen hast

Dr.Web for Microsoft Exchange Server
Version 11.0
Administrator Manual
10/12/2017

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

1. Document Conventions

The following conventions and symbols are used in this document:

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

2. Introduction

Thank you for purchasing Dr.Web for Microsoft Exchange Server (hereinafter referred to as Dr.Web). This anti-virus product is a powerful tool against threats propagated through email 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, and contains information on all the main features of the software and contact details for technical support.

2.1. What is Dr.Web

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

Dr.Web can perform the following functions:

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

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

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

The plug-in operates on the Dr.Web CMS (Central Management Service), which supports the central configuration of application settings and components and remote administration via protected protocol HTTPS. Dr.Web CMS features an internal web server Dr.Web CMS Web Con-

sole with client authentication, thus, only the authorized administrators can access the applica-
tion settings.

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

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

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

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

2.2. Scanned Objects

Dr.Web scans incoming and outgoing messages in real-time mode. It checks the following ele-
ments of email messages:

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

Dr.Web scans all objects before they are processed by the client part.

2.3. Technical Support

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

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

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

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

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

3. Licensing

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

3.1. 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 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.

3.2. Getting License Key File

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

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

> ⚠ If Dr.Web Agent is installed on your computer, you can select an option of getting key file from the central protection server during Dr.Web installation.

The key file should be obtained before installing Dr.Web, as the installer requests the path to a key file.

To acquire a license key file by email

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 that is typed on the registration card.

4. The license key file will be sent as an archived attachment to the email 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 evaluation purposes you may be provided with a *demo license key* file. Demo license allows you to access full functionality of the Dr.Web 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 email, 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 website at http://www.drweb.com.

3.3. Updating License

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 supports hot license update without stopping or reinstalling the plug-in.

To update the license key file

1. To update the license key file, replace an old license key file with the new file in the plug-in installation folder.

2. Restart Dr.Web for MSP Scanning Service.

3. Dr.Web automatically switches to the new license.

For more information on license types, visit the Doctor Web official website at http://www.drweb.com.

4. Principles of Operation of Dr.Web

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 integrates Dr.Web technologies into mail processing and storage carried out by Microsoft Exchange Server.

The product has a convenient web interface to facilitate management of scanning settings and virus events monitoring via Internet browser.

4.1. 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. **Application of filtering rules** (adjusted on the Filtering section).

   - 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.

   - 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.

2. **Spam check** (performed in case you have the "Anti-Virus&Anti-Spam" license and only for the emails 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 Anti-Spam section. Then the Anti-spam component 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.

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.

4.2. Quarantine

You can apply the **Quarantine** attachment action to objects that cannot be cured, to bad and suspicious objects. 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. For more information about quarantined objects, see section Working with Quarantine.

4.3. Virus Events Monitoring

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

- 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**.

- Statistics. It gives the possibility to view the information about a number of objects checked since the installation of Dr.Web or the last cleaning of statistics data.

- Incidents. It gives the possibility to view the list of messages processed by the application and that contained viruses or were spam, as well as the filtered messages.

5. Installation and Removal

Dr.Web is distributed as a ZIP-archived folder containing the installation file (**drweb-[version]-av-exchange-windows-x64.exe** or **drweb-[version]-av-exchange-windows-x86.exe**), where **[version]** indicates product's version number.

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

> For proper installation and removal of Dr.Web, you must be a member of the **Domain Users** group and the **local administrators** group on the computer where Microsoft Exchange Server is installed.
>
> ---
>
> If you are using Windows Terminal Services, use the **Add or Remove programs** utility to install and uninstall the Dr.Web software.

5.1. System Requirements

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

Specifica-tion	Requirement
RAM	512 MB or more
Disk space	1 GB or more

Operating system	**32-bit platforms**
	
	For Microsoft Exchange Server 2003:
	
	• Microsoft® Windows Server® 2003x86 with:
	  ▪ MSXML 4.0 Service Pack 3 (Microsoft XML Core Services);
	  ▪ SP1 or higher.
	
	64-bit platforms
	
	For Microsoft Exchange Server 2007/2010:
	
	• Microsoft® Windows Server® 2008 x64;
	• Microsoft® Windows Server® 2008 R2;
	
	For Microsoft Exchange Server 2013:
	
	• Microsoft® Windows Server® 2008 R2;
	• Microsoft® Windows Server® 2012;
	• Microsoft® Windows Server® 2012 R2:
	  ▪ SP1 or higher is required for Exchange Server 2013;
	
	For Microsoft Exchange Server 2016:
	
	• Microsoft® Windows Server® 2012;
	• Microsoft® Windows Server® 2012 R2;
	• Microsoft® Windows Server® 2016:
	  ▪ Cumulative Update 3 (or higher version) for Exchange Server 2016 is required.

Microsoft Exchange Server	• Microsoft® Exchange Server 2003; • Microsoft® Exchange Server 2007 x64 with SP1; • Microsoft® Exchange Server 2010 x64; • Microsoft® Exchange Server 2013; • Microsoft® Exchange Server 2013 with SP1 (Cumulative Update 5 or running Exchange2013-KB2938053-Fixit script is required); • Microsoft® Exchange Server 2016.

5.2. Compatibility

Before installation of Dr.Web, please review the following information on product compatibility:

1. Dr.Web for Microsoft Exchange Server of version 11.0 is compatible only with Dr.Web products of major version 11.

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 anther anti-virus software installed then it is necessary to uninstall it using the installation file or standard tools of the OS.

3. Dr.Web for Microsoft Exchange Server of version 11 is not compatible with Dr.Web for Microsoft ISA Server and Forefront TMG of version 11.

⚠️ When SpIDer Guard is enabled, exclude Microsoft Exchange Server folders and processes from scanning by SpIDer Guard (the recommended exclusions are listed in Microsoft documentation) in order to make sure Microsoft Exchange operates correctly.

5.3. Installing Dr.Web

Before installation

- Install all critical updates released by Microsoft for the OS version used on your computer (available at http://windowsupdate.microsoft.com).
- Check the file system with system utilities and remove the detected defects.
- Close all active applications.

⚠️ If you are using Microsoft Exchange Server 2013 with SP1, but without Cumulative Update 5, run the **Exchange2013-KB2938053-Fixit** script available on the Microsoft official website at http://support.microsoft.com/kb/2938053 before installation to prevent errors of registering the transport agents during the installation.

To install Dr.Web

1. Run the installation file **drweb-[version]-av-exchange-windows-x64.exe** if you are using Microsoft Exchange Server 2007/2010/2013/2016, or **drweb-[version]-av-exchange-windows-x86.exe** for previous versions of Exchange server. The **InstallShield Wizard** will open on the first window of the installation process.

2. To continue installation, you should read and accept the terms of the License Agreement by selecting **I accept the terms in the License Agreement**.

   Click **Next**.

3. Stop the Microsoft Exchange Transport service (only if you are using Microsoft Exchange Server 2007/2010/2013/2016).

To do so, click **Open the list of services** link, right-click the service in the list and then click **Stop**. Once the service is stopped, click **Next**.

> ⚠️ Stopping Microsoft Exchange Transport service manually is required to preserve the installation integrity on the server operating under load.
>
> In some cases Microsoft Exchange Transport service may take considerable time to stop.

4. Select the licensing type. You can register your license later, specify the path to the valid license key file or use the key file from the central protection server if Dr.Web Agent is installed on your computer.

   Click **Next**.

   > ⚠️ For correct plug-in operation, specify the path to the drweb32.key license key file.
   >
   > To register license after installation or to <u>renew</u> it, copy the valid license key file to the program installation folder, then restart Dr.Web for MSP Scanning Service.

5. Before starting the installation procedure, click **Installation parameters** to configure the following parameters:

   • **Install transport agents** – allows you to install transport agents (enabled by default). If you are using Microsoft Exchange Server 2007/2010/2013/2016, enabling this option registers the DRWTransportAgent.dll library and its transport agents (anti-virus and anti-spam) by Microsoft Exchange Transport service. If you are using Microsoft Exchange Server of previous versions, enabling this option registers the DrWebSink.dll library and enables the anti-spam agent in Microsoft Internet Information Services (IIS).

   • **Install VSAPI** – allows you to install the DrWebVSAPI.dll component for scanning via VSAPI (not supported in Microsoft Exchange Server 2013) provided by Microsoft Exchange Information Store service. If this option is enabled, you can also configure additional parameters: enable scanning of the outgoing messages, proactive and background scanning.

   You can also enable the transport agents installation and registration monitoring by selecting the **Enable transport agents monitoring** option. During the installation on Microsoft Exchange Server 2007/2010/2013/2016, transport agents are registered in SMTP transport system by Exchange PowerShell, which does not close automatically, so you will need to enter the `exit` command manually to complete installation.

   Click **OK**.

   > ⚠️ To avoid transport agents registration errors during the installation, please make sure that the RemoteExchange.ps1 script is installed on Microsoft Exchange Server (the script is located by default in the C:\Program Files\Microsoft\Exchange Server\V14\bin\ folder on Microsoft Exchange Server 2010 or in the C:\Program Files\Microsoft\Exchange Server\V15\bin\ folder on Microsoft Exchange Server 2013).

6. If you are re-installing the application, you may use the saved configuration (if the corresponding option was selected during its removal) or delete it and re-configure the application after installation.

Click **Next**.

The installation of Dr.Web on your computer will start. By default, program files are copied to %Program Files%\DrWeb for Exchange and %Program Files%\Common Files\Doctor Web folders. the event logs and auxiliary files are copied to %Program Data%\Doctor Web folder.

7. If you selected the **Enable transport agents monitoring** option when configuring thee installation parameters, you need to exit the monitoring window after the transport agents are installed and registered. Enter the `exit` command in PowerShell. The "**Dr.Web AntiVirus Agent enabled**" and "**Dr.Web AntiSpam Agent enabled**" messages in PowerShell indicate the successful agents registration by Microsoft Exchange Transport service. Enter the exit command in PowerShell.

8. Once the installation is complete, click **Finish**.

> ⚠ If Microsoft Exchange POP3 or Microsoft Exchange IMAP4 service do not operate correctly after Dr.Web is installed on the computer, it is recommended to restart them.
>
> When you install the application from the **drweb-[version]-av-exchange-windows-x86.exe** file, you will be prompted to restart the computer. If you install the plug-in form the **drweb-[version]-av-exchange-windows-x64.exe** file, the restart is not required: the Microsoft Exchange Transport service is started automatically, resulting the correct operation of the server. However, if the POP3 and IMAP4 supporting services are running on the server, restarting the Microsoft Exchange Transport service may disconnect them from the server transport system. In this case it is recommended to wait until Microsoft Exchange Transport and the installed application services are started and then to restart the Microsoft Exchange POP3 and/or Microsoft Exchange IMAP4 services manually (or to restart the computer).

To reinstall Dr.Web

1. Uninstall Dr.Web.

> ⚠ The application configuration file cmsdb is not deleted by default on deleting the application. Therefore, all user settings are saved and may be used after the next installation of the product. However, if you install a newer version that contains new basic configuration parameters, you cannot use the saved configuration file "as is", because it can lead to failures in the operation of application.
>
> If you prefer to re-use the saved configuration parameters, please contact Doctor Web technical support to inquire about the Dr.Web CMS parameters compatibility in different versions of the application. Generally, if the newer version contains additional parameters, it is sufficient to add the new variables to the existing configuration base and specify their types and default values correctly.

2. Delete the **cmsdb** and **cmstracedb** files from the %ProgramFiles%\DrWeb for Exchange folder manually.

3. Install Dr.Web, following the instructions given above.

5.4. Removing Dr.Web

To uninstall Dr.Web

1. Run the application installation file **drweb-[version]-av-exchange-windows-x64.exe** or **drweb-[version]-av-exchange-windows-x86.exe** depending on the Exchange server version you are using. The **InstallShield Wizard** will open on the first window of the installation process.

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

2. Stop the Microsoft Exchange Transport service (only if you are using Microsoft Exchange Server 2007/2010/2013/2016). To do this, click **Open the list of services** link, right-click the service in the list and then click **Stop**. Once the service is stopped, click **Next**.

3. If you want to save current application settings for further use, e.g., after reinstalling it, select **Save settings**. Click **Remove**.

4. During the application removal process, the transport agents for Microsoft Exchange Server 2007/2010/2013/2016 in SMTP transport system are deleted using Exchange PowerShell, where you need to confirm the removal by entering `Yes` (or `Y`). When transport agents are deleted, enter the `exit` command to close Exchange PowerShell.

5. To complete the application removal, you need to restart the computer. Click **Restart now** or **Later**.

6. Anti-Virus Scanning and Anti-Spam Check for Microsoft Exchange Server

The anti-virus plug-in Dr.Web supports the VSAPI (the Virus Scanning Application Programming Interface developed by Microsoft for Exchange Servers) when installed on Microsoft Exchange Server 2003/2007/2010.

The plug-in also supports server roles for Microsoft Exchange Server 2007/2010/2013 SP 1/2016 and can be installed on the servers with different roles.

Dr.Web also supports such concept of Microsoft Exchange Server 2007/2010/2013/2016 as transport agents (anti-virus and anti-spam agents).

Microsoft Exchange Server version	Available components for anti-virus scanning and mail filtering	Available components for anti-spam check and mail filtering
2003	DrWebVSAPI.dll (Backend)	DrWebSink.dll (IIS)
2007	DRWTransportAgent.dll (Hub, Edge) DrWebVSAPI.dll (Mailbox)	DRWTransportAgent.dll (Hub, Edge)
2010	DRWTransportAgent.dll (Hub, Edge) DrWebVSAPI.dll (Mailbox)	DRWTransportAgent.dll (Hub, Edge)
2013	DRWTransportAgent.dll (Frontend, Backend)	DRWTransportAgent.dll (Frontend, Backend)
2013 SP1	DRWTransportAgent.dll (Edge, MailBox)	DRWTransportAgent.dll (Edge, MailBox, CAS)
2016	DRWTransportAgent.dll (Edge, MailBox)	DRWTransportAgent.dll (Edge, MailBox)

> ⚠️ If you need to install Microsoft Exchange Server anti-spam agents after you install Dr.Web, you need to lower Dr.Web agent priority. This will allow Microsoft Exchange Server agents to scan messages, and then Dr.Web agents will scan them.

6.1. Virus-Scanning Applications Based on VSAPI

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

- Proactive

- On-demand
- Background

If the sender address is included into the values list of TrustedEmails variable, the email will not be checked for spam and viruses and will be considered as not being spam or virus.

