Dr.WEB®

Anti-virus
for Microsoft ISA Server and Forefront TMG

Defend what you create

Administrator Manual

Dr.Web Anti-virus for Microsoft ISA Server and Forefront TMG
Version 6.00.1
Administrator Manual
01.11.2012

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

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web

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

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

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

Table of Contents

Document Conventions and Abbreviations

The following conventions and symbols are used in this document:

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

The following abbreviations are used in the manual:

- AD – Active Directory
- CPU – Central Processing Unit
- HTML – Hypertext Mark-up Language
- HTTP – Hypertext Transfer Protocol
- FTP – File Transfer Protocol
- POP3 – Post Office Protocol Version 3
- GUI – Graphical User Interface
- OS – operating system
- RAM – Random Access Memory
- SMTP – Simple Mail Transfer Protocol
- SP1, SP2, etc. – Service Packs

Introduction

Thank you for purchasing Dr.Web Anti-virus for Microsoft ISA Server and Forefront TMG (hereinafter referred to as Dr.Web Anti-virus). This anti-virus product is a powerful tool against threats propagated through the HTTP, FTP, SMTP and POP3 protocols and offers a reliable protection scanning and neutralizing the infected objects inside a corporate network protected by Microsoft ISA Server or Microsoft Forefront TMG firewall.

This manual is intended to help administrators of large corporate networks to install, adjust and manage Dr.Web Anti-virus, and contains information on all the main features of the software and contact details for technical support.

What is Dr.Web Anti-virus

Dr.Web Anti-virus is an anti-virus plug-in designed to protect corporate systems against viruses and spam. It flexibly integrates into the system and processes all traffic transferred via HTTP, FTP, SMTP and POP3 protocols in order to detect and neutralize all types of malicious objects. The plug-in check the incoming Internet traffic for viruses, dialers, adware, hacktools, jokes and riskware. If a threat is detected, it is processed according to the application settings.

The application integrates into Microsoft ISA Server and Microsoft Forefront TMG by implementing its data filters, that give access to them to the Dr.Web anti-virus engine. Dr.Web Anti-virus operates on the Dr.Web CMS platform (Dr.Web Central Management Service), which supports the central configuration of application settings and components and remote administration via protected protocol HTTPS. Dr.Web CMS has an inner web server Dr.Web CMS Web Console with client authentication, thus, only the authorized administrators can access the application settings.

Dr.Web CMS services installed on different servers can be organized in a hierarchy tree by the administrator, to support replication of

parameters with the Shared attribute of the application working with Dr.Web CMS. The parameters are copied from the main server to the sub-server one (see Organizing clusters), thus, the servers tree parameters can be configured on the main host.

Dr.Web Anti-virus can perform the following functions:

- Scan all Microsoft ISA Server and Microsoft Forefront TMG traffic, transferred via HTTP, FTP (including FTP over HTTP), SMTP and POP3 protocols
- Block access to the infected objets for users within the network protected by Microsoft ISA Server or Microsoft Forefront TMG firewall
- Isolate infected and suspicious objects to Quarantine
- Add notifications on virus events to the Event log and to the internal event database in Dr.Web CMS
- Filter spam in the e-mails via SMTP protocol
- Add accompanying text to the e-mail messages containing security threats
- Restrict access to web resources using Office Control
- Collect statistics
- Automatically update virus databases and components of the plug-in
- Support the common application settings on a distributed system of firewalls, including those organized in clusters

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

Scanned Objects

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

Scanned objects in HTTP and FTP traffic

Dr.Web Anti-virus 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 the received data (including objects in archives and packed objects) and create temporary buffer or a file which is subsequently analysed by the anti-virus system.

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 Anti-virus scans incoming messages in real-time mode. It checks the following elements of e-mail messages:

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

Licensing

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

License Key File

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

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

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

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

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

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

Getting License Key File

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

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

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

To acquire a license key file by e-mail

1. Launch an Internet browser and go to the site, which is specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number 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 Anti-virus.

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

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

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

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

Updating License

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

To update the license key file

1. To update the license key file, replace an old license key file with the new file in the plug-in installation folder (usually, % DrWeb for ISA Server%).
2. Dr.Web Anti-virus automatically switches to the new license.

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

Principles of Operation of Dr.Web Anti-virus

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

The anti-virus and anti-spam solution Dr.Web Anti-virus integrates Dr.Web technologies into the Internet traffic processing, carried out by Microsoft ISA Server and Microsoft Forefront TMG firewall services.

The product has a convenient web interface to facilitate management of scanning settings and virus events monitoring via Internet browser. For more information about the settings, see Dr.Web for ISA Web Console.

Dr.Web Anti-virus Filters

Dr.Web Anti-virus intercepts the data from network connections to check for viruses by special filters, which are integrated into Microsoft Firewall Service (for Microsoft ISA Server) and Microsoft Forefront TMG Firewall (for Microsoft Forefront TMG).

The filters are ISAPI-based dynamic libraries, launched on the Microsoft Firewall Service or Microsoft Forefront TMG Firewall start and remaining active until the service stops. On the start, Microsoft Firewall Service and Microsoft Forefront TMG Firewall check the list of registered filters and assign different network events to them for processing. The filters can access to the data of the "client-server" session of the firewall service. If a client request or server response creates an event a filter is registered for, this filter intercepts and analyses the traffic data.

Dr.Web Anti-virus contains 4 application filters and one web filter, which analyse the traffic for viruses. Each filter is subscribed to the main service Dr.Web CMS and connects to it when loading to the wspsrv.exe process memory, then becomes visible in the CMS Administrative Console.

Application filters

Dr.Web Anti-virus contains the application filters (see Figure 1):

Filter	Path to the filter library
Dr.Web FTP Filter	%DrWeb for ISA Server%\FTPFilter.dll
Dr.Web HTTP Filter	%DrWeb for ISA Server%\HTTPFilter.dll
Dr.Web SMTP Filter	%DrWeb for ISA Server%\SMTPFilter.dll
Dr.Web POP3 Filter	%DrWeb for ISA Server%\POP3Filter.dll

These filters process the protocols' packets. They analyze the data and block sending them to the input and output completion buffer in case the security threats are detected. All filters are available for configuration 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.

You can disable any filter, if necessary. If a filter is disabled, a  sign is shown next to the filter name (see Figure 1a).

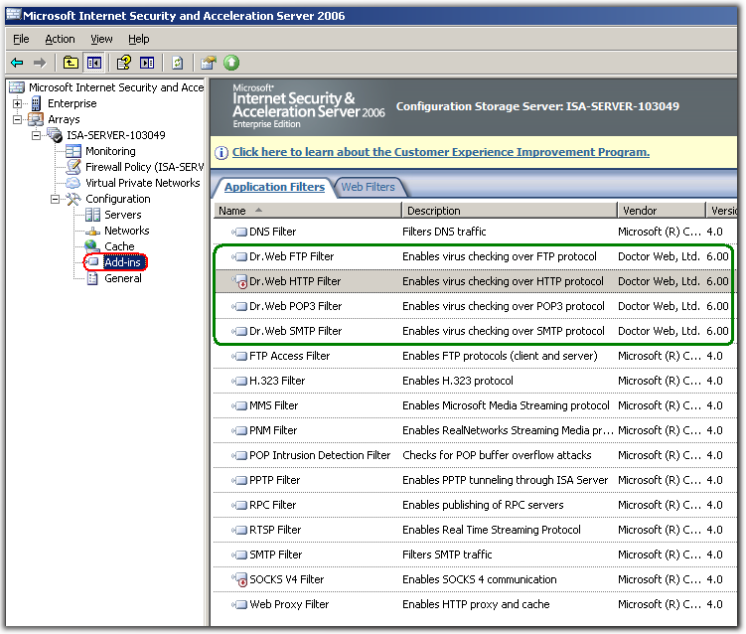

Figure 1a. Dr.Web application filters in Microsoft ISA Server console

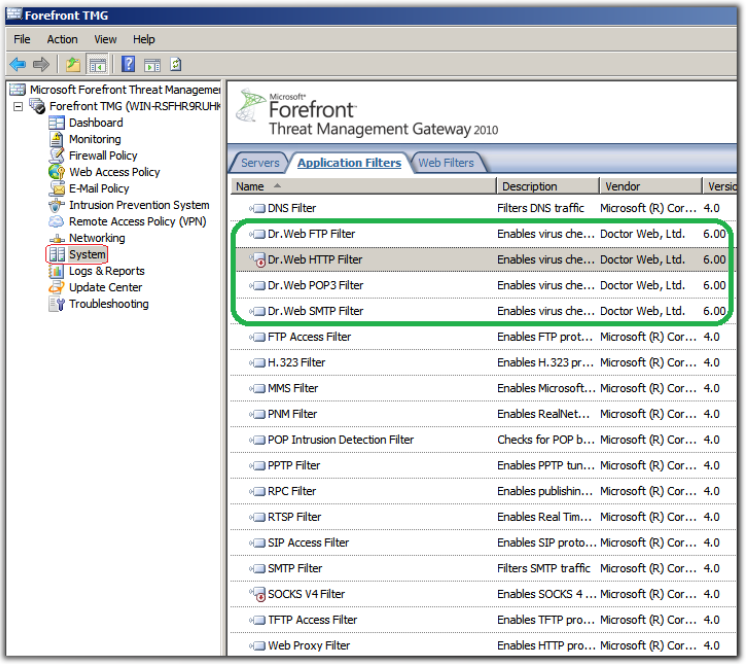

Figure 1b. Dr.Web application filters in Microsoft Forefront TMG console

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).

