Dr.WEB

for Microsoft ISA Server and Forefront TMG

Administrator Manual

Trademarks

Disclaimer

Dr.Web for Microsoft ISA Server and Forefront TMG
Version 11.0
Administrator Manual
1/31/2018

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya

Moscow, Russia

125040

Website: http://www.drweb.com/

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

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

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

Table of Contents

1. Document Conventions

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

Convention	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. 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.ru/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 technical support in one of the following ways:

- Fill in the web from in the corresponding section at http://support.drweb.ru/.
- 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.

3. Introduction

Thank you for choosing Dr.Web for Microsoft ISA Server and Forefront TMG (hereinafter – Dr.Web).

This manual is intended to help administrators of large enterprise 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.

3.1. About Dr.Web

Dr.Web is an application that protects enterprise networks against virus threats and spam. It integrates with the system in order to search and neutralize all types of threats in the stream of data going through Microsoft Internet Security and Acceleration Server (hereinafter – Microsoft ISA Server) and Microsoft Forefront Threat Management Gateway (hereinafter – Microsoft Forefront TMG) via HTTP, FTP, SMTP and POP3 protocols. The application checks the incoming Internet traffic for viruses, dialers, adware, hacktools, jokes and riskware.

The application builds in its filters into Microsoft Firewall Service and Microsoft Forefront TMG Firewall. This allows Dr.Web anti-virus engine receive and process data. Dr.Web operates on a platform that features its own password-protected web interface and an additional web console for advanced configuration.

Dr.Web services installed on different servers can be joined in a cluster (for more information, see Organizing Clusters).

Dr.Web performs the following functions:

- Scans all Microsoft ISA Server and Microsoft Forefront TMG traffic transferred over FTP (including FTP over HTTP), HTTP, SMTP and POP3 protocols.
- Blocks access to infected objects for users within the network protected by Microsoft ISA Server or Microsoft Forefront TMG firewall.
- Isolates infected and suspicious objects in the quarantine.
- Registers incidents in Windows Event log and in the internal event database.
- Filters suspected spam email messages sent via SMTP protocol.
- Adds notifications to email messages containing security threats.
- Restricts access to specific web resources.
- Collects statistics.
- Automatically updates virus databases and components.
- Allows for centralized management of firewalls in a distributed system, including a possibility to group servers in a cluster.

Dr.Web virus databases are constantly updated with new records to provide system protection. The application features a heuristic analyzer that ensures additional protection against viruses and threats that are not yet included into virus databases.

3.2. Scanned Objects

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

Scanned objects in HTTP and FTP over HTTP traffic

Dr.Web scans the HTTP and FTP traffic passing through Microsoft ISA Server or Microsoft Forefront TMG firewall in the real-time mode. The resource specified in the client request is scanned. Microsoft ISA Server and Microsoft Forefront TMG either connect the specified server and obtain the resources from it or return the resource from its own cache. The application filters intercept and analyze the received data (including objects in archives and packed objects).

Generally, the anti-virus analysis can be performed only for the whole file. Therefore, the accumulation and scanning of the requested data may require additional time.

Scanned objects in SMTP and POP3 traffic

Dr.Web scans incoming and outgoing messages in a real-time mode. The application scans the following email message elements:

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

4. Licensing

The use rights for Dr.Web are regulated by the license *key file*.

4.1. License Key File

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

- Licensing period.
- 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. the number of users).

A *valid* license key file meets the following requirements:

- 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 threats. License violation is registered in the Windows Event Log and in the text log of application.

The key file is write-protected. Editing the key file makes it invalid. We strongly advise you against opening your key file in a word processor to avoid accidental file corruption .

4.2. 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 file with .key extension.

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 e-mail address you specified in the registration form.
5. Extract the license key file and copy it to the computer where you plan to install Dr.Web.

At your request, 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 for demo licenses. On the expiration of the 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 https://download.drweb.com/demoreq/.

To buy a license key file, you can either contact Doctor Web local reseller 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.

4.3. Updating License

If your license has expired, or if the configuration of your system has changed significantly, you may need to update your license. The new license then should be registered with the product. Dr.Web supports hot license update that does not require stopping or reinstalling the application.

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 installation folder (%PROGRAMFILES%\DrWeb CMS for MSP\).
2. Dr.Web automatically switches to the new license.

For more information on licensing, visit Doctor Web official web site at http://www.drweb.com.

5. Dr.Web Components

All Doctor Web anti-virus solutions use the following general components that provide protection of all operating systems and platforms:

- Virus scanning engine drweb32.dll.
- Regularly updated virus database files (with the .vdb extension). They store information about viruses and other security threats.

The product features a web interface Dr.Web Administrator Web Console that allows you to configure application settings and track events. For more information about the settings, see Dr.Web Administrator Web Console.

Dr.Web also features an additional web console Dr.Web CMS Web Console designed for troubleshooting and advanced configuration. For more information, see Dr.Web CMS Web Console.

5.1. Dr.Web Filters

Dr.Web builds its filters into Microsoft Firewall Service (for Microsoft ISA Server) and Microsoft Forefront TMG Firewall (for Microsoft Forefront TMG) to intercept the data from network connections and scan this data for threats and spam.

All filters are implemented as dynamic libraries that start and operate together with Microsoft Firewall Service/Microsoft Forefront TMG Firewall. Filters receive access to the stream of data going through the firewall. If the client request or server response generates an incident a filter is configured to react on, the filter will intercept and analyze this data.

Dr.Web contains three application filters and one web filter.

5.1.1. Application filters

Dr.Web comprises three application filters:

- Dr.Web FTP Filter
- Dr.Web SMTP Filter
- Dr.Web POP3 Filter

Application filters are located in the following directories:

Filter	Path to the filter library
Dr.Web FTP Filter	In case Microsoft ISA Server is used: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll In case Microsoft Forefront TMG is used: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll
Dr.Web SMTP Filter	In case Microsoft ISA Server is used: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll In case Microsoft Forefront TMG is used: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll
Dr.Web POP3 Filter	In case Microsoft ISA Server is used: %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll In case Microsoft Forefront TMG is used: %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll

These filters process the protocols' packets. They analyze the data and block it in case security threats are detected. All filters are available in Microsoft ISA Server or Microsoft Forefront TMG console tree (see Figure 1a, Figure 1b):

- On the Application Filters tab of the Configuration -> Add-ins section in Microsoft ISA Server console.
- On the Application Filters tab of the System section in Microsoft Forefront TMG console.

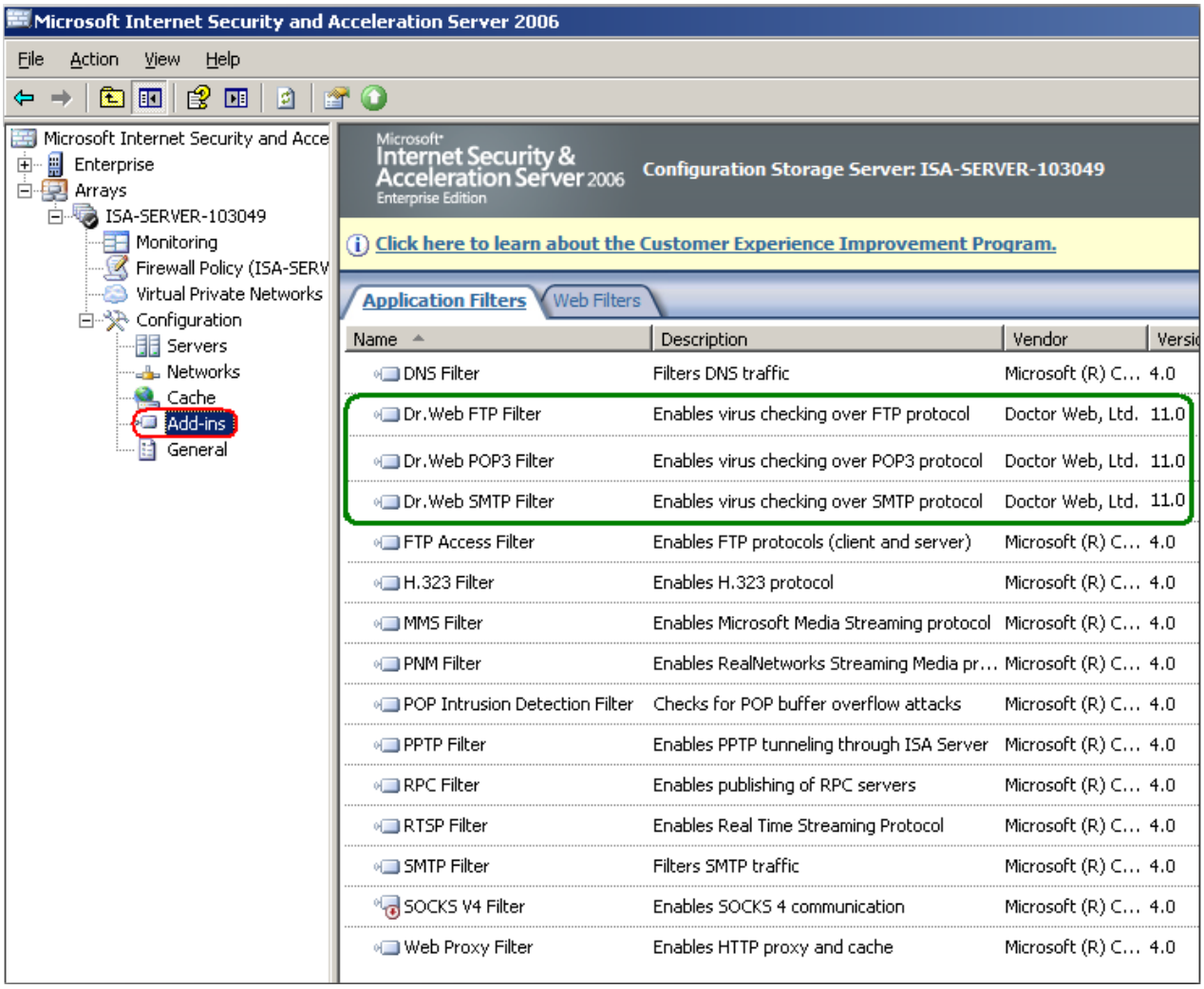

Figure 1a. Dr.Web application filters in Microsoft ISA Server console

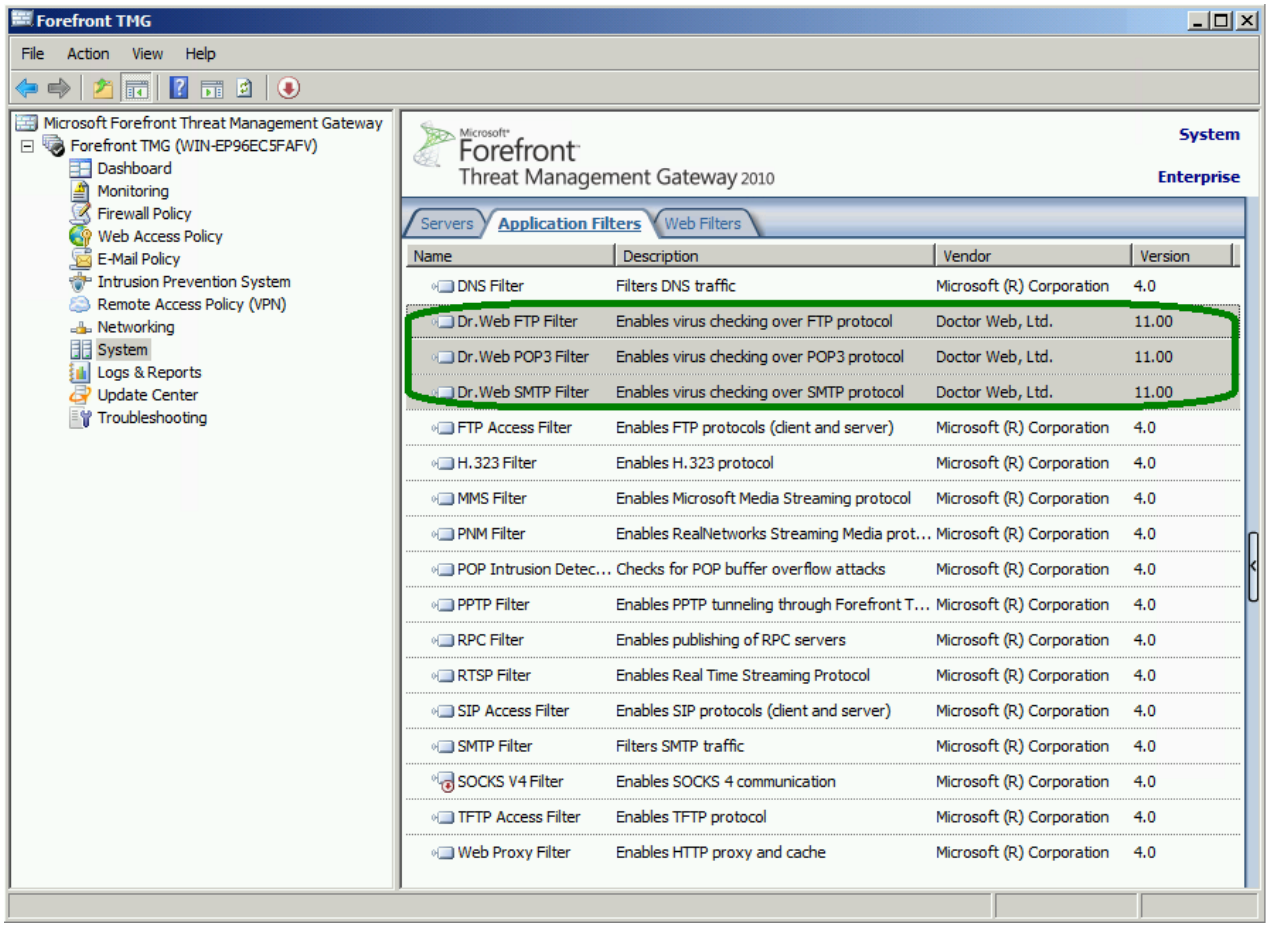

Figure 1b. Dr.Web application filters in Microsoft Forefront TMG console

After the application installation and registration, Dr.Web FTP Filter connects to the FTP protocol events and is displayed on the FTP protocol properties tab in the Microsoft ISA Server and Microsoft Forefront TMG console (see Figure 2).