Proactive scanning

All email 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 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 and manage scanning using the **Doctor Web For Exchange Start Background Scanning Task** in the Windows Task Scheduler. By default, the task starts daily at 01:15 AM.

> ⚠️ If you use both VSAPI and transport agents on the same server, you need to disable the check for outgoing messages by VSAPI when they are picked up by transport system from the Store. To disable it, specify the **0** value for the **TransportExclusion** parameter in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS \VirusScan` registry key.

For more information on the settings of anti-virus scanning based on VSAPI see Microsoft Exchange Server Anti-Virus Scanning Settings.

6.2. Server Roles

Exchange Server 2007/2010/2013 SP1/2016 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 and 2013 SP1 includes five server roles: Mailbox Server, Client Access Server, Hub Transport Server, Unified Messaging Server and Edge Transport Server. Exchange Server 2016 includes two server roles: Mailbox Server and Edge Transport Server.

The roles listed below support anti-virus and anti-spam scanning:

- **Mailbox Server** provides the main services, hosts mailbox and public folder databases and allows to perform the anti-virus scanning via VSAPI.

- **Hub Transport Server** routes mail within the Exchange organization, allows to apply security policies to the messages and check them for viruses and spam.

- **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 can be installed on the server with any of these roles or their combinations.

Microsoft Exchange Server 2013 does not use the concept of server roles and is based on the Frontend–Backend architecture, so the anti-virus and anti-spam checks are always performed by the agents on the SMTP transport level.

6.3. Transport Agents

The concept of Microsoft Exchange 2007/2010/2013/2016 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 reacting on events of message receiving.

- **Routing Agent** – allows reacting on events of message routing.

Exchange Server 2007/2010/2013/2016 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 email processing, anti-virus and anti-spam check.

Dr.Web uses transport agents to check for viruses and spam only the mail received via SMTP (in case you have "Anti-Virus&Anti-Spam" license).

6.3.1. Anti-Spam Transport Agents

Anti-spam transport agents respond to SMTP event **OnEndOfData** related to the completion of receiving the email contents by the server.

The email is not checked for spam and is considered as not being spam if

- the sender domain is included into the values list of TrustedDomains variable;
- the sender address is included into the values list of SpamTrustedEmails variable.

Unlike the white list of Anti-spam that contains the exclusions list based on the sender and recipient email addresses (for example, if the sender and the recipient addresses belong to the same domain, and the sender's address is from the white list, the message can still be considered as spam), the TrustedDomains and SpamTrustedEmails variables exclude the message from the spam check definitively. Therefore, it is not generally recommended to exclude domains by adding them to these variables values lists, but to use the white list of Dr.Web Administrator Web Console for this purpose.

If the sender domain does not belong to the trusted list, the message is put into the line waiting to be checked. If it is considered as spam after the check, it may be deleted, blocked, redirected to another email address, marked as Junk email, or a prefix can be added to its subject. All these actions are fixed in the Incidents section of the Dr.Web Administrator Web Console and in the server log.

If the message is deleted as spam or blocked by filtering rules, the transport agent either closes the connection to the client or produces the **RejectMessage** response containing the following text: **Dr.Web AntiSpam Agent: Message was rejected as spam**. You can select one of these actions using Dr.Web CMS Web Console. The message does not reach its recipients in any case.

If the message is redirected to another email address or marked as Junk email, an X-header is added to its header.

An **X-DrWeb-RedirectTo** header is added to the redirected message, together with new destination address. This header is used by anti-virus transport agent, as it deletes the list of initial recipients and replaces it by the address from the header, if the message does not contain any viruses or other threats. The message does not reach the initial recipients in this case. But it will reach the initial recipients if it is marked as **Junk** email. In this case, a **X-MS-Exchange-Organization-SCL** header is added to the message, together with the message distrust index score. This header is recognized by Microsoft mail clients and Microsoft Exchange Server. If the score is between 4 and 7, the clients move such message to the **Junk** folder (in case they are correctly configured). If the score is larger than 7, the message is rejected by the transport system of Microsoft Exchange Server.

Adding prefix to the message subject does not affect receiving it by the clients. The recipients can configure their own rules and filters to process messages with such prefixes.

6.3.2. Anti-Virus Transport Agents

The anti-virus transport agent responds to the SMTP event **OnSubmittedMessage** related to putting the message in waiting line for processing by the serve transport system. Messages cannot be excluded from the check by this agent.

If the sender address is included into the values list of TrustedEmails variable, the email will not be checked for spam and viruses and will be considered as not being spam or virus.

The check anti-virus agent consists of anti-virus checks of message body and all its attachements. The infected message can be deleted, blocked or moved to Quarantine (the suspicious objects can also be ignored without applying any actions to them). All these actions are fixed in the Incidents section of the Dr.Web Administrator Web Console and in the server log.

If the infected objects are configured to be deleted, after the first infected attachment is detected, the scanning cycle is interrupted and an event to delete the message is sent to the server transport system. All the events are fixed in the Incidents section of the Dr.Web Administrator Web Console and in the server log, but the recipients and senders are not notified about the message deletion. This is the mos rapid reaction on detection of the infected objects, but not the most secure, so it is recommended to move such objects to Quarantine to prevent possible data loss. Moreover, the EWS (Exchange Web Services) protocol is supported on the server, you can configure sending the notifications about deleting the infected objects to a special email address using Dr.Web Administrator Web Console or Dr.Web CMS Web Console.

If the attachment is blocked after it is filtered and the infected objects are configured to be moved to Quarantine, all the infected or blocked attachments in the initial messages are replaced by the text files describing the reason of deleting the initial files. Then, the messages is checked for a **X-DrWeb-RedirectTo** header added by the anti-spam transport agent, and in case the message has such header, it is delivered to the recipients. If the message should be redirected, each recipient gets the **SmtpResponce** notification with the following text: **Dr.Web AntiVirus Agent: Message was redirected as spam**. The message without the infected attachments is sent to the email address specified in the **X-DrWeb-RedirectTo** header.

6.4. Dr.Web Services

The operation of Dr.Web is based on the 7 following services:

- Dr.Web Scanning Engine – contains the Dr.Web scanning engine.
- Dr.Web CMS – supports the distributed application components management system, controls and analyzes the modules functionality. This service supports the application components settings database, the incidents database and controls the statistics of components parameters.

- Dr.Web CMS Web Console – has a built-in server providing the use of administrative consoles via Internet browser.

- Dr.Web for MSP Scanning Service – prepares objects intercepted by application filters to the anti-virus scanning, processes the scanning results.

- Dr.Web for MSP Component Host – instantiates all additional application components requested during its operation.

- Dr.Web for MSP Requests Queue – supports the asynchronous requests queue of application tasks, which allow to postpone their run.

- Dr.Web SSM – controls the operation of the applications based on the CMS platform and restarts the main services.

Dr.Web Scanning Engine, Dr.Web CMS and Dr.Web SSM services are started on completion of the application installation. Other services start when the application operation requires their start.

> ⚠ When restarting the services manually, it is important to stop the Dr.Web CMS and Dr.Web SSM services in a right order because they depend on each other: always stop the Dr.Web SSM service at first and then the Dr.Web CMS one. After both services are stopped, you can start only the Dr.Web SSM service to reactivate the operation of the application.

7. Dr.Web Administrator Web Console

Operation of Dr.Web can be configured by means of the Dr.Web Administrator Web Console (see Figure 1).

To launch Dr.Web Administrator Web Console

> ⚠️ For correct operation of Dr.Web Administrator Web Console use one of the following browsers:
>
> - Internet Explorer 11 or higher
> - Chrome
> - Microsoft Edge 20 or higher
>
> For correct operation of Dr.Web Administrator Web Console in Internet Explorer you need to additionally allow the use of the AJAX technology by disabling the enhanced security configuration for administrators:
>
> - In Windows Server 2003: open **Control Panel** -> **Add or Remove Programs** -> **Add/Remove Windows Components**, clear the **Internet Explorer Enhanced Security Configuration** check box, then click **Next**. Click **Done**.
> - In Windows Server 2008: open **Server manager** and click **Configure IE ESC**, then select the corresponding check box in the **Administrators section**.
> - In OC Windows Server 2012: open **Server manager**, open the **Local server** tab and select **IE Enhanced Security Configuration**, then select the corresponding check box in the **Administrators** section.

To launch Dr.Web Administrator Web Console, in an Internet browser open the following page:

`https://<Exchange Server address>:2080/exchange,`

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. Administrator accounts can be added, edited or deleted by means of Dr.Web CMS Web Console.
>
> On the first launch of the web console use the login **root** and the password **drweb** of the default administrator account.
>
> If you cannot launch Dr.Web Administrator Web Console on the remote computer, make sure that required inbound Windows Firewall rules are created.
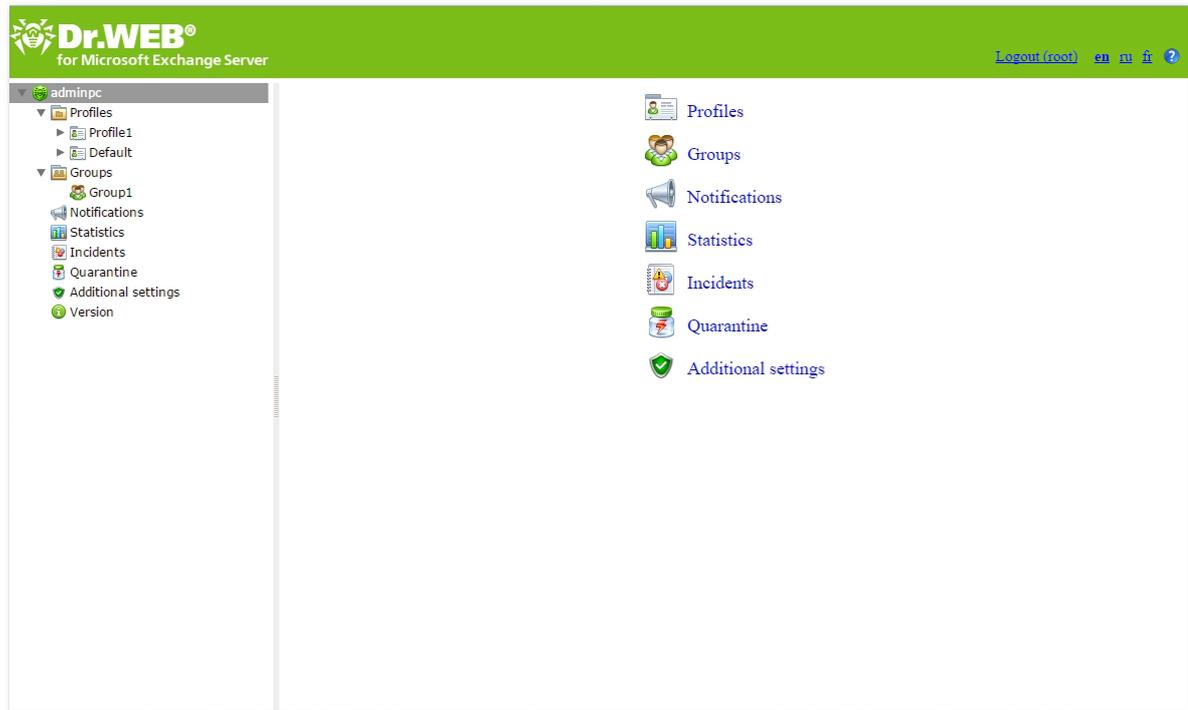
Figure 1. Dr.Web Administrator Web Console

Interface

Dr.Web Administrator Web Console consists of two parts:

1. Console tree 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 Dr.Web Administrator Web Console language changing option is located. You can select English, Russian or French language. An option which opens the help on the web console is located next to the language option.

Administration

Dr.Web Administrator Web Console has the following access levels:

- with a possibility to change settings
- without a possibility to change settings

You can specify the access level while adding a new administrator account.

7.1. Groups and Profiles

To simplify management of your Exchange environment Dr.Web 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 web console tree and are divided into the following subsections:

- 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 are available only with the "Anti-Virus&Anti-Spam" version of Dr.Web, i.e. if you have an appropriate license key file (see License Key File).

- Filtering – this section allows to configure the Internet traffic filtering.

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).

7.1.1. Creating and Configuring Profiles

During installation of Dr.Web the **Default** profile, which cannot be renamed or deleted, is created automatically. This profile will remain active for all the traffic as long as you do not create a new profile and assign it to a certain group of clients. 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 Dr.Web Administrator Web Console tree (see Figure 2).

Figure 2. Profiles pane

For each profile the information on its settings is displayed in the list and profile priority is determined by its location in the table.

To create a new profile

1. Click **Create profile** above the list of available profiles.

   > ⚠ Alternatively, to create a new profile, you can right-click **Profiles** in the console tree and select **Create profile**.

2. In the opened window, enter a profile name. A new profile will appear under **Profiles** in the console tree. If a profile with the same name already exists, a new profile will not be created.

To rename a profile

- select the profile on the **Profiles** pane and click **Rename profile**.

To delete a profile

- Select it on the **Profiles** pane and click **Remove profile**.

⚠️ Alternatively, to rename or delete a profile, you can right-click it in the console tree and select the corresponding item.

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: Scanning, Anti-spam or Filtering.

7.1.1.1. Profile Priority

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 the traffic sent to or by this client.

The priority level is adjusted on the **Profiles** pane by moving profiles up and down the list. Use the buttons ↑ and ↓ to move the profile. 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.