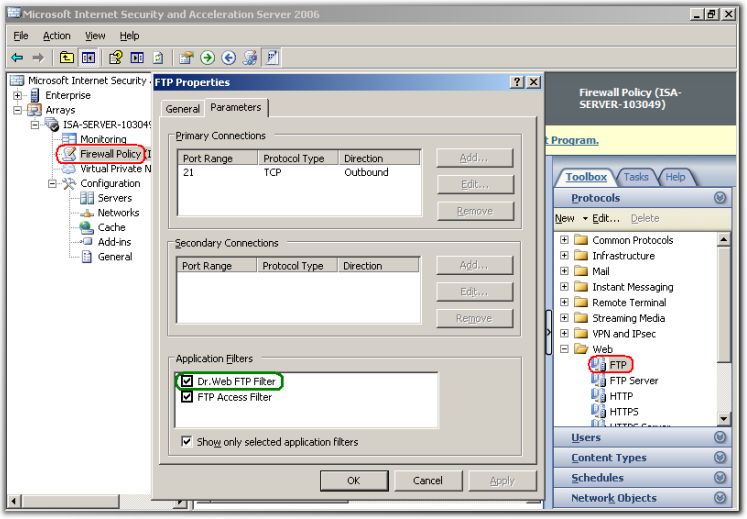

Figure 2. Dr.Web FTP Filter on the FTP protocol properties tab

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).

After registration, Dr.Web HTTP Filter is displayed on the HTTP protocol properties tab in Microsoft ISA Server and Microsoft Forefront TMG console (see Figure 3). On completing the application installation, Dr.Web HTTP Filter is disabled by default, because it cannot be activated together with Dr.Web HTTP Web Filter (see Figure 1).

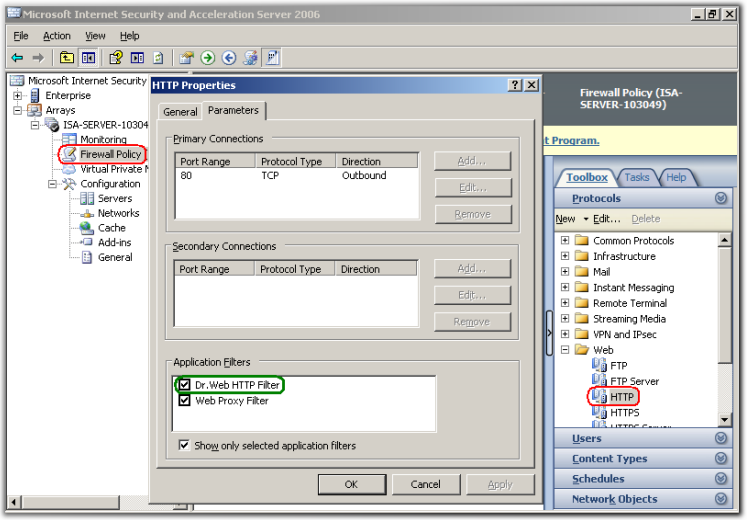

Figure 3. Dr.Web HTTP Filter on the HTTP protocol properties tab

Web Filter

Dr.Web Anti-virus contains Dr.Web HTTP Web Filter (HTTPWebFilter.dll library located in the %Microsoft ISA Server% \DrWeb\ or %Microsoft Forefront Threat Management Gateway% \DrWeb\ folder depending on the firewall used) – a filter, which is a runtime extension of Web Proxy Filter, a built-in filter of Microsoft ISA Server and Microsoft Forefront TMG, and responds to its events. Dr.Web HTTP Web Filter is displayed in Microsoft ISA Server and Microsoft Forefront TMG console tree on the Web Filters tab in the Configuration -> Add-ins branch (see Figure 4a, Figure 4b):

- 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.

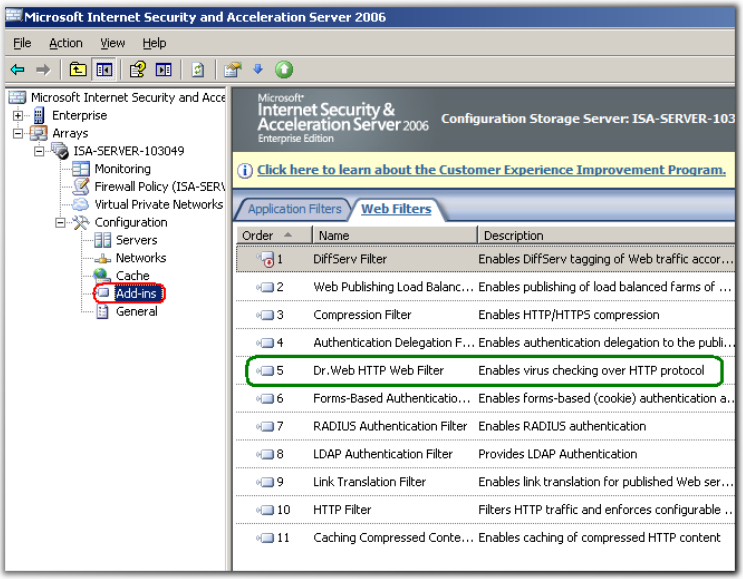

Figure 4a. Dr.Web HTTP Web Filter in the Microsoft ISA Server console

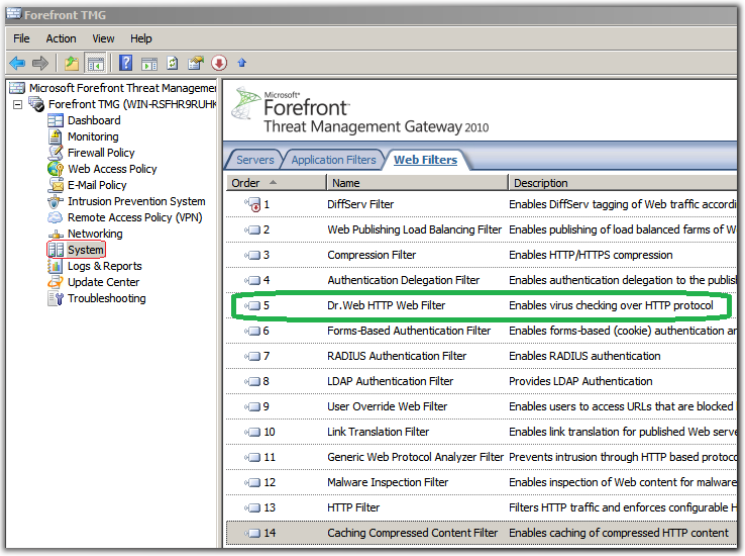

Figure 4b. Dr.Web HTTP Web Filter in the Microsoft Forefront TMG console

Anti-virus Check Using Filters

This section describes the anti-virus check using the following filters of Dr.Web Anti-virus:

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

Dr.Web HTTP Web Filter

The operation of Dr.Web HTTP Web Filter is configured by a set of parameters in CMS Administrative Console, available in the Application Settings group for HTTPWebFilter_1.0.

The anti-virus check starts within the "client-server" session 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 if the values of the PassCached parameter is false (the default value).

Once the value of the PassCached parameter is changed to true, the application stops scanning the objects received from the firewall cache. Therefore, it is recommended to clear cache before switching to such operation mode. To do this, disable the use of cache in the firewall management console, then delete the cache file (located in the Urlcache folder on each disk the caching is configured for). After deleting the file re-enable the use of cache.

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 the resource as a buffer of 1 MB by default or as a temporary file (if the resource size is large) for further anti-virus scanning.

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

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

Once the anti-virus scanning completes, the resource changes its state to the known one for the verification period specified by the ResetCachePeriodInSec parameter and equal to 30 minutes from the moment scanning is finished:

If the resource is clean, it becomes fully accessible for all the users protected by the firewall with any address or agent during the verification period.

- If the resource is clean, it becomes fully accessible for all the users protected by the firewall with any address or agent during the verification period.
- If the resource is infected, Dr.Web HTTP Web Filter returns the string "403 Forbidden. Infected by virus".
- If other users start their own cycles of the resource check before its state becomes known, its state is changed or prolonged for the verification period after the requested scanning is completed. When the verification period expires after the last scanning, the resource returns to the Unverified state, and a new request starts a new resource verification cycle.
- In case the resource is not requested anymore, all information about it and the users is deleted from the system after a time period specified by the CleanupCachePeriodInResetPeriod parameter (in number of verification periods).

Dr.Web HTTP Filter

Unlike Dr.Web HTTP Web Filter, which reacts on Web Proxy Filter events and performs anti-virus scanning only for external server responses, Dr.Web HTTP Filter is a filter of active data-dumping via two-way parser and it performs scanning before each transceiving operation is completed.

Dr.Web HTTP Filter and Dr.Web HTTP Web Filter should not be activated simultaneously, because they double the data check, that may lead to unstable system operation in case a threat is detected.

Dr.Web FTP Filter

During the installation of Dr.Web Anti-virus, 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 create the filter object to process 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. The client operates in one of the following modes: active or passive.
   - After the request to switch to the active mode is intercepted, Dr.Web FTP Filter installs a filter on the data connection of the FTP filter active mode.
   - In passive mode, Dr.Web FTP Filter is installed on the data connection of the passive mode.
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. Dr.Web FTP Filter gets the name of the requested file from the RETR file download request and sends the SIZE request to the server to obtain the size of the file. After that, Dr.Web FTP Filter sends the RETR request, sent by the client previously. In case the size of the requested file does not exceed the specified limit (1 MB by default), a memory buffer is used to save the data received via the channel. If the limit is exceeded, a file is used for data saving.
4. The filter can operate in one of the following modes:
   - *Preliminary check mode*. During the preliminary check, all data is added portionwise to buffer. When all data is collected or after a specified timeout (5 seconds by default), Dr.Web FTP Filter check the received data for viruses. If the anti-virus check takes a considerable time, the FTP connection may be closed after a certain time period. To prevent this situation, Dr.Web FTP Filter transfers the data to the client by small portions (of 1 byte by default) with the specified periodicity (every 2 seconds by default). So, the connection remains open. In the preliminary check mode the system performance decreases, but there is no possibility for a malicious object to appear on the client's computer.
   - *Post-check mode*. In this mode, the file is partially transferred to the client (80% by default). Then the transfer is paused and Dr.Web FTP Filter check the file. If the file does not contain the 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. In this mode, the system performance increases because it contains only one virus check, but the virus can possibly enter 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.

