



Defend what you create

Administrator Manual

© 2016, Doctor Web. All rights reserved.

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

TRADEMARKS

Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-desk are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

DISCLAIMER

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

**Dr.Web for Qbik WinGate
Version 6.0
Administrator Manual
2/8/2016**

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

Introduction	6
Conventions	8
Contacting Support	9
Licensing	10
License Key File	10
Acquire License Key File	10
Update License	11
Use License Key File	11
Licensing Parameters	11
Installation	13
System Requirements	13
Install Plug-in	14
Uninstall Plug-in	14
Start to Use	16
Plug-in Integration	17
Interface	18
Virus Check	21
Detection Methods	22
Check Settings	24
Quarantine	25
Anti-Spam	29
Black/White Lists	30
Update	32
Logging	33
Event Log	33
Debug Log	33
Troubleshooting	34
Check Installation	34
Check Functionality	35



Appendices	36
Appendix 1. Updater Command Line Parameters	36
Appendix 2. Troubleshooting Actions	38



Introduction

Thank you for purchasing **Dr.Web for Qbik WinGate**. This product is a plug-in that integrates into Qbik WinGate proxy server and protects the Internet traffic and emails against viruses and spam.

With the use of the plug-in, Qbik WinGate proxy server incorporates the latest and most advanced anti-virus technologies of **Doctor Web** aimed to detect the malicious objects which may present a threat to network operation and information security.

Dr.Web for Qbik WinGate checks the Internet traffic transferred via HTTP/POP3/FTP protocols and SMTP server for viruses, dialer programs, adware, riskware, hacktools and joke programs. On detection of security threats, they are treated according to the application settings.

The plug-in uses an efficient compact **Anti-Spam** component that does not require training and allows to define different program actions for three spam categories as well as to create black and white lists of email addresses.



Main Features

Dr.Web for Qbik WinGate performs the following functions:

- Anti-virus check of the files transferred via HTTP, FTP, SMTP and POP3 protocols, including the following:
 - Emails and their attachments
 - Web traffic files downloaded via HTTP and FTP protocols
- Check for spam the emails processed by SMTP server and POP3 proxy server services of WinGate proxy server
- Malware detection
- Curing of the infected files transferred via HTTP protocol
- Isolation of the infected objects in **Dr.Web quarantine** and/or WinGate quarantine
- Heuristic analyzer for additional protection against unknown viruses
- Fast and efficient check
- Automatic update of virus databases

This guide helps administrators to install and configure **Dr.Web for Qbik WinGate** to work with Qbik WinGate proxy server.


For detailed information on Qbik WinGate settings and traffic checks, see the company official web site at <http://www.wingate.com/products/wingate/index.php>.



Conventions

This guide utilizes the following content conventions and signs (see Table 1).

Table 1. Document Conventions and Signs

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



Contacting Support

Support is available to customers who have purchased a commercial version of **Doctor Web** products. Visit **Doctor Web Technical Support** web 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, see the **Doctor Web** official web site at <http://company.drweb.com/contacts/moscow>.



Licensing

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

License Key File

The license key file 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
- Users number limitation for the license

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

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

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

See [Logging](#) for detailed information about events logging.

Acquire License Key File

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

- By email in an archived attachment
- With the plug-in distribution kit if key file was included at kitting
- As a file on a separate carrier

To acquire a license key file by email

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. An archive with key file will be sent to the email address you specified in the registration form.
5. Extract the license key file and copy it to the computer where Qbik WinGate proxy server is installed and the installation of **Dr.Web for Qbik WinGate** is planned or has been already completed.

For demonstrative purposes you may be provided with a *trial key file*. Trial license allows you to access full functionality of **Dr.Web for Qbik WinGate** 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 trial key file by email, fill in the registration form at <http://download.drweb.com/demoreq/>.

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



Update 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 for Qbik WinGate** supports hot license update without stopping or reinstalling the plug-in.

To update the license key file

1. To update the license key file copy the new license key file to the program installation folder (by default, %ProgramFiles%\DrWeb for Qbik WinGate\).
2. **Dr.Web for Qbik WinGate** automatically switches to the new license.

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

Use License Key File

Installation Wizard copies the license key file to the plug-in installation folder (usually, %ProgramFiles%\DrWeb for Qbik WinGate).

During the operation of **Dr.Web for Qbik WinGate** the plug-in searches for the first valid key file in the installation folder (by the *.key mask). If no valid key is found, the plug-in stops functioning.



Do not edit or otherwise modify the file to prevent the license from compromise.

Licensing Parameters

The license key file regulates the use of **Dr.Web for Qbik WinGate**.

To view license details

1. View the license key file. (For instance, open the file with the Notepad text editor.)




The license key file is secured with digital signature. Do not edit or otherwise modify the file to prevent the license from compromise.

2. Review the following licensing parameters (see Table 2).



Table 2. Licensing Parameters

Parameter	Description
[Key] Applications	Determines the application components licensed with the key  To use the key with Dr.Web for Qbik WinGate the components Update and WinGatePlugin should be in the list determined by this parameter.
[Key] Expires	Determines the license expiration date
[User] Name	Determines the license owner
[User] Computers	Determines the number of users which the plug-in is licensed to protect simultaneously
[Settings] PluginsAdd	Indicates whether Anti-Spam is supported by the license (the WinGateSpamFilter value) or not

3. Close the file without saving.



Installation

Dr.Web for Qbik WinGate resides on computers where Qbik WinGate proxy server is installed. It operates as an external anti-virus integrated via the plug-in interface. For more information on use of anti-virus within Qbik WinGate proxy server see the official web site at <http://www.wingate.com/products/wingate/index.php>.

System Requirements

Before beginning installation, review the following system requirements and instructions (see Table 3).

Table 3. System Requirements

Component	Requirement
Disk Space	Minimum 350 MB of disk space
Operating System	One of the following: <ul style="list-style-type: none">• Microsoft® Windows® 2000 (Professional Edition, Server, Advanced Server or Datacenter Server) with SP4 and Update Rollup 1• Microsoft® Windows® XP (Home Edition or Professional Edition)• Microsoft® Windows Server® 2003 (Standard Edition, Enterprise Edition or Datacenter Edition)• Microsoft® Windows Server® 2003 R2• Microsoft® Windows Server® 2008 (Standard Edition, Enterprise Edition or Datacenter Edition)• Microsoft® Windows Server® 2008 R2• Microsoft® Windows Server® 2012• Microsoft® Windows Server® 2012 R2• Windows Vista® (Starter, Home Basic, Home Premium, Business, Enterprise or Ultimate) Both 32-bit and 64-bit versions of operating systems are supported.
Proxy server	Qbik WinGate 6  Function check of Dr.Web for Qbik WinGate was performed on the Qbik WinGate proxy server versions 6.2.2 and 6.6.4 that are available on the Qbik WinGate developer website at http://www.wingate.com/download/wingate/download.php .



In case an anti-virus file guard **Dr.Web Spider Guard** operates in the system besides **Dr.Web for Qbik WinGate**, you need to add to exclusions the files by `wgf*.tmp` and `*.quo` masks and the path to WinGate quarantine (by default, `C:\ProgramFiles\WinGate\Quarantine`) in the file guard settings to enable the anti-virus check by **Dr.Web for Qbik WinGate**.

A normal operation of **Dr.Web for Qbik WinGate** cannot be assured in case an anti-virus product of another vendor operates in the system.

For operating system protection use **Dr.Web** solutions for protection of workstations or of file servers (for server versions of operating systems).

For detailed information on them as well as on the other **Dr.Web** products see the official web site at <http://products.drweb.com/>.

