



User Manual



© Doctor Web, 2022. All rights reserved

This document is for information and reference purposes in relation to the specified software of the Dr.Web family. This document is not a ground for exhaustive conclusions about the presence or absence of any functional and/or technical features in the software of the Dr.Web family and cannot be used to determine whether the software of the Dr.Web family matches any requirements, technical task and/or parameters, and other third-party documents.

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, SplDer Mail, SplDer Guard, CureIt!, CureNet!, AV-Desk, KATANA and the Dr.WEB logo 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 KATANA
Version 1.0
User Manual
8/4/2022

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

Website: <https://www.drweb.com/>

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

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

Doctor Web

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

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

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

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

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



Table of Contents

1. About the Product	5
1.1. Conventions	5
1.2. Detection Methods	5
1.3. System Requirements	7
2. Installing, Restoring and Removing Dr.Web KATANA	9
2.1. Installation Procedure	9
2.2. Restoring and Removing Dr.Web KATANA	12
3. Licensing	13
3.1. Activation Methods	14
3.2. Renewing License	14
3.3. Registration Wizard	15
4. Getting Started	17
5. Tools	18
5.1. License Manager	18
5.2. Quarantine Manager	19
5.3. Support	20
5.3.1. Report	21
6. Update	23
7. Settings	24
7.1. Main	24
7.2. Update	25
7.3. Self-Protection	26
7.4. Dr.Web Cloud	27
7.5. Protection	28
8. Technical Support	32
9. Appendix A. Dr.Web Updater Command-line Parameters	33




1. About the Product

Dr.Web KATANA protects your system against computer threats by means of non-signature-based technologies—using behavior analysis, cloud-based threat detection, and preset rules. The program does not conflict with third-party anti-viruses and can operate in a team with them to enhance your computer security.

1.1. Conventions

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

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

1.2. Detection Methods

Behavior Analysis

The behavioral analysis technology Dr.Web Process Heuristic protects systems against latest, most dangerous malicious programs that are capable of avoiding detection by traditional signature-based analysis and heuristic routines.

Dr.Web Process Heuristic analyzes the behavior of each running program in real time by comparing it with Dr.Web Cloud which is constantly updated. It determines whether the program is dangerous and then takes whatever measures are necessary to neutralize the threat.

This data protection technology helps minimize losses resulting from the actions of unknown malware—and consumes very few of the protected system resources.



Dr.Web Process Heuristic monitors any attempts to modify the system:

- Detects malicious processes that modify files (for example, actions of encryption ransomware)
- Prevents malware from injecting its code into the processes of other applications
- Protects critical system areas from being modified by malware
- Detects and stops the execution of malicious, suspicious or unreliable scripts and processes
- Prevents malware from modifying boot sectors so that malicious code cannot be executed on the computer
- Blocks changes in the Windows Registry to make sure that the safe mode will not be disabled
- Prevents malware from changing launch permissions
- Prevents new or unknown drivers from being downloaded without the user's consent
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries into the Windows Registry, so that they could be launched automatically
- Locks registry sections containing information about virtual device drivers, ensuring that no new virtual devices are created.
- Prevents malware from disrupting system routines

Exploit prevention

Dr.Web Process Heuristic includes the Dr.Web ShellGuard technology which protects system from programs that exploit vulnerabilities. Exploits are malicious objects that take advantage of software flaws in order to gain control over a targeted application or the operating system.

Dr.Web ShellGuard protects common applications installed on computers running Windows:

- Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Vivaldi Browser)
- MS Office applications including MS Office 2016
- System applications
- Applications that use Java, Flash and PDF
- Media players (software)

To detect malicious actions, Dr.Web ShellGuard uses information stored by the anti-virus locally as well as reputation data from Dr.Web Cloud which includes:

- Information about the routines used by programs with malicious intentions
- Information about files that are 100% clean
- Information about the compromised digital signatures of well-known software developers
- Information about digital signatures used by adware and riskware
- Protection routines used by specific applications



1.3. System Requirements

Dr.Web can be installed and run on a computer that meets the following minimum requirements:

Parameter	Requirement
CPU	An i686-compatible processor.
Free RAM	Minimum 100 MB of RAM.
Hard disk space	150 MB for Dr.Web components. Files created during installation will require additional space.
Operating system	<p>For 32-bit platforms:</p> <ul style="list-style-type: none">• Windows XP with Service Pack 2 or later• Windows Vista with Service Pack 2 or later• Windows 7• Windows 8• Windows 8.1• Windows 10 21H2 or earlier• Windows Server 2003 with Service Pack 1 or later• Windows Server 2008 <p>For 64-bit platforms:</p> <ul style="list-style-type: none">• Windows Vista with Service Pack 2 or later• Windows 7• Windows 8• Windows 8.1• Windows 10 21H2 or earlier• Windows 11• Windows Server 2008 with Service Pack 2 or later• Windows Server 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019• Windows Server 2022
Screen resolution	1024x768 or higher.



To ensure a correct operation of Dr.Web the following ports must be opened:

Purpose	Direction	Port numbers
To activate and renew the license	outgoing	443
To update (if the option to update using https is enabled)	outgoing	443
To update	outgoing	80
To connect to Dr.Web Cloud	outgoing	2075 (including UDP), 3010 (TCP), 3020 (TCP), 3030 (TCP), 3040 (TCP)

Other system requirements are similar to those for the corresponding operating system.



2. Installing, Restoring and Removing Dr.Web KATANA

Before installing Dr.Web KATANA, get familiar with [system requirements](#). In addition, it is recommended that you do the following:

- Install all critical updates released by Microsoft for the OS version used on your computer (they are available on the company update website at <https://support.microsoft.com/help/12373/windows-update-faq>). If the operating system is no longer supported, then upgrade to a newer operating system.
- Scan the file system with system utilities and remove the detected errors.
- Close all active applications.

2.1. Installation Procedure

There are two installation modes of Dr.Web anti-virus software:

- The background mode
- The usual mode

Usual installation

To start usual installation, do one of the following:

- If you have an executable file (`drweb-1.0-katana.exe`), run it.
- If you have an original disk containing installation package, insert the disk into the CD/DVD drive. If autorun is enabled, the installation will start automatically. If autorun is disabled, run the `autorun.exe` file of the installation kit manually. The window opens and displays the autorun menu. Click **Install**.

At any installation step, before the wizard starts copying files to your computer, you can do the following:

- Return to the previous step by clicking **Back**.
- Go to the next step by clicking **Next**.
- Abort installation by clicking **Exit**.

To install the program

1. If Dr.Web anti-virus is installed on your computer, the Installation Wizard informs you on incompatibility between Dr.Web and another anti-virus product and offers to remove it.



Before the installation starts, the Wizard checks if the installation file is the latest one. If a newer installation file exists, you will be offered to download it before the installation.



- At this step, you are prompted to connect to [Dr.Web cloud services](#) that allow anti-virus components to use the latest information on threats. The information is stored and updated on the Doctor Web servers in real-time mode. This option is enabled by default.