Dr.Web SMTP Filter and Dr.Web POP3 Filter

The antivirus check of the SMTP and POP3 traffic has two stages:

1. 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 determined as spam, an action specified for the corresponding spam category in the Anti-spam section of Dr.Web for ISA Web Console by the administrator is applied to it.
2. The messages that passed the spam check (or were ignored according to the application settings), are then check for malware. Depending on the scanning results, the scanned objects (the body of the message or the attachments) are attributed to one of the categories (Cured, Not cured or Suspicious), and the corresponding actions specified by the administrator in the Scanning pane of Dr.Web for ISA Web Console are performed. Enabling the heuristic analysis in application settings allows to detect the objects containing 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.

Dr.Web Anti-virus Services

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

- Dr.Web Scanning Engine – contains the Dr.Web scanning engine.
- Dr.Web CMS – supports the distributed application components management system, controls and analyzes the modules functionality. This service supports the application components settings database, the incidents database and controls the statistics of components parameters.
- Dr.Web CMS Web Console – has a built-in server providing the use of administrative consoles via Internet browser.

- Dr.Web for MSP Scanning Service – prepares objects intercepted by application filters to the anti-virus scanning, processes the scanning results.
- Dr.Web for MSP Component Host – instantiates all additional application components requested during its operation.
- Dr.Web for MSP Requests Queue – supports the asynchronous requests queue of application tasks, which allow to postpone their run.
- Dr.Web SSM – controls the operation of the applications based on the CMS platform and restarts the main services.

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

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

Installation and Removal

Before installing or removing Dr.Web Anti-virus, 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 appendix Remove Dr.Web Anti-virus manually.

The Dr.Web Anti-virus software is distributed as a single installation file (drweb-600-isa-20042006-x86.exe or drweb-600-tmg-2010-x64.exe, depending of the firewall version) or a ZIP-archived folder containing 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, it is recommended to use the Add or Remove programs utility to install and uninstall the Dr.Web Anti-virus software.

Dr.Web Anti-virus is not compatible with other anti-virus software. Installing two anti-virus programs on one computer may lead to system crash and loss of important data. If you already have an earlier version of the product or other anti-virus software installed then it is necessary to uninstall it using the installation file or standard tools of the OS (see see Remove Dr.Web Anti-virus). Furthermore, Dr.Web Anti-virus is compatible with only those of other Dr.Web products for Windows servers that have the same version.

In case the server operates under load, it is recommended to stop the Microsoft Firewall service (or Microsoft Forefront TMG Firewall) manually. On completing the installation, it will restart automatically.

To enable logging during the installation/removal

You can configure logging the program installation or removal process for further examination and application control. To enable logging:

1. In Start -> Run console started as administrator open the directory where the installation file is located.
2. Run the program installation file using the command with the following parameters:
   - `drweb-600-isa-20042006-x86.exe /V"/lvx* <log_name.log>"` (if Microsoft ISA Server is used)
   - `drweb-600-tmg-2010-x64.exe /V"/lvx* <log_name.log>"` (if Microsoft Forefront TMG is used),

   where log_name.log is the name of the log file.

System Requirements

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

Hardware requirements

Specification	Requirement	
	In case Microsoft ISA Server is used	In case Microsoft Forefront TMG is used
CPU	733 MHz or higher frequency processor	1.86 GHz or higher frequency processor
RAM	1 GB or more	2 GB or more
Disk space	300 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 user requests intensity and the size of the downloaded files.	
Monitor	VGA-compatible monitor	

Operating system and software requirements

Specification	Requirement	
	In case Microsoft ISA Server is used	In case Microsoft Forefront TMG is used
Operating system	One of the following: • Microsoft® Windows Server® 2003 x86 with Service Pack 1 (SP1) • Microsoft® Windows Server® 2003 R2 x86	One of the following: • Microsoft® Windows Server® 2008 SP2 • Microsoft® Windows Server® 2008 R2
File system	NTFS	
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 Windows Installer 3.1 or higher Microsoft .NET Framework 3.5 Internet Explorer 7 or higher or Mozilla FireFox 3.5 or higher	

Install Dr.Web Anti-virus

Before installation it is strongly recommended

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

To install Dr.Web Anti-virus

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 application installation file
   - drweb-600-isa-20042006-x86.exe, if you are using Microsoft ISA Server.
   - drweb-600-tmg-2010-x64.exe, if Microsoft Forefront TMG is used.

   The window with a list of installation languages will open. Select Russian or English as the installation language. Click OK.
4. The InstallShield Wizard will open on the first window of the installation process. Click Next to continue.
5. 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.
6. Select the licensing type. You can use the key file obtained from Dr.Web Control Center or a local key file. Click Next.
7. If you have selected to use the local key file on the previous step, specify the path to it. Click Browse and select the necessary key file. Click Next.

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

8. On the Ready to install page, click Install to begin installation of Dr.Web Anti-virus on your computer.
9. If the service of the firewall Microsoft ISA Server/Microsoft Forefront TMG has not been stopped during step 1, the system attempts to stop it automatically for some. If these attempts fail, a window prompting to try again or stop the program installation and roll back all the system changes will open. To continue installation, stop the Microsoft ISA Server/Microsoft

Forefront TMG firewall service manually.

10. Further actions of the InstallShield Wizard do not require user interference. Once the installation is complete, click Finish.

During the installation you'll be prompted about Microsoft ISA Server/Microsoft Forefront TMG restart. After the installation completes, make sure that the Microsoft Firewall Service/Microsoft Forefront TMG Firewall service is started. If the service is not started automatically, you need to start it manually.

To reinstall Dr.Web Anti-virus

1. Stop the Microsoft ISA Server/Microsoft Forefront TMG firewall service.
2. Uninstall Dr.Web Anti-virus. The application configuration file cmsdb is not deleted by default on deleting the application. Therefore, all user settings are saved and may be used after the next installation of the product. However, if you install a newer version that contains new basic configuration parameters, you cannot use the saved configuration file "as is", because it can lead to failures in the operation of application. If you prefer tore-use the saved configuration parameters, please contact Doctor Web technical support to inquire about the Dr.Web CMS parameters compatibility in different versions of the application. Generally, if the newer version contains additional parameters, it is sufficient to add the new variables to the existing configuration base and specify their types and default values correctly.
3. Delete the cmsdb and cmstracedb files from the %ProgramFiles%\DrWeb for ISA Server folder manually.
4. Install Dr.Web Anti-virus, following the instructions given above.

Remove Dr.Web Anti-virus

To uninstall Dr.Web Anti-virus

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 application installation file
   - drweb-600-isa-20042006-x86.exe, if you are using Microsoft ISA Server.
   - drweb-600-tmg-2010-x64.exe, if Microsoft Forefront TMG is used.

   The InstallShield Wizard will open on the first window of the installation process. Click Next.

   

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

4. Select Remove and click Next.
5. In the opened window, click Remove.
6. Once removal is complete, click Close.

During the program removal you'll be prompted about Microsoft ISA Server/Microsoft Forefront TMG restart. After the removal completes, make sure that the Microsoft Firewall Service/Microsoft Forefront TMG Firewall service is started. If the service is not started automatically, you need to start it manually.

If you experience problems related to the firewall operation or errors have occurred during Dr.Web Anti-virus removal, you can uninstall the program manually.

Dr.Web for ISA Web Console

Operation of Dr.Web Anti-virus can be configured by means of the Dr.Web for ISA Web Console (see Figure 5).

To launch Dr.Web for ISA Web Console

For correct operation of Dr.Web for ISA Web Console use one of the following browsers:

- Internet Explorer 7 or higher
- Mozilla Firefox 3.5 or higher

For correct operation of Dr.Web for ISA Web Console in Internet Explorer you need to additionally allow the use of the AJAX technology by disabling the enhanced security configuration for administrators:

- In Windows Server 2003: open Control Panel -> Add or Remove Programs -> Add/Remove Windows Components, clear the Internet Explorer Enchanced Security Configuration check box, then click Next. Click Done.
- In Windows Server 2008: open Server manager and click Configure IE ESC, then select the corresponding check box in the Administrators section.

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

`https://`*<ISA Server address>*`:2080/isa`,

where *<ISA Server address>* is the IP-address of the ISA server/ Forefront TMG.

To access to the web console page, you need to enter the administrator login and password. Administrator accounts can be added, edited or deleted by means of Dr.Web CMS Web Console.

On the first launch of the web console use the login root and the password drweb of the default administrator account.

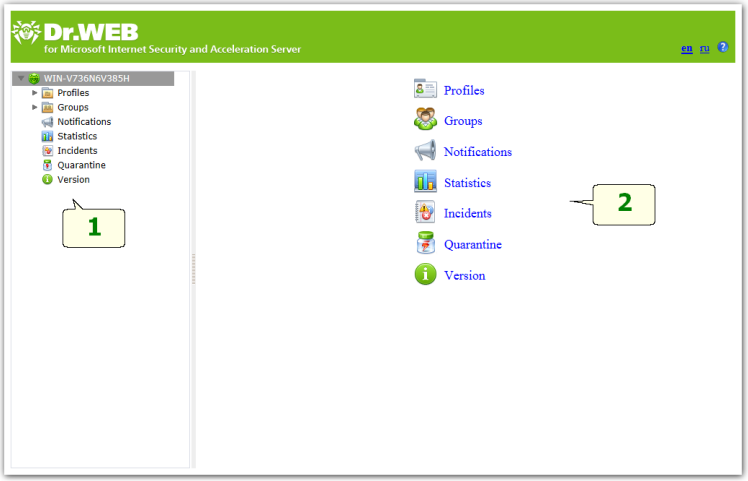

Figure 5. Dr.Web for ISA Web Console

Interface

The web console consists of two parts:

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

At the top of the details pane the Dr.Web for ISA Web Console language changing option is located. You can select English or Russian language.