7.1.1.2. Scanning

The scanning process is adjusted in the **Scanning** section. Changes in this section affect the types of checked objects and therefore they determine the anti-virus 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** in the web console tree. The **Scanning** pane will open (see Figure 3).
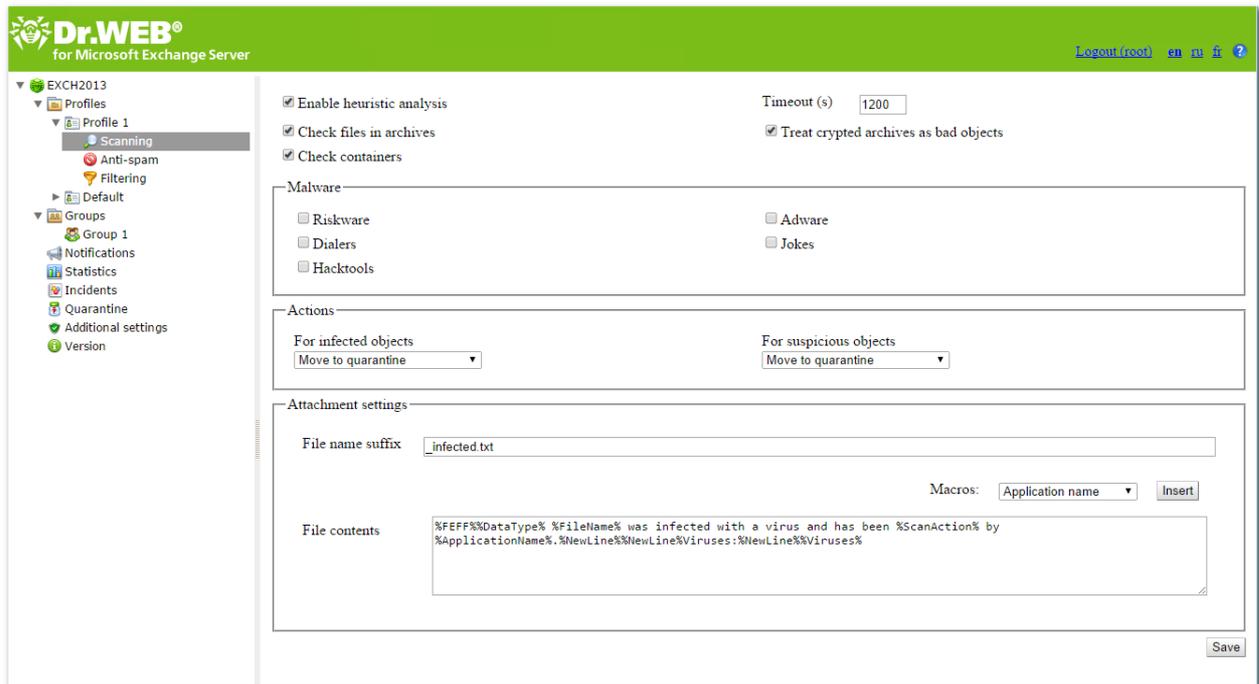
Figure 3. Scanning pane

2. By default, the heuristic analyzer and scanning of archives and containers 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**, **Check files in archives** and **Check containers** options at the top of the **Scanning** pane.

> ⚠ It is not recommended to disable the heuristic analyzer and scanning of files in archives in attachments as it considerably decreases the anti-virus protection level.

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 1200000 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. You can select types of objects that will be treated as bad in Dr.Web CMS Web Console.

3. In the **Malware** group box below, select the types of objects to check messages for. The action specified for infected objects will be applied to the selected programs.

4. In the **Actions** section below, use the drop-down lists to choose the actions for curable, incurable and suspicious objects. You can choose from the following:

    *   **Move to quarantine**. The object will be sent to the quarantine (see Working with Quarantine).

    *   **Delete**. The object will be deleted.

- **Skip**. The objects will be passed on to the recipient(s) untouched (available only for suspicious objects).

- **Archive**. The infected file will be renamed to **inf*.tmp**, where * is an arbitrary symbol set, and added to a ZIP archive and its copy will be moved to the quarantine. You can specify a password for the archive and maximum size of the archived file in the Additional settings section.

> ⚠ By default, the **Move to quarantine** action is set for all the types of objects.

5. In the **Parameters of added attachments** group box, you can change the name suffix for the text file which will be attached to an infected email 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. To add a macro, select it in the list and click **Insert**.

6. When you finish configuring scanning process, click **Save**.

7.1.1.3. Anti-spam

Before anti-spam scanning starts, the addresses of the recipients and senders are analyzed against the black and white lists, which are specified on the **Anti-spam** section. Then the Anti-spam component checks the message.

The Anti-spam component analyzes the contents of messages and determines whether it is spam or not according to the spam-rate value summed up from various criteria. Depending on the analysis result, Anti-spam assigns an integer number to the message. A large number means that the message is likely to be spam. You can change the threshold value that is used to detect if the message is spam in Dr.Web CMS Web Console.

> ⚠ Please forward false positive to vrnonspam@drweb.com and skipped spam to vrspam@drweb.com.

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. If your key file supports the Anti-spam component then spam filtering should be enabled by default, i.e. the **Enable Anti-spam** 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 (**%ProgramFiles%\DrWeb for Exchange\drweb32.key**) with a text editor and check 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! Do not save the file when closing the text editor.

To configure the settings of the Anti-spam component

1. Click **Anti-spam** in the Dr.Web Administrator Web Console console tree. The **Anti-spam settings** pane will open (see Figure 4).

Figure 4. Anti-spam settings pane

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

3. In the **Subject prefix** field, you can change the prefix, which will be added to the subjects of email messages considered as spam. The default prefix is ***** SPAM *****.

4. In the **Email** field, enter the email address you can specify the email address to redirect the spam messages.

5. 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:

   - **Add prefix to subject**. The prefix defined in the **Subject prefix** field will be added to the message subject.

   - **Skip**. The message will be passed through to the recipient.

   - **Move to junk**. The **X-MS-Exchange-Organization-SCL** header is added to the message, together with the message distrust index score. If the score is between 4 and 7, properly configured clients will move such message to the junk folder.

   - **Redirect**. The message will be redirected to the address specified in the **Email** field.

- **Block**. Message sending will be blocked.

6. On the **Black and white lists** section, you can configure the use of the lists of trusted and distrusted addresses:

   - Select **Enable** to enable the use of the lists. You can add email 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 address to the list, enter it in the **Email** field and click **Add** on the section of the white or black list. The address will be added to the selected list.

   - To delete an address from the list, select it and click **Remove** on the section of the list this address is included in.

   - You can also use the **Export** and **Import** 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 while creating and/or editing the files of black and white lists manually, you need to add prefix to the emails: **"+"** to add the email into the white list, **"-"** to add the email 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).
   >
   > In some cases adding a domain to the white list as described above might not work. To exclude this domain from spam check definitively, add it to the values list of the TrustedDomains variable.

7. When you finish setting up the Anti-spam component, click **Save**.

7.1.1.4. Filtering

Dr.Web allows to use a filtering system to reduce the server load in case of spam attacks by taking the unnecessary messages out of the server transport system before they are checked for viruses and spam. For effective filtering, creating an optimal filtering rules set without contradictory or excess rules is essential.

Before filtering, the group which sender of the message belongs to is identified. If the sender belongs to one of the created groups, filtering rules specified in the profile corresponding to this group will be applied to the message. If the sender does not belong to any groups, settings of the **Default profile** will be applied to the message. Therefore, if it is necessary to apply the filtering rule to all the messages not included in groups, create this rule in the **Default profile settings**.

If the sender profile does not contain any limits, the message is filtered by the rules created for the recipients addresses. Every address from the recipients list relates to its own group (an AD group or a list of email addresses), and every group has its own profile assigned to it. The pro-

file with the highest priority is applied. Therefore, if you want to set limitations on a created group of recipients, do not create filtering rules in the **Default profile**, but create a separate profile to assign to this group.

> ⚠ If it is necessary to create specific groups of recipient without any limits imposed by filtering, do not configure filtering rules in the Default profile, because if the message is filtered by applying the filters set for senders, it is excluded from further processing by recipients filters.

At first every message is processed by the anti-spam transport agent. At this stage the filtering rules are applied to the message as to the whole entity. Messages are filtered by the number of senders and recipient, by subject, number of attachments, etc. After the filtering, unfiltered messages are checked for spam (see Scheme 1).

After checking for spam, the message is processed by the anti-virus agent. At this stage the filtering rules are applied to the message as to the set of files, the message body is considered as a file too. Messages are filtered by by file size, name, extension, etc. After the filtering, unfiltered messages are checked for viruses (see Scheme 1).
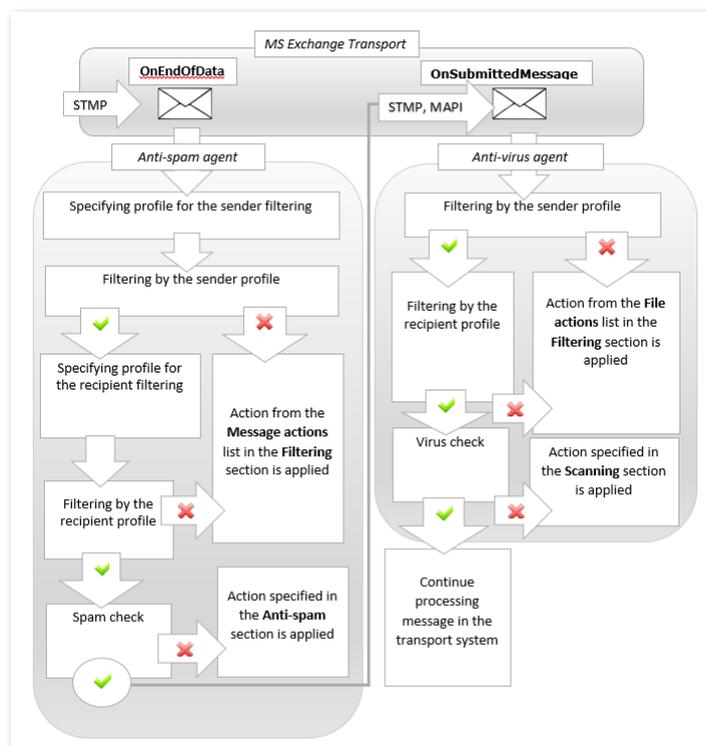
Scheme 1. Filtering messages in the transport system

The traffic filtering is configured in the **Filtering** pane (see Figure 5). Filters are applied according to certain rules which can be added by the administrator. These rules determine the conditions for the filtering by the properties of messages and their attachments.
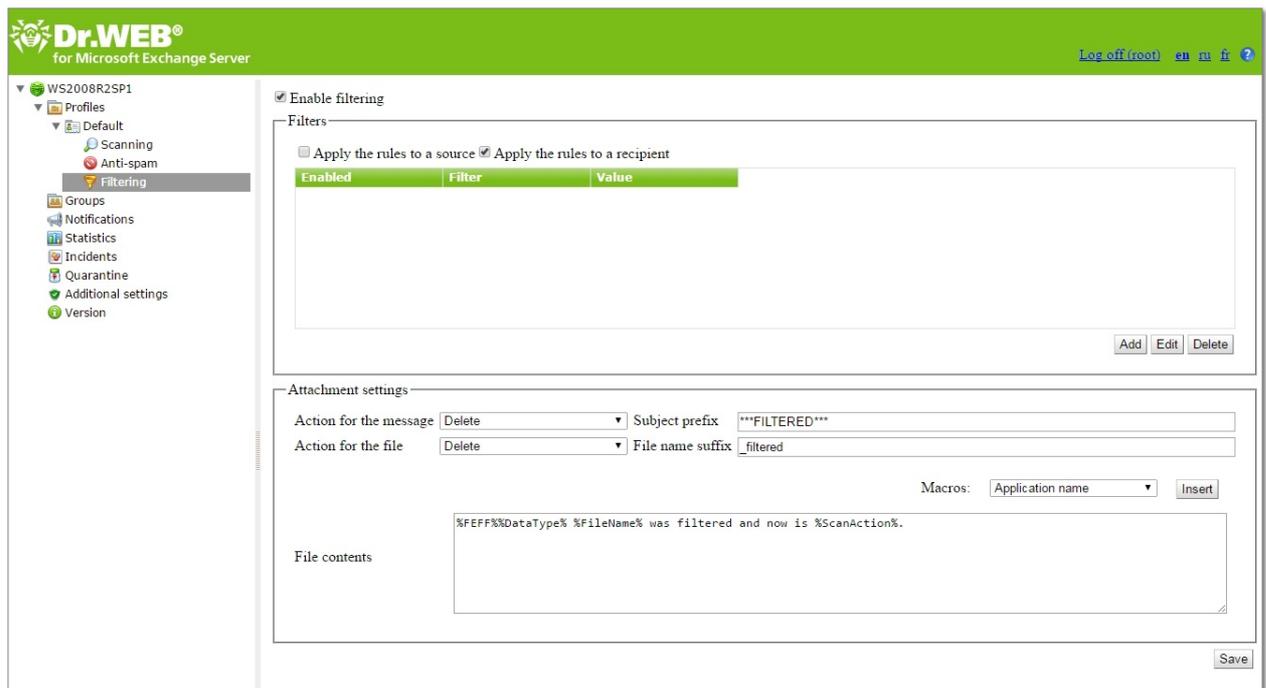
Figure 5. Filtering pane

If you are working with the **Filtering** component for the first time, the list of rules will be empty. You can create and configure filtering 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.

   You can apply fileting rules to either the source or to the recipient, or to both source and recipient.
   For example, you can create a rule for the message subjects that includes the word "Attention". If you set this rule for the source only, you will not be able to send messages with the word "Attention" in the subject. If you set this rule for the recipient, you will not be able to receive messages with the word Attention in the subject. If you set this rule for both source and recipient, you will not be able to receive nor to send messages with the word "Attention" in the subject.

2. Enable one or more filters from the list by selecting the corresponding check boxes. If the list of filters is empty, you can create them.

3. Select the actions for the email messages with attachments on the **Attachment settings** section.

   For the messages, you can select one of the following actions:

   • **Delete** – to delete message.

   • **Add prefix to subject** – to let the message through and add to its subject a prefix specified in the Subject prefix.

For attachments, the following actions are available:

- **Move to quarantine** – to isolate the attachment in quarantine.
- **Delete** – to delete the attachment.

In the **Subject prefix** field, specify the prefix added to the subject of the filtered message. The default prefix is *****FILTERED*****.

In the **File name** suffix field, specify the suffix added to the name of the text file attached to the filtered message. The default suffix is **_filtered.txt**.

In the **File contents** field, enter the text of the file added to the filtered message. While editing the text, you can add macros from the **Macros** drop-down list.

To create a filtering rule

1. Click **Add** under the filters list. A **Filter rule** window will open (see Figure 6). You can enter the name of the rule and specify its conditions in this window.