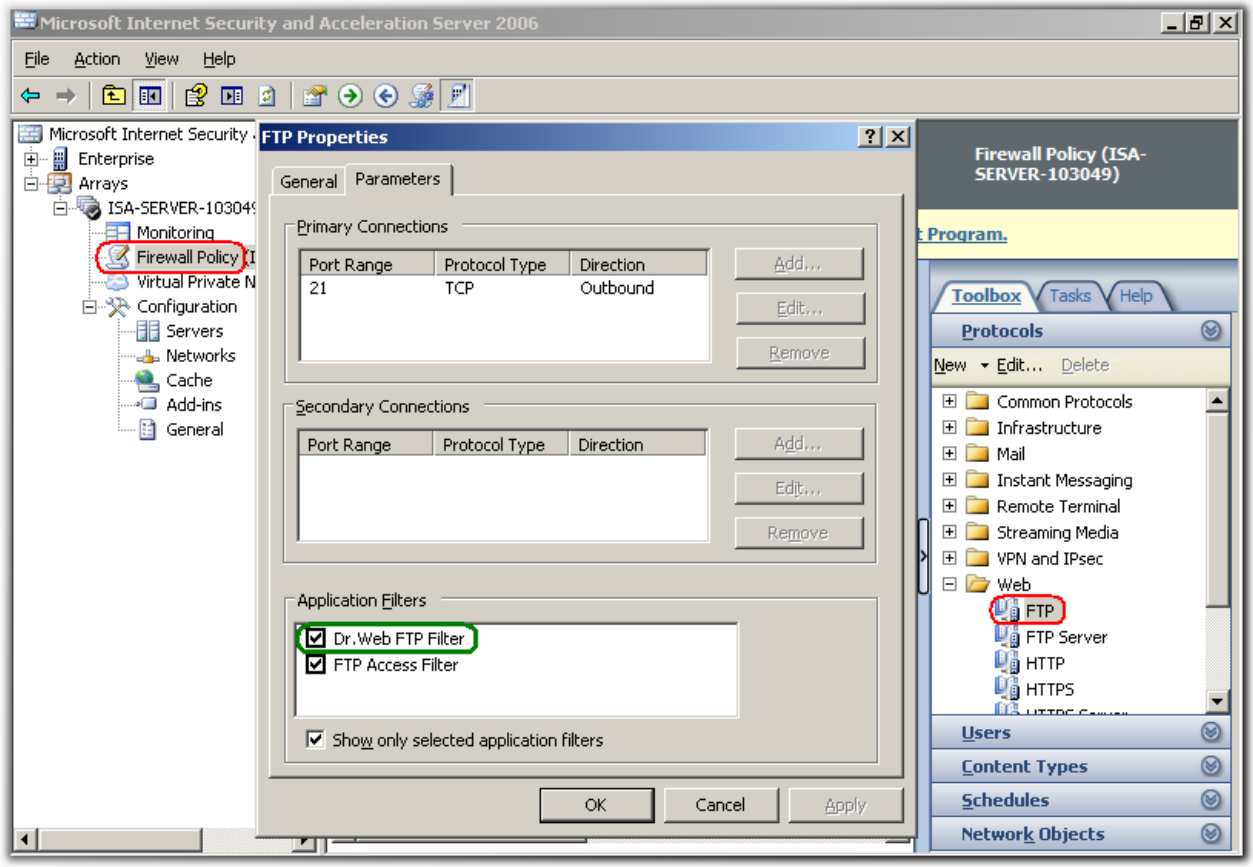

Figure 2. Dr.Web FTP Filter on the FTP protocol properties tab

Microsoft ISA Serverand Microsoft Forefront TMG contain FTP Access Filter. If this filter is disabled, the firewall does not control the applications interaction on the FTP protocol level. For operation of Dr.Web FTP Filter, FTP Access Filter needs to be enabled and displayed on the FTP protocol properties tab (see Figure 2).

5.1.1.1. Dr.Web FTP Filter

During the installation of Dr.Web, Dr.Web FTP Filter is registered as an FTP protocol events handler. Preparing to the anti-virus scanning starts when the client establishes connection to the FTP server. Microsoft ISA Server and Microsoft Forefront TMG processes the data transferred from the client to the server and vice-versa:

1. Analyzing the client requests, Dr.Web FTP Filter defines the time of the file download request.
2. After receiving a request to download a file, Dr.Web FTP Filter checks if the server IP address belongs to the black and white lists of the IP addresses.
3. From the request, Dr.Web FTP Filter picks the name of the requested file and checks file size. If the file size does not exceed the limit (the default file size limit is 0.5 Mbyte), received data will be stored in a memory buffer. If the file exceeds the size limit, data will be saved in a file.

4. The file is partially transferred to the client (80% by default). Then the transfer is paused and Dr.Web FTP Filter checks the file. If the file does not contain threats, the rest of it is transferred to the client, otherwise, the transfer stops. The client does not obtain the whole file, but the virus signature can appear on the client's computer.

If the connection to the FTP server was interrupted because of a threat detection in the dowloaded file, you need to reconnect to the server to continue working with the FTP protocol.

5.1.1.2. Dr.Web SMTP Filter and Dr.Web POP3 Filter

Dr.Web checks only unencrypted traffic over POP3 and SMTP protocols.

Scanning process has two stages:

1. On the first stage, the received message is checked by the Anti-spam module Vade Retro. It analyzes the text of the message and calculates the probability for the message to be spam. If a message is detected as spam, an action specified for the corresponding spam category in the Anti-spam section of Dr.Web Administrator Web Console will be applied to it.
2. On the second stage, messages that passed spam check (or were ignored according to the application settings), undergo scanning for malware. Depending on the scanning results, objects (the body of the message or attachments) are attributed to one of the categories (Infected or Suspicious), and the corresponding actions specified by the administrator in the Scanning pane of Dr.Web Administrator Web Console are performed.
   Enabling the heuristic analyzer in application settings allows you to detect objects with modified or unknown malicious code. Such objects are identified as Suspicious. A text file with information on the detected threat and performed actions is attached to the messages with malicious objects.
   If a message with infected objects is detected, the application will attach a text file with information about detected threats and performed actions .

5.1.2. Web Filter

Dr.Web features Dr.Web HTTP Web Filter. It is a run-time extension for Web Proxy Filter that is built into Microsoft ISA Server and Microsoft Forefront TMG. This allows Dr.Web HTTP Web Filter to react on events of Web Proxy Filter.

Dr.Web HTTP Web Filter is located in the HTTPWebFilter.dll library in the following directories:

%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\ (for Microsoft ISA Server);

%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\ (for Microsoft Forefront TMG).

Dr.Web HTTP Web Filter is displayed in the Microsoft ISA Server and Microsoft Forefront TMG console (see Figure 3a, Figure 3b):

- On the Web Filters tab in the Configuration -> Add-ins section of Microsoft ISA Server console
- On the Web Filters tab in the System section of Microsoft Forefront TMG console

Dr.Web HTTP Web Filter is not displayed on the HTTP protocol properties tab.