To the right of the language option the option, which opens the help on the web console, is located.

Groups and Profiles

To simplify management of your local network protected by Microsoft ISA Server/Microsoft Forefront TMG, Dr.Web Anti-virus 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 the Web Console tree and are divided into the following subsections:

- Scanning – this section allows you to control the operation of your main virus-detection component.
- Anti-spam – this section allows you to adjust the operation of the Anti-Spam component (settings in this section are available only with the «Anti-Virus&Anti-Spam» version of Dr.Web Anti-virus, i.e. if you have an appropriate license key file (see License Key File).
- Office Control – this section allows you to restrict the user access to web resources.
- Filtering – this section allows to configure the 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).

Creating and Configuring Profiles

During installation of Dr.Web Anti-virus the Default profile, which cannot be renamed or deleted, is created automatically. This profile will remain active for all the traffic as long as you do not create a new

profile and assign it to a certain group of clients. When you create a new profile, it has current settings of the Default profile.

To manage the existing profiles and create the new ones the Profiles pane is used. To open it select Profiles in the Web Console tree (see Figure 6).

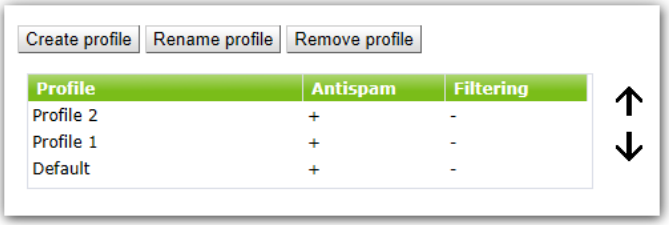

Figure 6. Profiles pane

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

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.

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

To change the name of a profile

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

To delete a profile

- Select it on the Profiles pane and click Remove profile

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

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

To change profile settings

- Click the name of the profile in the console tree and select the necessary settings section: Scanning, Anti-spam or Office Control.

Profile Priority

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

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

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

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. On the other part, increasing of the number of identified objects' types leads to decrease in server performance.

To adjust the settings of the scanning process

1. Click Scanning the Web Console tree. The Scanning pane will open (see Figure 7).

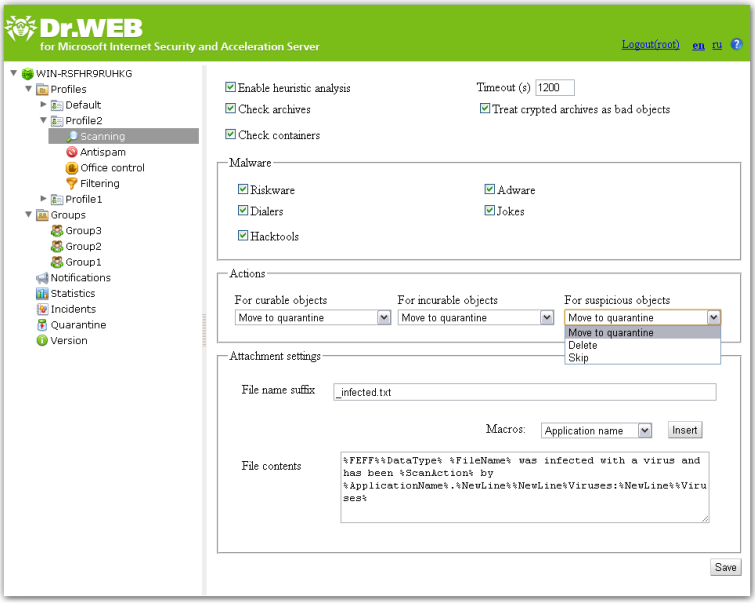

Figure 7. Scanning pane

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

Scanning pane.

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

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

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

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 curable, incurable and suspicious objects. You can choose from the following:
   - Move to quarantine – means that the object will be sent to the quarantine (see Quarantine).
   - Delete – means that the object will be deleted.
   - Skip – means that such objects will be passed on to the recipient(s) untouched (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 e-mail message after the assigned action is performed over it. In the Text field below, you can edit the text of the attached text file template, if necessary. You can add macros from the Macro list while editing the text.
6. When you finish configuring scanning process, click Save.

Anti-spam

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

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

Any editing of the key file makes it invalid! Do not save the file when closing the text editor.

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

To configure the settings of the Anti-spam component

1. Click Anti-spam in the Web Console tree. The Anti-spam settings pane will open (see Figure 8).

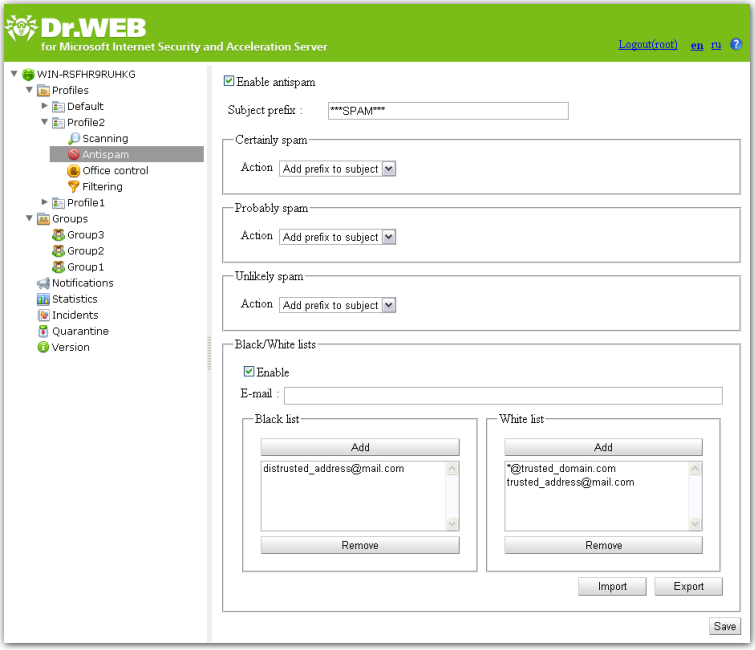

Figure 8. Anti-spam settings pane

2. To disable spam filtering, clear the Enable anti-spam check box. Once the check box is cleared, all parameters become unavailable for editing. Select the check box to enable spam filtering.
3. In the Subject prefix field, you can change the prefix, which will be added to the subjects of e-mail messages considered as spam. The default prefix is *** SPAM ***.

4. In the fields below, you can define the program actions for three categories of messages based on the probability level of their being spam (Certainly spam, Probably spam or Unlikely spam). To do this, select one of the following actions for each category:
   - Add prefix to subject – means that the prefix defined in the Subject prefix field will be added to the message subject.
   - Pass through – means that the message will be passed through to the recipient.
5. On the Black/White lists section, you can configure the use of the lists of trusted and distrusted addresses:
   - Select Enable to enable the use of the lists. You can add e-mail addresses you trust to the white list. In this case, messages from these addresses will not be checked for spam. If you add an address to the black list, all messages from it will be considered as Certainly spam.
   - To add an address to the list, enter it in the E-mail field and click Add on the section of the white or black list. The address will be added to the selected list.
   - To delete an address from the list, select it and click Remove on the section of the list this address is included in.
   - You can also use the Import and Export buttons to save the list into a special file with .lst extension or to load the lists from the file and to create or edit the lists manually using a text editor, for example While creating and/or editing the files of black and white lists manually, you need to add prefix to the e-mails: «+» to add the e-mail into the white list, «-» to add the e-mail into the black list, e.g. +trusted_address@mail.com and -distrusted_address@mail.com. The created text file must be saved with .lst extension in Unicode format.

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

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

Office Control

The Office Control component is used to restrict access to web resources and restrict a user to view undesirable web sites (e.g. pornography, violence, gambling, etc.) or allow access only to certain web sites, specified in the Office Control settings.

To configure Office Control

1. Select Office Control in the web console tree. A pane for editing parameters of the Office Control will open (see Figure 9).

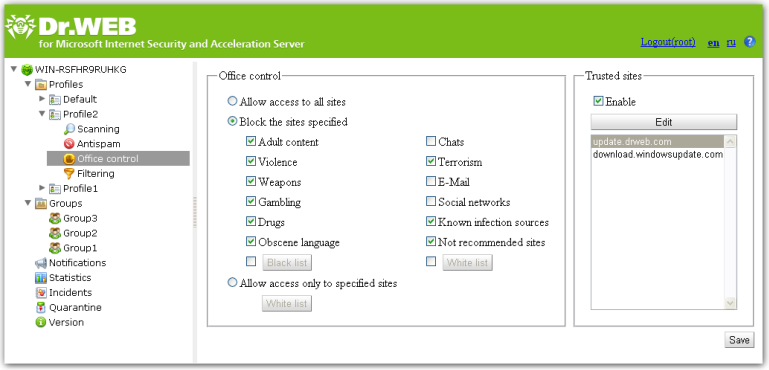

Figure 9. Configure Office Control pane

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.

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. You can enable an additional list of trusted sites. 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

To create a list of domain names

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.

Filtering

The traffic filtering is configured in the Filtering pane (see Figure 10). Filters are applied according to certain rules which can be added by the administrator. These rules determine the conditions for the filtering by the properties of messages and their attachments.