Filter rule

Name New rule

Satisfy:

◉ All conditions   ○ Any of conditions   Add Edit Delete

Ok Cancel
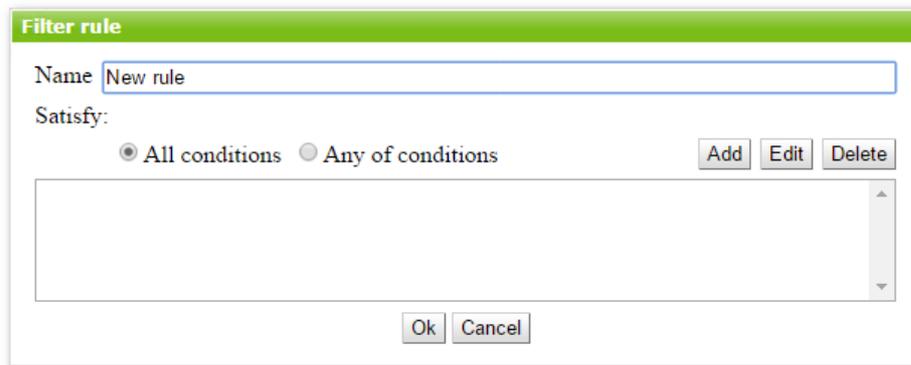
Figure 6. Configure filtering rule

2. You can add one or more filtering conditions and specify if the messages should comply with all of them or with any of them. To add a condition, click **Add**. In the new window, select the condition type, specify the value and the type of compliance with the specified value. The types of conditions, compliance and possible values are listed in the table below:

Condition type	Compliance type	Value
Data type	Equal	File
	Not equal	Message
Data source	Equal	Specified manually
	Not equal	
	Contains	
	Not contains	
	Matches	

Condition type	Compliance type	Value
	Not matches	
Data destination	Equal	Specified manually
	Not equal	
	Contains	
	Not contains	
	Matches	
	Not matches	
Protocol	Equal	SMTP
	Not equal	MAPI
Number of recipients	Equal	Specified manually
	Not equal	
	Contains	
	Not contains	
	Matches	
	Not matches	
File name	Equal	Specified manually
	Not equal	
	Contains	
	Not contains	
	Matches	
	Not matches	
File size	Equal	Specified manually (in bytes)
	Not equal	
	Greater	
	Not greater	
	Less	

Condition type	Compliance type	Value
	Not less	
Message subject	Equal	Specified manually
	Not equal	
	Contains	
	Not contains	
	Matches	
	Not matches	
Has attachment	Equal	True
	Not equal	False

> ⚠️ In case one of the **Contains**, **Not contains**, **Matches** or **Not matches** compliance types is selected for any of the **Data source**, **Data destination**, **File name** or **Message subject** conditions, you can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value.

3. To delete or edit any of the specified conditions, select it in the list and click **Delete** or **Edit** respectively.

Filtering rule example

To filter files whose size exceeds 20000 bytes, the rule (see Figure 7) containing the following conditions can be used:

Condition type	Compliance type	Value
Data type	Equal	File
File size	Greater	20000

Figure 7. Example of the filtering rule

To edit or delete an existing filtering rule

Select the rule in the list of filters an click **Edit** or **Delete** under the list.

Click **Save** when you are done configuring the filtering rules.

> In some cases, filtering may affect the mail system performance, so the following actions are recommended:
>
> • Add service mail boxes to exclusions list set by the TrustedEmails parameter. The system mail boxes accounts are stored in Active Directory and their names begin with "HealthMail-box".
>
> • Do not create filters that delete small files (less than 1000 bytes) to prevent filtering of the notifications. Otherwise, you may encounter "looping", when the notification is refiltered, over and over.

7.1.2. Managing Groups

By default, Dr.Web 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 Configuring Profiles for more information), join such users in a group and assign the profile to it. Thus you can divide all the clients into different groups, each of them with its own set of protection parameters.

> When creating groups and assigning profiles to them, please note that the Default profile is the only option to be applied to the users from the groups of the Security type in Active Directory. So, to join the domain users into the groups to assign other profiles to them, you need to create additional groups of the Distribution type in Active Directory settings at first.

7.1.2.1. Creating a New Group

To manage the existing groups and create the new ones the **Groups** pane is used. To open it, click **Groups** in the Dr.Web Administrator Web Console tree (see Figure 8).
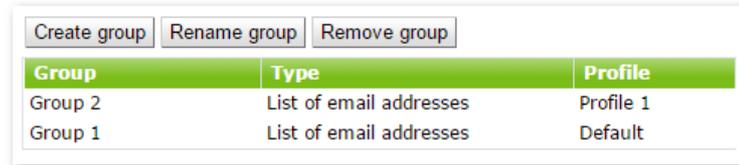
Figure 8. Groups pane

To create a new group

1. On the **Groups** pane, click **Create group** above the list of available groups.

   ⚠️ Alternatively, to create a new group, you can right-click **Groups** in the console tree and then click **Create group** on the context menu.

2. In the opened window, enter a group name. A new group will appear under **Groups** in the console tree. If a group with the same name already exists, a new group will not be created.

To rename a group

Select the group on the **Groups** pane and click **Rename group**.

To delete a group

Select it on the **Groups** pane and click **Remove group**.

   ⚠️ Alternatively, 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.

To configure group settings

Click the name of the group in the web console tree.

You can set up the parameters of the group, such as its type and the profile assigned to it (see Configuring and Forming Groups).

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

7.1.2.2. Configuring and Forming Groups

In the information pane that opens by clicking the group name in the Dr.Web Administrator Web Console tree (see Figure 9), you can set up the parameters of the selected group, including the manner of forming this group: by listing the email addresses or selecting the AD groups. Select the group type in the drop-down list **Type**.
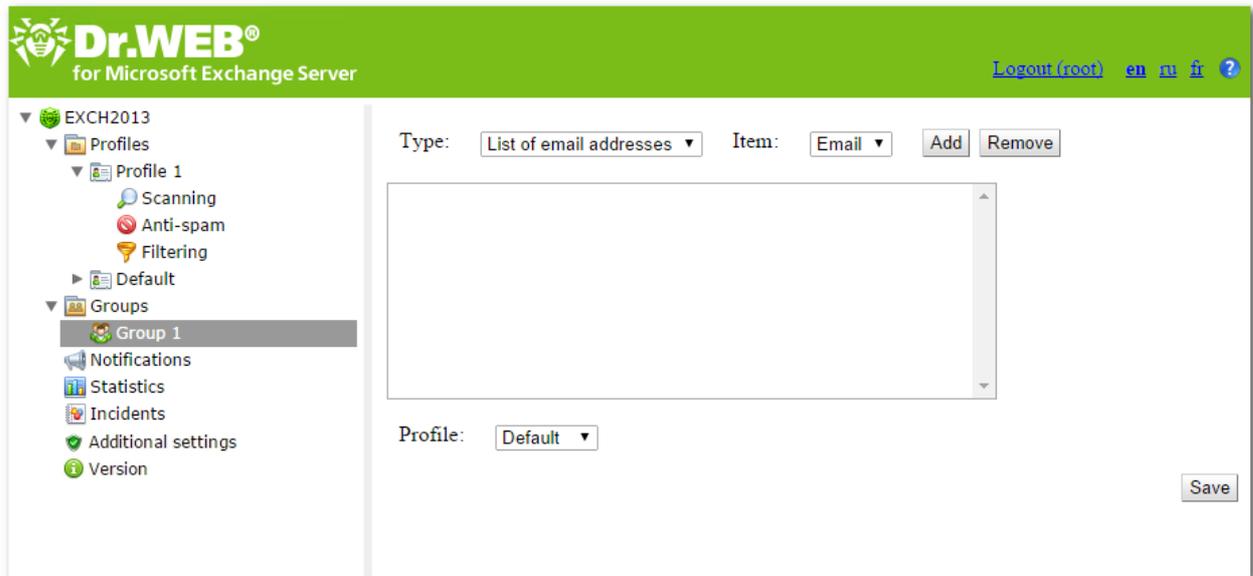
Figure 9. Group settings

To create a list of email addresses

1. In the the drop-down list **Type**, select **List of email addresses**.

2. To add an email address to the list, click **Add**. In the new window, enter the email address and click **Ok**.

3. To delete an email address from the list, select it and click **Remove**, then confirm the deletion of the selected address.

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

To create a list of AD groups

1. In the the drop-down list **Type**, select **List of AD groups**.

2. To add a new group to the list, click **Add**. In the new window, select the group to add and click **OK**.

> ⚠ When adding an AD group, make sure it has a Distribution type and not a Security one, otherwise, you would not be able to assign any profile other than Default to it.

3. To delete a group from the list, select it and click Remove, then confirm the deletion of the selected group.

> ⚠️ Creating the list of AD groups is possible only if the server is in domain. Otherwise, you need to add it to the domain or specify the name and the password of the user with access to AD as the values of the parameters **/DrWebADAccessor_1.0/Application Settings/ADAccUser-Name** and **/DrWebADAccessor_1.0/Application Settings/ADAccPassword** respectively using Dr.Web CMS Web Console. By default, the values of these parameters are empty.

You can select the profile you want to use for the current group in the **Profile** drop-down list.

When you are done setting up the group parameters, click **Save** to apply changes.

7.2. Notifications

Notifications are added to the operation system event log and are used to keep the administrator and other users informed about various events related to operation of Dr.Web (e.g. detection of infected or suspicious objects, attempts to cure them, filtering of messages, etc.).

To configure notifications

1. Click **Notifications** in the Dr.Web Administrator Web Console tree. A pane for editing parameters of notifications will open (see Figure 10).
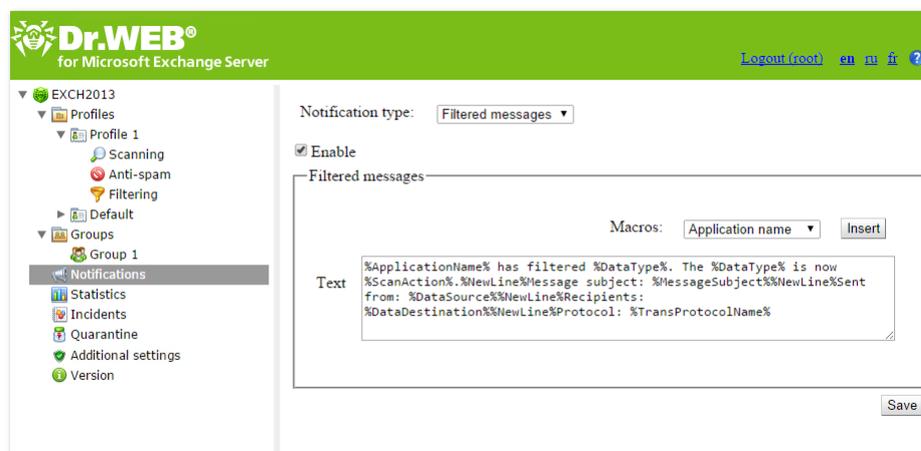
Figure 10. Configure notifications pane

2. In the **Notification type** list, select the type of event to configure notifications for:

   • **Filtered messages** – to configure notifications about messages filtering.

   • **Filtered files** – to configure notifications about attachments.

   • **Spam** – to configure notifications about spam.

   • **Infected** – to configure notifications about infected objects.

   • **Update** – to configure notifications with the last update information.

   • **Expired bases** – to configure notifications about virus databases expiration.

3. By selecting/clearing the **Enable** option, you can enable/disable sending notifications of selected type.

4. In the setting group below, you can modify the text template for the notifications of selected type by entering it in the **Text** field. While editing the text, you can use macros.

5. When you are done, click **Save**.

7.3. View Statistics

The **Statistics** section allows to review the total and average amounts of the objects processed by Dr.Web during a specified time period (see Figure 11).

To configure the statistics

1. In the **Statistics period** drop-down list, select the time interval to view the statistics information about. You can choose one of the following intervals:

   • **For all time** – to view the total statistics since Dr.Web start.

   • **For last day** – to view the statistics for the last 24 hours of Dr.Web operation.

   • **For last hour** – to view the statistics for the last hour of Dr.Web operation.

   • **For last minute** – to view the statistics for the last minute of Dr.Web operation.

2. In the **Type of statistics** drop-down list, select the information type to review. Depending on the selected time interval you can review the total or average numbers as well as the the minimum and maximum values during the specified time period.

Types of information

Depending on the selected options the **Statistics** pane can contain the following sections:

• **Loading**. This section allows to review the information on the total size of the scanned objects and on the average, minimum and maximum size of the objects scanned during the specified time period.

• **Scan results**. This section allows to review the total number of the scanned objects and the number of the scanned objects of different types (e.g., filtered, spam messages, suspicious objects, etc.).

• **Scan actions**. This section contains information on the actions applied by Dr.Web to the detected malicious objects.

• **Infection type**. This section contains information on different types of threats, detected by Dr.Web during the specified time period.

To refresh or clear the statistics, click **Refresh** or **Clear**.

Figure 11. Statistics

7.4. View Incidents

The **Incidents** section allows to review all incidents related to the operation of Dr.Web (see Figure 12).

Figure 12. Incidents

To view the incidents information

For each incident in the list the following information is displayed:

- Date and time of the incident
- Name of the object related to the incident
- Email with infected object sender and recipients' addresses
- Name of the threat
- Performed action
- Protocol used to transfer the email
- Name of the applied profile

You can configure the display parameters of the incidents list:

1. Right-click the header of the list and click Select columns in the context menu.
2. Select the items to display in the list.

The page can display a limited number of list entries. If the amount of incidents exceeds this limit, you can switch to previous page to view other entries by clicking **Next**.

To manage the incidents list

1. You can specify the time period to review the incidents. Enter the start and the end date of the interval, then click **Refresh**.

2. You can use filters and filter the incidents according to certain criteria to customize the way information about them is displayed. Select the filter type in the **Filter** list, enter the desired value in the **Mask** field, then click **Apply**.

> ⚠ You can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol.

3. You can save the incidents list in a text file. To do this, click **Export**. Select the format of the file to save the incidents list, then click **OK**. You can use the HTML or TSV (Tab Separated Values) format.

4. To sort the incidents list according to different criteria, click the title of the corresponding column.

5. To refresh the list, click **Refresh**. The list of incidents is refreshed every time you open Dr.Web Administrator Web Console or the **Incidents** section. It may take some time to be refreshed. To stop the refreshing process, for example, if you entered wrong filtering parameters, click **Cancel**.

7.5. Working with Quarantine

Quarantine of Dr.Web anti-virus serves for isolation of suspicious objects detected while checking the Internet traffic.

In the **Quarantine** section of the Dr.Web Administrator Web Console, the current quarantine information is displayed. You can also use Quarantine manager to review and edit the list of objects in quarantine.

7.5.1. Manage quarantine in Dr.Web Administrator Web Console

To view the list of objects moved to quarantine, click **Quarantine** in the web console tree. The **Quarantine** pane (see Figure 13) will open.