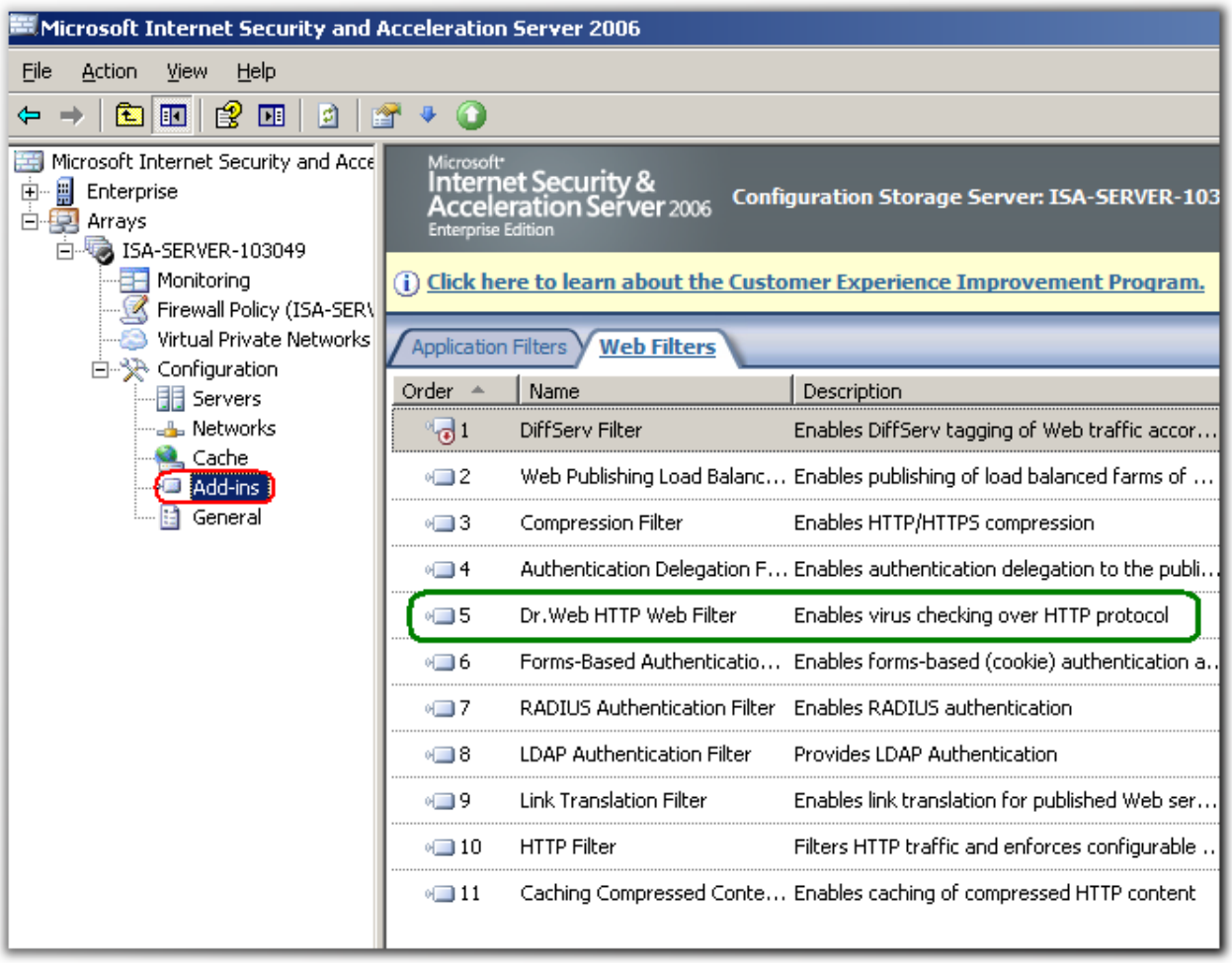

Figure 3a. Dr.Web HTTP Web Filter in Microsoft ISA Server

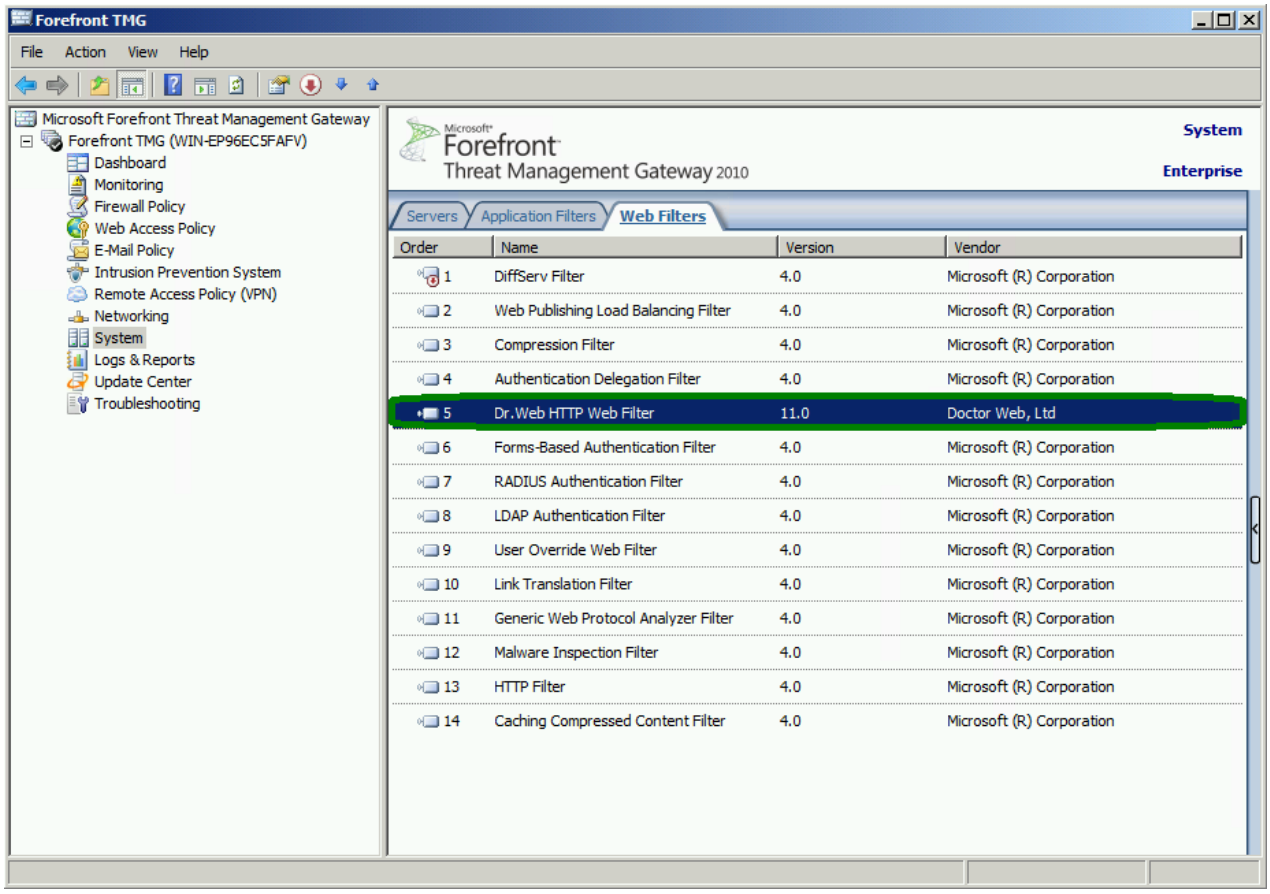

Figure 3b. Dr.Web HTTP Web Filter in Microsoft Forefront TMG

5.1.2.1. Dr.Web HTTP Web Filter

The anti-virus check starts when the server sends the data back to the client or obtains the requested data from the cache of Microsoft ISA Server or Microsoft Forefront TMG.

As the object to check is a web resource specified in the client's request, Dr.Web HTTP Web Filter analyzes the packets of the protocol, compiling a temporary file (if the resource size is too large) for further anti-virus scanning.

If an URL is not blocked by Office Control, one of the following four states (two of them are known, and two – unknown) may be assigned to it:

- Unverified
- Unknown
- Infected
- Clean (contains no threats)

The state is stored for 30 minutes from the end of scanning. After that the resource is considered unverified. Once 60 verification attempts are finished, information about the resource will be deleted from the system.

5.2. Dr.Web Services

The operation of Dr.Web is based on seven services:

- Dr.Web CMS – supports the distributed application components management system, controls and analyzes the modules functionality. This service supports the application components settings database.
- Dr.Web CMS Web Console – provides operation of web-consoles.
- Dr.Web for MSP Component Host and Dr.Web for MSP Scanning Service – ensure that all application components interact efficiently.
- Dr.Web for MSP Requests Queue – supports the asynchronous requests queue of application tasks, which allows to postpone their run.
- Dr.Web Scanning Engine – contains the Dr.Web scanning engine.
- Dr.Web SSM – provides start and stop of Dr.Web services.

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.

5.3. Quarantine

You can set the Move to Quarantine action for objects. In this case, objects are moved to a special supplementary database with the quarantine features. It means this base blocks the execution of the objects' code by all system applications. For more information about objects in quarantine, refer to the Working with Quarantine section.

5.4. Virus Events Monitoring

To receive information about events monitored by Dr.Web, you can configure notification options. Notification options include:

- Event log. Application events are registered in Windows Event Log.
- Incidents. Allows you to view the list of infected objects and filtered messages processed by the applications.
- Statistics. Contains information about a number of objects scanned over the specified period of time.

6. Installation and Removal

Before installing or removing Dr.Web, make sure that the built-in administrator account is enabled on the computer where Microsoft ISA Server or Microsoft Forefront TMG is installed.

Otherwise, it is possible that the system installer would not have enough permissions to create and/or remove application components. In case you experience problems during the removal process that lead to the firewall shutdown, refer to the appendix Removing Dr.Web manually.

The Dr.Web is distributed as a single installation file (`drweb-[version]-av-isa-windows-x86.exe` or `drweb-[version]-av-tmg-windows-x64.exe`, depending on the firewall), where `[version]` indicates product's version number, or a ZIP-archived folder with the installation file.

Extract the installation file to a folder on the local drive of the ISA server/Forefront TMG.

If you are using the Windows Terminal Services component, run the Windows utilityAdd or Remove Programs (in Windows Server 2003) or Programs and Features (in Windows Server 2008).

Installing multiple anti-virus applications on the same computer may lead to system errors and loss of data. If a version of Dr.Web different from 11 or another anti-virus application is already installed on your computer, you should remove them.

6.1. System Requirements

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

Specification	Requirement	
	For Microsoft ISA Server	For Microsoft Forefront TMG
RAM	1 GB or more	2 GB or more
Disk space	700 MB for installation. Additional disk space is needed for temporary data storage while performing the anti-virus check. The size of the disk space depends on the number of user requests and the size of the downloaded files.	
Monitor	VGA-compatible monitor	
Operating system	One of the following: • Microsoft® Windows Server® 2003 x86 with: J MSXML 4.0 Service Pack 3 (Microsoft XML Core Services) J Service Pack 1 (SP1) or higher • Microsoft® Windows Server® 2003 R2 x86 with: J MSXML 4.0 Service Pack 3 (Microsoft XML Core Services)	One of the following: • Microsoft® Windows Server® 2008 SP2 x64 • Microsoft® Windows Server® 2008 R2 x64
Firewall	Microsoft® ISA Server 2004 Microsoft® ISA Server 2006	Microsoft® Forefront® TMG 2010 (Standard Edition or Enterprise Edition) with SP1 or SP2
Additional software	Microsoft .NET Framework 3.5 SP1	

6.2. Compatibility

Before installation of Dr.Web please make yourself familiar with the following information on product compatibility:

1. Dr.Web for Microsoft ISA Server and Forefront TMG of the version 11 is only compatible with Dr.Web products for Windows server of the version 11.
2. Dr.Web for Microsoft ISA Server and Forefront TMG of the version 11 is not compatible with Dr.Web ES Agent and Dr.Web AV-Desk.
3. Dr.Web for Microsoft ISA Server and Forefront TMG is not compatible with another anti-virus software. Installing multiple anti-virus applications on the same computer may lead to system errors and data loss. If you already have another anti-virus software installed, it is necessary to uninstall it using Installation wizard or built-in OS tools.

6.3. Installing Dr.Web

Before installing the application, you are recommended to do the following:

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

Installing Dr.Web:

1. Stop the Microsoft ISA Server/Microsoft Forefront TMG firewall service.
2. Before installation, make sure, that the built-in administrator account is enabled.
3. Run the installation file. The window with a list of installation languages will open. Select Russian or English as the installation language. Click OK.
4. A window with the text of the License Agreement will open. To continue installation you should read and accept the license by selecting I accept the terms in the license agreement. Click Next.
5. If the firewall service is still running, you will be prompted to stop it.
6. Select a licensing option.

   By default, the Installation wizard searches for a life with the .key extension in %PROGRAMFILES%\DrWeb CMS for MSP\. Once the Wizard finds the key file, it will display the detailed license information.

   You can use a local key and specify its location manually. If you click Activate product later, you will not be able to use the application until you activate your license.

   Click Next.
7. On the Ready to install page, click Install to begin installation of Dr.Web on your computer.
8. Further actions of the Installation wizard do not require user actions. Once the installation is complete, you will be prompted to restart your computer.

While installing the application, it is necessary to restart Microsoft ISA Server/Microsoft Forefront TMG in order not to damage integrity of data on the server. Once the deletion is finished, start Microsoft Firewall Service/Microsoft Forefront TMG Firewall service again.

You may also need to restart your operating system after installation as well as after Dr.Web update.

6.4. Removing Dr.Web

Uninstalling Dr.Web

1. Stop the Microsoft ISA Server/Microsoft Forefront TMG firewall service.
2. Before uninstalling the application make sure that the built-in administrator account is enabled.
3. Run the Windows utilityAdd or Remove Programs (in Windows Server 2003) or Programs and Features (in Windows Server 2008).
4. Select Dr.Web from the list of installed applications and click Remove.
   The Installation wizard will appear.
5. If the firewall service is still running, you will be prompted to stop it. Stop the service and click Next.
6. If necessary, select Save settings. Click Remove.
7. Once the application is removed, you will be prompted to restart your computer.

While removing the application, it is necessary to restart Microsoft ISA Server/Microsoft Forefront TMG in order not to damage integrity of data on the server. Once the deletion is finished, start Microsoft Firewall Service/Microsoft Forefront TMG Firewall service again.

7. Administrative Console Dr.Web Administrator Web Console

Dr.Web Administrator Web Console allows you to configure Dr.Web (see Figure 4).

Starting Dr.Web Administrator Web Console

To ensure Dr.Web Administrator Web Console operates correctly, use one of the following browsers:

- Internet Explorer 11 or higher
- Chrome 46 or higher
- Microsoft Edge 20 or higher

Note that if you open Dr.Web Administrator Web Console in Internet Explorer you should 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 necessary check box in the Administrators section.
- In Windows Server 2012: open Server manager, open the Local server tab and select IE Enhanced Security Configuration, then select the necessary check box in the Administrators section.

In order to launch Dr.Web Administrator Web Console, enter the following address into the address bar of your browser:

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

where *<ISA Server address>* stands for the address of the Microsoft ISA server or Microsoft Forefront TMG.

To access Dr.Web Administrator Web Console, you have to enter credentials for the administrator account.

When you start Dr.Web Administrator Web Console for the first time, use default credentials: the login root and the password drweb. We strongly recommend you to change administrator credentials (for more information, see Changing Administrator Password).