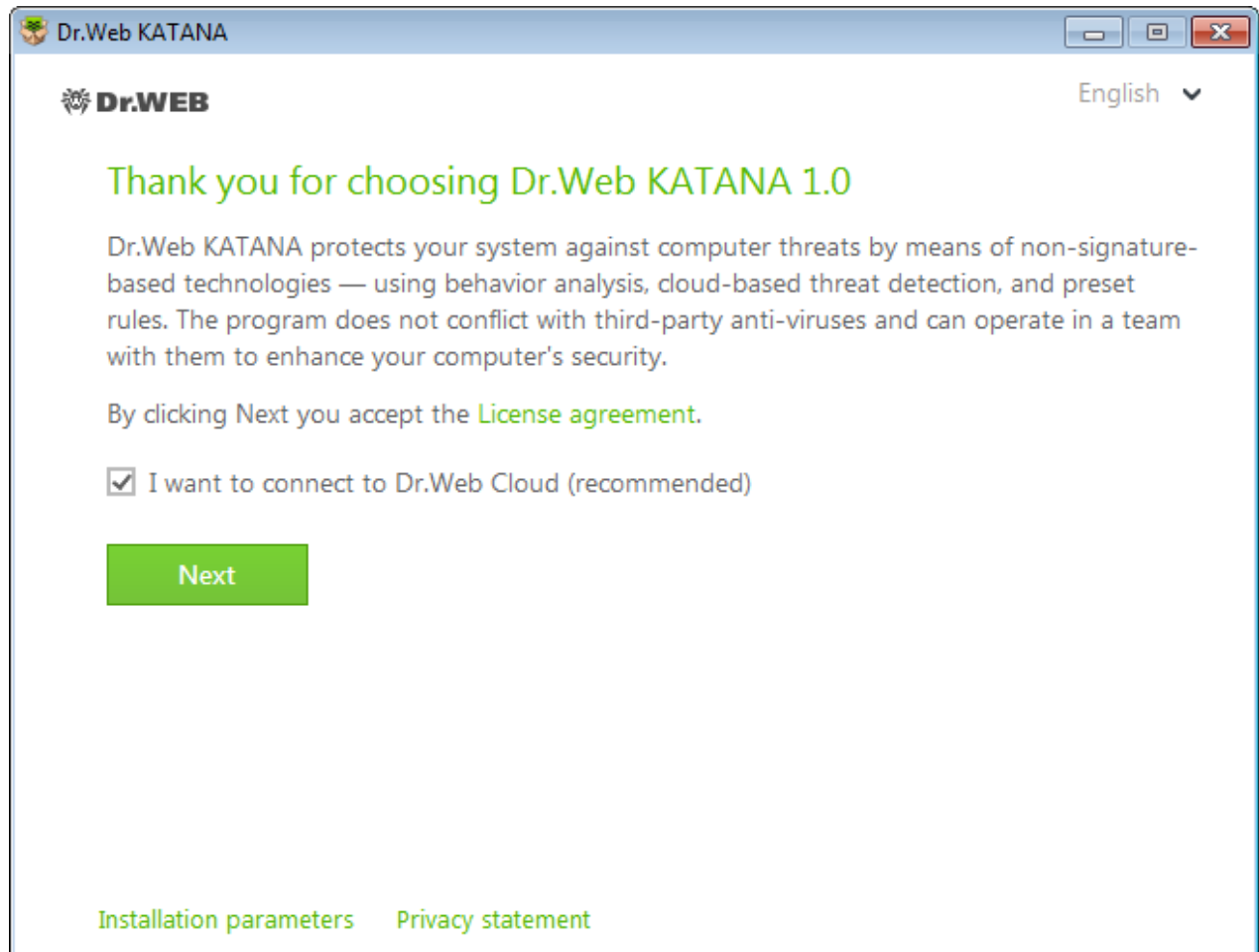


Figure 1. Installation Wizard

- If you want to use default installation settings, go to step 4. To select components you want to install, specify the installation path and configure other settings, click **Installation parameters**. The option is meant for experienced users.
 - On the first tab, you can change the installation path.
 - On the second tab, specify proxy server parameters if necessary.To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**.
- Click **Next**. Please note that by clicking the **Next** button you accept the terms of the License agreement.
- In the **Registration Wizard** window select one of the following options:
 - If a [key file](#) is present on the hard drive or removable media, select **Specify path to an available valid key file**. Click **Browse** and select the key file in the open window.



- If you want to receive a key file during the installation, select **Receive license during installation** and click **Install**.

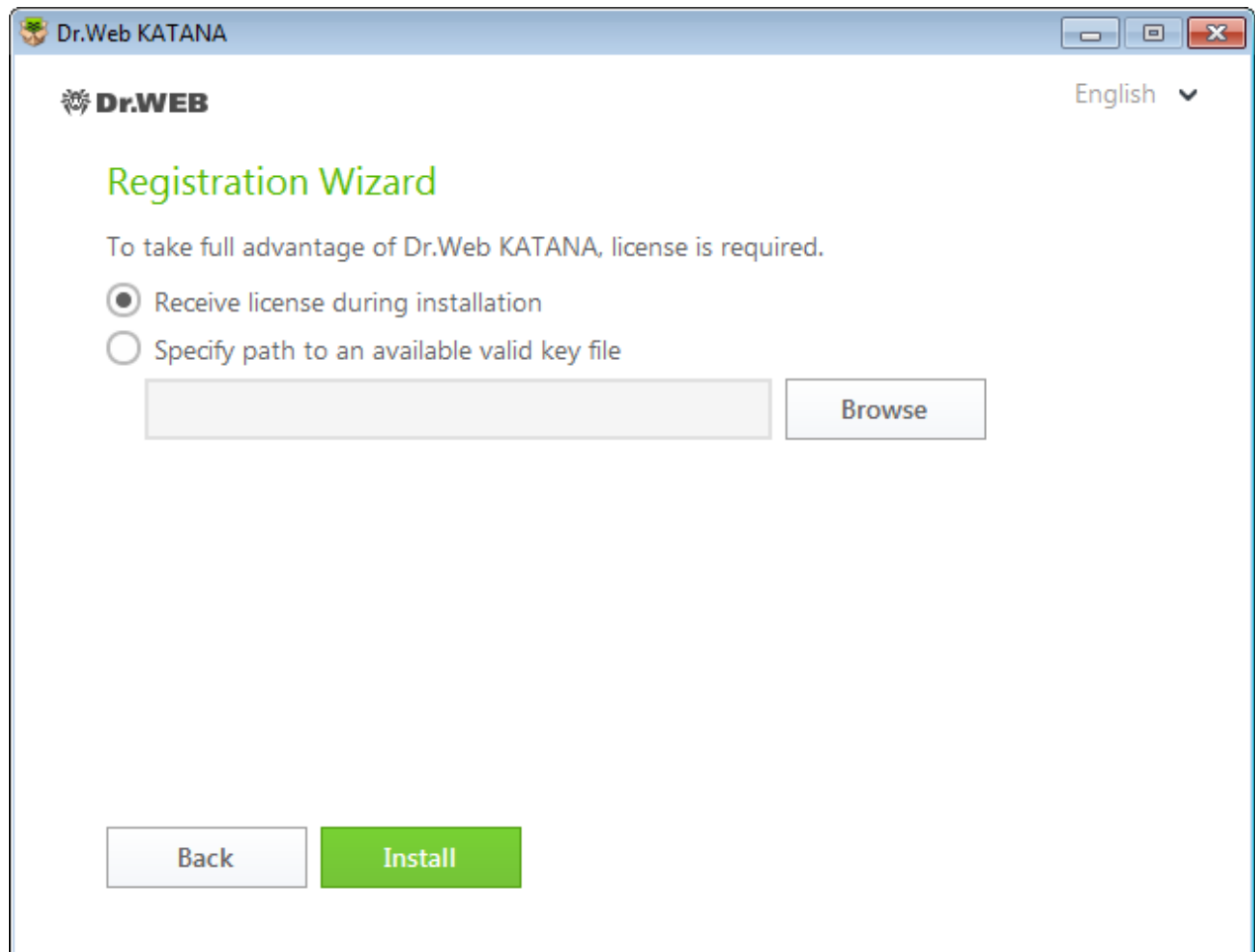


Figure 2. Registration wizard

Installation with command-line parameters

To install Dr.Web with command-line parameters, enter in the command line the executable file name with necessary parameters (they affect installation in the background mode, installation language, reboot after installation).

Parameter	Value
lang	Language used for the installation. The value of this parameter is language in ISO 639-1 format, e.g., /lang en.
reboot	Restart the computer automatically after installation is complete.
silent	Installation in the background mode.

For example, to start background installation of Dr.Web, execute the following command:

```
drweb-1.0-katana.exe /silent yes
```



2.2. Restoring and Removing Dr.Web KATANA

Restoring or removing Dr.Web components with standard Windows tools

1. To remove or restore Dr.Web KATANA, run the standard Windows uninstall tool.
2. In the list select the line with the program name.
 - To delete the program completely, click **Uninstall** and go to [step 5](#).
 - To restore Dr.Web, click **Change**. The window of the Restoring/Removing Wizard opens.