Figure 13. List of objects in quarantine

To view the information about the objects in quarantine

The following information is displayed for each object in the list:

- Date and time of moving the object to quarantine
- Name of the infected file
- Email addresses of the sender and the recipient of the infected object
- Threat name
- File size (in bytes)
- Protocol used to transfer the email with infected object

You can configure the display parameters of the quarantine:

- Right-click the header of the list and click **Select** columns in the context menu.
- Select the items to display in the list.

The following options are available to configure the quarantine:

- The page can display a limited amount of quarantine entries. If the number of entries exceeds this limit, you can switch to the previous page to view other quarantined objects. To do so, use the **Next** button.

- You can specify the time period to review the objects moved to quarantine during this time frame. Enter the start and the end date of the interval, then click **Refresh**.

- You can use a number of filters to filter the list according to certain criteria to customize the way information about the objects in quarantine is displayed. Select the filter type in the **Filter** list, enter the desired value in the **Mask** field, then click **Apply**.

> ⚠ You can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol.

- To sort the list according to different criteria, click the title of the corresponding column.

- To refresh the list, click **Refresh**. The list of objects in quarantine is refreshed every time you open the Dr.Web Administrator Web Console or the **Quarantine** section. It may take some time to be refreshed. To stop the refreshing process, for example, if you entered wrong filtering parameters, click **Cancel**.

To process objects in quarantine

1. To delete an object from the list, right-click it and select **Delete** in the context menu (to select several objects, press and hold SHIFT or CTRL).

2. To restore an object, right-click it and select **Restore** in the context menu. Then specify the path to the folder you would like to restore the object to.

7.5.2. Quarantine Manager

To start Quarantine Manager (see Figure 14) click the **Dr.Web Quarantine** icon on the Desktop.
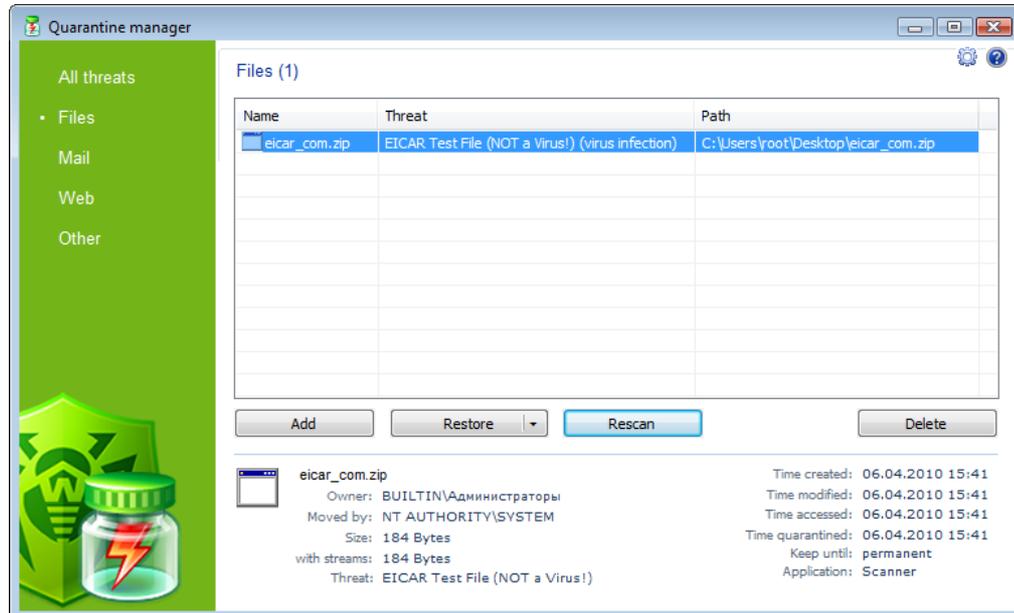
Figure 14. Quarantine window

In the center of the window the table with the quarantine state is displayed. The following columns are included by default:

- **Name** – name list of the objects in the Quarantine.
- **Threat** – malware classification, which is assigned by Dr.Web during automatic placing to the quarantine.
- **Path** – full path to the object before it was moved to quarantine.

In the bottom of the quarantine window the detailed information about selected items is displayed. You can display the columns with detailed information similar to the data in the bottom of the quarantine window.

To configure columns

1. To configure the display parameters of the table of quarantine, right-click the table header. Select **Customize columns** in the context menu.

2. In the opened window, select the items to display in the table. Clear the check boxes for the items you want to hide. Click **Check all/Uncheck all** to select/clear all items.

3. To change the columns order in the table, select the corresponding column in the list and click one of the following buttons:

   - **Move up** – to move the column up in the table (to the head of the settings list and to the left in the objects table).

- **Move down** – to move the column down in the table (to the foot of the settings list and to the right in the objects table).

4. To save changes, click **OK**. To close window without saving, click **Cancel**.

The left pane serves to filter the quarantine objects to display. Click the corresponding option to display all quarantine objects or just specified groups: files, mail objects, webpages or all other objects, not classified.

> ⚠ In the quarantine window users can see only those files that are available by access rights.
>
> To view hidden objects, run the `dwqrui.exe` quarantine file from the installation folder under an administrative account.

7.5.2.1. Manage Quarantine

To process the objects in quarantine

Use the following buttons to manage the quarantine:

- **Add**—to add the file to the quarantine. Select the necessary file in the file system browser.
- **Restore**—to remove the file from the quarantine and restore it in its original location, i.e. restore the file to the folder where it had resided before it was moved to the quarantine. The path to the folder to restore the file is specified in the **Path** column on Figure 14. If the path is not specified, the user will be prompted to select the folder to restore the file to.

> ⚠ Use this option only when you are sure that the objects are not harmful.

The drop-down menu item **Restore to** allows to restore the file to the folder specified by the user.

- **Rescan**—to scan the file again. If a file is defined as clean after that, quarantine will offer to restore the file.
- **Remove**—to delete the file from the quarantine and from the system.

To manage several objects simultaneously, select necessary objects in the quarantine window, press and hold CTRL or SHIFT and select necessary action in the drop-down menu.

In the context menu of the table the **Send file(s) to Doctor Web Anti-virus Laboratory** option is available for sending files to Doctor Web Anti-virus Laboratory for analysis.

7.5.2.2. Configure Quarantine Properties

To configure quarantine parameters

1. Click the ⚙ button in the quarantine window.

2. The **Quarantine properties** window will open. In this window you can change the following parameters:

    -   The **Set quarantine size** section allows to configure the amount of disk space for quarantine folder. Move the slider to change the maximum limit for quarantine size, which is calculated as percentage of total disk space (for several logical drives, this size is calculated for every drive that includes the quarantine folder). The 100% value means an unlimited quarantine folder size.

    -   In the **View section**, select the **Show backup files** option to display backup copies of quarantine files in the object's table.

3. To save changes, click **OK**. To close window without saving, click **Cancel**.

7.6. Additional Settings

In the **Additional settings** section, you can configure the exclusion list and parameters of infected files archiving (see Figure 15).
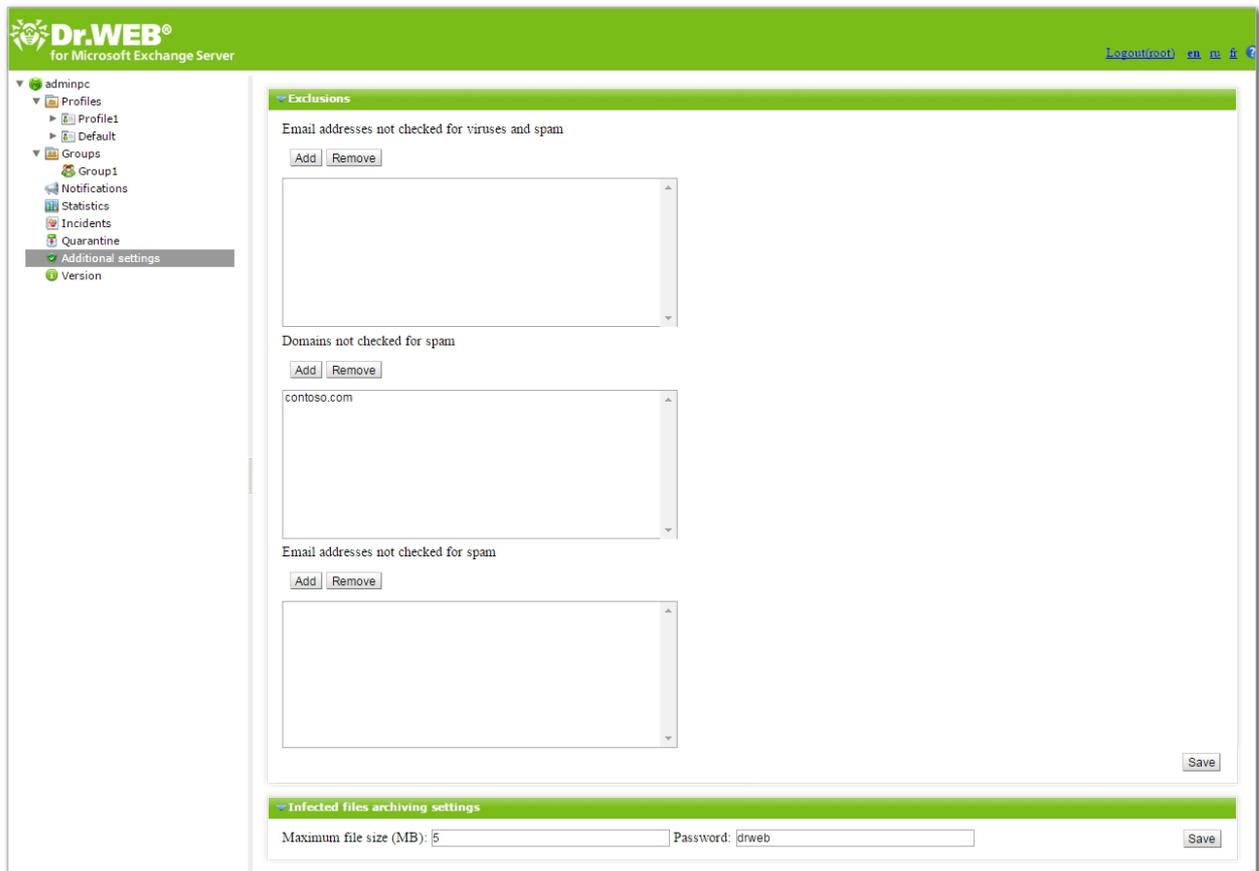
Figure 15. Additional settings

Exclusions

You can exclude messages from trusted senders from check for spam and viruses by adding the addresses or domains of senders to corresponding fields of the **Exclusions** section. You can also configure the exclusion list in Dr.Web CMS Web Console.

Infected files archiving settings

These settings apply to ZIP archives containing infected and suspicious files if in the Scanning section the **Archive** action was selected for these files. In the corresponding fields, you can specify the maximum size of the file which can be added to the archive and a password for the archive.

8. Updating Virus Databases

Dr.Web uses virus databases to detect malicious software. These databases contain details and signatures for all viruses and malicious programs known at the moment of the plug-in release. However modern computer viruses are characterized by the high-speed evolvement and modification. More than that, within several days and sometimes hours, new viruses emerge which can infect millions of computers around the world. To mitigate the risk of infection during the licensed period, Doctor Web provides you with regular updates to virus databases and plug-in components. The Updater component of Dr.Web helps you download the updates via Internet and automatically installs them.

You can review the information about the application version, license, virus databases and also the date, time and result of the last update on the **Version** pane in the Dr.Web Administrator Web Console tree. You can start the virus databases update by clicking **Start** on the **Update task** section.

You can change parameters of the update using drwupsrv.bat file.

An updating task is created during installation of Dr.Web setting the optimal periodicity for downloading the updates from the Dr.Web update servers. You can adjust this schedule using Windows Task Scheduler:

1. Open Windows Task Scheduler.
2. Right-click the **Doctor Web for Exchange Update Task** task and click **Properties**.
3. In the **Doctor Web for Exchange Update Task** window, open the **Triggers** tab (or **Schedule** tab, if you are using Windows Server 2003) and modify the update periodicity. By default, virus databases are updated every hour.
4. Click **OK**.

9. Dr.Web CMS Web Console

Dr.Web CMS Web Console is supported by the managing service Dr.Web CMS Web Console, which is controlled by another managing service – Dr.Web CMS.

Dr.Web CMS Web Console connects to the managing service via administration protocol.

To start Dr.Web CMS Web Console

To launch Dr.Web CMS Web Console (see Figure 16), open the following page in a browser:

`https://<Exchange Server address>:2080/admin,`

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

> ⚠️ To access to the Dr.Web CMS Web Console page, you need to enter the administrator login and password. Administrator accounts can be added, edited or deleted by means of Dr.Web CMS Web Console.
>
> On the first launch of Dr.Web CMS Web Console use the login **root** and the password **drweb** of the default administrator account.

Figure 16. Dr.Web CMS Web Console

Interface

Dr.Web CMS Web Console consists of three parts:

1. Hosts and groups tree

Displays all connected hosts. Click a group in the variables window to open the list of variables. Right-click a group to open a context menu, where you can select one of the following options:

- Create group
- Rename group
- Delete group
- Create variable

Right-click a host to open a context menu, where the following options are available:

- **Add host**. Add a connection to a new host to the tree.
- **Remove host**. Remove a connection to the host from the tree.
- **Create group**. Create a new group.
- **Create variable**. Create a new variable.
- **View traces**. Display tracing messages in real-time mode.
- **Debug traces**. Enable debug tracing.
- **Load traces**. Download tracing messages for the past periods.
- **Edit trace filter**. Change tracing messages filtering parameters.

2. Variables list

The variables window contains the list of variables for the selected group with their attributes and values. If allowed by the attributes, you can click any field to edit the value. Right-click a variable to open a context menu, where you can select one of the following options:

- Create variable (opens a window to create new variable)
- Delete variable (if allowed by the attributes)
- Reset statistics variable (if this variable has the Statistics attribute)

3. Tracing messages window

Tracing messages containing information on the events registered by Dr.Web CMS Web Console are displayed in this window.

To display the tracing messages in real-time mode, select the **View traces** check box in the context menu, which opens on right-clicking the host address.