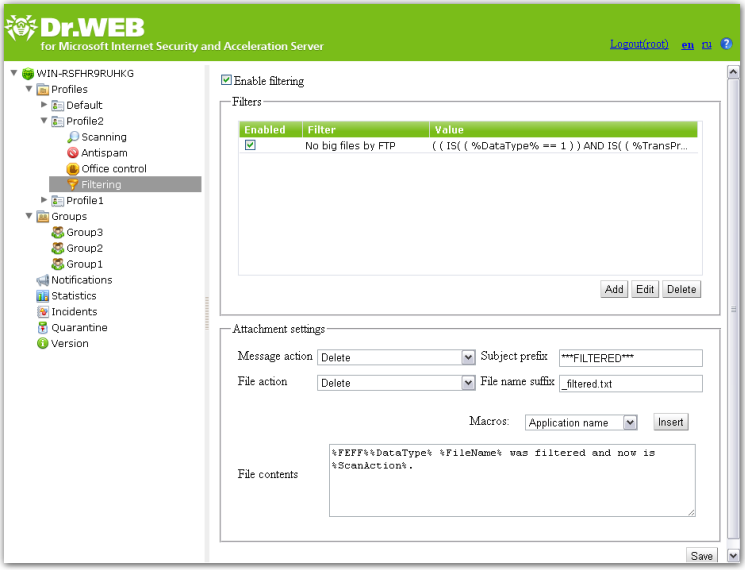

Figure 10. Filtering pane

To configure messages filtering

1. Select Enable filtering at the top of the Filtering pane. This makes the parameters in the section available for editing.
2. Enable one or more filters from the list by selecting the corresponding check boxes. If the list of filters is empty, you can create them.
3. Select the actions for the e-mail 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 pass through the message and add to its subject a prefix specified in the Subject prefix

   For attachments, the following actions are available:

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

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

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

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

To create a filtering rule

1. Click Add under the filters list. A Filter rule window will open (see Figure 11). You can enter the name of the rule and specify its conditions in this window.

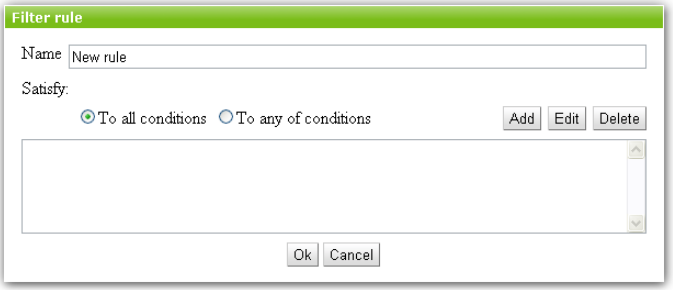

Figure 11. Configure filtering rule

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

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

Condition type	Compliance type	Value
	Matches Not matches	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.
Protocol	Equal Not equal	HTTP FTP POP3 SMTP
Number of recipients	Equal Not equal Contains Not contains Matches Not matches	Specified manually
File name	Equal Not equal Contains Not contains Matches Not matches	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.
File size	Equal Not equal	Specified manually (in bytes)

Condition type	Compliance type	Value
	Greater Not greater Less Not less	
Message subject	Equal Not equal Contains Not contains Matches Not matches	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	Equal Not equal	True False

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

Filtering rule example

To filter files whose size exceeds 20 MB, transferred over the FTP protocol, the rule (see Figure 12) containing the following conditions can be used:

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

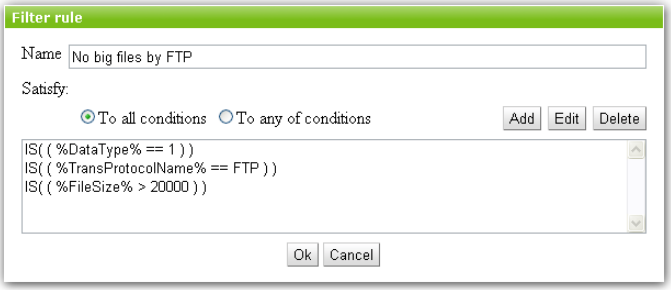

Figure 12. Example of the filtering rule

To edit or delete an existing filtering rule

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

Click Save when you are done configuring the filtering rules.

Managing Groups

By default, Dr.Web Anti-virus 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.

Creating a New Group

To manage the existing groups and create the new ones the Groups pane is used. To open it, click Groups in the Web Console tree (see Figure 13).

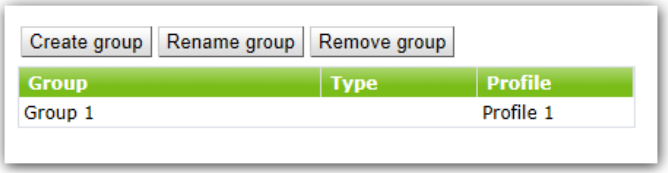

Figure 13. Groups pane

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 context menu.

A new group named Group1 will be created and it will appear under Groups in the console tree. If this name already exists, it will be named Group2 and so on. The Default profile is set for each new group.

To change the name of a group

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

To delete a group

- Select it on the Groups pane and click Remove group

Alternatively, to rename or delete a group, you can right-click it in the console tree and then click the corresponding item on the context menu.

To configure group settings

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

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

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

Configuring and Forming Groups

In the information pane that opens by clicking the group name in the web console tree (see Figure 14), you can set up the parameters of the selected group, including the manner of forming this group: by listing the e-mail addresses, the IP addresses or selecting the AD groups. Select the group type in the drop-down list Type.

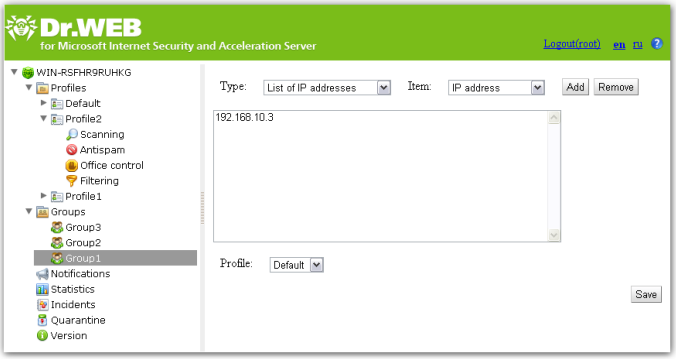

Figure 14. Group settings

To create a list of e-mail addresses

1. In the the drop-down list Type, select List of e-mail addresses.
2. To add an e-mail address to the list, click Add. In the new window, enter the e-mail address and click Ok.

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

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

To create a list of IP addresses

1. In the the drop-down list Type, select List of IP addresses.
2. In the Element 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.

To create a list of AD groups

1. In the the drop-down list Type, select List of AD groups.
2. To add a new group to the list, click Add. In the new window, select the group to add and click Ok.
3. To delete a group from the list, select it and click Remove, then confirm the deletion of the selected group.

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

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

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

Notifications

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

To configure notifications

1. Click Notifications in the Web Console tree. A pane for editing parameters of notifications will open (see Figure 15).

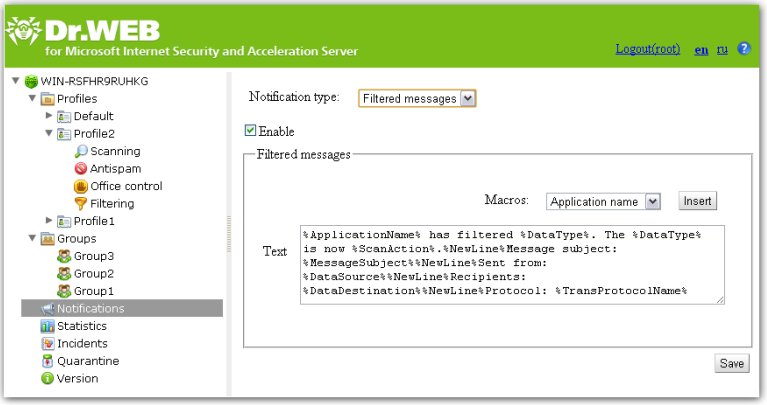

Figure 15. Configure notifications pane

2. In the Notification type list, select the type of event to configure notifications for:
   - Filtered messages – to configure notifications about messages filtering.
   - Filtered files – to configure notifications about attachments.
   - Infected – to configure notifications about infected objects.

- Spam – to configure notifications about spam.
- Office control – to configure notifications about web ressources filtering using Office Control.
- Update – to configure notifications with the las update information.
- Expired bases – to configure notifications about virus databases expiration.

3. By selecting/clearing the Enable option, you can enable/ disable sending notifications of selected type.
4. In the setting group below, you can modify the text template for the notifications of selected type by entering it in the Text field. While editing the text, you can use macros.
5. When you are done, click Save.

View Statistics

The Statistics section allows to review the total and average amounts of the objects processed by Dr.Web Anti-virus during a specified time period (see Figure 16).

To configure the statistics

1. In the Statistics period drop-down list, select the time interval to view the statistics information about. You can choose one of the following intervals:
   - For all time – to view the total statistics since Dr.Web Anti-virus started its operation
   - For last day – to view the statistics for the last 24 hours of Dr.Web Anti-virus operation
   - For last hourc – to view the statistics for the last hour of Dr.Web Anti-virus operation
   - For last minute – to view the statistics for the last minute of Dr.Web Anti-virus 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 Anti-virus to the detected malicious objects.

- Infection type. This section contains information on different types of threats, detected by Dr.Web Anti-virus 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.