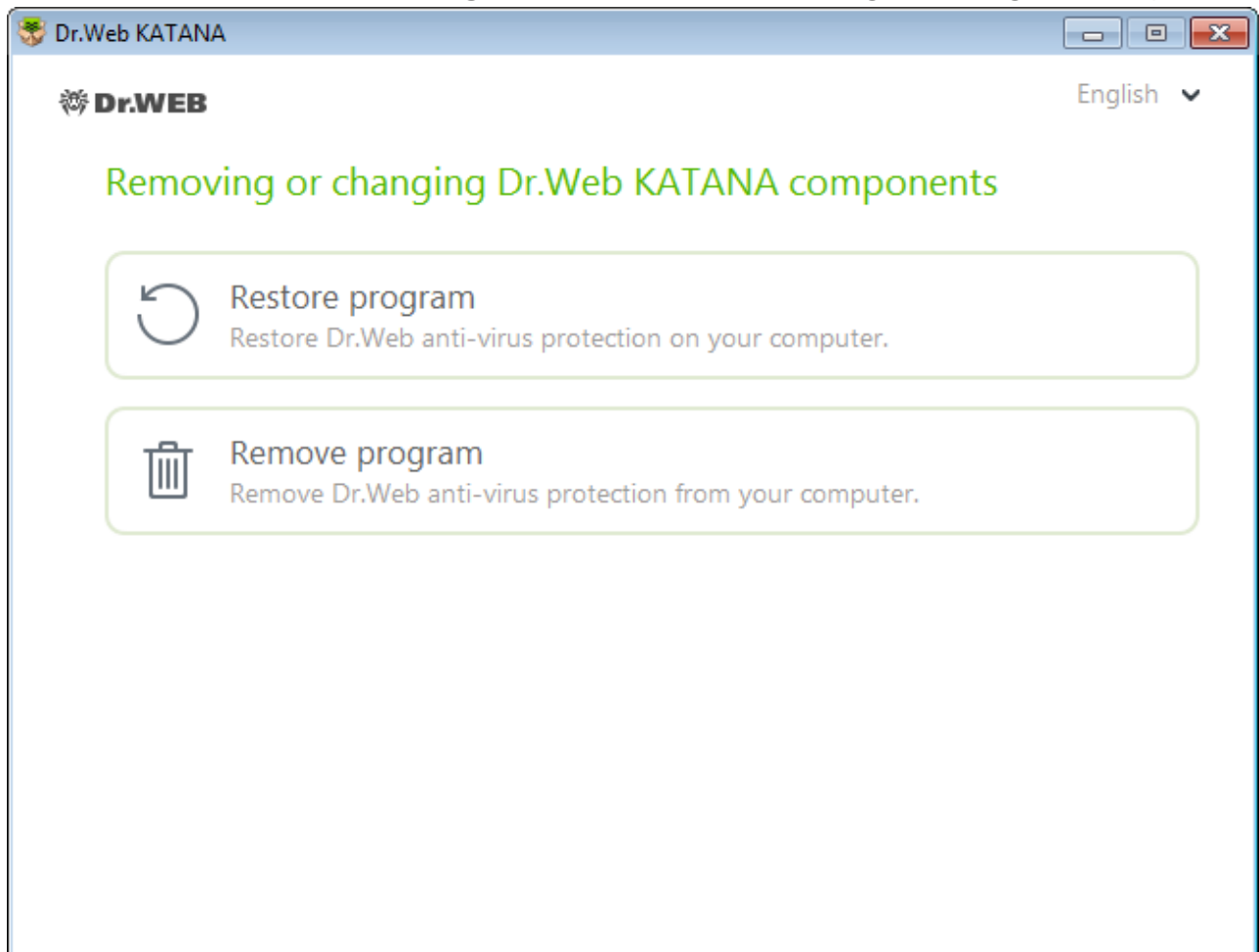


Figure3. Restoring/Removing wizard

3. To restore anti-virus protection on your computer, select **Restore program**. This function is applied in case when some of Dr.Web components have been corrupted.
4. To delete all installed components, select **Remove program**.
5. In the **Parameters to save** window, select check boxes of those components that you do not want to remove from your system. Saved objects and settings can be used by the program if it is installed again. Click **Next**.
6. In the next window, confirm deletion of Dr.Web by entering the displayed code and then click **Remove program**.
7. Restart the computer to complete the procedure of Dr.Web removal.



3. Licensing

To use Dr.Web for a long period of time, activate a license. You can purchase a license with the product, on the official Doctor Web [website](#) or through authorized partners. A license allows to take advantage of all product features during the whole period. Parameters of the license are set in accordance with the software license agreement.

If you want to evaluate the product before purchasing it, you can activate a trial version. It provides you with full functionality of the main components, but the period of validity is considerably restricted.



You can activate a trial version for the same computer no more than once a year.

A trial version is valid for 1 month. For that purpose, no serial number is required and no registration data is requested.

Key file

The user rights for Dr.Web are specified in the key file. Key files received during installation or within the product distribution kit are installed automatically.

The key file has the `.key` extension and contains the following information:

- List of licensed anti-virus components
- Licensed period for the product
- Availability of technical support for the user
- Other restrictions (for example, the number of remote computers allowed for simultaneous anti-virus scan)



By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.

If no valid key file is found, Dr.Web components are blocked.

A valid key file for Dr.Web satisfies the following criteria:

- License is not expired.
- Integrity of the key file is not violated.

If any of the conditions is violated, the key file becomes invalid.

It is recommended that you keep the key file until the license or the trial version expires.



A key file for a trial version activation can be used only on the computer where the registration procedure was run.

3.1. Activation Methods

You can activate your license in one of the following ways:

- Using [Registration Wizard](#) during installation or later
- Obtaining the key file during registration on the official Doctor Web [website](#)
- Specifying the path to the valid key file residing on your computer during installation or in the [Registration Wizard](#) window.

Reactivating license

You may need to reactivate a license or a trial version if the key file is lost.



When reactivating a license or a trial version, you receive the same key file as during the previous registration providing that the validity period is not expired.

When you reinstall the product or install it on several computers, if the license allows for that, you will be able to use the previously registered key file. Reactivation of the key file is not required.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact your [technical support](#) describing your problem in detail, stating your personal data input during the registration and the serial number. The key file will be send by our technical support to your email address.

3.2. Renewing License

In some situations, for example, when the license expires or characteristics of the protected system change, you may need to renew or extend the Dr.Web license. If so, you should change the current key file. Dr.Web supports hot license update without stopping or reinstalling the product.

To change the key file

1. To change your current license, open [Registration Wizard](#).
2. If the current key file is invalid, Dr.Web automatically switches to using the new key file.




3.3. Registration Wizard

SplDer Agent checks whether you have a [key file](#). If no key file is found, you are prompted to obtain a key file via the internet.

A key file can be obtained during the installation procedure. For this, select the **Receive license during installation** option [at step 5](#) of the installation procedure, and activation of a license or a trial version will start.

You can also obtain a key file by starting activation of a license or a demo period after the product is installed on your system. For that, do one of the following:

- Click the SplDer Agent icon  in the notification area and select **License**.
- The [License Manager](#) window opens. Click **Obtain new license** and select **via the Internet** in the drop-down list.

After activation is started, the Registration Wizard window opens.

To activate the license, you need to enter the registration serial number, supplied to you when purchasing Dr.Web.

To evaluate the program, you can activate a trial version for 1 month. For that purpose, no serial number is required and no registration data is requested.

The first window prompts you to select one of the following activation methods:

- activate license
- get demo
- purchase license

If you have a serial number for activation of a license, select **Activate license**. Enter the serial number and click **Next**. The [registration data entry](#) window opens.

If you do not have a serial number and want to evaluate functionality of the product, you can activate a demo period for 1 month by selecting **Get demo**. Click **Next**. A window with the [activation results](#) opens.

To purchase a license from Doctor Web online store, click **Purchase license**.

If you already have a valid key file, click **Other activation types**. In the open window, specify the file path.

Registration data entry

To register a license, enter personal data (your registration name and email address) and select the country from the drop-down list. All the listed fields are obligatory and must be filled in.

Click **Next**.




Activation results

If the activation procedure completes successfully, the corresponding message is displayed. Click **Finish** to proceed to updating the virus databases and other package files. This procedure does not require user intervention.

If activation failed, an error message displays. Click **Connection parameters** to adjust internet connection parameters or click **Repeat** to correct invalid data.






4. Getting Started



When Dr.Web is installed, the SplDer Agent icon  is displayed in the notification area.



If SplDer Agent is not running, select the Dr.Web application group on the Windows Start menu and then select SplDer Agent.