Every message contains the following information:

- Event time
- Host name
- Application name
- Logging level
- Message text

To filter the messages displayed in the tracing window, select the **Edit trace filter** item in the context menu, which opens on right-clicking the host address. In the opened window, specify the following filtering parameters:

- **Log level**. Events logging level.

- **Instances**. Event sources.
- **Contents**. Text included in the message (in the **Text** field).
- **NonContents**. Text not included in the message (in the **Text** field).

To delete the message, select the **Clear** item in the the context menu, which opens on right-clicking the host address.

9.1. Changing Administrator Password

On the first launch of Dr.Web Administrator Web Console or Dr.Web CMS Web Console you can log in using the predefined administrator account **root** with password **drweb**. Then it is strongly recommended to change the password for this account.

To change the password of the administrator account

1. In the hosts and groups tree, select the **CMS_1.0** -> **Security** -> **Users** -> **root** group.
2. In the variables list of the **root** group, double-click **Value of the Password variable**. The window **Change password variable value** will open.
3. Enter a new password in the **Password** field, the n confirm it in the **Confirm password** field.

9.2. Adding New Administrator

You can add a number of administrator accounts besides the default **root** account.

To add an administrator account

1. In the hosts and groups tree, select the **CMS_1.0** -> **Security** -> **Users** group.
2. Click the **Users** group to open a context menu. Select **Create group**.
3. The **Enter new group name** window will open. Enter the name of the administrator account in the **Group name** field. Click **OK**.
4. To set a password for the administrator account, click the corresponding group in the hosts and groups tree. Select **Create variable** in the context menu.
5. The **Add new variable** will open. Enter **Password** as the name of the variable and select **Password** for its type. In the **Value field**, enter the administrator password. Click **Append**.
6. To set an access level for the administrator account, click the corresponding group in the hosts and groups tree. Select **Create variable** in the context menu.
7. The **Add new variable** will open. Enter **UserLevel** as the name of the variable and select **UInt32** for its type. Specify one of the following values:

    0 – full access to Dr.Web Administrator Web Console settings.

    1 – access to Dr.Web Administrator Web Console without a possibility to change settings.

> If the value of the **UserLevel** variable is not specified, administrator will be granted full access to Dr.Web Administrator Web Console settings.

9.3. Organizing Clusters

Dr.Web CMS Web Console allows creating hosts cluster trees with any nesting level. In a cluster any changes of a variable with attribute **Shared** initiate the same change of variables on all sub-hosts.

To create a cluster

On the sub-host (that is being added to cluster), do the following:

1. Create the group **/CMS_1.0/Security/Users/host**. This group specifies the user account used by the main host to transfer the variables with the **Shared** attribute to a local server.

2. In the **host** group, a variable **Password** of the **Password** type will be created automatically to connect to the created account. The default password is **drweb**. For security reasons, it is strongly recommended to change it.

On the main host, do the following:

1. Create a group of any name at **/CMS_1.0/Shared/**. This group will be the sub-host.

2. In the host group, a variable **Address** of the **String** type is created automatically. By default, it has an empty value. This variable should contain the IP address of the sub-host MS connection in the following format: *<IP address>:<Port>*, e.g., `192.168.1.1:2056`.

3. In the host group, a variable **Password** of the **Password** type is created automatically to connect to the host account on the sub-host. The default password is **drweb**. For security reasons, it is strongly recommended to change it. If the password is the same for all the hosts, you can create the **Password** variable in the **Shared** group. It will be used by default for all connections.

4. The variables configuring the connection to the sub-host cannot have the **Shared** attribute, therefore, the settings cannot be transferred to the sub-hosts. On the attempt to change the attributes of the connections settings, an access denied message will be received.

In the Shared folder, the variable **Enabled** of the **Boolean** type is created automatically. This variable enables/disables the cluster functions. If this variable has the **True** value, all the described connections are active, in case of the **False** value — all connections are interrupted. By default, the variable is created with the value **True**.

When a host group is created in the **Shared** folder, a variable **Enabled** of the **Boolean** type is created there automatically with the default value **False**. This variable enables/disables a specific connection.

If the address (the **Address** variable value) is changed, the active connection is switched to a new address. Changing the password does not lead to the connection switching. To switch the

connection with a new password, you need to disable and re-enable the connection using the **Enabled** variable.

In case the connection is created correctly, CMS will automatically establish connection to the sub-host and will propagate it to all variables with **Shared** attribute. If the remote host already has a variable with such name, but without **Shared** attribute, this variable will be ignored with the **MB_RC_SKIPPED** code returned.

You can create a list of the sub-hosts on any level.

> ⚠️ If Windows Firewall is enabled, for cluster to work properly, it is necessary to allow TCP-communication between the main host and the sub-hosts. To do this, you need to create the following Windows Firewall rules:
>
> - Inbound rule for TCP-communication between **drwcms.exe** control service of the main host and the sub-host through any port.
> - Outbound rule for TCP-communication between **drwcms.exe** control service of the main host with the sub-host through 2056 port.
> - Inbound rule for TCP-communication between the sub-host and the **drwcms.exe** control service of the main host through 2056 port.
> - Outbound rule for TCP-communication between the sub-host with the **drwcms.exe** control service of the main host through any port.

Managing Scanning and Filtering Settings for AD Groups

The variables with **Shared** attribute of the profiles and groups created as the lists of email addresses, as well as such groups and profiles are easily distributed between **cmsdb** databases of the main host and sub-host as they do not depend on Active Directory. If the main host and the sub-host are connected to one Active Directory GC (Global Catalog) server, the settings of the AD group created via Dr.Web Administrator Web Console on the main host, are transferred to the sub-host. But if the mail servers forming a cluster do not have common Global Catalog, to create the AD groups with shared settings managing, perform the following actions:

1. On the sub-host, create a new Distribution group using the Active Directory management console.

2. Use Dr.Web Administrator Web Console to add the created group to the list of the application groups.

3. In Dr.Web CMS Web Console, find this group in the **DrWebScanSrv_1.0** -> **Application Settings** ->**Groups** -> <*group name*> section. Change the attribute from **Shared** to **Default** for the **ItemList** variable (it specifies GUID of the created AD group).

4. Use the Active Directory management console on the main host to create a new Distribution group with the same name as on the sub-host.

5. Add the created group to the list of the application groups using Dr.Web Administrator Web Console on the main host. Enter the same name for the group.

6. The groups are now associated with each other (despite the fact that they have different GUID and are composed from different users), so that assigning profiles, as well as configur-

ing scanning and filtering for them can be performed using Dr.Web Administrator Web Console on the main host, being transferred to both servers.

9.4. Configuring Notifications About Messages Deleting Using Exchange Web Services

In case of operating in the mode featuring messages deleting during the anti-virus check or filtering by anti-virus agent, the recipient does not get any information about the message, except the corresponding records in the server event log. You can configure sending mail notifications via EWS (Exchange Web Services) protocol to the email address specified by the **OWSNotificationEmail** parameter. Such notifications contain the information on the sender, recipients and subject of the deleted message, but do not provide any data on its body or attachments.

EWS (Exchange Web Services) resides on the servers Client Access (CAS) role and acts as mediator between the client requests and internal structure of the Exchange Server.

The notifications about deleting messages via EWS (Exchange Web Services) are configured in the **DrWebAgentStub_1.0** -> **Application Settings** section of the Dr.Web CMS Web Console by setting up the following variables:

- **OWSUrl** – the server where EWS resides. By default, the "localhost" is specified, but it can be the IP address of any other server with EWS.
- **OWSAdministrator**, **OWSPassword**, **OWSDomain** – the access parameters (the name of the user with access to EWS, the password and domain name) to the mailbox set by the **OWSOutgoingEmail** parameter.
- **OWSNotificationEmail** – the email address to receive the notifications about the messages deleting.
- **OWSOutgoingEmail** – the email address, the notifications about the messages deleting are sent from.

The specified parameters are transferred to anti-virus agent when the transport service is started. Sending notifications via EWS is not enabled if the value of any of the parameters is left blank.

Every time the message is deleted, the anti-virus agent initiates connection to the server specified by the **OWSUrl** parameter. In case the connection fails, the alert **444** is registered in the OS Event log describing the reason of the failure to send the notification.

9.5. Antispam Agent Actions on Deleting or Blocking a Message

If a message is deleted as spam or blocked by filtering rules, antispam transport agent can either close the connection to the client or produce the **RejectMessage** response.

To select an action which will be performed on deleting or blocking the message:

1. In the hosts and groups tree, select **AgentStub** -> **Application Settings**.

2. In the **Value** field set the value for the **Disconnect** variable:

   - **false**. The sender will receive the **RejectMessage** response containing the following text: **Dr.Web AntiSpam Agent: Message was rejected as spam**. This action is performed by default.

   - **true**. SMTP connection to the client will be closed.

9.6. Changing Licensing Mode

It is necessary to change licensing mode if central protection mode was enabled or disabled.

To change licensing mode

1. In the hosts and groups tree, select **DrWebScanSrv_1.0** -> **Application Settings**.

2. In the **Value** field set the value for the **LicenseMode** variable:

   0 – for Dr.Web to operate, it is necessary to get the key file (by default);

   1 – for Dr.Web to operate, it is necessary to use the key file from the central protection server.

3. After changing the mode, restart Dr.Web for MSP Scanning Service.

9.7. Selecting Types of Bad Objects

In certain cases some attachments can be treated as bad objects. These objects cannot be checked for viruses. The same actions are applied to bad and infected objects. To specify types of objects that will be treated as bad, do the following:

1. In the hosts and groups tree, select the **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Scanner**.

2. Select variable corresponding to the type of objects:

   - **ScannerTreatPswrdArchivesAsBad** – encrypted archives
   - **ScannerTreatIncompleteArchivesAsBad** – incomplete archives
   - **ScannerTreatPackedArchivesAsBad** – archives packed incorrectly
   - **ScannerTreatRestrictedArchivesAsBad** – archive with restricted access
   - **ScannerTreatDeepArchivesAsBad** – archives containing subfolders
   - **ScannerTreatBigArchivesAsBad** – too large archives

3. In the **Value** field set the value for selected variable:

   true – object of this type will be treated as bad. Action selected for infected objects in the Scanning section will be applied to this object.

   false – object of this type will be treated as clean and will be skipped.

9.8. Assigning Message to Spam

The Anti-spam component assigns an integer number (*score*) to every message. The score allows to determine if the message is spam.

To change the threshold values used to assign a message to one or another group (**Certainly spam**, **Probably spam** or **Unlikely spam**), do the following:

1. In the hosts and groups tree, select the **DrWebScanSrv_1.0** -> **Application Settings** -> **Profiles** -> **%Profile name%** -> **Antispam**.

2. Set values for the following variables:

> ⚠ For Anti-spam to operate properly, do not change default values of the **AntispamDefaultScoreMin** and **AntispamExactlyScoreMax** variables.

   - **AntispamDefaultScoreMin**. The least score value that assigns the message to the **Unlikely spam** group. Default value: 1.
   - **AntispamDefaultScoreMax**. The largest score value that assigns the message to the **Unlikely spam** group. Default value: 199.
   - **AntispamProbablyScoreMin**. The least score value that assigns the message to the **Probably spam** group. Default value: 200.
   - **AntispamProbablyScoreMax**. The largest score value that assigns the message to the **Probably spam** group. Default value: 4999.
   - **AntispamExactlyScoreMin**. The least score value that assigns the message to the **Certainly spam** group. Default value: 5000.
   - **AntispamExactlyScoreMax**. The largest score value that assigns the message to the **Certainly spam** group. Default value: 2147483647.

9.9. Excluding Messages from Scanning

You can exclude messages from trusted senders from check for spam and viruses by specifying the addresses or domains of senders in corresponding variables:

1. In the hosts and groups tree, select the **DrWebAgentStub_1.0** -> **Application Settings**.

2. Set values for the following variables:

> ⚠ The variable values must be separated by ";" without space: **example1@mail.com;example2@mail.com**.
>
> You can also configure the exclusion list in the Additional settings section of Dr.Web Administrator Web Console.

   - **TrustedDomains**. The list of domains, which will be excluded from check for spam. The domain name must include only the part of the email address specified after @. Example: **domain.org;mail.com;drweb.com**.

- **SpamTrustedEmails**. The list of email addresses, which will be excluded from check for spam.

- **TrustedEmails**. The list of email addresses, which will be excluded from check for spam and viruses. You also need to set the same values for the **TrustedEmails** variable from the **DrWebVSAPIModule_1.0** -> **Application Settings** section.

9.10. Filtering Files in Archive by Their Extensions

If you need to detect archives containing files with certain extensions and apply to them actions specified for suspicious objects, you can use the **SuspiciousTypesInsideContainer** variable:

1. In the hosts and groups tree, select the **DrWebScanSrv_1.0** -> **Application Settings**.

2. Set as a value of the **SuspiciousTypesInsideContainer** variable a list of file extensions in the following format: `exe;vbs;scr`

Firstly, the archive will be checked for infected files. If these files are detected, the action selected for infected objects will be applied to the archive. Otherwise, the archive will be checked for files with the specified extensions. If at least one such file is found, the action selected for suspicious objects will be applied to the archive.

10. Logging

Dr.Web registers the errors and application events in following logs:

- Windows Event Log
- Text log of the installation program
- CMS event log

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

10.1. Event Log

Dr.Web 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 the malicious objects and spam detection (see the Notifications section)

  Dr.Web events are registered in the **Application** and **Doctor Web** logs.

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** (or **Doctor Web**).
3. The application Event Log displays in the right pane. The source for the plug-in events are the applications Dr.Web Scanning Engine, Dr.Web CMS, Dr.Web CMS Web Console, Dr.Web for MSP Scanning Service, Dr.Web for MSP Component Host and Dr.Web for MSP Requests Queue.

Redirect Dr.Web events

To redirect Dr.Web events to the specified event log, do the following:

1. In Dr.Web CMS Web Console, select the **DrWebScanSrv_1.0** -> **Application Settings** group.

2. Specify the name of a log where Dr.Web events will be registered as a value of the **EventLog** variable, for example, **Doctor Web**.

> ⚠️ If the **EventLog** variable is absent or its value is not specified, Dr.Web events will be registered in the **Application** log.

3. Restart Dr.Web for MSP Scanning Service.

4. Delete **Dr.Web for Exchange Server** event source from the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\application`.

5. Restart the operating system.

10.2. Installation Program Text Log

The installation logs **setup-starter.log** and **exchange-setup.log** can be found by environment variable %ProgramData% (i.e. by executing it in **Start** -> **Run** console) in the %ProgramData% \Doctor Web\Logs folder.