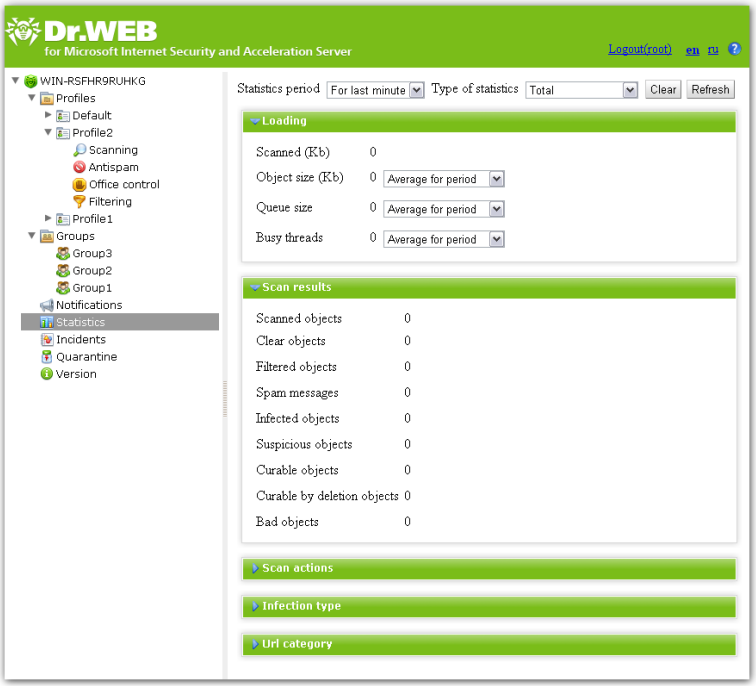

Figure 16. Statistics

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

View Incidents

The Incidents section allows to review all incidents related to the operation of Dr.Web Anti-virus (see Figure 17).

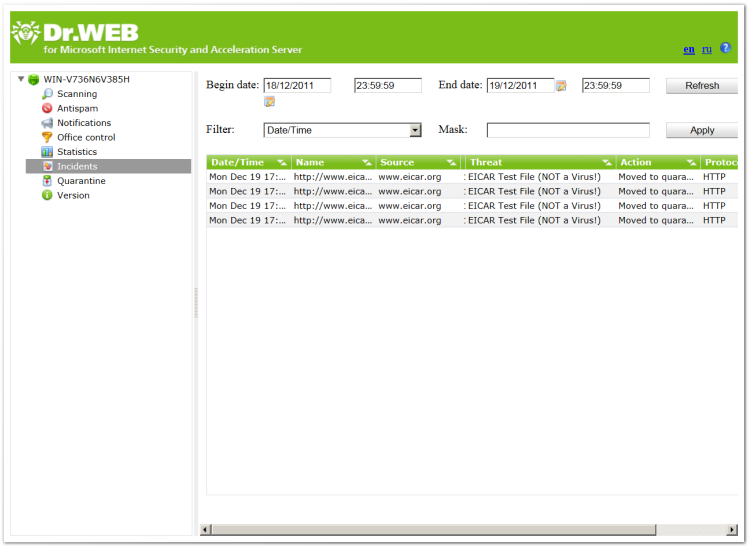

Figure 17. Incidents

To view the incidents information

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

- Date and time of the incident
- Web resource name
- Source and destination name
- Name of the threat
- Performed action

To manage the incidents list

1. You can specify the time period to review the incidents. Enter the start and the end date of the interval.
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.
3. You can save the incidents list in a text file. To do this, click Export.
4. To sort the incidents list according to different criteria, click the title of the corresponding column.
5. To refresh the list, click Refresh.

Quarantine

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

In the Quarantine section of the web console, the current Quarantine information is displayed. You can also use Quarantine Manager to review and edit the list of objects in Quarantine.

Manage Quarantine via Dr.Web for ISA Web Console

To view the list of objects moved to Quarantine, click Quarantine in the web console tree. The Quarantine pane (see Figure 18) will open.

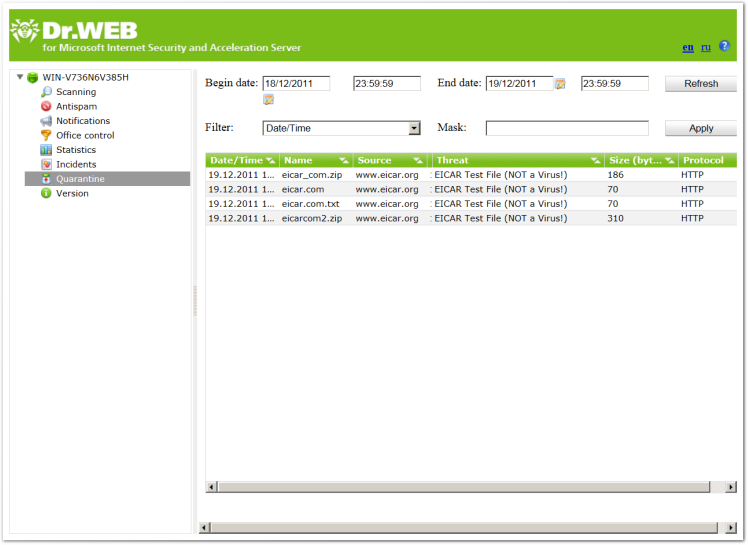

Figure 18. List of objects in Quarantine

To view the information about the objects in Quarantine

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

- Date and time
- File name
- Source and destination
- Threat name
- File size

The following options are available to configure the Quarantine:

1. 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.
2. You can use a number of filters to filter the list according to certain criteria to customize the way information about the objects in Quarantine is displayed. Select the filter type in the Filter list, enter the desired value in the Mask field, then click

Apply.

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

To process objects in Quarantine

1. To delete an object from the list, right-click it and select Delete in the context menu. To delete all object, press Ctrl+A, then select Delete.
2. To restore an object, right-click it and select Restore in the context menu. Then specify the path to the folder you would like to restore the object to.

Quarantine Manager

To start Quarantine Manager (see Figure 19) open Start -> All Programs -> Dr.Web for ISA Server -> Quarantine.

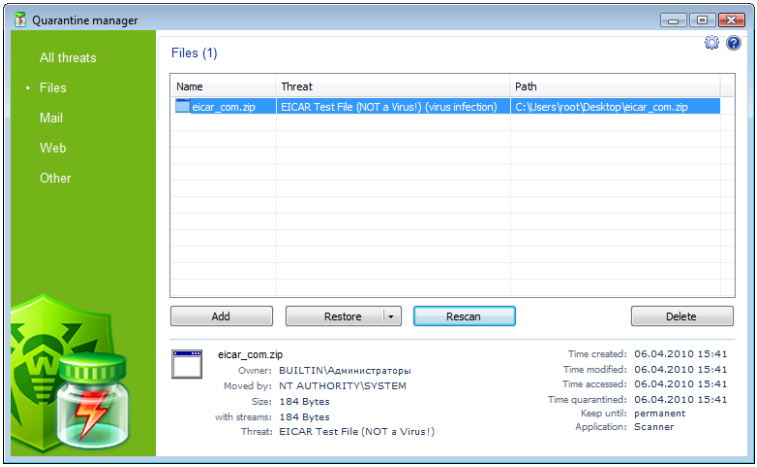

Figure 19. Quarantine window.

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

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

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

To configure columns

1. To configure the display parameters of the table of Quarantine, right-click the table header. Select Customize columns in the context menu.
2. In the opened window, select the items to display in the table. Clear the check boxes for the items you want to hide. Click Check all/Uncheck all to select/clear all items.
3. To change the columns order in the table, select the corresponding column in the list and click one of the following buttons:
   - Move up – to move the column up in the table (to the head of the settings list and to the left in the objects table).
   - Move down – to move the column down in the table (to the foot of the settings list and to the right in the objects table).
4. To save changes, click OK. To close window without saving, click Cancel.

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

In the Quarantine window users can see only those files that are available by access rights.

To view hidden objects, run the `dwqrui.exe` Quarantine file from the installation folder under an administrative account.

Manage Quarantine

To process the objects in Quarantine

Use the following buttons to manage the Quarantine:

- Add – to add the file to the Quarantine. Select the necessary file in the file system browser.
- Restore – to remove the file from the Quarantine and restore it in its original location, i.e. restore the file to the folder where it had resided before it was moved to the Quarantine. The path to the folder to restore the file is specified in the Path column on Figure 19. If the path is not specified, the user will be prompted to select the folder to restore the file to.

  

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

  The drop-down menu item Restore to allows to restore the file to the folder specified by the user.
- Rescan – to scan the file again. If a file is defined as clean after that, Quarantine will offer to restore the file.
- Remove – to delete the file from the Quarantine and from the system.

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

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

Configure Quarantine Properties

To configure Quarantine parameters

1. Click the  button in the Quarantine window.
2. The Quarantine properties window will open. In this window you can change the following parameters:
   - The Set quarantine size section allows to configure the amount of disk space for Quarantine folder. Move the slider to change the maximum limit for Quarantine size, which is calculated as percentage of total disk space (for several logical drives, this size is calculated for every drive that includes the Quarantine folder). The 100% value means an unlimited Quarantine folder size.
   - In the View section, select the Show backup files option to display backup copies of Quarantine files in the object's table.
3. To save changes, click OK. To close window without saving, click Cancel.

Updating Virus Databases

You can review the information about the application version, license, virus databases and also the date, time and result of the last update on the Version pane in the web console tree.

An updating task (Dr.Web update for ISA plug-in) is created in the Windows Task Scheduler (the C:\Windows\Tasks folder) during installation of Dr.Web Anti-virus. The task runs the updating module DrWebUpW.exe, which downloads the virus databases and components of the program.

The task can be adjusted by changing its properties (double-click the task in the list). The operation of the updating module can be adjusted by specifying certain command-line parameters (see Appendix A) in the Run field of the task properties.

To configure update without using Internet connection

1. Create a folder on your computer's local drive (e.g. C:\MyDocs\DrWebUpdate).
2. Put the components that need to be updated into this folder. You can find the list of components that can be updated in the file drweb32.lst located in the following folder:
   - %AllUsersProfile%\Application Data\Doctor Web\Bases\ if Microsoft ISA Server is used
   - %ProgramData%\Doctor Web\Bases\ if you are using Microsoft Forefront TMG
3. Add the following command-line parameter to the Run field of Dr.Web update for ISA plug-in: /URL:*<path to created folder>* (for example, /URL:"C:\MyDocs\DrWebUpdate").