The SplDer Agent icon indicates the status of Dr.Web:

- —all necessary components are running and protect your computer.
- —Dr.Web self-protection or computer protection is disabled.
- —components are expected to start after the operating system startup process is complete, thus wait until the components start; or an error occurred while starting one of the main Dr.Web components, and your computer is at risk of virus infection. Check that you have a valid key file and, if required, [install](#) it.

The SplDer Agent menu  allows to manage and configure the main settings of Dr.Web. To open the menu, click the SplDer Agent icon  in the Windows notification area.

License. Opens [License Manager](#).

Update. Information on the current status of components. Launches the update.

Protection. Quick access to enabling or disabling preventive protection. Every time the preventive protection is enabled or disabled, the information is logged into Windows Event Viewer in **Application and Services Logs** → **Doctor Web**.

Settings . Opens a window with access to the settings.

Tools . Opens access to:

- [License Manager](#)
- [Quarantine Manager](#)
- [Support](#).

Help . Opens this help file.



5. Tools

To view the isolated files list or restore files from quarantine, go to [Quarantine Manager](#).

If you encounter any questions or problems while using Dr.Web, go to [Support](#).

5.1. License Manager

This window displays information on Dr.Web [licenses](#).

At the top of the window, you can find information about the license you are using.

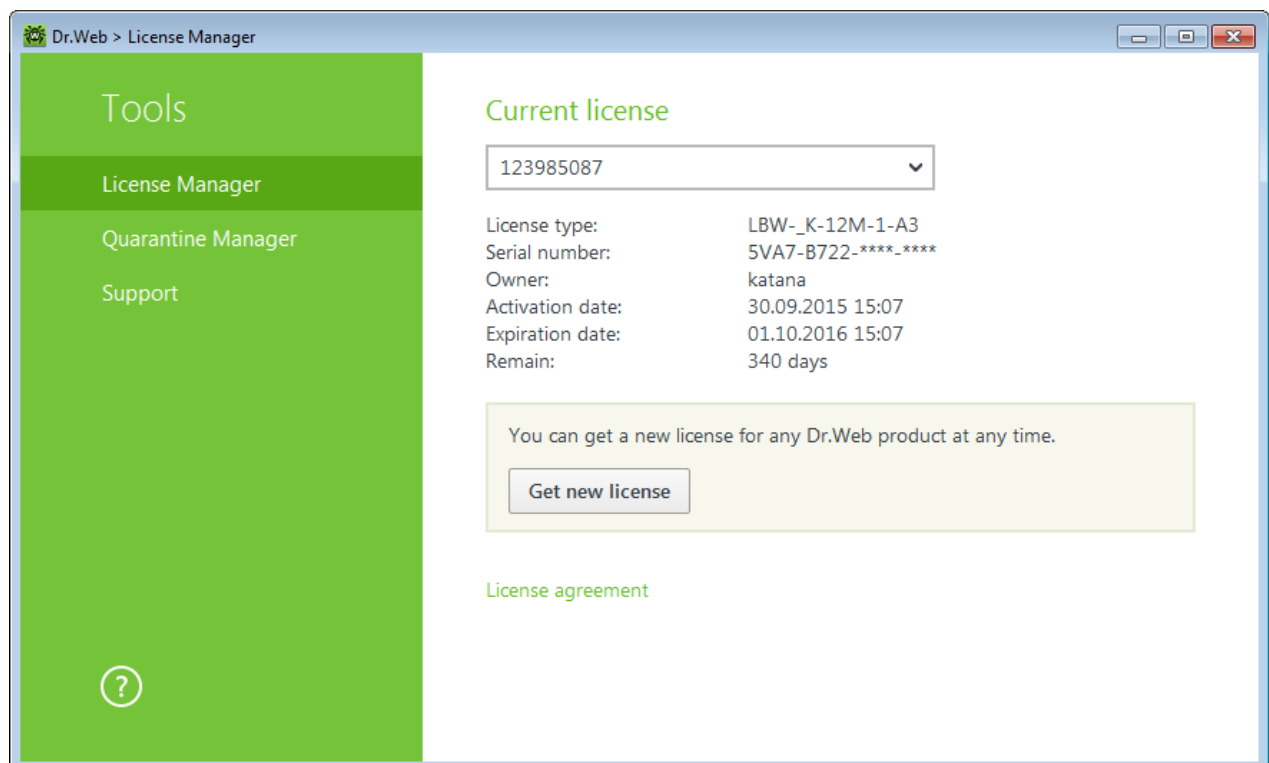



Figure 4. Current license information

The **Get new license** button opens the [Registration Wizard](#), where you can activate a new license, specify a path to another license key file, or purchase a license for any Dr.Web product.

Click  to delete the selected license by removing the corresponding key file.

To enable operation of Dr.Web, install a Dr.Web key file on the system. The key files received during installation or within the product distribution kit are installed automatically.



By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.



If no valid key file is found, Dr.Web components are blocked.

5.2. Quarantine Manager

Quarantine Manager is an instrument that allows you to manage isolated files. The quarantine contains backup copies of objects created before they are deleted by Dr.Web. The quarantine stores malicious programs that are identified by Dr.Web Process Heuristic as programs that modify user files (for example, encryption ransomware), and programs that inject their code into the processes of other applications.

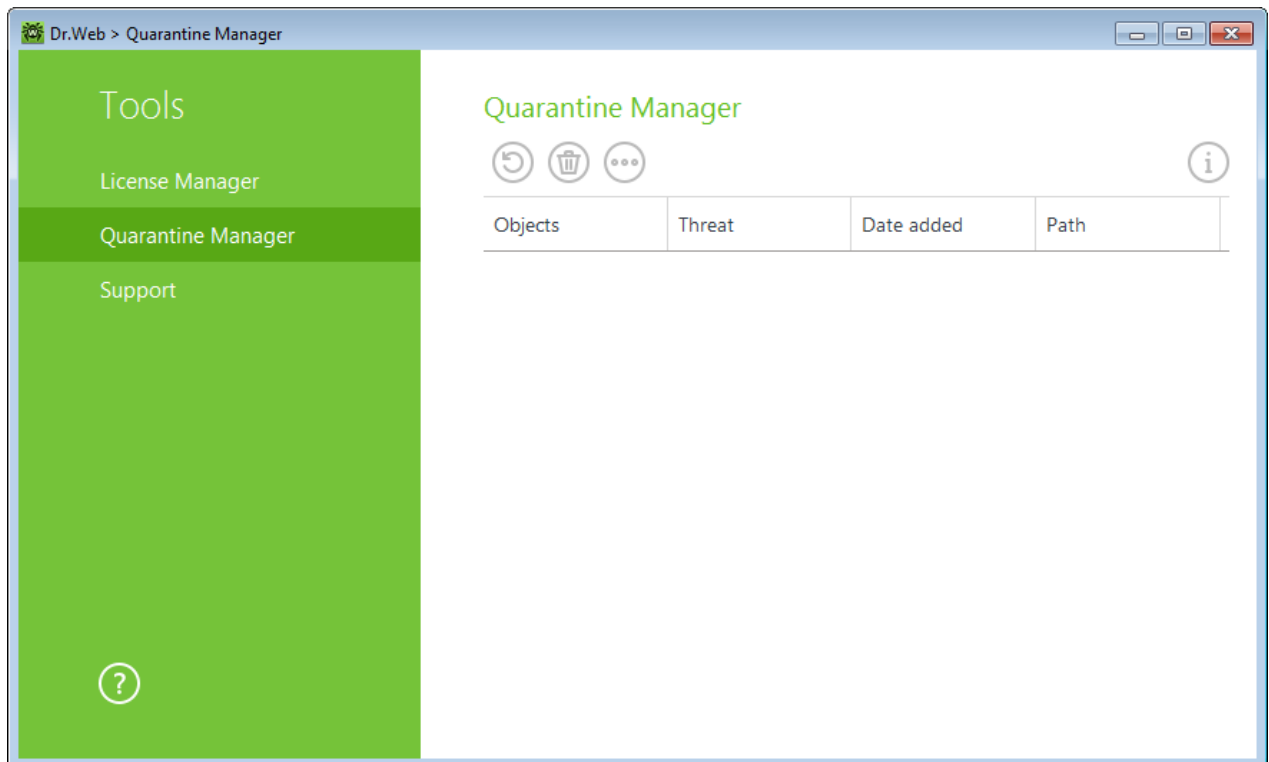


Figure 5. Objects in Quarantine

The central table lists the following information on quarantined objects:

- **Object**—name of the quarantined object.
- **Threat**—malware class of the object, which is assigned by Dr.Web when the object is quarantined.
- **Date added**—date and time when the object was moved to the Quarantine.
- **Path**—full path to the object before it was quarantined.