10.3. CMS Log

The events are logged by Dr.Web CMS managing service into the cmstracedb database located in the application installation folder %Program Files%\DrWeb for Exchange. The managing service logs the application events of different types and allows setting up different logging level for each application.

You can delete the cmstracedb database, if necessary.

The list of events is displayed in the tracing messages window of Dr.Web CMS Web Console.

10.3.1. Types of Events

The managing service logs the application events of different types:

Value	Description
Audit	The records of this type are logged by the managing service and contain the information on administrator actions (e.g., changing the variables values).
Incident	The security events logged by external applications (e.g., virus detection)
Fatal	Events resulting in application crushes
Error	Errors that admit the return to the normal operation
Warning	Messages about different events for administrator

Value	Description
Information	Information messages
Debug	Debug records

The list of events is recorded by the managing service into a separate database.

The managing service can display the registered events in the real-time mode filtered by different criteria. It also allows to review the past events for a specified time interval.

10.3.2. Logging Level

By modifying the value of **LogLevel** (**UInt32**) variable in the **Settings** group, you can set up the application logging level:

Value	Description
0	Error, Fatal, Incident, Audit messages are registered
1	Warning messages are added to all previous types
2	Information messages are added to all previous types
3	Debug messages are added to all previous types

The default log level set for all applications subscribed to Dr.Web CMS service is 2. If the **Debug Traces** option is selected in the context menu when right-clicking the root element of the Dr.Web CMS Web Console tree, the log level changes to 3 for all subscribed applications. However, enabling this option may cause the system overload and it is not recommended to enable the 3 log level for all the application at one time. If you managed to localize the problem of a specific module, you can change the log level only for one application to explore it.

> When setting the logging level to 3 in Dr.Web CMS Web Console opened in Internet Explorer and then enabling the **View Traces** option to monitor the events in real-time mode, you need to control the memory size allocated for the iexplorer.exe process corresponding to the console window. This process in such monitoring mode starts using all the available memory, that may considerably decrease the system performance.

10.3.3. Deleting cmstracedb Database

If necessary, you can delete the cmstracedb database located in the application installation folder %Program Files%\DrWeb for Exchange:

1. Before deleting the database, it is recommended to unload the server using one of the following procedures:

- Stop the transport service the transport agents are installed to, and Microsoft Exchange Information Store service, if VSAPI is installed.

- If the server cannot be stopped for some reason, disable transport agents and restart the transport service. If VSAPI is installed, set the **0** value for the **Enabled** parameter in `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]` registry key and restart службу Microsoft Exchange Information Store service.

3. Run the command-line tool with administrator rights.

4. Stop the application services in the following order:

```
net stop "Dr.Web SSM"
net stop "Dr.Web for MSP Scanning Service"
net stop "Dr.Web for MSP Components Host"
net stop "Dr.Web for MSP Requests Queue"
net stop "Dr.Web CMS Web Console"
net stop "Dr.Web CMS"
```

5. Delete the **cmstracedb** file located in the application installation folder %Program Files%\DrWeb for Exchange.

6. Start the application services in the following order:

```
net start "Dr.Web CMS" (please wait until this service is started
before proceeding to the next step)
net start "Dr.Web SSM"
```

7. After starting the Dr.Web SSM service make sure that it has started other application services.

11. Troubleshooting

To check whether Dr.Web is installed and configured properly, use the following tests:

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

11.1. Check Installation

If you work with Windows Server 2003, Dr.Web is installed into the following folders:

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

If you work with Windows Server 2008 or higher, Dr.Web is installed into the following folders:

- C:\ProgramData\Doctor Web
- C:\Program Files\DrWeb for Exchange
- C:\Program Files\Common Files\Doctor Web

Make sure these folders are created and contain necessary files.

After that, run Windows **Event Viewer** and make sure no errors connected with Dr.Web are detected.

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

- Dr.Web Scanning Engine (DrWebEngine)
- Dr.Web CMS
- Dr.Web SSM
- Dr.Web CMS Web Console
- Dr.Web for MSP Scanning Service
- Dr.Web for MSP Component Host
- Dr.Web for MSP Requests Queue

If Dr.Web is correctly installed, you can see in the results of executing the get-transportagent command in Exchange PowerShell the following agents:

- Dr.Web AntiSpam Agent;
- Dr.Web AntiVirus Agent.

11.2. Check Updater Functionality

The updating module **drwupsrv.exe** automatically starts after the installation of Dr.Web. 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 a task for Dr.Web 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\dwupdater.log and make sure that there are no errors in it.

11.3. Virus Detection Test

To check the functionality of the plug-in 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 **Download Anti-Malware Testfile** section of 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 email message and send it to any test email 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 email address of the administrator specified during installation.

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

11.4. Spam Detection Test

⚠️ The Anti-spam component works only with the «Anti-Virus&Anti-Spam» version of Dr.Web, i.e. if you have an appropriate license key file (see License Key File).

To test the functionality of your **Anti-spam** component, you are recommended to use one of email messages with a special test string: GTUBE (Generic Test for Unsolicited Bulk Email) or with a string for built-in check.

To create a GTUBE test message:

1. In the email subject, specify: **Test spam mail**.

2. Copy the following string to the body an email message:

`XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X`

⚠️ The test spam message must not contain any attachments, signatures or other information except the mentioned email subject and the test string.

3. Send the message to a test email address via SMTP.

4. Open the Windows **Event Viewer** -> **Doctor Web** and find the information that Dr.Web has detected spam.

To create a built-in test spam message:

1. In the email subject, specify: **Vade Secure**.

2. Copy the following string to the body an email message:

`tiUS4kVZrTfBBZXZPuLrnstNpdo8vJ-Spam-high-PQQMbQu22jePzuV8TLwVdPo81QpGXNJxRI`

⚠️ The test spam message must not contain any attachments, signatures or other information except the mentioned email subject and the test string.

3. Send the message to a test email address via SMTP.

4. Open the Windows **Event Viewer** -> **Doctor Web** and find the information that Dr.Web has detected spam.

12. Appendices

12.1. 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:

- Global settings
- Database settings
- SMTP transport scanning

> ⚠️ The anti-virus scanning settings listed below are available for Microsoft Exchange Server 2003, 2007 and 2010.

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\Services\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\Services\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 *<*number of processors*> + 1.

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.

SMTP transport scanning

⚠️ The transport scanning settings are available only for Microsoft Exchange Server 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.

12.2. Registering Transport Agents Manually

In some cases, for example, if you encounter problems with registering transport agents during Dr.Web installation, you may need to register them manually. To do this, execute the following commands in Exchange Management Shell:

```
Install-TransportAgent -Name "Dr.Web AntiSpam Agent" -TransportAgentFactory
"DRWTransportAgent.AntiSpamAgentFactory" -AssemblyPath "C:\Program Files\DrWeb
for Exchange\DRWTransportAgent.dll"

Install-TransportAgent -Name "Dr.Web AntiVirus Agent" -TransportAgentFactory
"DRWTransportAgent.AntiVirusAgentFactory" -AssemblyPath "C:\Program Files
\DrWeb for Exchange\DRWTransportAgent.dll"

Enable-TransportAgent "Dr.Web AntiSpam Agent"

Enable-TransportAgent "Dr.Web AntiVirus Agent"
```

To cancel the registration of the transport agents, execute the following commands in Exchange Management Shell:

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"

Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

12.3. Disabling The Use of Dr.Web by The Mail Server Manually

In case you encounter problems during the installation or operation of Dr.Web, you can disable the use of plug-in by the mail server:

- If transport agents are installed:

> ⚠️ Transport agents are available for Microsoft Exchange Sever 2007, 2010, 2013, 2016.

☺ In Exchange Management Shell, execute the `Get-Transportagent` command (if the agents have been installed in transport services, specify them in `-TransportService` parameter). For detailed information on the command please refer to the website: http://technet.microsoft.com/en-gb/library/bb123536%28v=exchg.150%29.aspx.

☺ The agents registered in the specified transport service will be listed in In Exchange Management Shell. For each agent related to Dr.Web (the ones that contain the **Dr.Web** prefix in their names), copy the name into the `Disable-TransportAgent <agent name>` command (specify the `-TransportService`, if necessary). For detailed information on the command please refer to the website: http://technet.microsoft.com/en-gb/library/aa997880%28v=exchg.150%29.aspx.

☺ Restart Microsoft Exchange Transport service (and Microsoft Exchange Frontend Transport service, if required). The transport agents will be disconnected from transport services.

☺ Re-execute the `Get-Transportagent` command to make sure that the agents have the **Disable** status.

The application is now disconnected from the transport pipeline.

- If VSAPI module is installed:

> ⚠️ VSAPI module is available for Microsoft Exchange Sever 2003, 2007, 2010.

☺ Verify the value of the `Enabled` parameter in `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan]` registry key: if `"Enabled"=dword:00000001`, you need to set it to zero: `"Enabled"=dword:00000000`. If this registry key is missing or the specified parameter is already set to zero, the VSAPI module is already disabled.

☺ Restart the Microsoft Exchange Information Store service. The VSAPI module will be disconnected from this service.

The application is now disconnected from the mail stores manager.

- If DrWebSink moduleis installed:

> ⚠️ DrWebSink module is available for Microsoft Exchange Sever 2003.

☺ Run the command-line tool with administrator rights and execute the following command:

```
regsvr32 /u "C:\Program Files\DrWeb for Exchange\DrWebSink.dll"
```

☺Restart Microsoft Internet Information Services (IIS).

Once disconnected from the mail server, the application has no influence on its operation.

12.4. Deleting Dr.Web Manually

If you encounter issues with mail server operation, you can delete Dr.Web manually:

1. Disconnect Dr.Web from the mail server.

2. Cancel the registration of the transport agents by executing the following commands in Exchange Management Shell:

```
Uninstall-TransportAgent "Dr.Web AntiSpam Agent"
Uninstall-TransportAgent "Dr.Web AntiVirus Agent"
```

3. Run the command-line tool with administrator rights.

4. Stop the application services in the following order:

```
net stop "Dr.Web SSM"
net stop "Dr.Web for MSP Scanning Service"
net stop "Dr.Web for MSP Components Host"
net stop "Dr.Web for MSP Requests Queue"
net stop "Dr.Web CMS Web Console"
net stop "Dr.Web CMS"
```

5. Delete the application services:

```
sc delete "Dr.Web SSM"
sc delete "Dr.Web for MSP Scanning Service"
sc delete "Dr.Web for MSP Components Host"
sc delete "Dr.Web for MSP Requests Queue"
sc delete "Dr.Web CMS Web Console"
sc delete "Dr.Web CMS"
```

> ⚠️ To remove Dr.Web Scanning Engine service, use drw_remover.exe utility, which you may obtain by contacting Droctor Web Technical Support.

6. Delete the following folders:

```
rd /S /Q "C:\Program Files\DrWeb for Exchange"
rd /S /Q "C:\Documents and Settings\All Users\Application Data\Doctor Web"
rd /S /Q "C:\Program Files\Common Files\Doctor Web"
```

12.5. CMS Platform

CMS (Central Management System) is a cross-platform distributed application management system (hereinafter any module subscribed to the main managing service is considered as application). In the center of the system lies the managing service Dr.Web CMS. This service controls the applications operation, manages the applications and their settings and logging.

The applications interact by means of the TCP protocol. They can interact with the managing service in the following ways:

- The controlled application uses the MB (Management Base) protocol to interact with the managing service.
- The managing (administrator) applications use the MS (Management System) protocol to interact with the managing service.

Dr.Web CMS service uses an arborescent database to store the information on the application data.

12.5.1. Database

Dr.Web CMS managing service database is a tree consisting of groups and variables. Variables are of different (data) types and have different attributes.

Data types of managing service variables:

Data type	Comment
Int32	32-bit integer
UInt32	32-bit unsigned integer
Int64	64-bit integer
UInt64	64-bit unsigned integer
Float	32-bit real number
Double	64-bit real number
String	String of unlimited length
Boolean	Logical value (true or false)
Time	Date and time
Binary	Binary data of unlimited length
Password	Data type for passwords storage

Variables can have the following attributes:

Attribute	Comment
Default	Simple variable
Shared	Shared variable
Statistics	Statistics variable
System	System variable
Hidden	Hidden system variable
Readonly	Variable, which cannot be modified

12.5.2. Application Control

The application control via CMS starts by registering its name in the managing service database. Dr.Web CMS service assigns a unique name to the application. This name contains the name of the application and its version. Then, the service creates a group with the name if the registered application. By default, a group has two service subgroups named **Application Status** and **Settings**. During the operation of the application, the managing service collects statistics for the protocols. The statistical information is located in the **Application Statistics/Connections** group, the **MB** and **MS** subgroups contain the interaction protocols statistics. The load on the services and applications can be evaluated using this statistical information.

Application Status group

This group contains information on the registered application as the values of the variables of different types:

Variable (its type is indicated in parentheses)	Comment
Active (Boolean)	Indicates the application activity. The **true** value means that the application is active.
Crash (Boolean)	Indicates the correctness of the application stop. The **true** value means that the application stopped incorrectly.
HomeDir (String)	Application directory in the file system
InstanceName (String)	Name the application instantiated for
LogicCrash (Boolean)	Application logics state. The **true** value means that the application operates incorrectly.

Variable (its type is indicated in parentheses)	Comment
ModuleName (String)	Application executable file name. If the subscribed application is a *.dll library, the value contains the name of the process it was instantiated by.
ModulePath (String)	Path to the application executable file in the file system
PID (UInt32)	Application process number in the operating system
StartedOn (Time)	Last application start time
StoppedOn (Time)	Last application stop time
Version (String)	Application version
VersionBuild (UInt32)	Application build number
VersionMajor (UInt32)	Application major version
VersionMinor (UInt32)	Application minor version
VersionRevision (UInt32)	Application revision number
WorkDir (String)	Application working directory in the file system

Settings group

This group contains the general settings of the registered application.

12.5.3. Statistics

The system allows collection the application statistics for time intervals. The applications allow creating the statistics variables to register the applications events and return the statistical information intime intervals specified by the statistic variables settings.

In the Dr.Web CMS managing service database, such variable have the **Statistics** attribute. The variables with this attribute are temporary, they are not saved to the constant database and exist only when the managing service is active. After restarting the managing service, these variables are lost.

12.5.4. Administration

The system in managed via the administration protocol. This protocol allows to modify the values of the variables, reset the statistics, track the system operation in the real-time mode with filtering the traces, review the past messages and filter them.