CMS Administrative Console

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

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

To start CMS Administrative Console

To launch CMS Administrative Console (see Figure 20), open the following page in a browser:

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

where *<ISA Server address>* is the IP address of the ISA server/ Forefront TMG.

To access to the CMS Administrative Console page, you need to enter the administrator login and password. Administrator accounts can be added, edited or deleted by means of Dr.Web CMS Web Console.

On the first launch of CMS Administrative Console use the login `root` and the password `drweb` of the default administrator account.

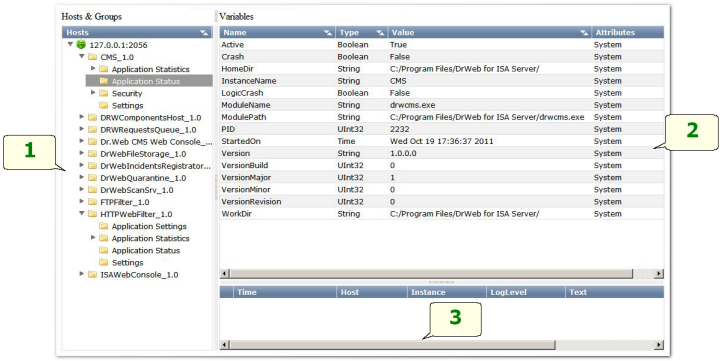

Figure 20. CMS Administrative Console

Interface

CMS Administrative Console consists of three parts:

1. Hosts and groups tree.

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

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

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

   - Add host (adds a connection to a new host to the tree)
   - Delete host
   - Enable tracing mode (enables tracing in the real-time mode)
   - Load events (downloads events for the past periods)
   - Edit event filter (editing real-time trace filter)

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. Messages tracing window.

   When real-time tracing is enabled, the application messages are displayed in the tracing window. You can set up a filter for the messages. Every message contains the following information:

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

   To empty the messages list, right-click the list and select the corresponding option in the context menu.

Changing Administrator Password

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

To change the password of the administrator account

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

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.

Organizing Clusters

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

To create cluster

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

1. Create the group /CMS_1.0/Security/Users/host. This group specifies the user account used by the main host to transfer the variables with the Shared attribute to a local server.
2. In the host group, a variable Password of the Password type will be created automatically to connect to the created account. The default password is drweb. For security reasons, it is strongly recommended to change it.

On the main host, do the following:

1. Create a group of any name at /CMS_1.0/Shared/. This group will be the sub-host.
2. In the host group, a variable Address of the String type is created automatically. By default, it has an empty value. This variable should contain the IP address of the sub-host MS connection in the following format: <*IP address*>:<*Port*>, e.g., 192.168.1.1:2056.
3. In the host group, a variable Password of the Password type is created automatically to connect to the host account on the sub-host. The default password is drweb. For security reasons, it is strongly recommended to change it. If the password is the same for all the hosts, you can create the Password variable in the Shared group. It will be used by default for all connections.
4. The variables configuring the connection to the sub-host cannot have the Shared attribute, therefore, the settings cannot be transferred to the sub-hosts. On the attempt to change the attributes of the connections settings, an access denied message will be received.

In the Shared folder, the variable Enabled of the Boolean type is created automatically (see Figure 21). 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.

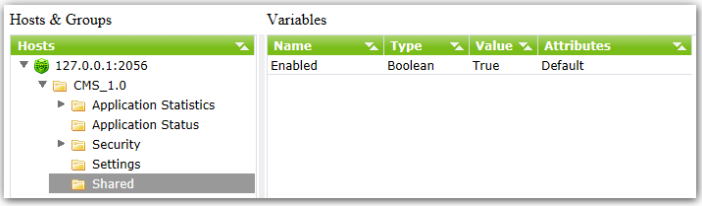

Figure 21. The Enabled variable created in the Shared folder

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.

If the address (the Address variable value) is changed, the active connection is switched to a new address. Changing the password does not lead to the connection switching. To switch the connection with a new password, you need to disable and re-enable the connection using the Enabled variable.

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

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

Logging

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

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

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

Event Log

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

- Plug-in starts and stops
- License key file parameters including validity, licensed period
- Parameters of the plug-in components including scanner, core, virus databases (information is registered when the plug-in starts or components are updated)
- License invalidity notifications if the license key file is missing, some of the plug-in components are not licensed, license is blocked or license key file is corrupted (information is registered when the plug-in checks the license)
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)
- Information on the malicious objects and spam detection (see the Notifications section)

To view Event Log

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

Installation Program Text Log

The installation program of Dr.Web Anti-virus also keeps a log of the installation process so that it could be viewed later for bug-tracking purposes. The log file drweb-isa-setup.log or drweb-tmg-setup.log (depending on the firewall version) is created in the C:\Windows\Temp folder, or can be found by environment variable %temp%, i.e. by executing the %temp% command in Start -> Run console.

CMS Log

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

Value	Description
Debug	Debug records

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

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

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 CMS Administrative 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 CMS Administrative 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.

Trobleshooting

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

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

Check Installation

Dr.Web Anti-virus must be installed to the following folders:

1. In case Microsoft ISA Server is used:
   - %ProgramFiles%\DrWeb for ISA Server
   - %Microsoft ISA Server%\DrWeb
   - %ProgramFiles%\Common Files\Doctor Web
   - %Documents and Settings%\All Users\Application Data\Doctor Web
   - Hidden folder %DrWeb Quarantine%
2. In case Microsoft Forefront TMG is used:
   - %ProgramFiles(x86)%\DrWeb for ISA Server
   - %ProgramFiles(x86)%\Common Files\Doctor Web\Scanning Engine
   - %ProgramFiles%\DrWeb for ISA Server
   - %Microsoft Forefront Threat Management Gateway% \DrWeb
   - Hidden folders %ProgramData%\Doctor Web and %DrWeb Quarantine%

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

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

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

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

Check Updater Functionality

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

To make sure that an update was successful:

1. Depending on the version of the operating system, run the Tasks command to open the C:\WINDOWS\Tasks folder or open the Task Scheduler.
2. Check that a task for Dr.Web Anti-virus has been created and it is working correctly (the return code in the Last Result field must be 0x0).
3. Open the updater log file %AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log (if Microsoft ISA Server is used) or %ProgramData%\Doctor Web\Logs\drwebupw.log (if you are using Microsoft Forefront TMG) and make sure that there are no errors in it.

Virus Detection Test

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

To create the EICAR test file:

- Open the Notepad text editor and copy the following string to it:
  `X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*`

To check the virus detection capabilities of Dr.Web Anti-virus for SMTP and POP3 protocols, save the file with a .com extension (you can use any name, e.g. eicar.com), attach it to an e-mail message and send it to any test e-mail address. The received message should contain an attached text file with the _infected.txt suffix and the following contents:

> File eicar.com was infected with a virus and has been moved to quarantine by Dr.Web for ISA Server.
>
> Viruses: EICAR Test File (NOT a Virus!).

To check the virus detection capabilities of Dr.Web Anti-virus for HTTP protocol, download the EICAR test file via this protocol (e.g., from the page at http://www.eicar.org/85-0-Download.html).

The file download should be blocked. The following message should be displayed in the browser window:

> Forbidden
>
> URL is blocked by anti-virus
>
> Reason: Infected by virus

In both cases the application log should contain the Warning event with the following description (if the Move to quarantine action is selected in the scanning settings):

> Infection detected. Dr. Web for ISA Server has detected that File is infected with a virus and it is incurable. The File is now moved to quarantine.

The Incidents pane of the Dr.Web for ISA Web Console should contain the corresponding notifications (see Figure 22).

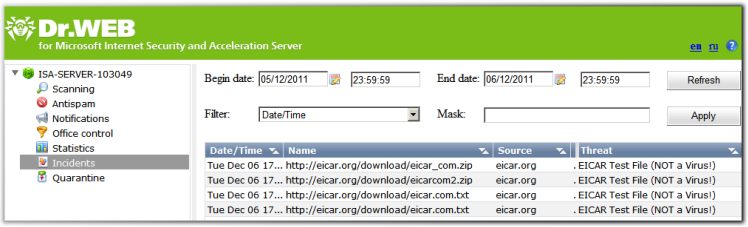

Figure 22. Notifications about EICAR files download in the Incidents pane.

If moving malicious objects to Quarantine is enabled, the Quarantine pane should contain the records on the added objects (see Figure 23).

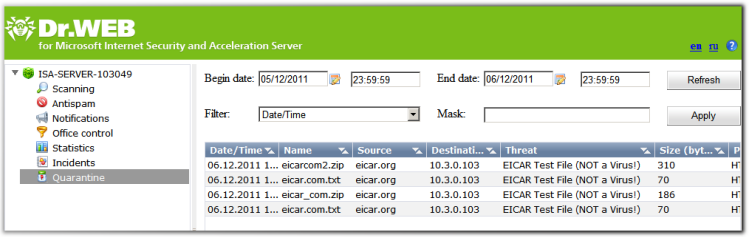

Figure 23. The list of downloaded EICAR files in the Quarantine pane.

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

Spam Detection Test

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

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

To create a test spam message:

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

  ```
  Start enjoying the benefits of Generic Medic1ne. Order quickly and easily, and save a ton of money. Try them out, they're 100% m0ney back guarantee.
  ```

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

Appendices

Appendix A. Updater's Command-Line Parameters

Below is a list of command-line parameters that can be added to the Run entry field of the updating task (C:\Windows\Tasks\ Dr.Web update for ISA plug-in) in order to adjust the operation of the updating module.