Dr.Web for Qbik WinGate is not compatible with the following software:

- Webroot Spy Sweeper
- Webroot AntiVirus with Spy Sweeper



This section reflects requirements for the **Dr.Web for Qbik WinGate** only. See Qbik WinGate guides for proxy server requirements. **Dr.Web for Qbik WinGate** operates successfully on computers which meet the Qbik WinGate requirements.

Install Plug-in

Before beginning installation, review the [system requirements](#).



To install **Dr.Web for Qbik WinGate** you must have the Administrator privileges.

To install Dr.Web for Qbik WinGate

1. Copy the following files to the computer where Qbik WinGate resides:
 - Installation file
 - License key file
2. Run the installation file depending on the type of the operating system that is used on the computer:
 - **drweb-6.0.2-av-qbikwingate-windows-x86.exe** in case the 32-bit operating system is used
 - **drweb-6.0.2-av-qbikwingate-windows-x64.exe** if the operating system is 64-bit
3. Stop WinGate Engine service.
4. The window with a suggestion to choose the language of installation will appear. You can choose English or Russian language of installation. Click **OK**.
5. InstallShield Wizard for Qbik WinGate will open. Click **Next**.
6. On the **License Agreement** page read the Dr.Web License Agreement, select **I accept the terms in the license agreement** and click **Next**.
7. On the **License Key** page enter the path to the license key file or click **Browse** to select the file. Click **Next**.
8. On the **Destination Folder** page enter the path to the folder where the plug-in will be installed. By default, it is the folder **%ProgramFiles%\DrWeb for Qbik WinGate**. If you want to choose another folder click **Change** and specify the path to it. Click **Next**.
9. On the **Ready to Install the Program** page click **Install** to start installation of **Dr.Web for Qbik WinGate** on your computer.
10. After the installation of **Dr.Web for Qbik WinGate** is completed you can launch the virus databases update by selecting the checkbox **Run update**. Then click **Finish** to exit the wizard.

This completes the plug-in installation. You need to [configure](#) Qbik WinGate proxy server to use the plug-in.

Uninstall Plug-in



To uninstall **Dr.Web for Qbik WinGate** you must have the Administrator privileges.



To uninstall Dr.Web for Qbik WinGate

Use one of the following methods to uninstall **Dr.Web for Qbik WinGate**:

1. Stop the WinGate service.
2. On the **Control Panel**, double-click **Add or Remove Programs**, then in the programs list select **Dr.Web for Qbik WinGate** and click **Remove**. At the prompt, click **Yes**.
3. Launch the installation file of the plug-in. Choose the language of the dialog (English or Russian) and click **OK**. The InstallShield Wizard will open. Click **Next**. On the **Remove the Program** page click **Remove** to uninstall **Dr.Web for Qbik WinGate**. On completion of program removal click **Finish** to exit the wizard.

The plug-in files and update task will be removed.



Some files created during the plug-in operation are not deleted by default. You need to delete these files manually:

- Configuration file %ProgramFiles%\DrWeb for Qbik WinGate\ drweb32.ini
 - Program statistics file %ProgramFiles%\DrWeb for Qbik WinGate\drwebwingate.stat
 - License key file indicated during installation (by default, %ProgramFiles%\DrWeb for Qbik WinGate\drweb32.key)
 - Debug log file %ProgramFiles%\DrWeb for Qbik WinGate\ drwebforwingate.log
 - File with the list of updatable components %ProgramFiles%\ DrWeb for Qbik WinGate\drweb32.lst
 - Updater log %AllUsersProfile%\Application Data\Doctor Web\ Logs\drwebupw.log
-



Start to Use

Before start working with **Dr.Web for Qbik WinGate**, you need to configure WinGate proxy server to use it.

To launch the graphic interface of the program do one of the following:

- Double-click the **drwebforwingateconfigurator.exe** file located in the program installation folder %ProgramFiles%\ DrWeb for Qbik WinGate.
- Launch **Wingate engine** – open **GateKeeper** (see [Figure 1](#)) and select menu **Options** -> **Plugins** -> **Dr.Web for Qbik WinGate**.



The plug-in can be configured via graphic interface only on the local computer.



Plug-in Integration

Dr.Web for Qbik WinGate is enabled and operates as an external anti-virus software within Qbik WinGate proxy server and provides the check of different traffic types according to the application settings.

To integrate Dr.Web for Qbik WinGate:

1. Launch **Wingate engine** - open **GateKeeper** (see Fig. 1).

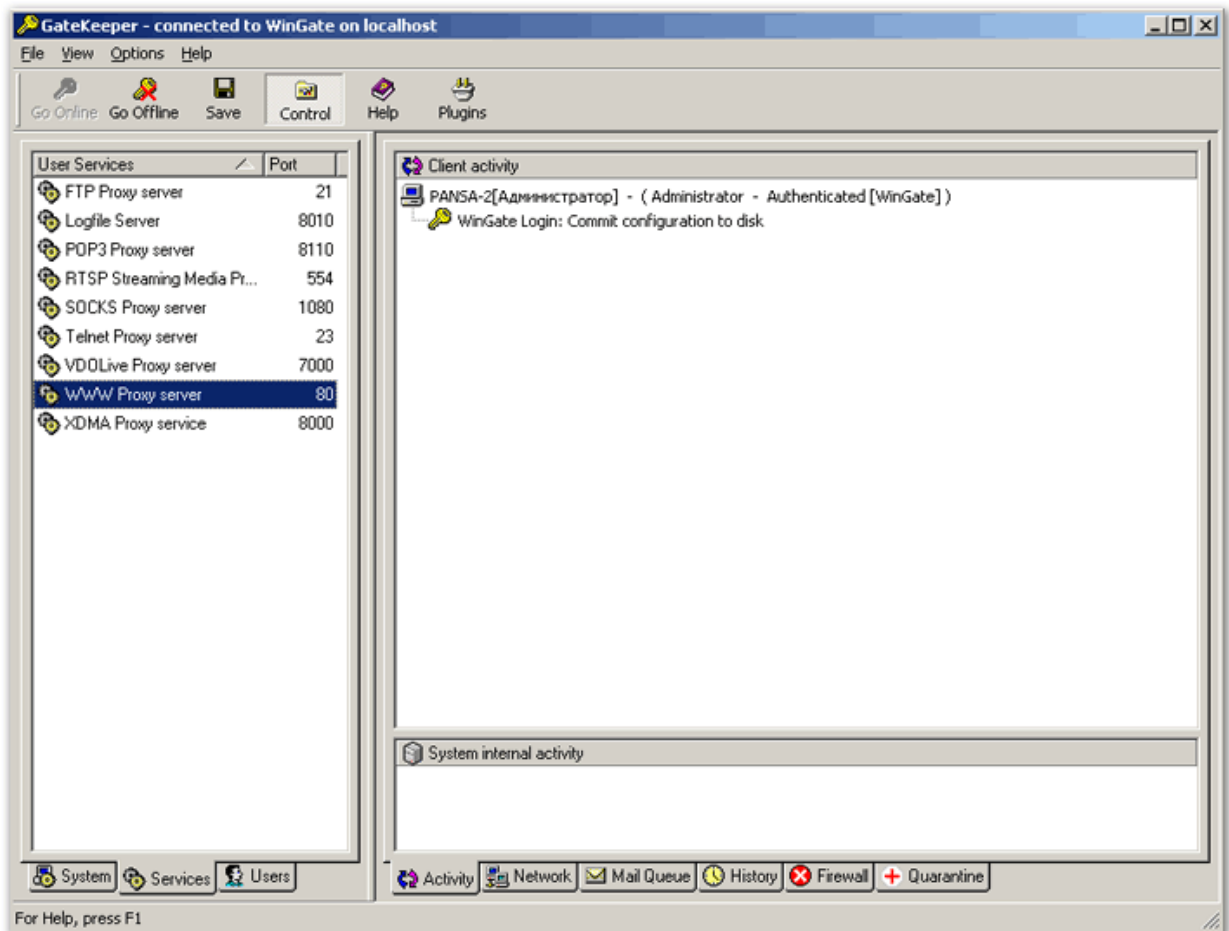


Figure 1. GateKeeper

2. Select one of the following sections corresponding to the system services protected by **Dr.Web for Qbik WinGate**:
 - SMTP Server system service
 - FTP Proxy server user service
 - POP3 Proxy server user service
 - WWW Proxy server user service
3. In the window of service properties (see Figure 2 for the example of WWW Proxy server properties window) select **Configuration** -> **Plug-ins**.