Changing the variables values

The values of the variables are changed synchronously. All registered applications receive notifications about changing the values of the variables or disable such changes. Once the variable value is changed, all applications that use it, obtain its new value.

Reset statistics

The administration protocol allows to reset the collected statistics for the variable settings, so the statistics is recollected from zero.

Restrictions

Using variable has the following restrictions:

- The variables with **Hidden** attribute exist in the database, but are not available for review and editing. They are created by the managing service for internal use.

- The variables with **System** attribute are created by the managing service to display the service information for administrator. Such variable cannot be modified or deleted.

- The variables with **Statistics** attribute are created by the application. These variables cannot be deleted.

- The variables with **Readonly** attribute are created by the application to inform the administrator. These variables cannot be modified.

- The variables with **Default** attribute are ordinary variables, and allow any action to be applied.

- The variables with **Shared** attribute are the distributed variables. Their values are modified synchronously within the distribution system.

- The variables, which cannot be modified, cannot be deleted as well. However, the groups containing such variables can be deleted with all their variables, if the application related to this group, is not launched.

Security

To access to the system, you need to enter a user name and a password. The default user of the system has the user name **root** and the password **drweb**. It is strongly recommended to change the password after system installation. Or you can also add new users.

The users and their passwords are stored in the **Security** -> **Users** subgroup of the managing service group, i.e. /CMS_1.0/Security/Users. The name of the group is the name of the user. The password is stored in the **Password** variable.

12.5.5. Connecting to Servers

Dr.Web CMS Web Console allows you to connect to other servers that have CMS running. Perform the following steps to establish a connection:

1. Right-click the host icon in the console tree and select **Add** host.

2. In the next window, specify address of a host you want to connect to and click **OK**.

3. Enter credentials used to connect to the host. If the credentials are correct, the connection will be established and the console tree will display the new host.

This way you can connect to an unlimited number of machines and manage their operation. The settings of each connection are stored in a separate group of Dr.Web CMS Web Console and can be found in **/Dr.Web CMS Web Console_1.0/Application Settings/Hosts**. Each added host is shown as a group. The name of each group is composed of host connection address. Each group contains three variables:

- **Address** – host connection address.
- **Login** – login for connecting to the host.
- **Password** – password used for connecting to the host.

If any of the credentials change, you may not be able to connect to the host. In this case you have to change Dr.Web CMS Web Console connection settings used for connecting to this host.

At next launch,Dr.Web CMS Web Console will automatically connect to all added hosts. In order to remove a host, you have to delete a corresponding group with connection settings from Dr.Web CMS Web Console settings groups in **Dr.Web CMS Web Console_1.0/Application Settings/Hosts**.

12.6. Dr.Web SSM Service

The Dr.Web SSM (Dr.Web Start/Stop Manager) service controls the applications operation based on the CMS platform and performs the following functions:

- Dr.Web CMS service operation maintenance in the automatic mode
- Automatic start of the applications registered by the service (having the **SSM** group of variables in Dr.Web CMS Web Console) in case of failures
- Forced start of the applications even if they terminated their operation correctly
- Applications launch using Windows Service Manager
- Starting services as applications developed using CService from CommonComponents
- Starting services using the assigned scripts
- Applications start and stop in manual mode by user commands

The parameters of the Dr.Web SSM service operation are defined by the **SSM** variables group in the Dr.Web CMS Web Console. The **SSM** group can contain the following variables:

Variable (its type is indicated in parentheses)	Comment
Enabled (Boolean)	Signifies whether the SSM control is enabled or not
Run (Boolean)	Allows to start/stop the application
KeepAlive (Int32)	Signifies the application operation maintenance type: • 0 – the application is disabled • 1 – The application is active • 2 – forced maintenance, the application is enabled even if it stopped correctly
StartType (Int32)	Signifies the application start method: • 0 – as a Windows service • 1 – as a CService application • 2 – start using a script
StartScript (String)	Contains the script to start the application
StopScript (String)	Contains the script to stop the application
Restart (Boolean)	Restarts the application
Timeout (UInt32)	The timeout for application reaction (in seconds). By default, the timeout is 10 seconds.
ServiceName (String)	the service name in Windows Service Manager. By default, the name of the variable /Application Status/InstanceName is used.

The Dr.Web SSM service setting may include the following:

- **KeepAlivePeriod** (**UInt32**) – the time to check the service (in seconds). By default, the value 60 is set.
- **RestartCMSPause** (**UInt32**) – the delay before restarting the CMS (in seconds). By default, the value 5 is set.

12.7. Configuring Update Parameters

To configure virus databases and Dr.Web components update parameters, use **drwupsrv.bat** file. This file is located in Dr.Web installation folder. Commands included in this file are executed while running **Doctor Web for Exchange Update Task** in Windows Task Scheduler.

To configure update settings, specify required parameters for **- c update** and **- c postupdate** commands.

- c update command parameters

- c update command updates virus databases and Dr.Web components.

Parameter	Description
--type arg	Type of update: • update-revision – try to update all components of the current revision to the newest if exists.
--disable-postupdate	Post-update is disabled. Work of update module will be stopped when the update operation has completed.
--verbosity arg	Log level: • error – standard • info – extended • debug.
--interactive	If parameter is specified, more resources will be used during execution of some operations.
--param args	Additional parameters passed to the script: Format: *<name>=<value>*. Default value is "plugin=exchange".
-n [--component] arg	List of the components that need to be updated: • updater – drwupsrv.exe file; • antispam – vrcpp.dll file; • scan-engine – dwengine.exe, ccsdk.dll, dwsewsc.exe, dwinctl.dll, dwark-daemon.exe, arkdb.bin, dwqrui.exe and dwarkapi.dll files; • av-engine – virus databases (*.vdb files); • exchange-plugin-setu – exchange-setup.exe file. ⚠ Several components can be updated simultaneously, e.g.: -n av-engine updater

Parameter	Description
-g [--proxy] agr	Proxy server for updating. *<address>:<port>*.
-u [--user] agr	Username for proxy server.
-k [--password] arg	Password for proxy server.

Example of **- c update** command for updating virus databases using proxy server:

```
-c update --type=update-revision --disable-postupdate --verbosity=de-
bug
--interactive --param="plugin=exchange" -n av-engine
--proxy=192.168.134.128:808 --user=qwerty --password=qwerty
```

- c postupdate command parameters

- c postupdate command post-updates virus databases and Dr.Web components.

Parameter	Description
--verbosity arg	Log level: • error – standard • info – extended • debug.
--interactive	If parameter is specified, more resources will be used during execution of some operations.
--param arg	Additional parameters passed to the script: Format: *<name>=<value>*. Default value is "plugin=exchange".

- c postupdate command example:

```
-c postupdate --verbosity=debug --interactive --param="plugin=ex-
change"
```


Configuring an update mirror

If you cannot update Dr.Web directly from the Internet or if you want to reduce the amount of external traffic, you can configure an update mirror in order to update Dr.Web via LAN.

To configure an update mirror, perform the following steps on a machine with an access to the Internet:

1. Run the **drwupsrv.exe** with the following parameters:

```
-c   download   --zones=<file_path>   --key-dir=<folder_path>   --re-
podir=<folder_path>   --version=90   --verbosity=debug   --log-dir=C:
\Repo
```

Specify the necessary values for:

zones=<*file_path*>—path to the update zone file drwzones.xml;

key-dir=<*folder_path*>—path to the license key file;

repo-dir=<*folder_path*>—path to the folder with updates. Make sure the updates folder is shared.

For example:

```
drwupsrv.exe   -c   download   --zones=C:\Mirror\drwzones.xml   --key-
dir=C:\Mirror\   --repodir=C:\Mirror\Repo\   --version=90   --verbos-
ity=debug --log-dir=C:\Mirror\Repo\
```

2. On the server with Dr.Web installed, open the **drwupsrv.bat** file and add the following parameter in the string `set upparams`, and then run the file:

```
--zone="file://<repo_folder_path>"
```

For example:

```
set upparams=-c update   --type=update-revision   --disable-postupdate
--verbosity=debug     --interactive     --param="plugin=exchange"     --
zone="file://<repo_folder_path>"
```

12.8. Operation in Central Protection Mode

Dr.Web 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 17).

Workstations and servers are protected by local anti-virus components (clients; herein, Dr.Web) 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.

	Central protection server	_____	**Network based on TCP, NetBIOS**
	Anti-virus network administrator	- - - -	**Management via HTTP/HTTPS**
	Protected local computer	_____	**Transmitting updates via HTTP**
	Doctor Web update server		
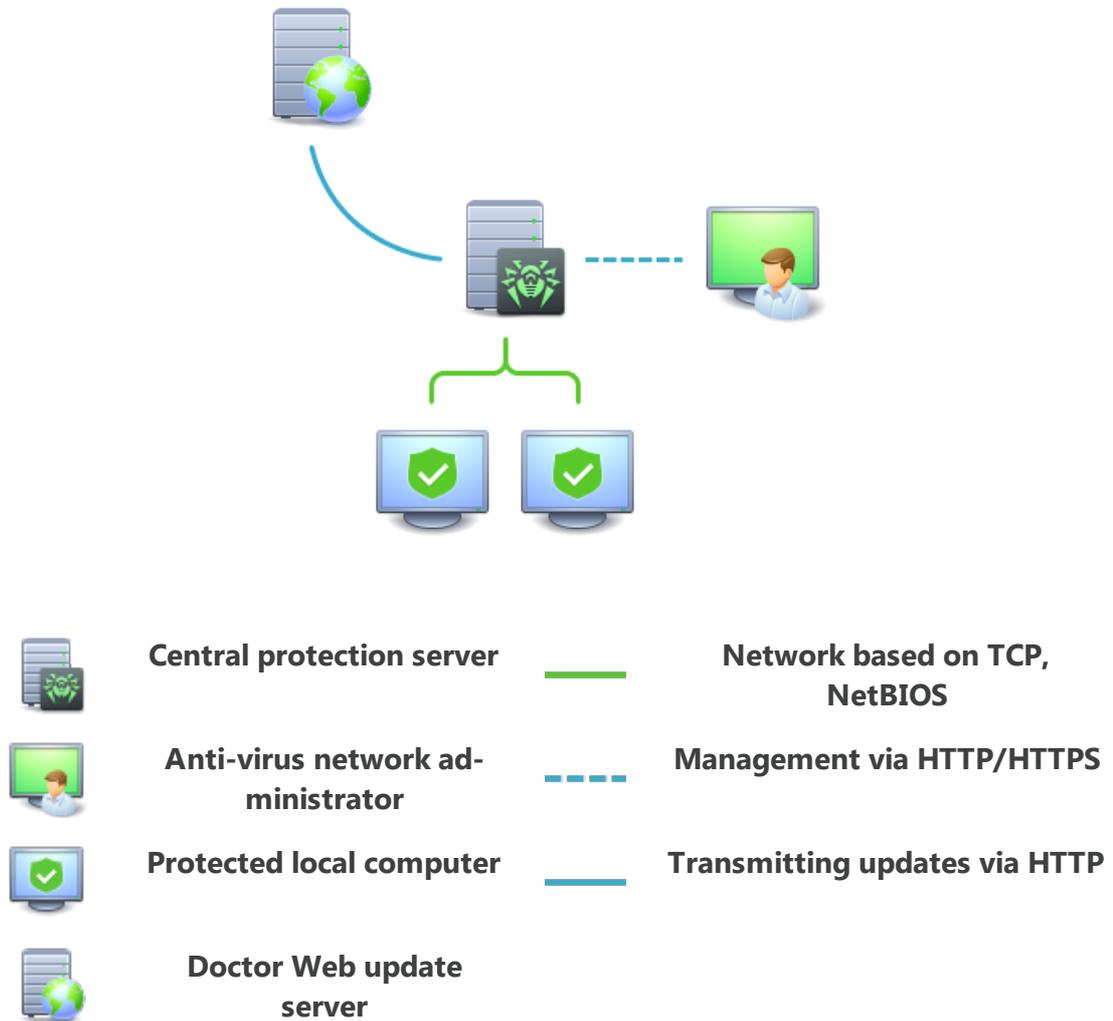
Figure 17. Logical structure of anti-virus network.

All necessary updates are downloaded to central protection server from Dr.Web update 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.

Operation of Dr.Web in Central Protection Mode

For operation of Dr.Web in central protection mode, Dr.Web Agent has to be installed and has to operate correctly on the same operating system.

> ⚠️ The version 11.0 of Dr.Web is not compatible with Dr.Web Agent version 6 and previous.
>
> ---
>
> If Dr.Web Agent was installed after Dr.Web, do the following:
>
> 1. Enable **Doctor Web for Exchange Update Task** in Windows Task Scheduler.
> 2. In Dr.Web CMS Web Console, change the licensing mode – select use of a license from the central protection server (see Changing Licensing Mode).
>
> Next, execute update from console on the central protection server and make sure that update has been performed successfully.

Licensing

License key file for Dr.Web that is registered at the anti-virus network is used in central protection mode. If option of using license from the central protection server was selected during the installation, the license key file for the station in the anti-virus network will be used on the start of Microsoft Exchange Server with the installed plug-in Dr.Web. If this key is invalid, the anti-virus check is not performed. If during the installation another licensing mode was selected, it is necessary to change it in Dr.Web CMS Web Console (1).

Update

Virus databases and anti-virus engine updates from Dr.Web Control Center repositories. This action allow disabling the standard updater of Dr.Web, which starts by default according to a schedule. In this case components update starts from Dr.Web Control Center repositories according to its schedule.

Actions after removing Dr.Web Agent

If Dr.Web Agent was removed, to ensure that Dr.Web will work properly, do the following:

1. In Windows Task Scheduler add the task for Dr.Web update:

   - Open Windows Task Scheduler.

   - Create a task named **Doctor Web for Exchange Update Task**.

   - On the **General tab** of the **New Task Wizard**, select the **Run whether user is logged on or not** radio button **Run with highest privileges** check box. Select Windows Server 2003, Windows XP or Windows 2000 option in the **Configure for** list.

   - On the **Triggers** tab, set periodicity of task execution.

   - On the **Actions** tab, create the **Start a program** action and specify the program *<path to Dr.Web installation folder>*\drwupsrv.bat.

   - Clear all default check boxes on the **Conditions** tab.

2. Change license mode. It is necessary to select licensing by getting the key file (0).

Keyword Index

Keyword Index

Keyword Index