Managing quarantined objects

In the objects context menu, the following buttons are available:

- **Restore**—move one or several objects to the selected folder.



Use this option only when you are sure that the selected object is not harmful.

- **Delete**—delete one or several objects from quarantine and from the system.

You can also access these settings by right-clicking the selected object or several selected objects.

To delete all objects from quarantine at once, click and select **Delete all** from the drop-down list.

5.3. Support

This section provides information on the product version, components, the last update date, and the useful links that may help you to resolve issues or solve problems encountered while using Dr.Web.

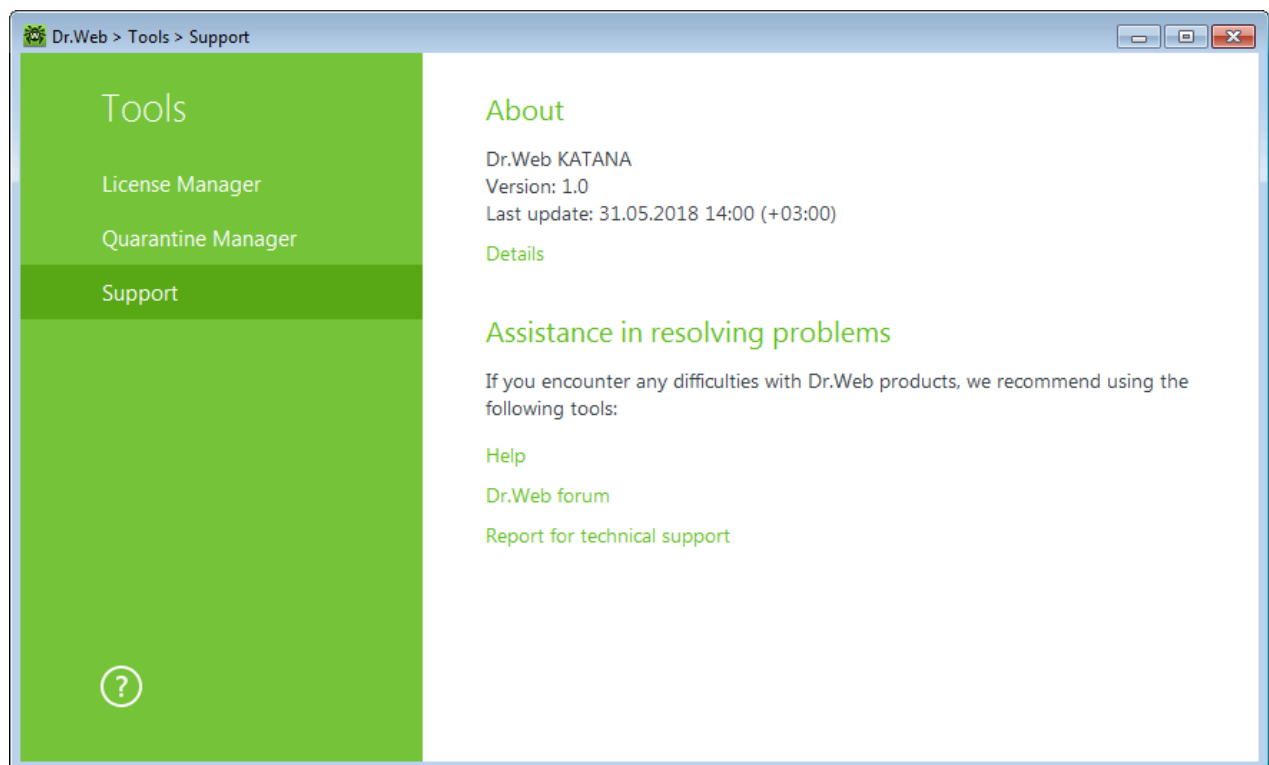


Figure 6. Product version information and support

In case of questions, we recommend using one of the following tools:

Help. Opens help file.

Dr.Web forum. Opens Dr.Web forum at <https://forum.drweb.com/>.

Report for technical support. Launches the wizard that will help you to [create a report](#) containing important information on your system configuration and computer working.



If you have not found a solution for the problem, you can request direct assistance from the Doctor Web technical support by filling in the form in the corresponding section of <https://support.drweb.com/>.

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

5.3.1. Report

When contacting Doctor Web technical support, you can generate a report on your operating system and Dr.Web operation.

The report will be stored as an archive in the Doctor Web subfolder of the %USERPROFILE% folder.

To generate a report, click the corresponding button. The report will include the following information:

1. Technical information about the operating system:
 - General information about your computer
 - Information on running processes
 - Information on scheduled tasks
 - Information on services, drivers
 - Information on default browser
 - Information on installed applications
 - Information on policies
 - Information on HOSTS file
 - Information on DNS servers
 - System event log
 - System directories
 - Registry branches
 - Winsock providers
 - Network connections
 - Dr.Watson logs
 - Performance index
2. Information on installed Dr.Web product:
 - Type and version of Dr.Web product
 - Information on installed components and Dr.Web modules
 - Information on settings and configuration parameters of Dr.Web product
 - License information



- Dr.Web Operation Logging

Information about Dr.Web anti-virus solutions is located in Event Viewer, in **Application and Services Logs** → **Doctor Web**



6. Update

To ensure the software algorithms being most up-to-date, Doctor Web provides you with regular updates, which are distributed via the internet.

Update start


During update, Dr.Web downloads and installs all updated files that correspond to your version of Dr.Web and upgrades Dr.Web when a newer version is released.



For Dr.Web to update, you need a connection to the internet.

All necessary parameters can be defined on the **Update** page of Dr.Web [main settings](#).

Start from the SpIDer Agent menu

Click the SpIDer Agent icon  and select **Update**. This opens information on update status as the date of last update. Start updating by clicking **Update**.

Start from the command line

Open the Dr.Web installation folder and run the `drwupsrv.exe` file. The list of command-line parameters can be found in [Appendix A](#).

Automatic start

If launched automatically, Dr.Web installs updates silently and logs all changes into the `dwupdater.log` file located in the `%allusersprofile%\Doctor Web\Logs\` folder.



After an update of executable files, drivers, or libraries, a program restart may be required. In such cases, the corresponding warning is displayed.



7. Settings

Open the SplDer Agent menu  and run **Settings** .

7.1. Main

On this page, you can select the program language, import and export settings.

Language

To set another program language, select it from the corresponding drop-down list. New languages are automatically added to the list. Thus, it contains all localization languages that are currently available for the Dr.Web graphical interface.