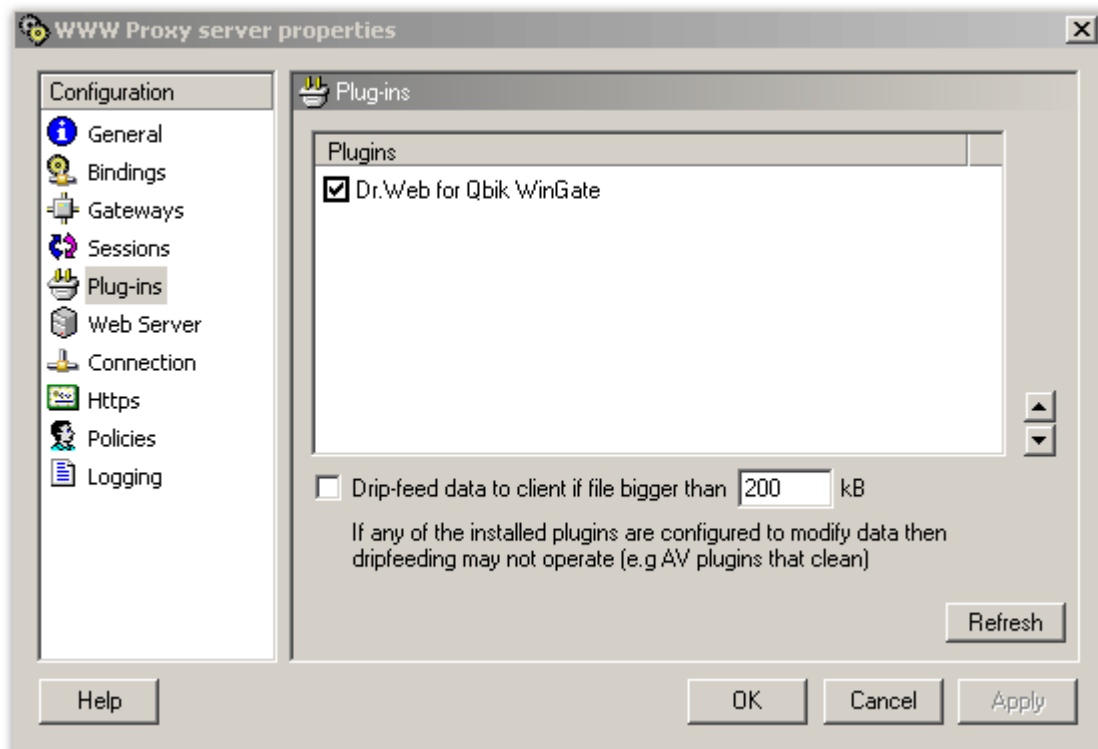


Figure 2. WWW Proxy server properties window

4. In the **Plug-ins** window select the check box **Dr.Web for Qbik WinGate**. If **Dr.Web for Qbik WinGate** is missing in the list of plug-ins, click the **Refresh** button.
5. Click **Apply** or **OK**.

If the integration failed and an error is reported, [check the installation](#) of the plug-in and consult the Qbik WinGate documentation as well to solve the problem.

For detailed information on use of anti-virus software with Qbik WinGate proxy server and possible errors of integration, see Qbik WinGate documentation and the company official website at <http://www.wingate.com/products/wingate/index.php>.

Interface

The program interface is used to check the current status and to configure the parameters of its operation.

On the program launch the main program window opens on the Status section (see Figure 3).

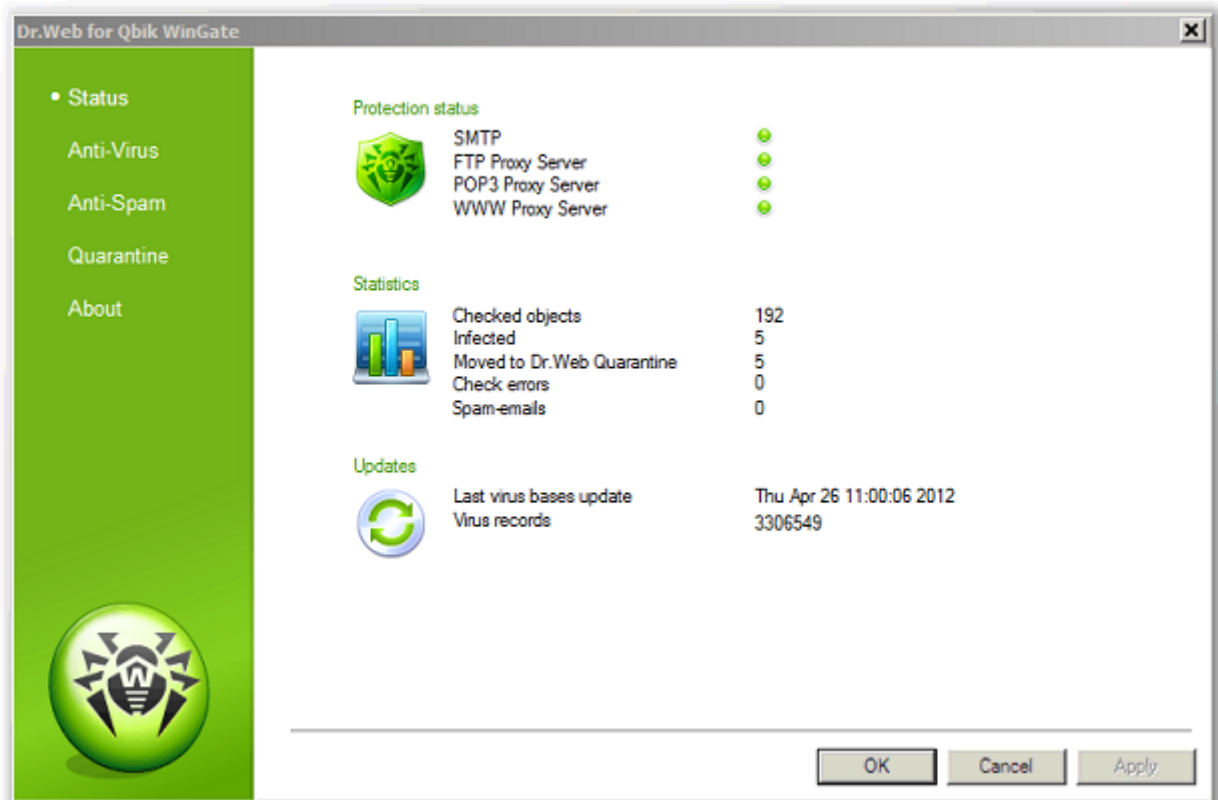


Figure 3. Status section. General information

On this section you can review the information on the current protection level, program statistics and updates.

Protection status

On this section you can review the list of system services protected by the plug-in. A green circle to the right of each service name indicates that it uses **Dr.Web for Qbik WinGate** for the data check.



Statistics

On the **Statistics** section you can review the total number of the checked objects, the number of the infected objects, the number of the objects moved to Quarantine and also the number of check failures.