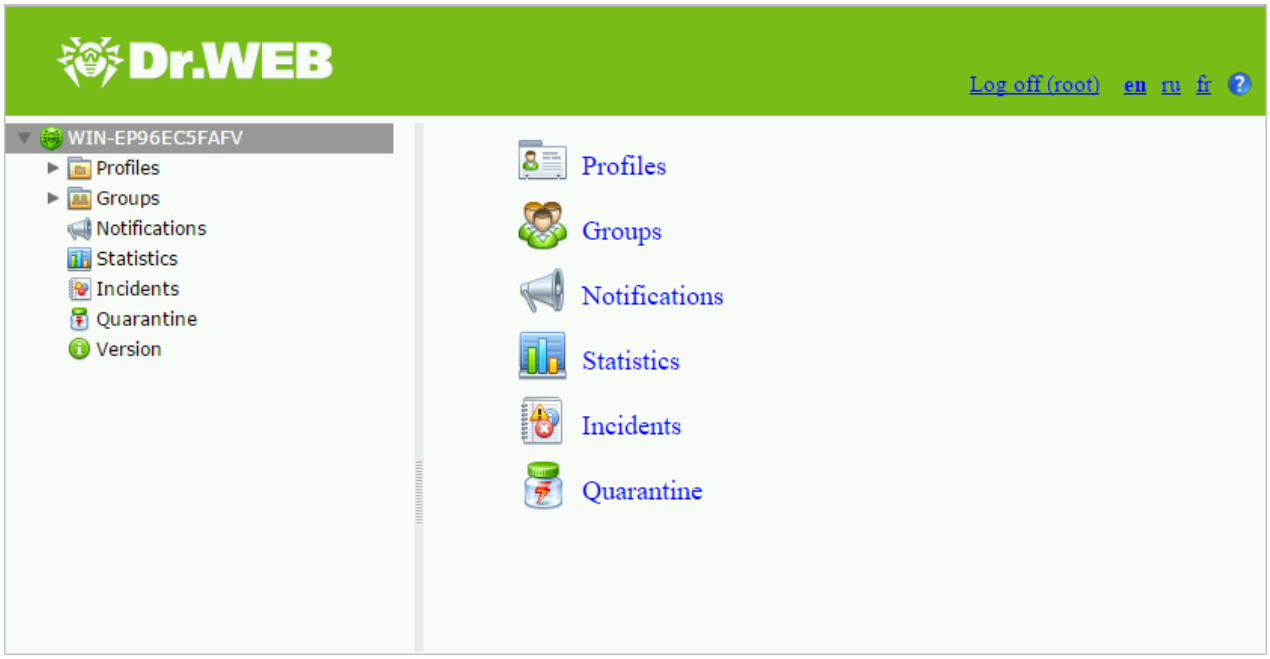

Figure 4. Dr.Web Administrator Web Console

Interface

Dr.Web Administrator Web Console comprises two sections:

1. The tree is used for navigation between different sections of application settings.
2. The details area is used for selecting configuration parameters.

You can change the interface language in the top right-hand corner of Dr.Web Administrator Web Console. You can select either Russian, English or French language. You also use the Help icon to open the Administrator manual.

7.1. Groups and Profiles

To simplify management of your local network protected by Microsoft ISA Server/Microsoft Forefront TMG, Dr.Web provides the ability to form groups of clients and assign profiles to them.

A profile is a set of adjustable traffic processing settings which determine the manner of protection of your local network. The settings of a profile can be found in the Profiles section of Dr.Web Administrator Web Console 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 and your license covers this functionality (see License Key File).
- Office control – restricts access to specific web resources.

- Filering – allows you to configure Internet traffic filtering.

For more information on creating and managing profiles, please refer to Creating and Configuring Profiles.

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

7.2. Creating and Configuring Profiles

Dr.Web creates the Default profile automatically. This profile cannot be removed nor renamed. It will be applied to all traffic as long as you do not create a new profile and assign it to a certain group of clients.

To manage the existing profiles and create the new ones the Profiles pane is used. To open it, select Profiles Dr.Web Administrator Web Console (see Figure 5).

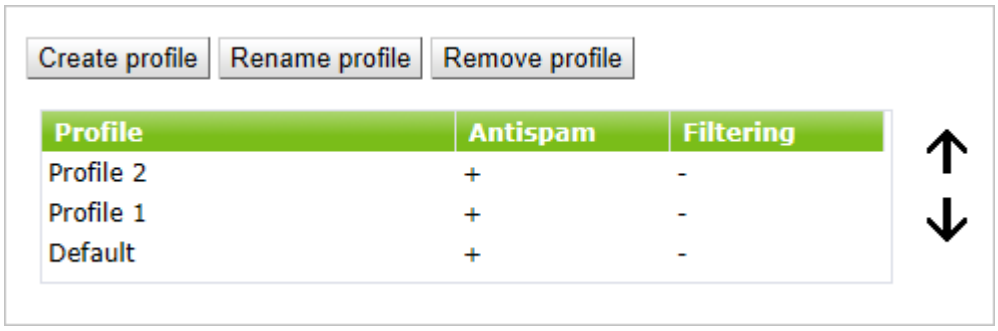

Figure 5. Profiles section

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

Creating a new profile

To create a new profile:

- 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.

In the Create profile window, enter the name for the new profile and click OK.

For profile names, use Latin characters only.

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

Renaming a profile

To change the name of a profile, select the profile on the Profiles pane and click Rename profile.

Changing profile settings

To change profile settings, select it in Dr.Web Administrator Web Console tree and open the necessary area: Scanning, Anti-spam or Office Control.

Removing a profile

To remove a profile, select in the list of profile in the Profiles area and click Remove profile.

7.2.1. Profile Priority

Each profile can have a certain priority level. 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. To move created profiles up and down the list, use the buttons ↑ and ↓ located to the right from the list. The higher the profile is located in the list, the higher its priority is.

The Default profile has the lowest priority; it always occupies the lowest position in the list of profiles.

7.2.2. 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 protection level. However note that increasing the number of object to scan types leads to server performance decrease.

To adjust scanning settings

1. Click Scanning for the necessary profile in console tree. The Scanning section will open (see Figure 6).

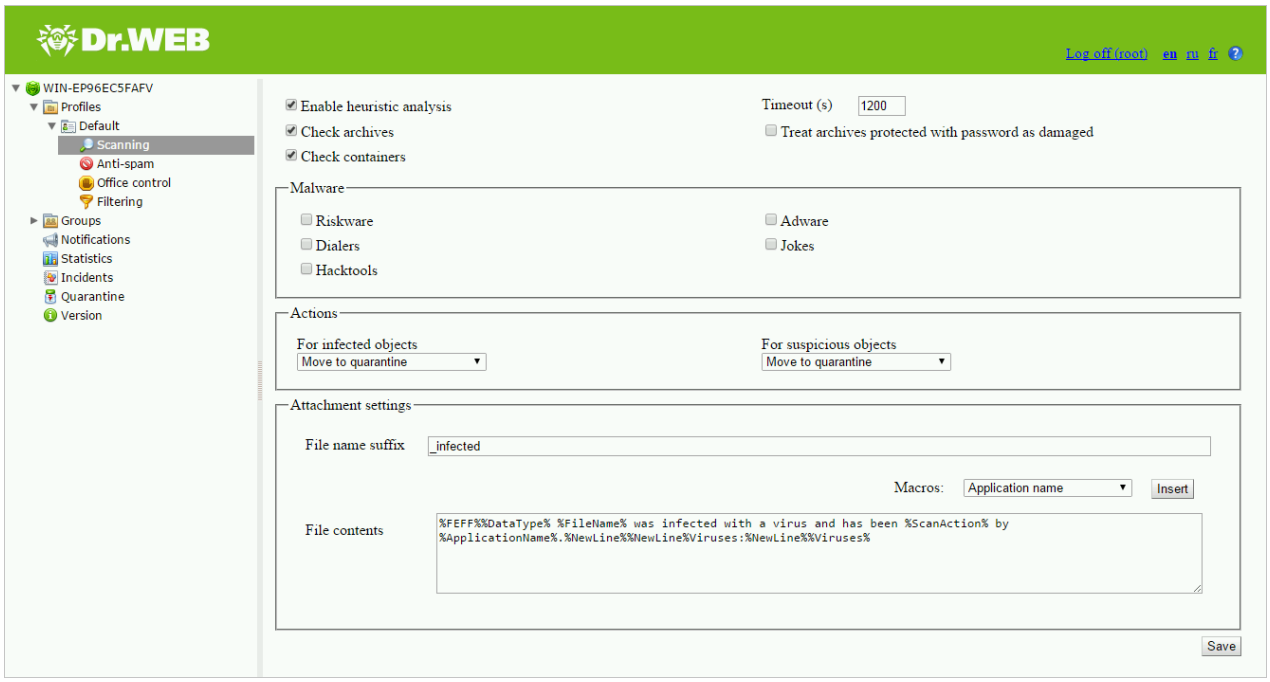

Figure 6. Scanning section

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 archives and Check containers options at the top of the Scanning pane.

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

The Timeout field allows to specify the timeout for scanning of a single file. If this timeout is exceeded during the scanning, the file is considered as bad object. By default, the timeout is set to 1200 sec. If necessary, you can change this value.

The Treat archives protected with password as damaged option defines whether encrypted archives should be ignored by the scanner or treated as infected (see Selecting Types of Damaged Objects).

3. In the Malware group box below, select the types of objects to check messages for.
4. In the Actions section below, use the drop-down lists to choose the actions for infected and suspicious objects. You can choose from the following:
   - § Move to quarantine – means that the object will be sent to the quarantine (see Working with Quarantine).
   - § Delete – means that the object will be deleted.
   - § Ignore – means that such objects will be passed on to the recipient (available only for suspicious objects).

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

7.2.3. Anti-spam

The Anti-spam component analyzes contents of email messages. The component concludes whether a message is spam on not following the results of this analysis.

The Anti-spam component is configured in the Anti-spam section of the profile settings. Please note that it is available only with the Anti-Virus&Anti-Spam version of Dr.Web. If your license covers the Anti-spam component, then the spam filtering option will be enabled automatically. You can check it in the Anti-Spam section (the Enable Anti-spam check box will be selected).

If the the Anti-spam section is disabled, it is likely that your license does not cover the Anti-spam component (for more information, see License Key File).

You can check, whether your license covers the component in the Version section of Dr.Web Administrator Web Console. If the component is supported, you will see its information in the Product information area.

Editing the key file makes it invalid! Do not open it in text editors as you might accidentally corrupt it.

Configuring the Anti-spam Component

1. Click Anti-spam in the tree pane. The Anti-spam settings area will open (see Figure 7).

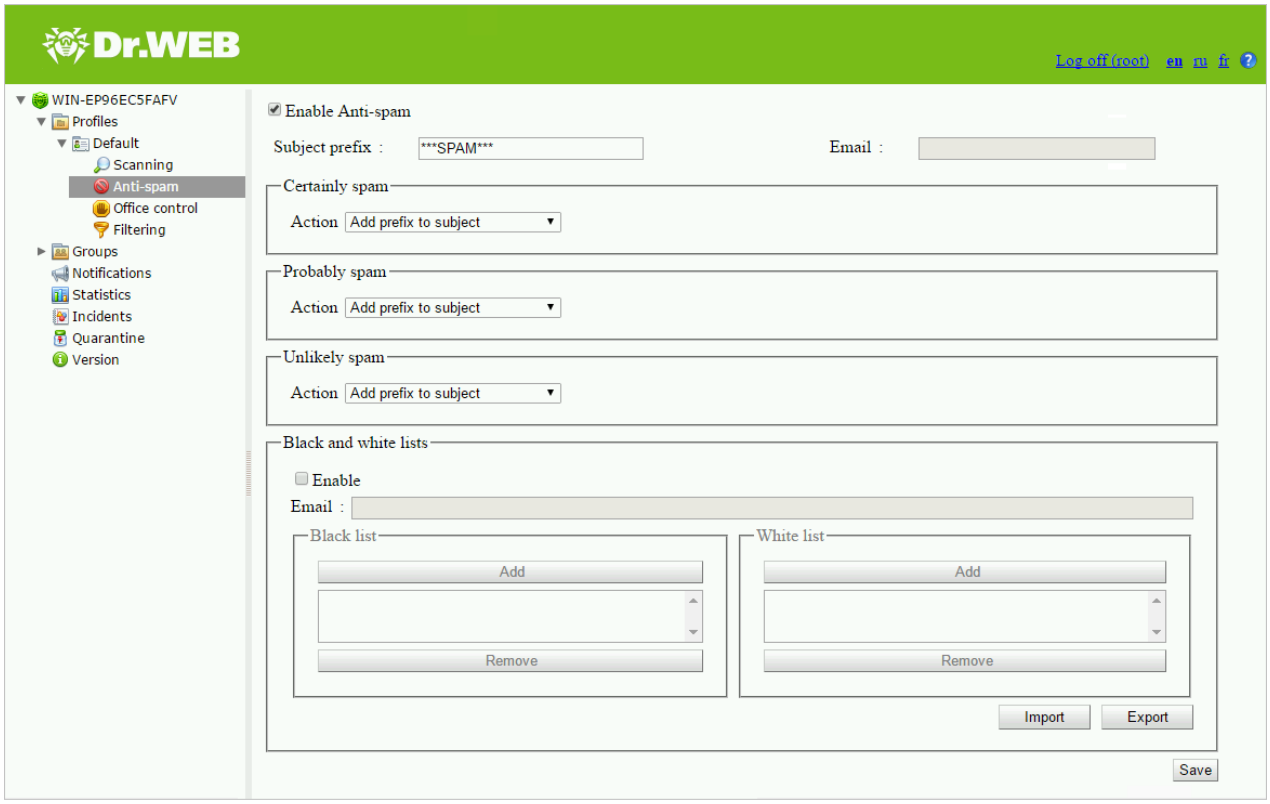

Figure 7. Anti-spam settings area

2. Select the Enable Anti-spam check box to enable spam filtering (if disabled). To disable spam filtering, clear the check box. Once the check box is cleared, all parameters become unavailable for editing.
3. In the Subject prefix field, you can change the prefix, which will appear the subject of email messages that the application will detect as spam. The default prefix is ***SPAM***.
4. According the received data, when the application detects spam, it may treat it as Certainly spam, Probably spam or Unlikely spam. For each of these three categories, you can specify an action. To do so, select one of the following actions for each category:
   - Ignore means that the message will be delivered to the recipient.
   - Add prefix to subject means that the prefix defined in the Subject prefix field will be added to the message subject.
   - Put the stamp Move to junk means that the message will be delivered to the recipient but will be marked with the stamp Move to junk.
   - Redirect means that the message will be redirected to another recipient.
     When you select this option, the Email field becomes available in the top right-hand corner. In this field, you can specify an email address to which you want the messages to be redirected. You can specify only one email address.
   - Block means that the message will be blocked and will not be delivered.