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

Parameter	Description
/PURL:<*proxy address*>	Address of the proxy server.
/URL:<*URL of the updating server*>	Only UNC names are accepted.
/QU	Compulsory close the Automatic Updating Utility after the updating is finished, regardless whether it was successful or not. The success of the updating can be checked via the drwebupw.exe return code, e.g. from the BAT file by the errorlevel variable value: • 0 = successful • other values = unsuccessful
/REG	Launch the updater for registration and to receive the license key file.
/UPD	Regular updating; used together with the /REG parameter to run the updating session itself during the registration.
/RP<*file_name*> or /RP+<*file_name*>	Log to a file, the name of which is specified in the parameter. If no name is specified log to a file with the default name. If the + character is present the file is appended; if there is no + character a new file is created.
/NR	Do not create a log file.
/SO	Enable sounds (only when errors occur).
/ST	Run the updater in invisible mode (*stealth mode*).
/UA	Download all files specified in the updating list regardless the used OS and the installed components. This mode is designed to receive the full local copy of the Dr.Web server updating area; this mode cannot be used for updating the anti-virus installed on a computer.
/UVB	Update the virus databases and drweb32.dll (the anti-virus engine) only (disables /UA, if it is set).

Parameter	Description
/UPM:*<proxy mode>*	Mode of using a proxy server; it can have the following values: • direct – do not use proxy server • ieproxy – use system settings • userproxy – use settings specified by the user (the /PURL, /PUSER and /PPASS parameters)
/URM:*<mode>*	Restart after the updating is finished. It can have the following values: • prompt – prompt whether a reboot is needed after the updating session is finished • noprompt – if necessary reboot without prompting • force – always reboot (regardless whether it is required after the updating or not) • disable – do not reboot

Appendix B. CMS Platform

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

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

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

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

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

Data type	Comment
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

Application Control

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

Application Status group

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

Variable (its type is indicated in parentheses)	Comment
Active (Boolean)	Indicates the application activity. The true value means that the application is active.
Crash (Boolean)	Indicates the correctness of the application stop. The true value means that the application stopped incorrectly.
HomeDir (String)	Application directory in the file system
InstanceName (String)	Name the application instantiated for
LogicCrash (Boolean)	Application logics state. The true value means that the application operates incorrectly.
ModuleName (String)	Application executable file name. If the subscribed application is a *.dll library, the value contains the name of the process it was instantiated by.
ModulePath (String)	Path to the application executable file in the file system
PID (UInt32)	Application process number in the operating system
StartedOn (Time)	Last application start time
StoppedOn (Time)	Last application stop time
Version (String)	Application version
VersionBuild (UInt32)	Application build number
VersionMajor (UInt32)	Application major version
VersionMinor (UInt32)	Application minor version
VersionRevision (UInt32)	Application revision number
WorkDir (String)	Application working directory in the file system

Settings group

This group contains the general settings of the registered application.

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.

Administration

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

Changing the variables values

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

Reset statistics

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

Restrictions

Using variable has the following restrictions:

- The variables with Hidden attribute exist in the database, but are not available for review and editing. They are created by the managing service for internal use.
- The variables with System attribute are created by the managing service to display the service information for administrator. Such variable cannot be modified or deleted.
- The variables with Statistics attribute are created by the application. These variables cannot be deleted.
- The variables with Readonly attribute are created by the application to inform the administrator. These variables cannot be modified.
- The variables with Default attribute are ordinary variables, and allow any action to be applied.
- The variables with Shared attribute are the distributed variables. Their values are modified synchronously within the distribution system.
- The variables, which cannot be modified, cannot be deleted as well. However, the groups containing such variables can be deleted with all their variables, if the application related to this group, is not launched.

Security

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

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

Appendix C. Dr.Web SSM Service

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

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

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

Variable (its type is indicated in parentheses)	Comment
Enabled (Boolean)	Signifies whether the SSM control is enabled or not
Run (Boolean)	Allows to start/stop the application
KeepAlive (Int32)	Signifies the application operation maintenance type: • 0 – the application is disabled • 1 – The application is active • 2 – forced maintenance, the application is enabled even if it stopped correctly

Variable (its type is indicated in parentheses)	Comment
StartType (Int32)	Signifies the application start method: • 0 – as a Windows service • 1 – as a CService application • 2 – start using a script
StartScript (String)	Contains the script to start the application
StopScript (String)	Contains the script to stop the application
Restart (Boolean)	Restarts the application
Timeout (UInt32)	The timeout for application reaction (in seconds). By default, the timeout is 10 seconds.
ServiceName (String)	the service name in Windows Service Manager. By default, the name of the variable /Application Status/InstanceName is used.

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

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

Appendix D. Remove Dr.Web Anti-virus Manually

If you experience firewall failures, you can remove Dr.Web Anti-virus manually. To do this:

1. Run the command-line tool with administrator rights.
2. Unregister the application filter using the following commands:

```
regsvr32 /u /s "C:\Program Files\DrWeb for ISA Server\FTPFilter.dll"
regsvr32 /u /s "C:\Program Files\DrWeb for ISA Server\HTTPFilter.dll"
regsvr32 /u /s "C:\Program Files\DrWeb for ISA Server\POP3Filter.dll"
regsvr32 /u /s "C:\Program Files\DrWeb for ISA Server\SMTPFilter.dll"
```

3. Unregister the web filter using the command:
   - `regsvr32 /u /s "C:\Program Files\Microsoft Forefront Threat Management Gateway\DrWeb\HTTPWebFilter.dll"` (if you are using Microsoft Forefront TMG);
   - `regsvr32 /u /s "C:\Program Files\Microsoft ISA Server\DrWeb\HTTPWebFilter.dll"` (if you are using Microsoft ISA Server);
4. Stop the application services in the following order:

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

5. Start the standard utility Windows Installer Cleanup Utility (msicuu.exe) to delete the application from the system.
6. Delete the application services:

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

7. Delete the following folders:
   - in case you use Microsoft ISA Server

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

   - in case Microsoft Forefront TMG is used

```
rd /S /Q "C:\Program Files\DrWeb for ISA Server"
rd /S /Q "C:\Program Files (x86)\DrWeb for ISA Server"
rd /S /Q "C:\ProgramData\Doctor Web"
rd /S /Q "C:\Program Files\Microsoft Forefront Threat Management Gateway\DrWeb"
```

Appendix E. Operation in Central Protection Mode

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

Logical Structure of Anti-virus Networks

Solutions for central protection from Doctor Web use client-server model (see Figure 24).

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

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

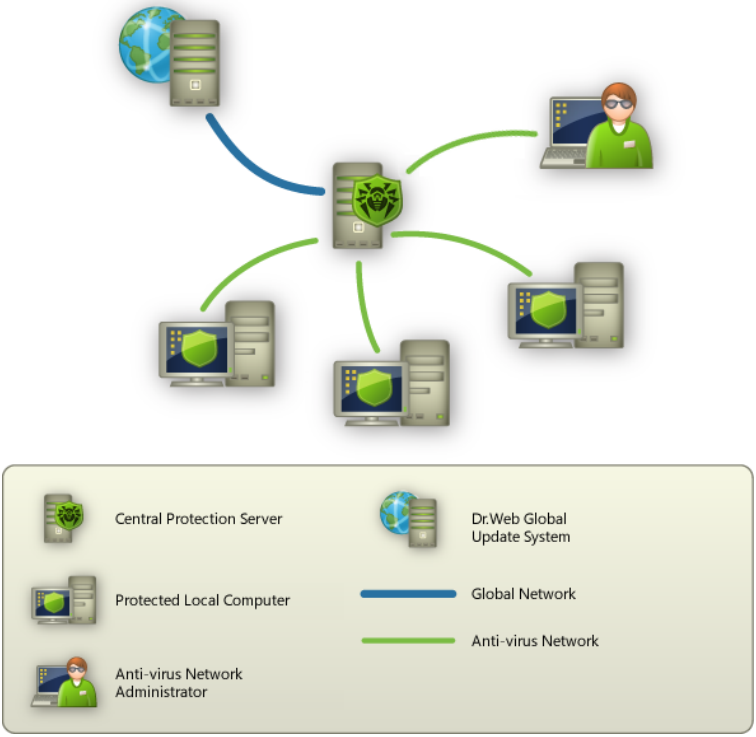

Figure 24. Logical structure of anti-virus network.

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

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

Operation of Dr.Web Anti-virus in Central Protection Mode

For operation of Dr.Web Anti-virus in central protection mode, version 6 or higher of Dr.Web Agent is required to be installed and operate correctly on the same operating system.

The version 6.00.1 of Dr.Web Anti-virus is not compatible with Dr.Web Agent version 5.

Dr.Web Anti-virus operating in the central protection mode provides the following possibilities:

- Recording the start events of Microsoft ISA Server or Microsoft Forefront TMG with the installed plug-in Dr.Web Anti-virus. Start events are displayed in the Start/Stop table of Dr.Web Control Center. Stop time of Microsoft ISA Server or Microsoft Forefront TMG is not recorded.
- Sending statistics of Dr.Web Anti-virus operation. The statistics is displayed in the Statistics and Summary statistics tables of Dr.Web Control Center.
- Sending notifications on detected viruses with information on the infections and performed actions. These events are displayed in the Infection table of Dr.Web Control Center.
- Virus databases and anti-virus engine updates from Dr.Web Control Center repositories. This action allow disabling the standard updater of Dr.Web Anti-virus, which starts by default according to a schedule. In this case components update starts from Dr.Web Control Center repositories according to its schedule.
- Using a license key file for Dr.Web Anti-virus that is registered at the anti-virus network. If the Enterprise mode was selected during the installation, the license key file for the station in the anti-virus network will be used on the start of Microsoft ISA Server or Microsoft Forefront TMG with the installed plug-in Dr.Web Anti-virus. If this key is invalid, the anti-virus check is not performed.

Appendix F. Technical Support

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

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

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in Dr.Web knowledge database at http://wiki.drweb.com/
- Browse the Dr.Web official forum at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from Doctor Web Technical Support by filling in the web-form in the corresponding section of the support site at http://support.drweb.com/.

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

Index

Index

E

F

Index

Index