Updates

On this section you can review the date of the last program update and the number of the virus records.

You can also review the information on the license and program components on the **About** section.

The operation of **Dr.Web for Qbik WinGate** is configured on the following sections:

- [Anti-Virus](#) – this section allows to configure the virus check and to specify the actions for the detected malicious objects
- [Anti-Spam](#) – this section allows to configure the spam filter and to create black and white lists
- [Quarantine](#) – this section allows to configure quarantine and to access to **Dr.Web Quarantine**



Virus Check

Dr.Web for Qbik WinGate detects the infected attachments in emails and also the infected objects transferred via HTTP and FTP protocols, including the following malicious objects:

- Infected archives
- Bomb viruses in files or archives
- Adware
- Hacktools
- Dialer programs
- Joke programs
- Riskware

Dr.Web for Qbik WinGate does not check:

- Encrypted objects transferred via HTTP (HTTPS)
- Encrypted emails
- Corrupted and password protected archives

Dr.Web for Qbik WinGate uses different [detection methods](#) and in case a virus is detected it is processed according to the program settings.

You can specify the [program actions](#) for infected files and the different types of malware neutralization as well as for the case when virus check fails.



If during the file transfer via the FTP protocol **Dr.Web for Qbik WinGate** detects a threat, the data transmission process interrupts and FTP client may alert an error. The secure part of the copied file may be saved on the disk, but all the information in it will be lost.

If you experience problems when checking large files via HTTP then you can configure the **Dr.Web for Qbik WinGate** plug-in in the **WWW Proxy server properties** window (see [Figure 2](#)).

To do this:

1. Select the **Drip-feed data to client if file bigger than** checkbox.
2. Enter the maximum size of a file.
3. Click **Apply** or **OK**.

This feature sends the client part of the downloaded data while a file is being scanned. This prevents clients like Outlook or Internet Explorer from timing out while waiting for the data to arrive.

Detection Methods

Signature analysis

The scans begin with signature analysis which is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web** anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing™

On completion of signature analysis, the **Dr.Web** use the unique **Origins Tracing** method to detect new and modified viruses which use the known infection mechanisms. Thus, **Dr.Web** users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the **Origins Tracing** mechanism allows to considerably reduce the number of false triggering of the heuristics analyzer. Objects detected using the **Origins Tracing** algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator* – a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristics analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) than might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristics analyzer calculates the



probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the **FLY-CODE™** technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers **Dr.Web** is aware of, but by also new, previously unexplored programs. While checking packed objects, **Dr.Web** anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristics analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristics analyzer are treated as "suspicious".

While performing any of the abovementioned checks, the **Dr.Web** anti-virus solutions use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus Laboratory** discover new threats, the update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web** resident guards and penetrates the system, then after an update the virus is detected in the list of processes and neutralized.



Check Settings

You can set up the Internet traffic anti-virus check by specifying the program actions for the detected malicious objects on the **Anti-Virus** section (see Figure 4).

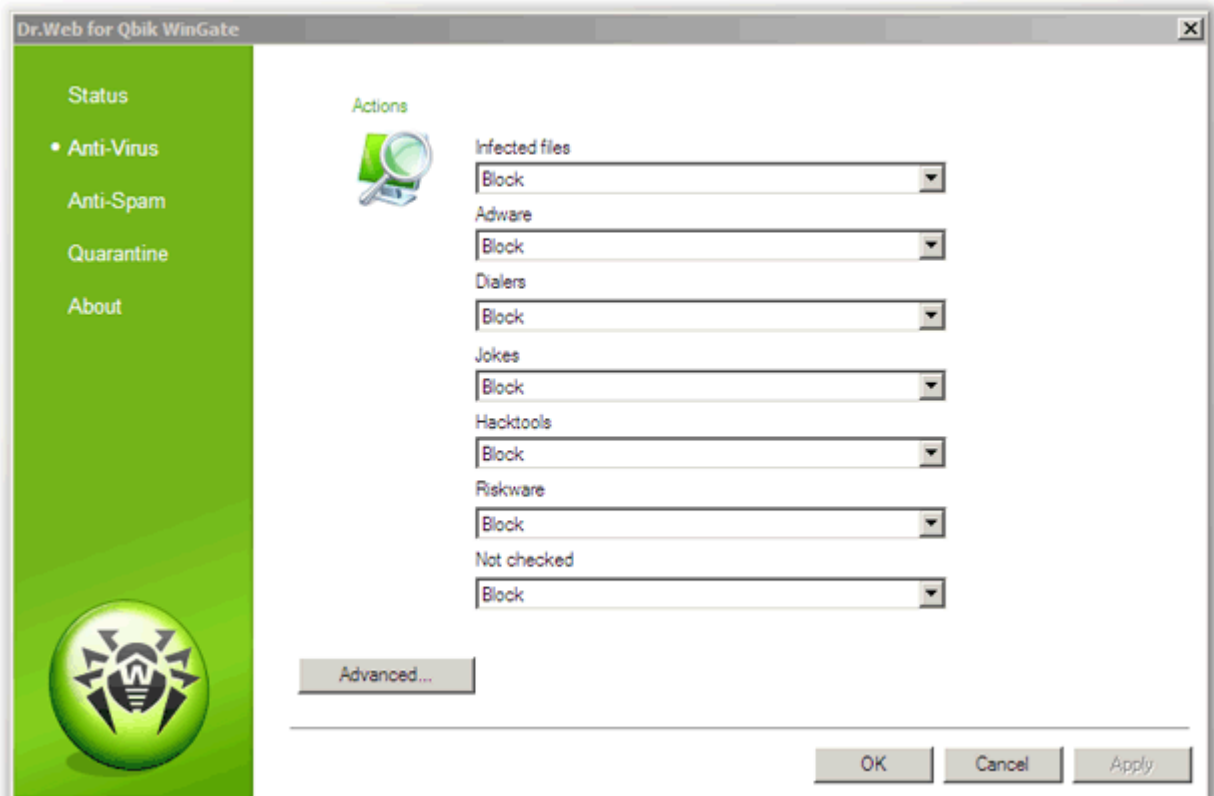


Figure 4. Anti-Virus section

In case a file contains a virus or any type of the malware, or the file check failed, the following actions can be performed:

- **Cure** – the plug-in tries to cure the object. If it cannot be cured, it will be blocked.
- **Move to Quarantine** – the object will be blocked and its copy will be saved in **Dr.Web quarantine** and/or WinGate quarantine (depending on the [quarantine](#) settings).
- **Block** – the object will be blocked without saving its copy in quarantine.
- **Ignore** – the object will be passed through without any changes.

Additional scan settings

Additional scan settings can be accessed by clicking the **Advanced** button on the **Anti-Virus** section. In the **Additional settings** window (see Figure 5) you can specify the scanning options and configure the program logging.