5. In the Black and white lists section you can configure a list of trusted and suspicious email 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 use the Import and Export buttons to save the list into a special file with .lst extension or to load the lists from the file and to create or edit the lists manually using a text editor. The created text file must be saved with .lst extension in Unicode format..

     To create or edit black and white lists manually, you should add prefix to emails addresses: "+" to add the email address into the white list, "-" to add the email address into the black list.

     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).

     For example:

     +trusted@example.com;+trusted_email@example.com;-suspicious@example.com;-spam@example.com;+*example.com.
6. When you finish configuring the settings of the Anti-spam component, click Save.

7.2.4. Office control

The Office control component is used to restrict access to specific web resources (e.g. pornography, violence, gambling, etc.) or allow access only to certain web sites, specified in the Office control settings.

Configuring Office Control

1. Select Office control in Dr.Web Administrator Web Console. A pane for editing parameters of the Office control will open (see Figure 8).

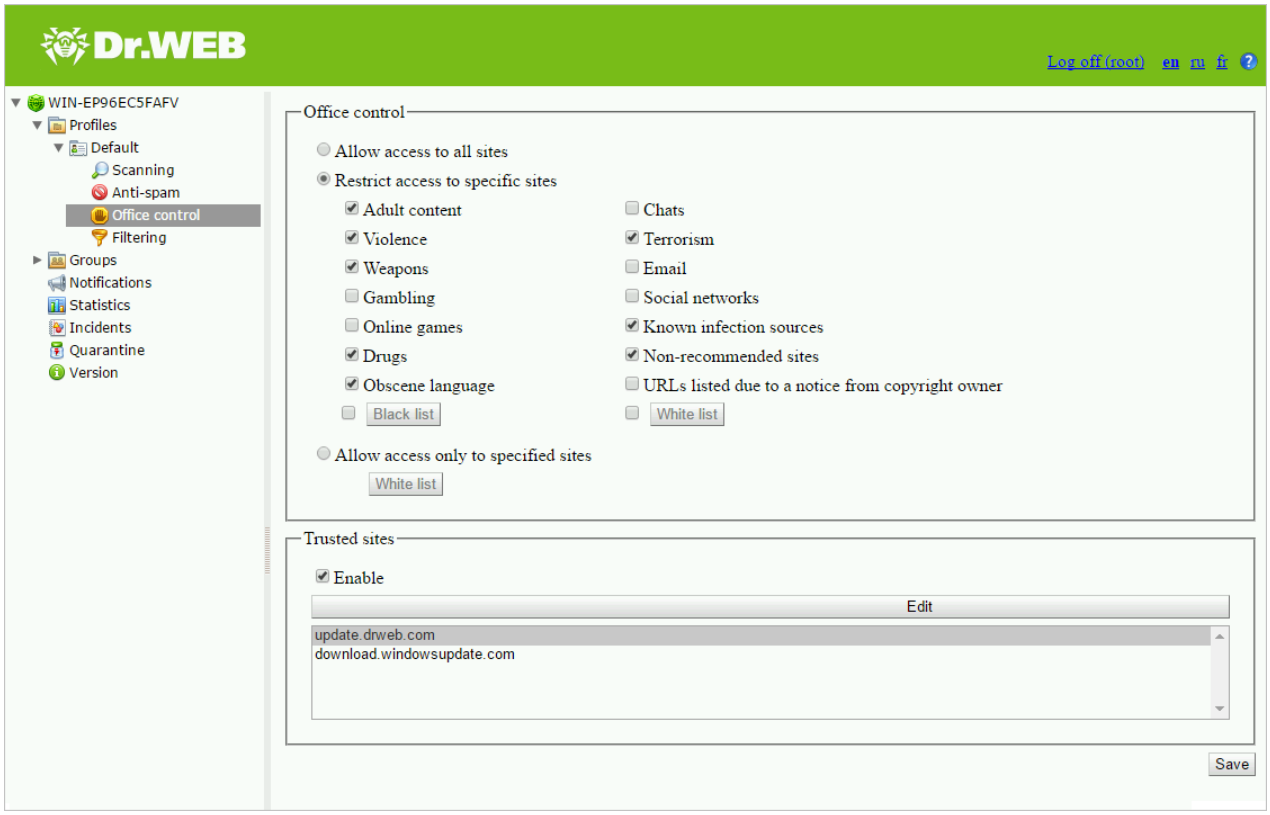

Figure 8. Office control section

2. Choose one of the following modes:
   - Allow access to all sites. There are no restrictions in this mode.
   - Block the sites specified. In this mode you can select the types of blocked web sites. Besides, you can set lists of blocked and allowed web sites regardless of restrictions by categories. To configure the list of blocked sites, click Black list, enter the site name and then click Add. To configure the list of allowed sites, click White list, enter the site name and then click Add.

     To configure the list of allowed sites, click White list, enter the site name and then click Add.

     Lists of web sites in all categories are constantly updated by the Automatic Updating Module along with virus databases.

   - Allow access only to specified sites. In this mode access to all resources except those in White list will be restricted. To configure the list of allowed sites, click White list, enter the site name and then click Add.
3. Trusted sites. Sites from the list of trusted have the highest priority and do not undergo any checks.
   To use the list, select the Enable check box on the Trusted sites section. To edit the list of trusted sites, click Edit, enter the resource name and click Add.
4. When you finish setting up Office control, click Save

Forming black and white lists

1. Enter a domain name (or part of it) into the field:
   - If you wish to add a specific web site, enter its full address (e.g. www.example.com). Access to all resources on that web site will be allowed/restricted.
   - If you wish to allow/restrict access to web sites, which contain certain text in their address name, enter that text into the field (e.g. example means that access to example.com, example.test.com, test.com/example, test.xample222.ru, etc. will be allowed/restricted).
     If the string contains the "." symbol, it will be considered a domain name. In this case all resources on the domain will be filtered.

     If the string also contains the "/" symbol (e.g. example.com/test), then the part to the left of it will be considered the domain name and the part to the right will be allowed/restricted on the domain (e.g. example.com/test11, template.example.com/test22, etc. will be filtered).
2. Click Add. The address (or part of it) will be added to the list above.
   The address may be converted to a more simple structure (e.g. http://www.example.com will be converted to www.example.com).
3. To delete a web resource from the list, select it and click Delete.

7.2.5. Filtering

The application allows you to configure rules to filter messages and their attachments. You can set these rules in the Filtering section (see Figure 9).

To create and apply filtering rules, you should enable the component. To do so, select the checkbox Enable filtering at the top of the section.

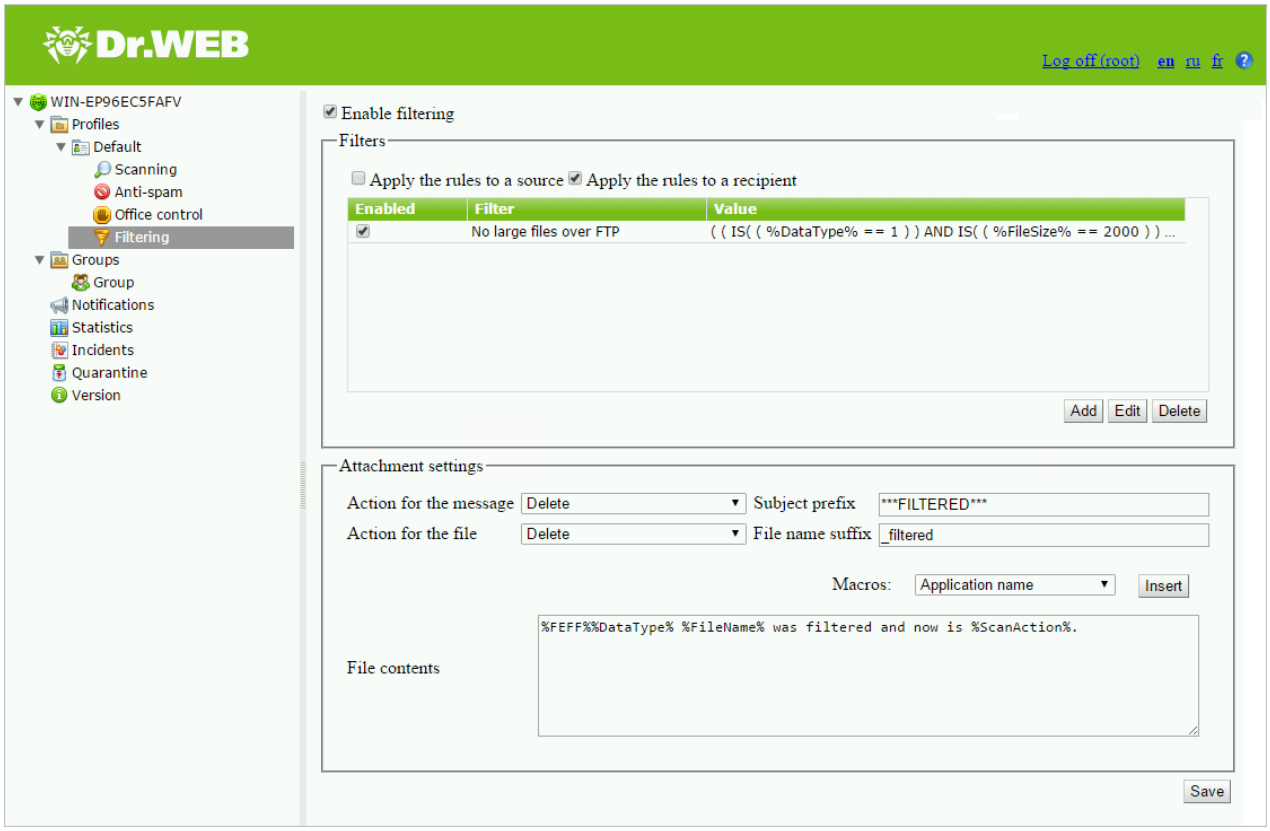

Figure 9. Filtering section

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.

Creating filtering rules

1. Click Add under the filters list. A Filtering rule window will open (see Figure 10). You can enter the name for the new rule and specify its conditions.
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 (types of conditions, compliance and possible values are listed in the table below).
3. Click OK to save the new rule. To close the window without saving the rule, click Cancel.

To change or delete a new rule, select it from the list and click Edit or Delete.

Below there is an example of how you can create a rule.

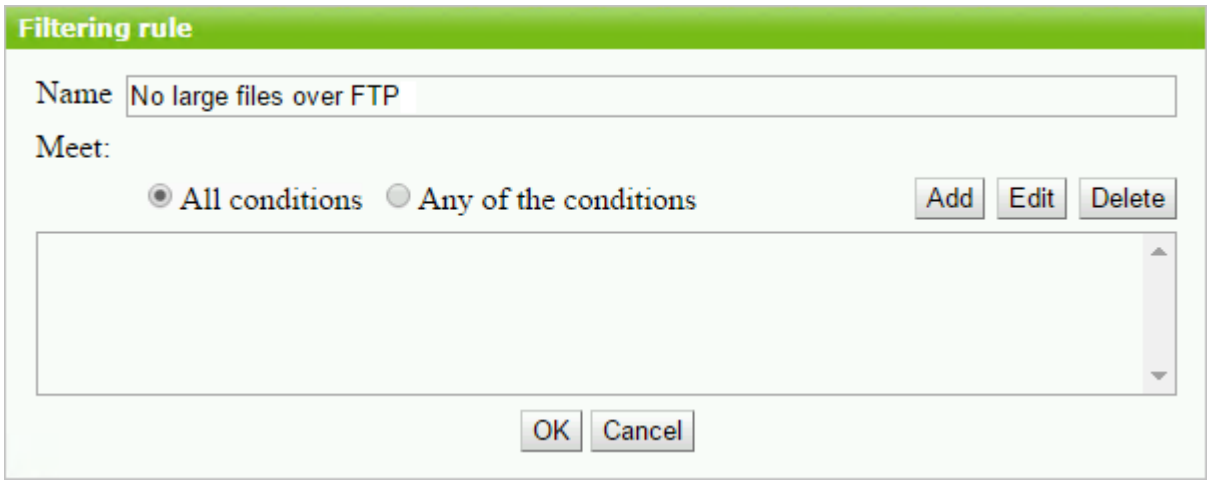

Figure 10. Creating a filtering rule

Configuring filtering for email messages

1. Enable one or more rules from the list by selecting their check boxes.

   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. 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 ignore the message and add to its subject a prefix specified in the Subject prefix

   For attachments, the following actions are available:

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

   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. You can add macros from the Macros drop-down list.