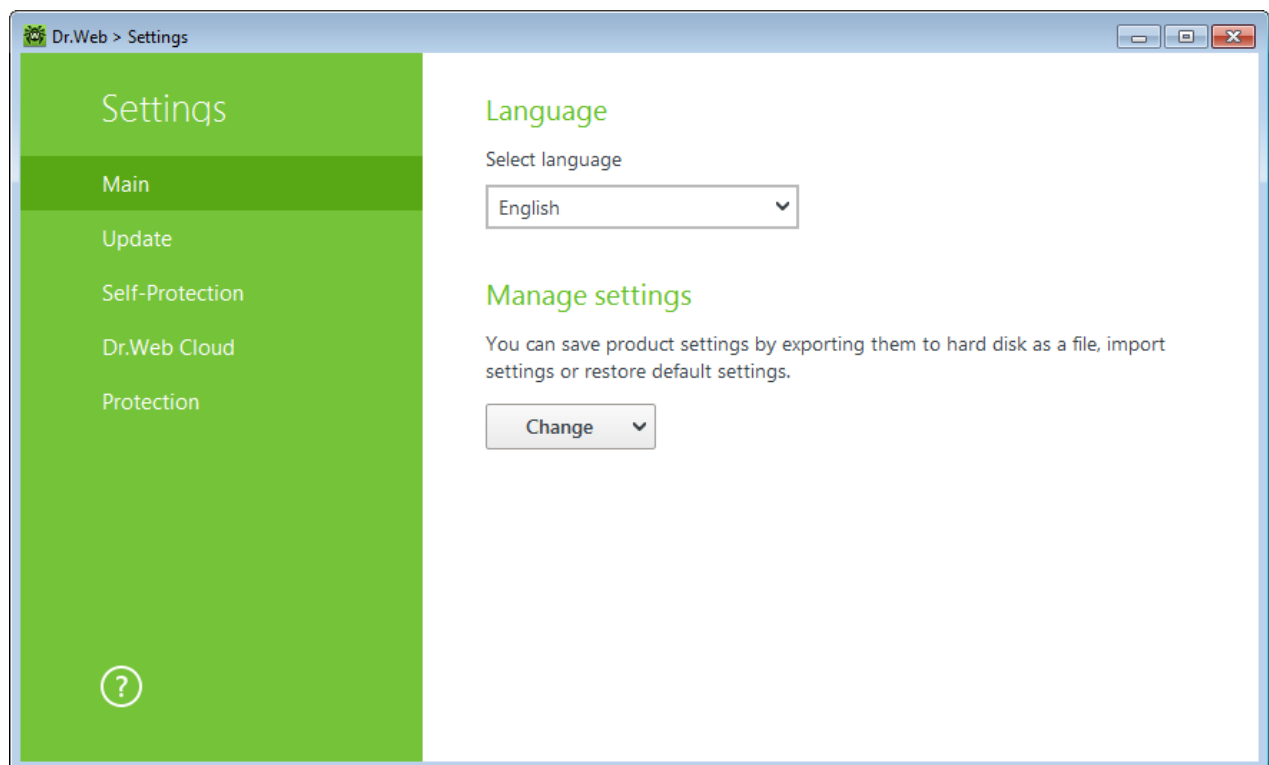


Figure 7. Main settings

Manage settings

To restore default settings, select **Reset settings** from the drop-down list.

If you want to use settings of Dr.Web that you already configured on another computer, select **Import** from the drop-down list.

If you want to use your settings on other computers, select **Export** from the drop-down list. Then apply them on the same page of another anti-virus.



7.2. Update

General update settings

Update frequency. Specify the frequency of update check. The default value (30 minutes) is optimal to keep information on threats up-to-date.

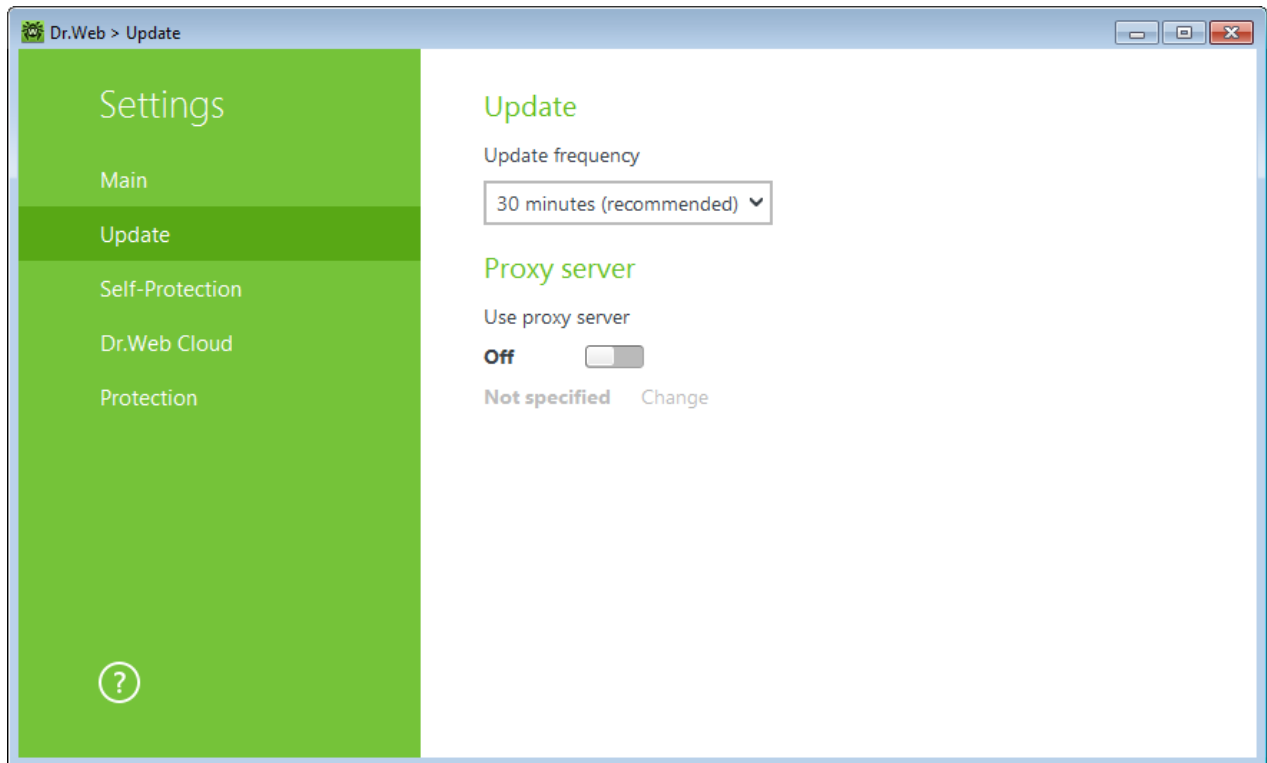


Figure 8. Update settings

Proxy server

By default, all components use direct connection mode. If necessary, you can enable use of a proxy server and specify its connection settings. Click **Change** to specify the following proxy server parameters:

Option	Description
Address	Specify the address of the proxy server.
Port	Specify the port of the proxy server.
User	Specify the username to use when connecting to the proxy server.
Password	Specify the password to use when connecting to the proxy server under the provided username.



Option	Description
Authorization type	Select an authorization type required to connect to the proxy server.

7.3. Self-Protection

Self-Protection Settings

On this page, you can configure Dr.Web self-protection of from unauthorized modification by anti-antivirus programs or from accidental damage. The **Enable Self-protection** option allows to protect Dr.Web files and processes from unauthorized access. It is not recommended to disable Self-protection.

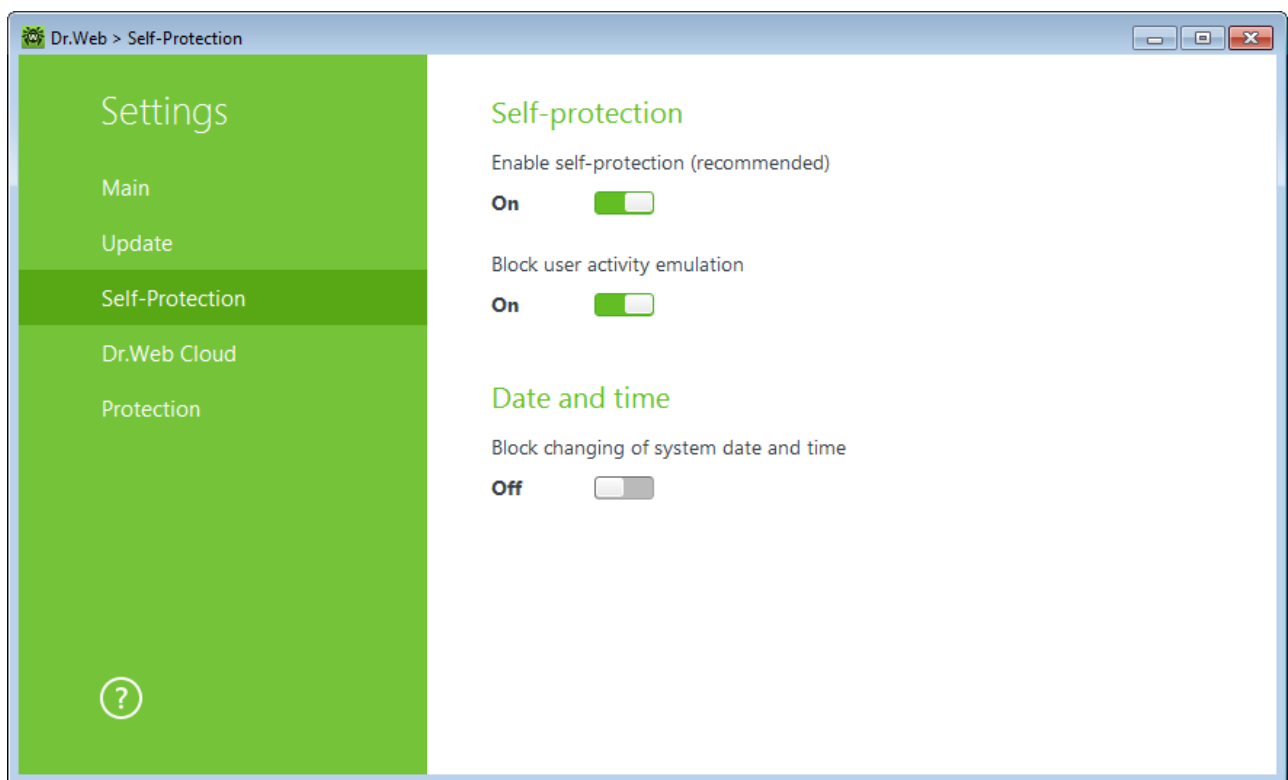


Figure 9. Dr.Web Self-Protection settings



If any problems occur during operation of defragmentation programs, disable self-protection temporary.