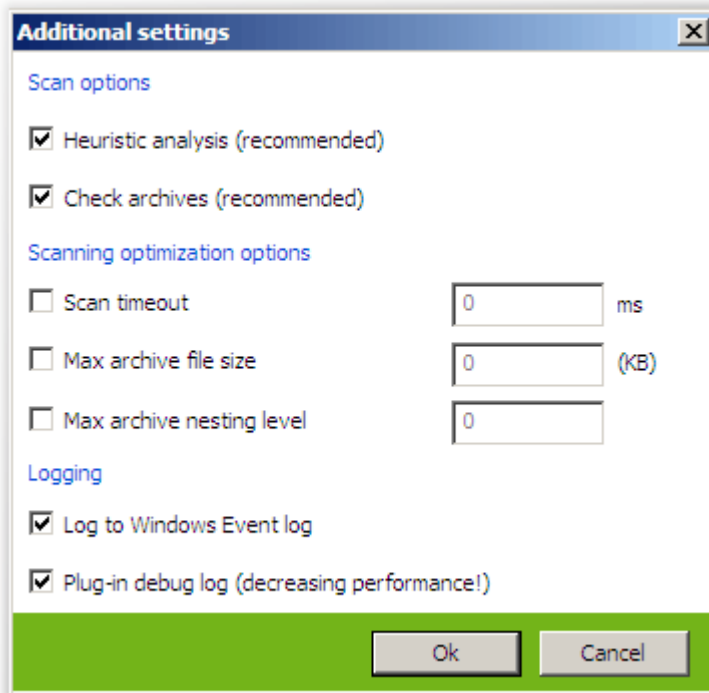


Figure 5. Additional scan settings

On the **Scan options** section, specify the following options:

- **Heuristic analysis** – select/clear this check box to enable/disable the heuristic analyzer that allows to detect the unknown viruses.
- **Check archives** – this option allows to enable/disable the archives scanning.

On the **Scanning optimization options** section, specify the limitations for the scanning time and scanned objects characteristics:

- **Scan timeout** – this option allows to specify the maximum time for scanning of an object (in milliseconds). By default the scan time is unlimited.
- **Max archive file size** – this parameter defines the maximum size (in kilobytes) of an archive to scan. By default, the archive file size is no limited.
- **Max archive nesting level** – this parameter defines the maximum number of nesting levels in an archive. The values from 0 to 16 are possible. By default, the archive nesting level is not limited.

If the corresponding parameters of a checked object exceed the values specified by the **Scan timeout**, **Max archive size** and **Max archive nesting level** parameters, the actions defined by the **Not checked** parameter will be performed for such object.

Besides, you can configure the program logging on the **Logging** section. Logging to Windows Event log and/or to the plug-in debug log can be selected.

Quarantine

The infected attachments and spam messages can be moved to **Dr.Web quarantine**, where the malicious objects are isolated from the rest of the system.

On the threat detection in traffic transferred via FTP and HTTP protocols, the infected file is moved to quarantine. If a threat is detected in email transferred via SMTP and POP3 protocols or if it contains spam, the initial email is moved to quarantine (in .msg format) as it came to the sever.



The quarantined objects are located in **Dr.Web Quarantine** folders in the root directories on the local disk and remain on the disk after **Dr.Web for Qbik WinGate** is uninstalled. However, the access to these folders is denied. If necessary, you can remove the folders by setting your Windows account as root user (in case NTFS is used).

Enable Quarantine

You can enable **Dr.Web quarantine** as well as the in-built WinGate quarantine by selecting the corresponding options on the **Quarantine** section (see Figure 6).

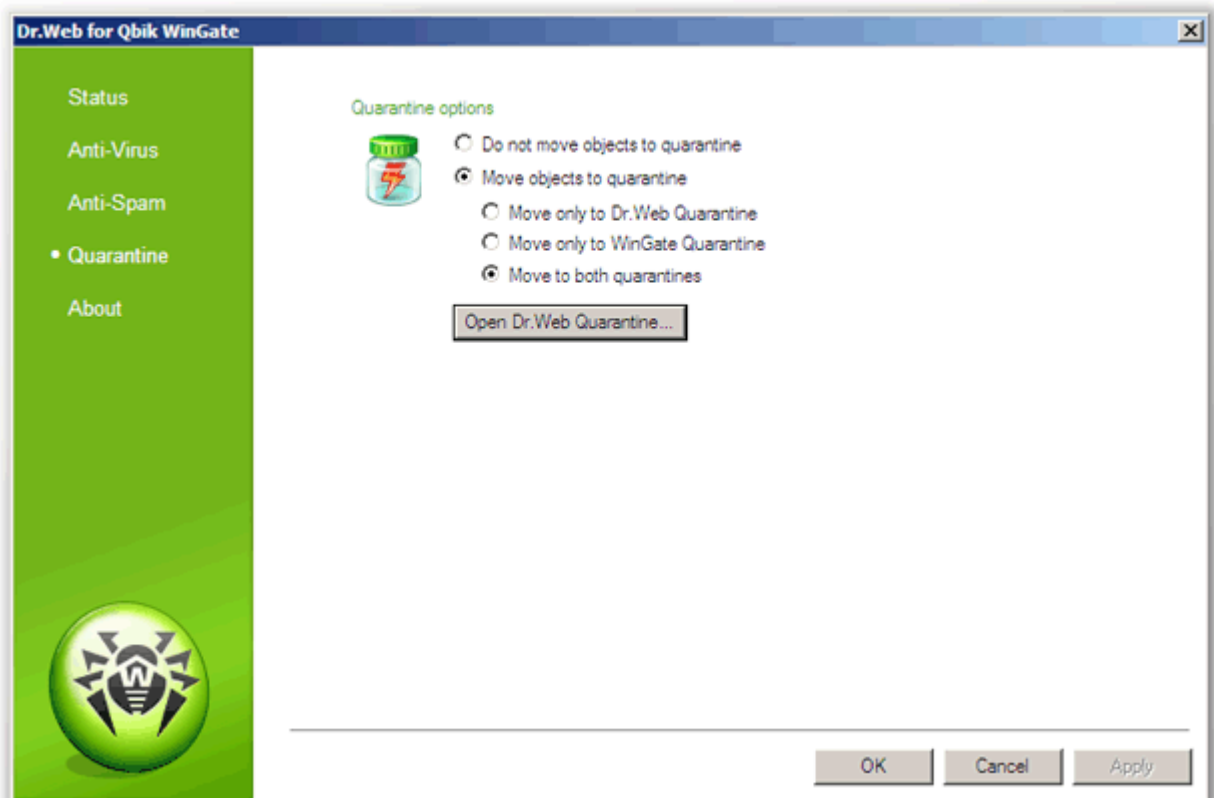


Figure 6. Quarantine section

Manage Quarantine

The quarantined files can be reviewed and processed using the special utility **Dr.Web Quarantine**. To launch the utility, select **Start -> Programs -> Dr.Web for Qbik WinGate -> Dr.Web Quarantine**. The list of objects in quarantine will be displayed (see Figure 7).