4. Click Save when you finish configuring filtering rules.

Creating filtering rules

Condition type	Compliance type	Value
Data type	Equals Does not equal	File Message
Data source	Equals Does not equal Contains Does not contain Matches Does not match	Specified manually In case the Contains, Does not contain, Matches or Does not match compliance types is selected, you can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value when entering the value.
Data recipient	Equals Does not equal Contains Does not contain Matches Does not match	Specified manually In case the Contains, Does not contain, Matches or Does not match compliance types is selected, you can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value when entering the value.
Protocol	Equals Does not equal	HTTP FTP POP3 SMTP

Number of recipients	Equals Does not equal Greater than Less than or equal to Less than Greater than or equal to	Specified manually
File name	Equals Does not equal Contains Does not contain Matches Does not match	Specified manually In case the Contains, Does not contain, Matches or Does not match compliance types is selected, you can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value when entering the value.
File size	Equals Does not equal Greater than Less than or equal to Less than Greater than or equal to	Specified manually (in bytes)

Message subject	Equals Does not equal Contains Does not contain Matches Does not match	Specified manually In case on of the Contains, Not contains, Matches or Not matches compliance types is selected, you can use the wildcard characters «*» and «?» to substitute a sequence of symbols or only one symbol in the entered text value when entering the value.
Has attachment	Equals Does not equal	False True

Filtering rule example

To filter files over 20 MB, transferred via the FTP protocol, you can configure a rule with the following parameters (see Figure 11):

Condition type	Compliance type	Value
Data type	Equals	File
Protocol	Equals	FTP
File size	Greater than	20000

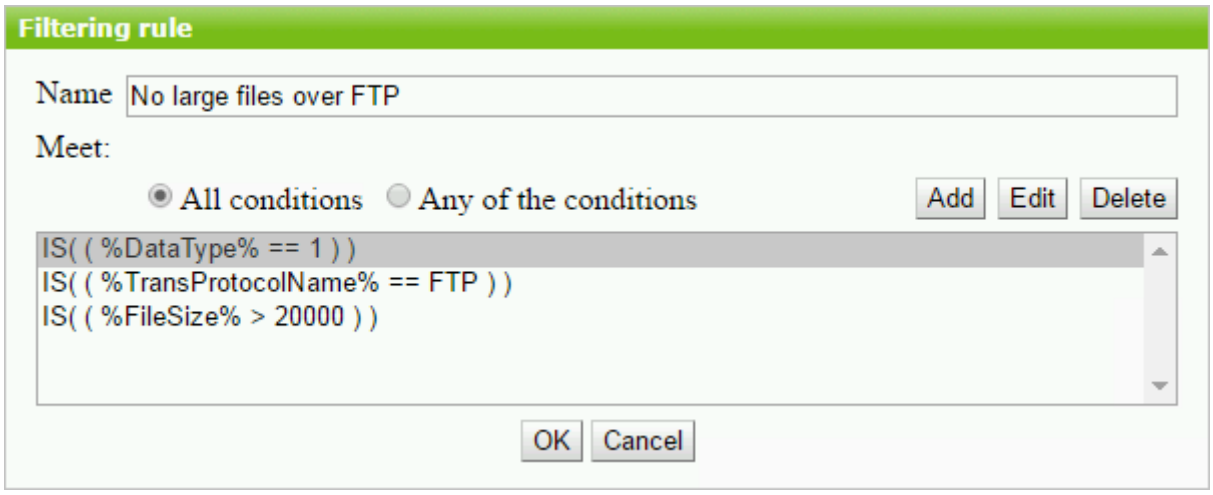

Figure 11. Example of a filtering rule

7.3. 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.

7.3.1. 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 Dr.Web Administrator Web Console (see Figure 12).

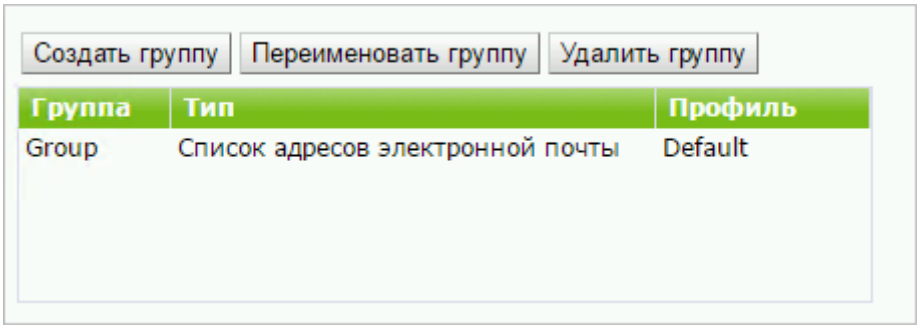

Figure 12. Groups section

Creating a New Group

To create a new group:

- 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 right-click menu.

In the Create group window, specify the name for a new group and click OK. The Default profile is automatically assigned for new groups.

For group names, use Latin characters only.

Renaming groups

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

Deleting groups

To delete a group, select it on the Groups pane and click Remove group.

Viewing group settings

Click the name of the group in the 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 or editing group settings, click Save.

7.3.2. Configuring and Forming Groups

In the information pane that opens by clicking the group name in the administrative console tree (see Figure 13), you can set up the parameters of the selected group, including the manner of forming this group: by listing the email addresses, the IP addresses or selecting the Active Directory groups.

Select the group type in the drop-down list Type.
Type selection depends on the protocol you are going to work in the current profile. For example, if you work with the SMTP protocol, you are recommended to select the List of email addresses; if you work with FTP, specify the List of IP addresses option.

Figure 13. Group settings

Creating a list of email addresses

1. In the the Type drop-down list, 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.

Creating a list of IP addresses

1. In the the Type drop-down list, select List of IP addresses.
2. In the Item list, select the elements type: IP address or IP addresses range.
3. To add an element to the list, click Add. In the new window, depending on the selected elements type, enter the IP address or specify the IP addresses range. Click OK.
4. To delete an element from the list, select it and click Remove, then confirm the deletion of the selected element.

Creating a list of Active Directory groups

1. In the the drop-down list Type, select List of Active Directory groups.
2. To add a new group to the list, click Add. In the new window, select the group to add and click OK.

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

You can create a list of Active Directory groups if the server is in a domain.

If the server is not in a domain, you can still create a list of Active Directory groups in Dr.Web CMS Web Console:

1. Open Dr.Web CMS Web Console.
2. For the parameter /DrWebADAccessor_1.0/Application Settings/ADAccUserName, specify username of the account that has access to Active Directory.
3. For the parameter /DrWebADAccessor_1.0/Application Settings/ADAccUserName, specify password of the account that has access to Active Directory.

By default, these values 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.

7.4. Notifications

Notifications are added to the operation system event log and are used to keep the administrator 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.).

Configuring notifications

1. Click Notifications in the administrative console tree. A pane for editing parameters of notifications will open (see Figure 14).

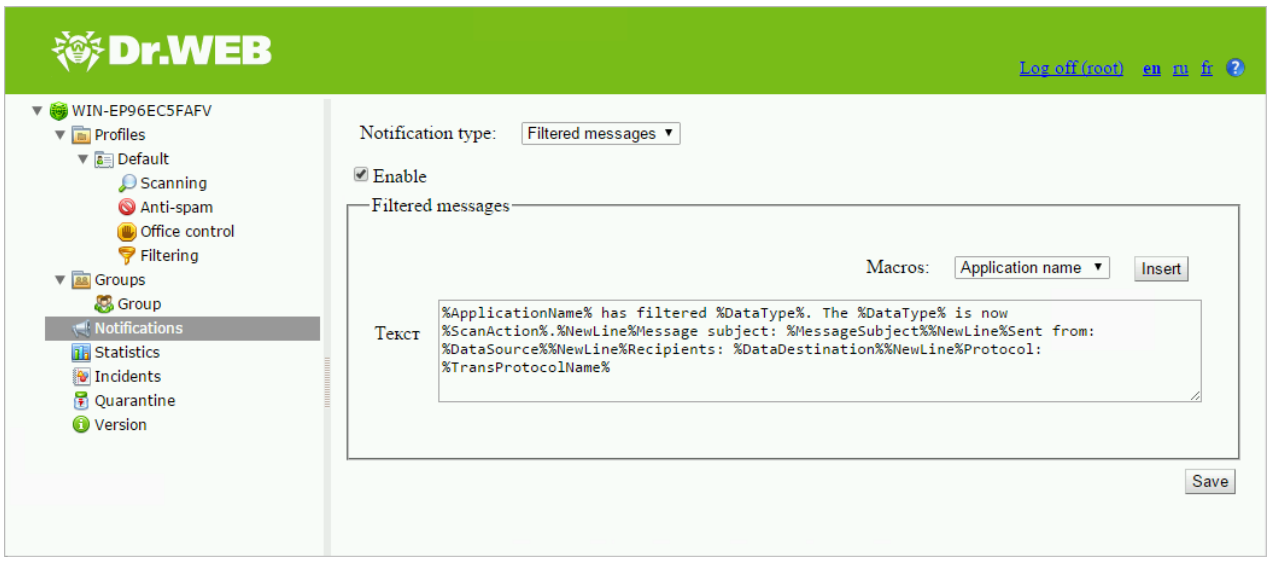

Figure 14. Notifications section

2. In the Notification type list, select the type of event to configure notifications for:
   - Filtered messages – to send notifications about filtered messages.
   - Filtered files – to send notifications about filtered attachments.
   - Infected – to send notifications about infected objects.
   - Spam – to send notifications about spam.
   - Update – to send notifications with the last update.
   - Expired bases – to send notifications about virus databases expiration.
   - Office control – to send notifications about web resources filtered by Office Control.
3. By selecting/clearing the Enable option, you can enable/disable sending notifications of the selected type.
4. In the settings group below, you can modify the text template for the notifications of selected a type by entering it in the Text field. While editing the text, you can use macros.
5. When you finish configuring the settings, click Save.

7.5. Viewing 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 15).

Configuring statistics display

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 started its operation.
   - 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 types. This section displays information about the number of threats that Dr.Web detected during the specified time period.
- URL category. This section contains the statistics of the operation of Office control and the number of blocked resources of each category.