To rollback to a system restore point, disable self-protection.

The **Block user activity emulation** option allows to prevent any automatic changes in the Dr.Web operation, including execution of scripts that emulate user interaction with Dr.Web and are launched by the user.



Date and time

The **Block changing of system date and time** option allows to prevent manual and automatic changes of the system date and time as well as of the time zone. This restriction is set for all system users.

7.4. Dr.Web Cloud

On this page, you can connect to the Doctor Web cloud service and take part in Dr.Web quality improvement program.

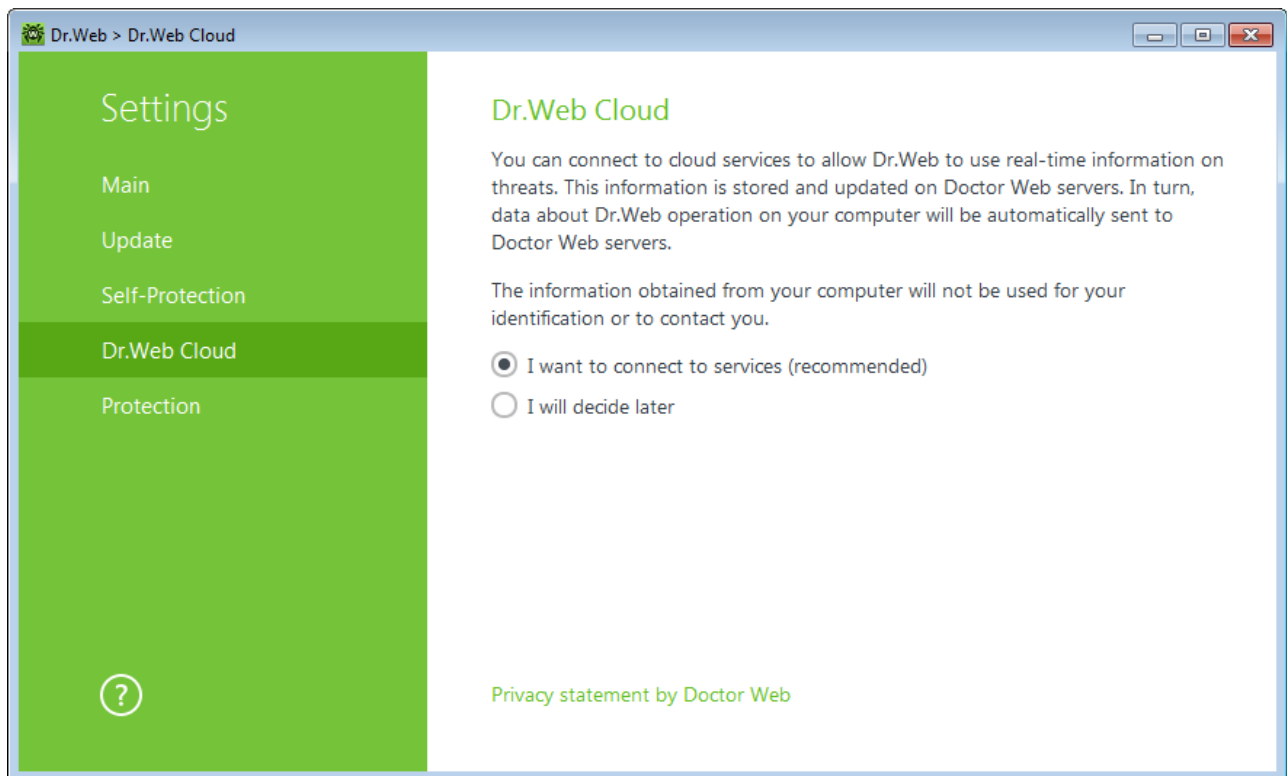


Figure 10. Connecting to Dr.Web Cloud

Cloud service

Dr.Web Cloud provides most recent information on threats which is updated on Doctor Web servers in the real-time mode and is used for anti-virus protection.

Software quality improvement program

If you participate in the software quality improvement program, impersonal data about Dr.Web operation on your computer will be periodically sent to Doctor Web servers. Received information is not used to identify or contact you.



Click the **Privacy statement by Doctor Web** link to look through a privacy statement on the Doctor Web official website.

7.5. Protection

On this page, you can configure Dr.Web reaction to such actions of other programs that can compromise security of your computer and select protection level against exploits.

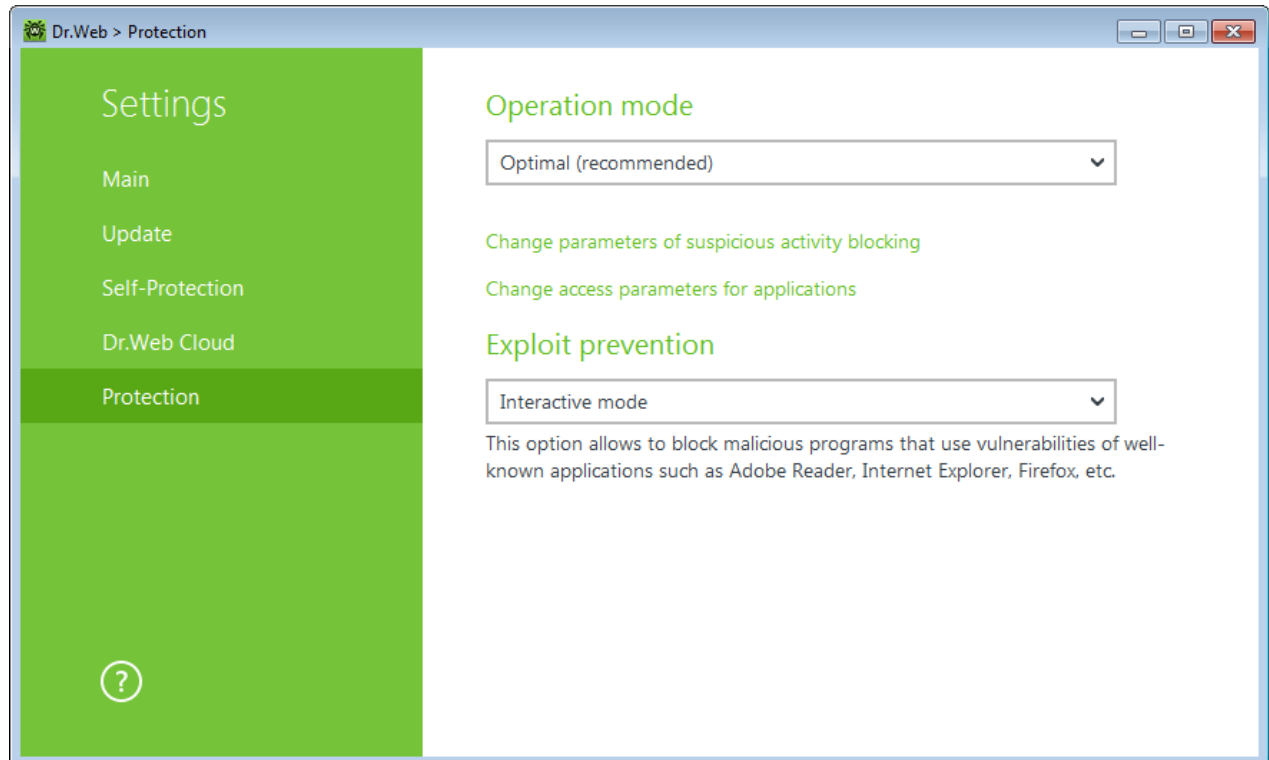



Figure 11. Selecting Protection operation mode

At that, you can configure a separate protection mode for particular applications or configure a general mode whose settings will be applied to all other processes.