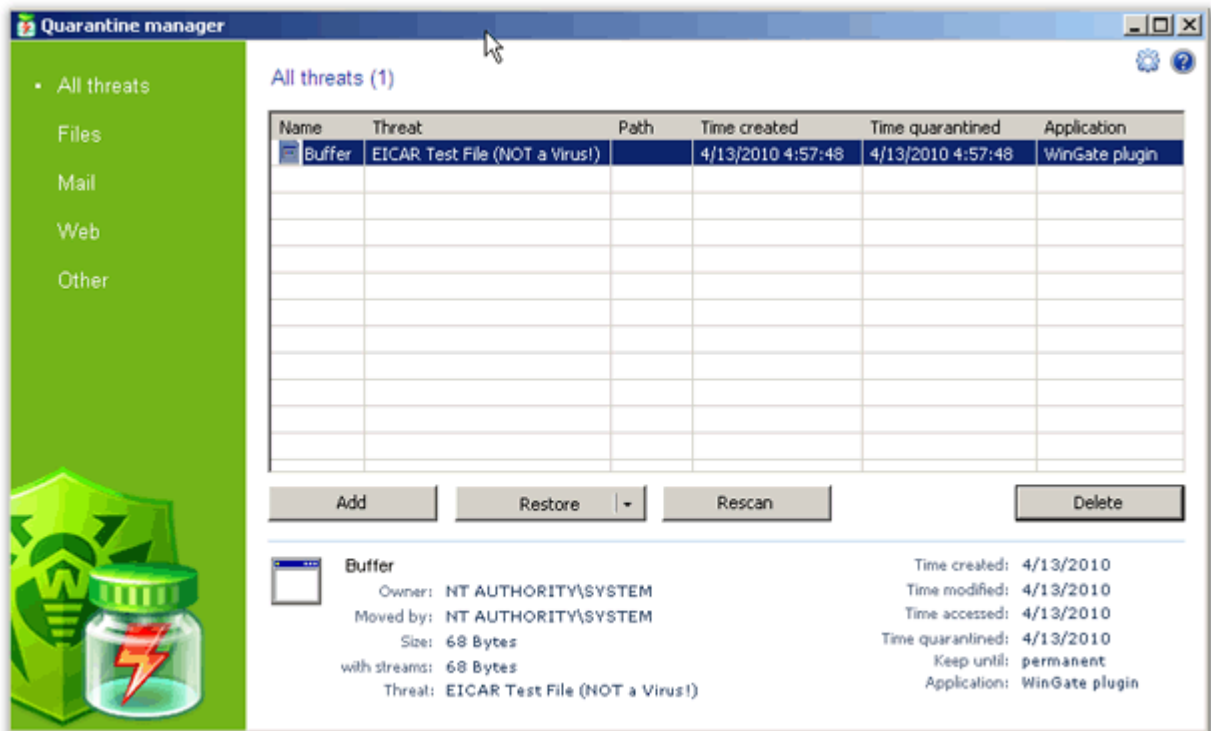


Figure 7. Dr.Web Quarantine

For each object in the list the information on the infected file name and size, the name of the virus and the path to the storage folder is displayed. You can specify the types of the information that is displayed in the list. To do this:

1. Right-click any column in the table and select **Customize columns**.
2. Select the types of the information you want to be displayed.

Process objects in quarantine

You can remove the quarantined objects or restore them. To do this:

1. Select one or several objects in the list.
3. To delete the selected file(s) click the **Delete** button.
4. To restore the selected file(s) select **Restore** -> **Restore to** and then specify the folder for restored file(s).

You can also scan the quarantined objects, e.g. the suspicious files, again, after [updating Dr.Web virus databases](#). To check the files again, click the **Rescan** button.

The **Add** button is used to add files from the local or removable disk to quarantine. Then you can scan these files for viruses.

Quarantine properties

To access to quarantine properties click the **Properties**  button in the top part of the **Quarantine** window. In the **Quarantine properties** window (see Figure 8) you can specify the following settings:

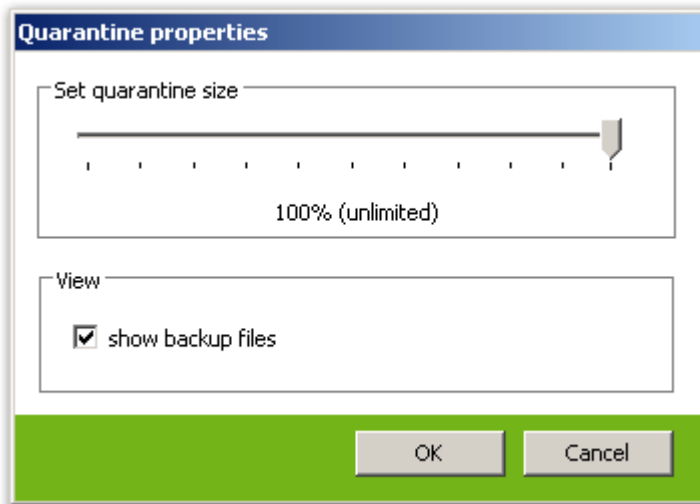


Figure 8. Quarantine properties

1. You can set up the quarantine size. To do this, specify the amount of the disk space for the quarantine in the **Set quarantine size** section (see [Figure 8](#)).
2. Before the infected file is cured, its backup is saved in the quarantine to allow restoring the file in case it is corrupted during its curing. To enable viewing backups in quarantine list, select the **show backup files** check box in the **View** section (see [Figure 8](#)).



Anti-Spam

Anti-Spam allows to filter the emails processed by SMTP server and POP3 proxy server services to avoid receiving of the unsolicited messages, for example, advertising emails. **Anti-Spam** supports three categories of spam, each of them having its own specified program action. You can choose one of four actions for each category: skip, move to quarantine, delete and pass through with spam notification.

You can enable/disable the check for spam on the **Anti-Spam** section (see Figure 9). There you can also specify the program actions for three spam categories – high, medium and low spam probability.

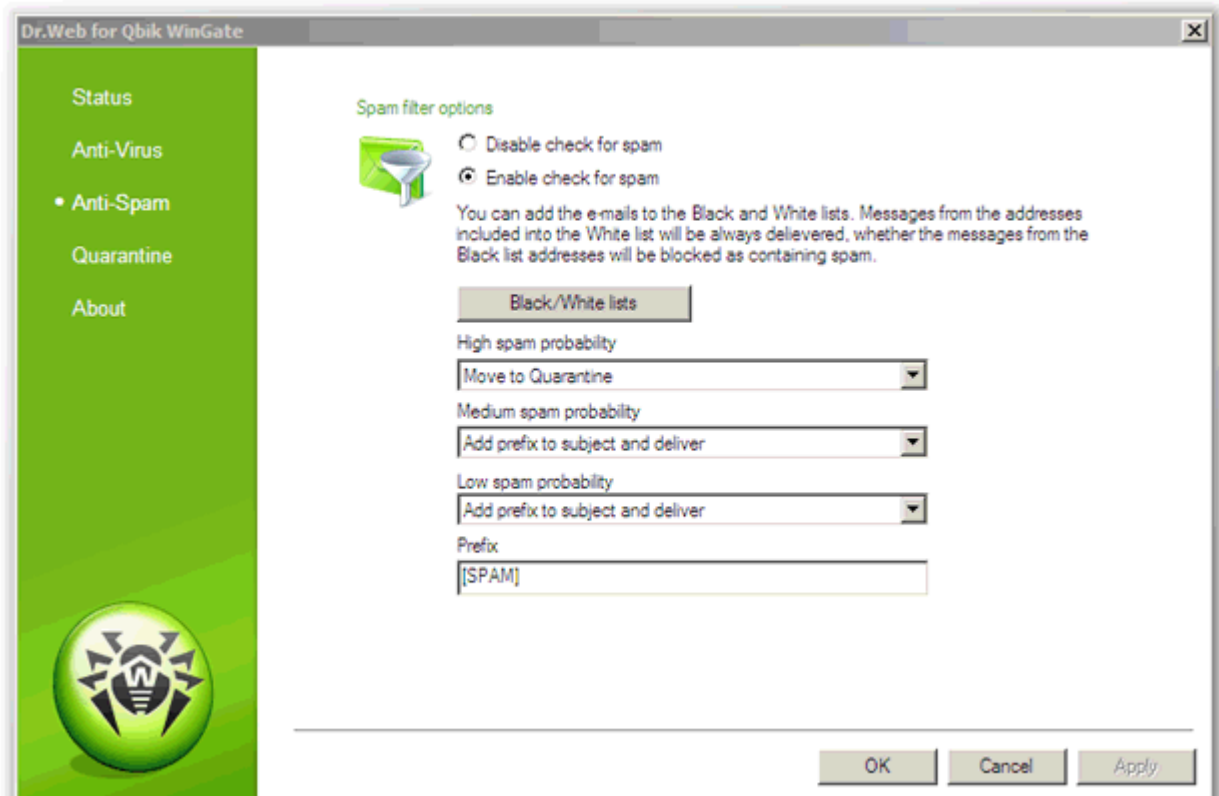


Figure 9. Anti-Spam section



The options on the **Anti-Spam** section are available only if the license key file [supports](#) the use of **Anti-Spam**. You can review the information on the license key file on the **About** section окне настроек **Dr.Web for Qbik WinGate**.