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

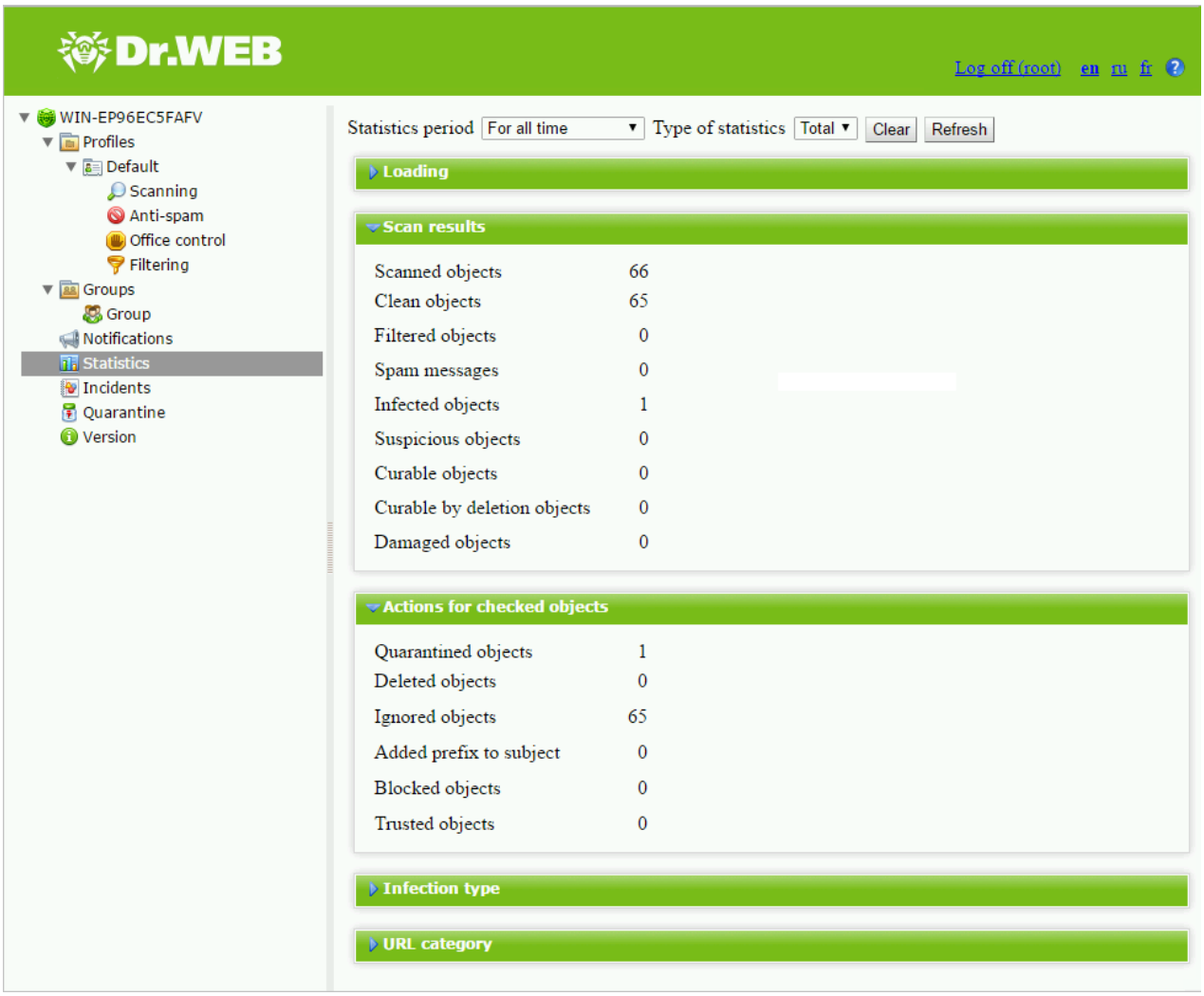

Figure 15. Statistics section

7.6. Viewing Incidents

The Incidents section allows you to view the list of events connected with anti-virus and Anti-spam triggering for the specified period of time. You can also view basic information about these events (see Figure 16).

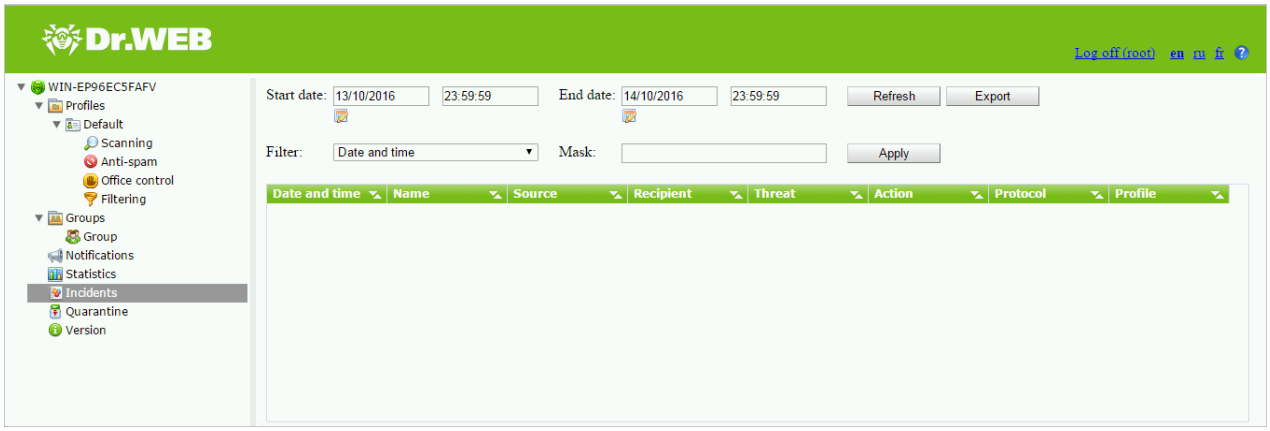

Figure 16. Incidents

Viewing incidents information

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

- Date and time
- Name of the object related to the incident
- Source and recipient
- Type of the threat
- Performed action
- protocol
- Name of the applied profile

You can configure the display parameters of the list of incidents:

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

Managing the list of incidents

1. You can specify the time period to review the incidents. Enter the start and the end date of the interval and 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 in the entered text value.

3. You can save the list of incidents as a text file. To do so, click Export. Select format to save the file in and click OK. You can save the list in 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 update the list of incidents manually, click Refresh. The list gets updated each time you start the Dr.Web Administrator Web Console and open the Incidents section. It may take some time to refresh the list. To stop the refreshing process, for example, if you entered wrong filtering parameters, click Cancel.

7.7. Working with Quarantine

Quarantine of Dr.Web is used to isolate suspicious objects detected while checking the network traffic.

In the Quarantine section of Dr.Web Administrator Web Console, the current information about quarantine state is displayed.

You can also use the Quarantine Manager utility to review and edit the list of objects in the quarantine.

7.7.1. Viewing Quarantine in Dr.Web Administrator Web Console

The Quarantine section (Figure 17) of Dr.Web Administrator Web Console is used for viewing the list of isolated objects and basic information about these objects.

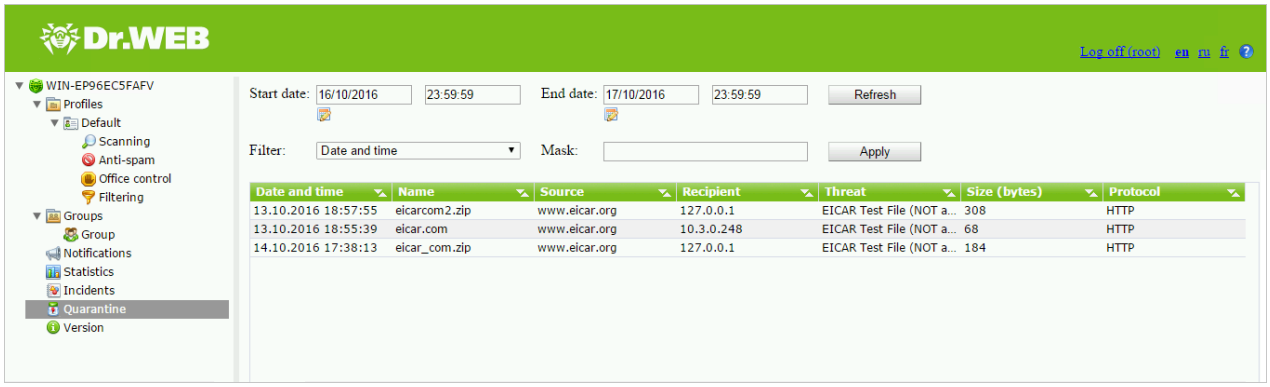

Figure 17. List of objects in the quarantine

Viewing information about objects in the quarantine

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

- Date and time the object has been moved to the quarantine
- Name of the infected file
- Source and recipient
- Name of the threat
- File size (in bytes)

- protocol

The following options are available to configure the Quarantine:

- 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 and click Refresh.
- You can use a number of filters to sort the items 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 in the entered text value.

- To sort the list, click the title of the corresponding column.
- To update the list, click Refresh. The list also gets automatically updated each time you start Dr.Web Administrator Web Console and open the Quarantine section. It may take some time to refresh the list. To stop the refreshing process, for example, if you entered wrong filtering parameters, click Cancel.

Actions you can perform with objects in the 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.

To configure quarantine options, use the Quarantine Manager utility.

7.7.2. Quarantine Manager

Quarantine manager is an additional utility supplied together with Dr.Web. It is used for configuring quarantine parameters and working with isolated objects.

To start Quarantine manager (see Figure 18) click the Dr.Web Quarantine icon on the Desktop.

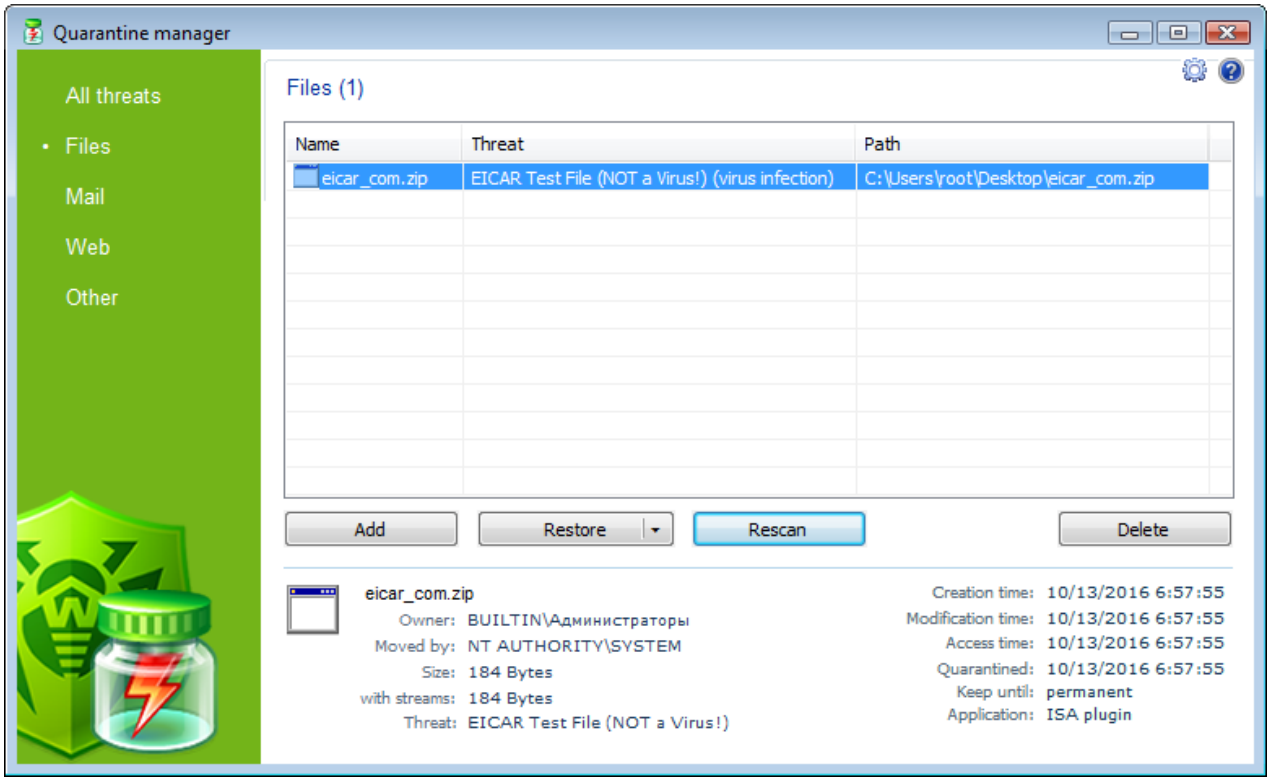

Figure 18. Dr.Web Quarantine utility window

The Quarantine manager window comprises several areas:

1. The left pane is used for sorting the list of objects that are grouped by their types. Click on a necessary type in the pane to view objects:
   - Files
   - Mail objects
   - Web pages
   - Other objects
2. In the center of the window occupies a table with the Quarantine state. The following columns are included by default:
   - Name – names of isolated objects
   - Threat – threat classification, which is assigned by Dr.Web.
   - Path – full path to the object before it was moved to the quarantine.
3. In the bottom of the Quarantine manager window the detailed information about selected items is displayed.

You can display the columns with detailed information about isolated objects.

Configuring columns

1. Select Customize columns in the right-click menu.

2. 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 the window without saving any changes, click Cancel.

7.7.2.1. Working with Quarantine in Quarantine Manager

To manage objects in Quarantine manager, you can use the following buttons:

- Add – to add file to the quarantine.
- 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 18. 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 object is clean.

  The drop-down menu item Restore to is used to to restore files to the specified folder.
- Rescan – to scan file again. If a file is defined as clean, the quarantine will prompt 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.

7.7.2.2. Configuring Quarantine Properties

In Quarantine manager you can configure quarantine settings. To do so:

1. Click the Settings icon in the Quarantine manager window.
2. The Quarantine properties window will open. In this window you can change the following parameters:
   - The Set quarantine size section allows you to configure the amount of disk space for the Quarantine folder. Move the slider to change the 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 that the size of the quarantine is unlimited.