To configure the general mode, select it from the **Operation mode** list or click **Change parameters of suspicious activity blocking**. As a result of the second action, a window opens providing you with details on each mode and editing options. All changes are saved in the **User** mode. In this window, you can also create a new profile for saving necessary settings.


To create a new profile

1. Click .
2. In the open window, enter a name for the new profile.
3. Look through default settings and, if necessary, edit them.

To configure preventive protection settings for particular applications, click **Change access parameters for applications**. In the open window, you can add a new rule or edit or delete an existing rule.



To add a rule

1. Click .
2. In the open window, click **Browse** and specify the executable path to the application.
3. Look through default settings and, if necessary, edit them.

To edit an existing rule, select it from the list and click .

To delete an existing rule, select it from the list and click .

Preventive protection level

In the default **Optimal** mode, Dr.Web disables automatic changes of system objects, whose modification explicitly signifies a malicious attempt to harm the operating system. It also blocks low-level access to the disk and protects the HOSTS file from modification.

If there is a high risk of your computer getting infected, you can increase protection by selecting the **Medium** mode. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.



Using this mode may lead to compatibility problems with legitimate software that uses the protected registry branches.

When required to have total control of access to critical Windows objects, you can select the **Paranoid** mode. In this mode, Dr.Web also provides you with the interactive control over driver loading and automatic running of programs.

With the **User-defined** mode, you can set a custom protection level for various objects.

Protected object	Description
Integrity of running applications	This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security.
Integrity of user files	This option allows detection of processes that modify user files with the known algorithm which indicates that the process may compromise computer security.
HOSTS file	The operating system uses the HOSTS file when connecting to the internet. Changes to this file may indicate virus infection.
Low level disk access	Block applications from writing on disks by sectors while avoiding the file system.



Protected object	Description
Drivers loading	Block applications from loading new or unknown drivers.
Critical Windows objects	<p>Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).</p> <p>Image File Execution Options:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options <p>User Drivers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Drivers32• Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers <p>Winlogon registry keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL <p>Winlogon notifiers:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify <p>Windows registry startup keys:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows NT\CurrentVersion\Windows, ApplInit_DLLs, LoadApplInit_DLLs, Load, Run, IconServiceLib <p>Executable file associations:</p> <ul style="list-style-type: none">• Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys)• Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) <p>Software Restriction Policies (SRP):</p> <ul style="list-style-type: none">• Software\Policies\Microsoft\Windows\Safer <p>Browser Helper Objects for Internet Explorer (BHO):</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects <p>Autorun of programs:</p> <ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Run• Software\Microsoft\Windows\CurrentVersion\RunOnce• Software\Microsoft\Windows\CurrentVersion\RunOnceEx• Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup• Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup• Software\Microsoft\Windows\CurrentVersion\RunServices• Software\Microsoft\Windows\CurrentVersion\RunServicesOnce <p>Autorun of policies:</p>



Protected object	Description
	<ul style="list-style-type: none">• Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Safe mode configuration: <ul style="list-style-type: none">• SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal• SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager parameters: <ul style="list-style-type: none">• System\ControlSetXXX\Control\Session Manager\SubSystems, Windows System services: <ul style="list-style-type: none">• System\CurrentControlSet\Services



If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), temporarily disable Preventive Protection.

Exploit prevention

This option allows to block malicious programs that use vulnerabilities of well-known applications. From the corresponding drop-down list, select the required level of protection.

Protection level	Description
Prevent unauthorized code from being executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be blocked automatically.
Interactive mode	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, Dr.Web will display the corresponding message. Read the information and select a suitable action.
Allow unauthorized code to be executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be allowed automatically.



8. Technical Support

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

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

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

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

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



9. Appendix A. Dr.Web Updater Command-line Parameters

Common options

Parameter	Description
-h [--help]	Show a short help message on how to use the program.
-v [--verbosity] arg	Log level. Can be one of the following: <code>error</code> (standard), <code>info</code> (extended), <code>debug</code> .
-d [--data-dir] arg	Folder where repository and settings are located.
--log-dir arg	Folder for storing the log file.
--log-file arg (=dwupdater.log)	Log file name.
-r [--repo-dir] arg	Repository folder (<code><data_dir>/repo</code> by default).
-t [--trace]	Enable tracing.
-c [--command] arg (=update)	Command to execute: <code>getversions</code> , <code>getcomponents</code> , <code>update</code> , <code>uninstall</code> , <code>exec</code> , <code>keyupdate</code> , and <code>download</code> .
-z [--zone] arg	Zones that are to be used instead of those specified in the configuration file.

update command parameters

Parameter	Description
-p [--product] arg	Product name. If specified, only this product will be updated. If neither a product nor certain components are specified, all products will be updated. If certain components are specified, only they will be updated.
-n [--component] arg	Components that are to be updated to the specified version. Format: <code><name></code> , <code><target revision></code> .
-x [--selfrestart] arg (=yes)	Reboot after an update of Dr.Web Updater. Default value is <code>yes</code> . If the value is set to <code>no</code> , notification that reboot is required will appear.
--geo-update	Get the list of IP addresses from <code>update.drweb.com</code> before updating.
--type arg (=normal)	Can be one of the following: <ul style="list-style-type: none">• <code>reset-all</code>—forced update of all components• <code>reset-failed</code>—reset revision for damaged components



Parameter	Description
	<ul style="list-style-type: none">• <code>normal-failed</code>—try to update all components including damaged from the current revision to the newest or specified• <code>update-revision</code>—try to update all components of the current revision to the newest if exists• <code>normal</code>—update all components
<code>-g [--proxy] arg</code>	Proxy server for updating <code><address>:<port></code> .
<code>-u [--user] arg</code>	Username for proxy server.
<code>-k [--password] arg</code>	Password for proxy server.
<code>--param arg</code>	Pass additional parameters to the script. Format: <code><name>: <value></code> .
<code>-l [--progress-to-console]</code>	Print information about downloading and script execution to the console.

exec command parameters

Parameter	Description
<code>-s [--script] arg</code>	Execute this script.
<code>-f [--func] arg</code>	Execute this function in the script.
<code>-p [--param] arg</code>	Pass additional parameters to the script. Format: <code><name>: <value></code> .
<code>-l [--progress-to-console]</code>	Print information about script execution to the console.

getcomponents command parameters

Parameter	Description
<code>-s [--version] arg</code>	Version number.
<code>-p [--product] arg</code>	Specify the product to get the list of components that are included in this product. If the product is not specified, all components of this version will be listed.



getrevisions command parameters

Parameter	Description
-s [--version] arg	Version number.
-n [--component] arg	Component name.

uninstall command parameters

Parameter	Description
-n [--component] arg	Name of the component that is to be uninstalled.
-l [--progress-to-console]	Print information about command execution to the console.
--param arg	Pass additional parameters to the script. Format: <i><name></i> : <i><value></i> .
-e [--add-to-exclude]	Components to be removed. Update of this components will not be performed.

keyupdate command parameters

Parameter	Description
-m [--md5] arg	MD5 hash of the previous key file.
-o [--output] arg	Output file name to store new key.
-b [--backup]	Backup of an old key file if exists.
-g [--proxy] arg	Proxy server for updating <i><address></i> : <i><port></i> .
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-l [--progress-to-console]	Print information about downloading of the key file to the console.

download command parameters

Parameter	Description
--zones arg	Zone description file.



Parameter	Description
--key-dir arg	Folder where the key file is located.
-l [--progress-to-console]	Print information about command execution to the console.
-g [--proxy] arg	Proxy server for updating <address>:<port>.
-u [--user] arg	Username for proxy server.
-k [--password] arg	Password for proxy server.
-s [--version] arg	Version number.
-p [--product] arg	Name of the product to download.