If **Anti-Spam** is not supported by the license, the spam filter options will be disabled and the messages check for spam will not be performed.

For each spam category on email of the following action can be selected:

- **Skip** – to skip the email without any changes.
- **Move to Quarantine** – to move the email to quarantine (according to the quarantine settings). In this case the email will not be delivered to the recipient.
- **Delete** – to delete the email (without moving it to quarantine). In this case the email will not be delivered to the recipient.
- **Add prefix to subject and deliver** – to pass through the email with the notification prefix added to its subject. In this case the email will be delivered to the recipient.

The spam notification prefix is specified in the **Prefix** field.



If **Anti-Spam** identifies certain messages incorrectly, you are advised to forward such messages to the following special email addresses for analysis:

- Messages which are wrongly regarded as spam should be forwarded to vrnonspam@drweb.com
- Unblocked spam messages should be forwarded to vrspam@drweb.com

Forward messages as attachments; do not include them to the message body.

Black/White Lists

Black and white lists are used to filter the emails.

You can add the trusted email addresses to the white list. No actions will be performed for the messages from these addresses. If you add an email address to the black list, messages from this address will be considered as **High spam probability** and the corresponding action will be performed.

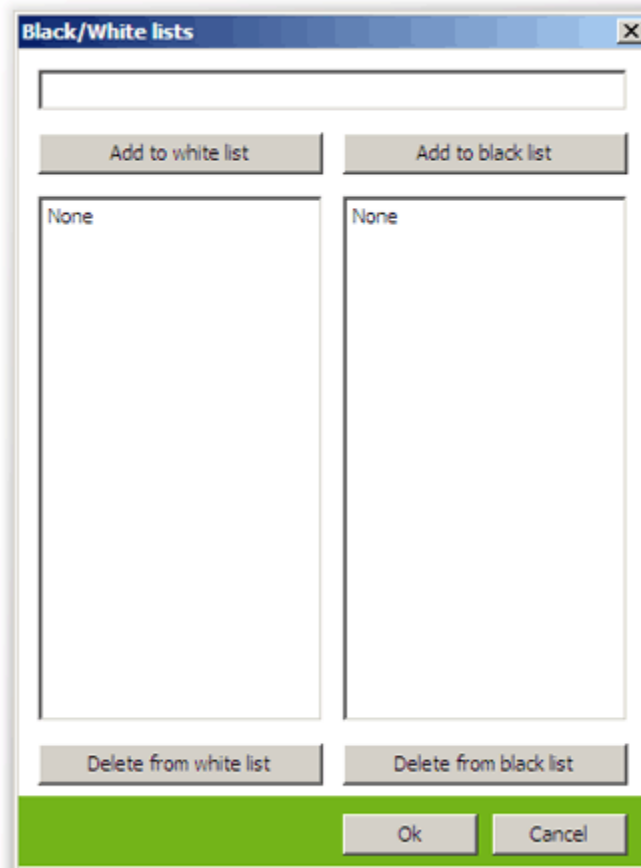


Figure 10. Black/White lists

To open the black and white lists click the **Black/White lists** on the **Anti-Spam** section (see [Figure 9](#)).

To add an email address to black or white list, enter it in the text field in the **Black/White lists** window and then click the **Add to white list** or **Add to black list** button (see [Figure 10](#)).

To delete an address from the list, select it and click the **Delete from white list** or **Delete from black list** button.



You can use the wildcard «*» instead of any part of an address (e.g., *@domain.org stands for all addresses in the **domain.org** domain).



Update



The **Updater** component (drwebupw.exe) may be launched just on the completion of the plug-in installation by selecting the corresponding checkbox at the last step of [installation](#). This component updates the scanning engine (drweb32.dll) and virus databases (*.vdb).


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

The **Updater** component of **Dr.Web for Qbik WinGate** helps you download the updates via Internet and automatically installs them.

For computers without access to the Internet, you can configure updates from the central storage of update files.

When you install **Dr.Web for Qbik WinGate**, the installation wizard creates a task which schedules Updater to check for new updates at the **Doctor Web** global update server. You can change the schedule using the standard Windows Scheduled Tasks utility. You can also configure the update process using the command line parameters listed in the [Appendix 1](#).

To modify update schedule

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **Dr.Web Update for Qbik WinGate Plugin**  and select **Properties**.
3. On the **Schedule** tab, modify the task schedule. By default, the plug-in checks for updates each 30 minutes.
4. Click **OK**.


To configure update without Internet connection

1. Create a central storage for the update files.



You can use folder available through UNC paths only, which include:

- Local folder on the computer
- Shared network folders

2. Copy the new updates for plug-in components and virus databases from the **Doctor Web** official download web site at <http://download.drweb.com/bases/> to the storage. You can view the list of updatable components in the drweb32.lst file which is located in the installation folder of **Dr.Web for Qbik WinGate** (usually, %ProgramFiles%\DrWeb for Qbik WinGate).
3. On the local computer where you want to configure updates from the central storage, open the Control Panel and double-click **Scheduled Tasks**.
4. Right-click **Dr.Web Update for Qbik WinGate Plugin**  and select **Properties**.
5. On the **Task** tab, add the following command line parameter to the command string in the **Run** field:
/URL:<storage> where <storage> is the path to the central updates storage.
6. Click **OK**.



Logging

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

- Windows Event Log
- Text Dr.Web debug log

The update information is logged in a separate drwebupw.log file, which is located in the %AllUsersProfile%\Application Data\Doctor Web\Logs\ folder.

Event Log

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

- Plug-in starts and stops (starts and stops of WinGate service with installed application **Dr.Web for Qbik WinGate**)
- License absence or invalidity notifications
- Information on threats detection
- Notifications on moving the infected objects to WinGate quarantine and/or **Dr.Web quarantine** (in case the corresponding [anti-virus parameters](#) are enabled)
- License expiration notifications (a message is registered in 30, 15, 7, 3, 2 and 1 days before expiration)

Enable/disable logging

1. On the **Anti-Virus** section click the **Advanced** button to open the additional scan settings, then select/clear the **Log to Windows Event log** check box.
2. Restart WinGate service.

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 is application Dr.Web for Qbik WinGate.

Debug Log

The plug-in debug log contains the information that is used for search and analysis of errors in operation of **Dr.Web for Qbik WinGate**.

To enable the debug logging

1. On the **Anti-Virus** section click the **Advanced** button to open the additional scan settings, then select/clear the **Plug-in debug log** check box.
2. Restart WinGate service.



Logging to the **Dr.Web for Qbik WinGate** debug log decreases the system performance.

The drwebforwingate.log file of the debug log will be created in **Dr.Web for Qbik WinGate** installation folder (by default, %ProgramFiles%\DrWeb for Qbik WinGate\).



Troubleshooting

If you're experiencing trouble protecting the Internet traffic from virus threats, follow the steps below to ensure that **Dr.Web for Qbik WinGate** is installed and configured properly:

- [Check installation](#)
- [Check plug-in operation](#)
- [Check Updater module](#)

Check Installation

To check whether the plug-in is correctly installed:

1. Ensure that during the plug-in installation the following folders have been created and contain all necessary files:
 - %ProgramFiles%\DrWeb for Qbik WinGate\

File name	Description
drwebupw.exe	Executable file of Updater
update.drl	List of URLs for updating
drweb32.key	License key file
dwqrui.exe	Utility to access to Dr.Web quarantine
locale.ini	Localization file
drwmsg.dll	Service library
drwebforwingate.dll	Dr.Web for Qbik WinGate application library
drweb32.ini	Application configuration file
DrWebForWingateConfigurator.exe	Dr.Web for Qbik WinGate graphic interface

- %CommonProgramFiles%\Doctor Web\Scanning Engine\

File name	Description
drweb32.dll	Anti-virus engine
dwinctl.dll	–
dwengine.exe	Dr.Web Scanning Engine service

- %AllUsersProfile%\Application Data\Doctor Web\Bases\

File name	Description
*.vdb	Virus databases

2. On the Control Panel, double-click **Administrative Tools** and then double-click **Services**. Ensure that the service Dr.Web Scanning Engine (DrWebEngine) is running.
3. [View Event Log](#) and ensure that there is no errors which originate from the application **Dr.Web for Qbik WinGate**.