- In the View section, select the Show backup files option to display backup copies of files in the object's table, which have been previously deleted or cured. Backups are created automatically when files are deleted or cured. Backup copies are kept temporarily.

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

8. Updating Virus Databases

To mitigate the risk of infection during the licensed period, Doctor Web provides you with regular updates of virus databases and application 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 section in Dr.Web Administrator Web Console.

You can start the virus databases update by clicking Start in 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 Doctor Web update servers. You can adjust this schedule using Windows Task Scheduler:

1. Open Windows Task Scheduler.
2. Right-click the Doctor Web for MSP Update Task task and click Properties.
3. In the Doctor Web for MSP 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.

8.1. Version of the Application and Virus Databases

In the Version section (Figure 19), you can review the information about the application version, license, virus databases and also the date, time and result of the last update.

Figure 19. Version section

9. Dr.Web CMS Web Console

Dr.Web CMS Web Console is an additional configuration console and a part of Dr.Web. You can use it to change configuration parameters manually by entering custom values, detect and troubleshoot errors. For example, you can create clusters, add user accounts, change account settings and much more.

Use Dr.Web CMS Web Console only if you know for sure which values to change. For general configuration, use Dr.Web Administrator Web Console.

Starting Dr.Web CMS Web Console

In order to launch Dr.Web CMS Web Console (Figure 20), enter the following address into the address bar in your browser:

```
https://<ISA Server address>:2080/root,
```

where *<ISA Server address>* stands for the address of the Microsoft ISA server or Microsoft Forefront TMG.

To access Dr.Web CMS Web Console, you have to enter credentials for the administrator account.

When you start Dr.Web CMS Web Console for the first time, use default credentials: the login `root` and the password `drweb`. We strongly recommend you to change administrator credentials (for more information, see Changing Administrator Password).

Figure 20. Dr.Web CMS Web Console

Interface

Dr.Web CMS Web Console comprises 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 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 debugging mode.
   - 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.

- Log level. Events logging level.
- Instances. Even source;
- Contents. Text in the message (text in the File content field);
- NonContents. Text that is not included in the message (text in the File content 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

When you start Dr.Web Administrator Web Console or Dr.Web CMS Web Console for the first time, you should use default credentials to log in (username root, password drweb). We strongly recommend you to change administrator credentials as soon as you access the settings.

Changing password of the administrator account

1. In the hosts and groups tree, select 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 right-click menu.
7. The Add new variable window will open. Enter UserLevel as the name of the variable and select UInt32 for its type. Set the following values for the variable:

0 – full access to the settings.

1 – access to the 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 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 nodes.

Creating a cluster

On a host that you want to add to a new 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. 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 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.

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 so, 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 Active Directory 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 in Dr.Web Administrator Web Console on the main host, are transferred to the sub-host.

1. On the sub-host, create a new Distribution group using the Active Directory management console.
2. In the Dr.Web Administrator Web Console, add the new group to the list of application groups.
3. 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 configuring

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. Selecting Types of Damaged Objects

In some cases attachments may be treated as *damaged* objects, because application cannot scan them for viruses. The application treats damaged objects as infected. To configure which objects should be treated as damaged, 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
     This action is also available in Dr.Web Administrator Web Console. For more information, see Scanning.
   - 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 damaged. Action selected for infected objects in the Scanning section will be applied to this object.

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

9.5. Filtering Files in Archive by Their Extensions

If you need to detect archives containing files with certain extensions and treat them as 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`

First of all, the archive will be scanned for infected objects. If an infected object is detected, the application will treat as in infected object and will apply the relevant action to it. If nothing is found, the application will scan it for files with the specified extensions. If a file with the specified extension is detected, the application will treat is as a suspicious object.

10. Event Logging

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

- Windows Event Log
- Installation text log
- Application event log

Information about updates is registered in a dedicated text file drwebupw.log (see Checking Updater Functionality) that is located in the following folders:

- %ALLUSERSPROFILE%\Application Data\Doctor Web\Logs in Windows Server 2003
- %PROGRAMDATA%\Doctor Web\Logs in Windows Server 2008

10.1. Event Log

Dr.Web registers the following information in the Windows Event Log:

- Plug-in starts and stops events
- License key file parameters including validity and licensing 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). These notifications you can configure:
  - Filtered messages – notifications about filtered messages.
  - Filtered files – notifications about filtered attachments.
  - Infected – notifications about infected objects.
  - Spam – notifications about spam.
  - Filtered files – notifications about filtered infected objects.
  - Update – notification about update;
  - Expired bases – notifications about virus databases expiration.
  - Office control – notifications about web resources filtered byOffice Control.

Viewing Event Log

1. On the Control Panel, double-click Administrative Tools and then double-click Event Viewer.

2. In the tree view, select Administrative Tools and then select Event Viewer.
3. In the left part of the window of Even Viewer, select Doctor Web. The list of registered events will show up. The sources for Dr.Web notifications are 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.

Redirecting 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.
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 Doctor Web log.

3. Restart Dr.Web for MSP Scanning Service.
4. Remove Dr.Web CMS for MSP from the registry `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Doctor Web\Dr.Web for Microsoft Server Products`.
5. Restart the operating system.

10.2. Program Installation Text Log

In order to simplify troubleshooting in the process of installation or operation, the application registers events in the txt log. The log file isa-tmg-setup.log is located in the:

- %ALLUSERSPROFILE%\Application Data\Doctor Web\Logs in Windows Server 2003;
- %PROGRAMDATA%\Doctor Web\Logs in Windows Server 2008.

10.3. Dr.Web Even Log

The list of event is registered by Dr.Web CMS and is stored in a dedicated database cmstracedb, which is located in the %PROGRAMFILES%\DrWeb CMS for MSP\.

The service registers different events, and allows you to select the level of logging for each Dr.Web CMS-dependent application.

The maximum size for the database is 500 Mbyte. Once the database reaches this size, it gets archived and stored in the installation folder. Each archived file has a timestamp. After that a new database file is created.

You can delete the cmstracedb database, if necessary.

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
Information	Information messages
Debug	Debug records

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 %PROGRAMFILES%\DrWeb CMS for MSP:

1. Run the command-line tool with administrator rights.
2. 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"
   ```

3. Remove the cmstracedb file located in the application installation folder %PROGRAMFILES%\DrWeb for CMS for MSP.
4. 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"
   ```

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

11. Diagnostics

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

- Application installation check
- Updater check
- Virus detection test
- Spam detection test

11.1. Checking Installation

Dr.Web must be installed into the following folders:

In case Microsoft ISA Server is used:

- %ALLUSERSPROFILE%\Application Data\Doctor Web
- %PROGRAMFILES%\Common Files\Doctor Web
- %PROGRAMFILES%\DrWeb CMS for MSP
- %PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG

In case Microsoft Forefront TMG is used:

- %PROGRAMDATA%\Doctor Web
- %PROGRAMFILES%\DrWeb CMS for MSP
- %PROGRAMFILES%\Common Files\Doctor Web
- %PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG

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

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

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

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

11.2. Checking Updater Functionality

The updating module drwupsrv.exe automatically starts after the installation of Dr.Web. It updates the anti-virus engine drweb32.dll, virus databases and other elements except the application components.

To make sure that an update was successful:

1. Depending on the version of the operating system, run the Tasks command to open the %WINDIR%\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 (if you work in Windows Server 2003) or %PROGRAMDATA%\Doctor Web\Logs\dwupdater.log (if you work in Windows Server 2008) 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, you are 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 Download Anti-Malware Testfile at http://www.eicar.org or create in manually.

Testing virus detection with EICAR test file

1. Create a file:
   - Open Notepad.
   - Paste the following string into it:
     ```
     X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
     ```
2. Save the file with the .com extension. You can use any name, for example eicar.com.
3. Attach this file to an email message and send it to any test email address.

   The message you receive should contain the 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 Microsoft ISA Server and Forefront
   TMG. Virus name: EICAR Test File (NOT a Virus!).
   ```

Do not use actual viruses to test 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. Appendix A. Removing Dr.Web Manually

If you experience firewall failures, you can remove Dr.Web manually. To do so:

1. Stop the Microsoft ISA Server/Microsoft Forefront TMG firewall service.
2. Run the command-line tool (cmd) with administrator rights.
3. Unregister the application filter using the following commands:
   - For Microsoft ISA Server:

     ```
     regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\FTPFilter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\POP3Filter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\SMTPFilter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG\HTTPWebFilter.dll"
     ```

   - For Microsoft Forefront TMG:

     ```
     regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\FTPFilter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\POP3Filter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\SMTPFilter.dll"

     regsvr32 /u /s "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG\HTTPWebFilter.dll"
     ```

3. 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"
   ```

4. Delete 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"
```

6. Delete the following folders:

- For Microsoft ISA Server:

```
rd /S /Q "%ALLUSERSPROFILE%\Application Data\Doctor Web"
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"
rd /S /Q "%PROGRAMFILES%\Microsoft ISA Server\DrWeb for ISA and TMG"
```

- For Microsoft Forefront TMG:

```
rd /S /Q "%PROGRAMDATA%\Doctor Web"
rd /S /Q "%PROGRAMFILES%\DrWeb CMS for MSP"
rd /S /Q "%PROGRAMFILES%\Microsoft Forefront Threat Management Gateway\DrWeb for ISA and TMG"
```

12.2. Appendix B. CMS Platform

CMS (Central Management System) is a cross-platform distributed system for application management (hereinafter any module subscribed to the main managing service is considered as application). The key component of the system is Dr.Web CMS, which is a managing service. It is used for controlling and managing operation of applications, application settings and participates in event logging.

The applications interact between each other over the TCP protocol. With the managing service, they can interact in the following ways:

- Controlled applications use 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 a tree-structured database to store information on the application data.

12.2.1. 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 can not be modified

Physically, database is a cmsdb file located in the application installation folder (%PROGRAMFILES%\DrWeb CMS for MSP\).

12.2.2. 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.

12.2.3. Connecting to Servers

Dr.Web CMS Web Console allows you to connect to other servers that have CMS running. To connect to a server, do the following:

1. Right-click the host icon in the console tree and select Add host.
2. Specify the 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 host is shown as a group that has the same name as the connection. There are three variables inside such groups:

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

Dr.Web CMS Web Console stores connection settings to each host in its CMS group in /Dr.Web CMS Web Console_1.0/Application Settings/Hosts.

Each new added host is shown as a group that takes the name of the connection. Inside such a group, there are three variables: Address, Login and Passsword. The variable Address contains the address of the connection to the host. The Login variable contains user name for connection. The variable Password contains password that is used for connection.

If the credentials are modified, you may not be able to connect to the host. In this case you need to update connection settings for this host in Dr.Web CMS Web Console.

The next time you launch Dr.Web CMS Web Console, it will automatically connect to added hosts. If you want to remove a host, you need to delete the group with connection settings from the console configuration in /Dr.Web CMS Web Console_1.0/Application Settings/Hosts.

In Dr.Web CMS Web Console, you can also create clusters. In a cluster, you can set the same settings for all hosts.

12.3. Appendix C. Configuring Update Parameters

To configure virus databases update parameters, use the drwupsrv.bat file. The file is located in the Dr.Web directory. Commands frol the file are executed when the Doctor Web for MSP Update Task is started 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	Please do not edit this parameter. Type of update: • update-revision—update components within the current revision.
--disable-postupdate	Please do not edit this parameter. Post-update is disabled. Operation of the update module will be stopped as soon as the update operation is 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	Please do not edit this parameter. Additional parameters passed to the script: Format: <name>=<value>.
-n [--component] arg	List of the components that need to be updated: • updater—drwupsrv.exe file; • antispam—vrcpp.dll file; • scan-engine—dwengine.exe, dwsewsc.exe, dwinctl.dll, dwarkdaemon.exe, arkdb.bin, dwqrui.exe and dwarkapi.dll files; • av-engine—virus databases (*.vdb files); • isa-and-tmg-setup - isa-and-tmg-setup.exe file. ⚠ Several components can be updated simultaneously, e.g.: `-n av-engine updater`
-g [--proxy] agr	Proxy server for updating. <address>:<port>.
-u [--user] agr	User name for the proxy server.

Parameter	Description
-k [--password] arg	User password for the proxy server.

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

```
-c update --type=update-revision --disable-postupdate --verbosity=debug
--interactive --param="<plugin_name>" -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>.

- c postupdate command example:

```
-c postupdate --verbosity=debug --interactive --param="<plugin_name>"
```

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> --repodir=<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 --verbosity=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=<plugin_name>" --zone="file://<repo_folder_path>"`

Keyword Index

Keyword Index

Keyword Index

U

V