Check Functionality

To make sure the plug-in operates properly, it is recommended to check the program's virus detection capabilities and functionality of the Updater.

To check plug-in operation

1. On the **Protection status** section (see [Figure 3](#)) ensure that WWW Proxy Server service is protected by the plug-in.
2. Specify your browser to work via Qbik WinGate proxy server with installed application **Dr.Web for Qbik WinGate**.
3. Open the page <http://www.eicar.org/download/eicar.com> the Internet browser to download the test virus EICAR-Test-File. For information on EICAR test virus see http://en.wikipedia.org/wiki/EICAR_test_file. The mentioned page must not open, and the alert page about the infected file should be displayed. The detected file with EICAR test virus will be moved to quarantine.

To check Updater

1. On the Control Panel, double-click **Scheduled Tasks** and ensure that the **Dr.Web Update for Qbik WinGate Plug-in**  task is created.
2. Launch Dr.Web Update for Qbik WinGate Plug-in task.
3. In the %AllUsersProfile%\Application Data\Doctor Web\Logs\ folder, view the drwebupw.log update log and ensure that it contains no errors.




Appendices

Appendix 1. Updater Command Line Parameters

The Updater can operate in command line mode. You can use parameters to configure the update process.

To configure update task

1. On the Control Panel, double-click **Scheduled Tasks**.
2. Right-click **Dr.Web Update for Qbik WinGate Plug-in**  and select **Properties**.
3. In the **Run** field add command line parameters.

Available Parameters

Below is the list of command line parameters which can be used to configure the updating process:

Parameter	Description
/DBG	Sets detailed logging in the %AllUsersProfile%\Application Data\Doctor Web\Logs\drwebupw.log file
/DIR: <folder>	Specifies the folder where to store the update files The default is the directory where Updater runs.
/GO	Sets the package operation mode when Updater does not display dialogs
/INI: <path>	Specifies an alternative configuration file to use
/LNG: <filename>	Specifies the language resources file name The default language is English.
/NI	Sets Updater to ignore parameters specified in the configuration file (drweb32.ini)
/NR	Sets Updater to work without logging
/PASS: <password>	Specifies the password to use when connecting to the updates server
/PPASS: <password>	Specifies the password to use when connecting to the proxy server
/PURL: <address>	Specifies location of the proxy server
/PUSER: <name>	Specifies the user name to use when connecting to the proxy server
/QU	Sets compulsory closure of Updater after finishing an update regardless of its results Update result is returned in the ERRORLEVEL environment variable. If update completes successfully, the ERRORLEVEL environment variable is set to 0. Other values indicate an error.
/REG	Launches Updater to register the product or request a license key file
/RP <file> or /RP+ <file>	Specifies the log file The default is %AllUsersProfile%\Application Data\ Doctor Web\Logs\drwebupw.log. Use /RP+ to append new records to the file. Use /RP to overwrite the file.
/SO	Enables sound notifications on errors
/ST	Sets the Updater to run in stealth (invisible) mode
/UA	Sets the Update All mode when Updater downloads all files specified in the updating list regardless of the operating system used and the product components installed



Parameter	Description
	This mode allows you to download all updates from the Doctor Web global update server. This mode cannot be used to update the anti-virus installed on a computer.
/UPD	Sets the Usual mode Use this parameter together with /REG to update the product after completing registration.
/UPM:<mode>	Configures connection via proxy You can set one of the following values: <ul style="list-style-type: none">• direct – direct connection without proxy• ieproxy – connection via proxy, system settings are used• userproxy – connection via proxy, user-defined settings are used
/URL:<url>	Specifies location of the updates server Only UNC-paths are accepted.
/URM:<mode>	Sets the Restart mode In this mode the computer is restarted when update finishes. You can set one of the following values: <ul style="list-style-type: none">• prompt – prompt for reboot if needed• noprompt – reboot without prompting if needed• force – always• disable – disable reboot
/USER:<name>	Specifies the user name to use when connecting to the updates server
/UVB	Sets update of virus databases and the core (drweb32.dll) only This option disables /UA parameter.



Appendix 2. Troubleshooting Actions

In case you experience problems while using or installing **Dr.Web for Qbik WinGate** contact [Dr.Web Technical Support](#).

To help you to fix the problems as soon as possible, please provide to the **Doctor Web** specialists the full information on the problem. You can review the recommendations listed below. This information should be sent with your request to the [Technical Support](#) or to the [Dr.Web Bug Tracker system](#).

Recommendations

1. Save the configuration file `drweb32.ini` with **Dr.Web for Qbik WinGate** settings which is located in program installation folder (by default, `%ProgramFiles%\DrWeb for Qbik WinGate`).
2. Save the report file with system information in the `.nfo` format. To do this:
 - Run the `msinfo32` command from the **Start -> Run** menu.
 - Select **File -> Save**.
 - Enter the file name and click **OK**.
3. Save the **Application** and **System** logs in the `.evt` format. To do this:
 - Run the `eventvwr` command from the **Start -> Run** menu.
 - Right-click the **Application/System** log and select **Save log file as**.
 - Enter the file name and select the **Event Log (.evt)** file type, then click **Save**.
4. If the problem persists, enable the [Dr.Web debug log](#) and reproduce the problem. Then you can disable the debug log. By default, the text debug log file `drwebforwingate.log` is created in the `%ProgramFiles%\DrWeb for Qbik WinGate\` folder.

If you experience problems on the program installation or removal:

1. Include the version of the **Dr.Web for Qbik WinGate** installation file you experience problems with (e.g., 5.00.2.02190). To view the installation file version do the following:
 - Find the **Dr.Web for Qbik WinGate** installation file in Windows Explorer (e.g., `drweb-6.0.2-av-qbikwingate-windows-x86.exe`).
 - Right-click the installation file name and select **Properties**.
 - In the **Properties** window open the **Version** tab and select **Product version**.
2. Verify the digital signature of the **Dr.Web for Qbik WinGate** installation file. To do this:
 - Find the **Dr.Web for Qbik WinGate** installation file in Windows Explorer (e.g., `drweb-6.0.2-av-qbikwingate-windows-x86.exe`).
 - Right-click the installation file name and select **Properties**.
 - In the **Properties** window open the **Digital signatures** tab, then select the digital signature in the list and click **Details**.
 - The **Digital Signature Details** window should contain an inscription "This digital signature is OK". If this inscription is missing, try to reload the installation file from the **Doctor Web** server and repeat the digital signature verification procedure.
3. Attach the `drweb-qbikwingate-setup.log` file located in the temporary folder. To do this:
 - Open the temporary folder `%Temp%` from the **Start -> Run** menu and copy the `drweb-qbikwingate-setup.log` file.
4. Attach the following information on the license key file:
 - Applications, Created and Expired parameters' values. Example:

```
Applications=Update, Scheduler, WinGatePlugin
Created=2010-01-05 (12:00) UTC
Expires=2010-07-05 (12:00) UTC
```



- The [Settings] section. Example:

```
FileServer=No  
InetGateway=No  
SpamFilter=No  
LotusSpamFilter=No  
EmailAddresses=Unlimited  
TrafficLimit=Unlimited
```

