



User Manual



© 2021 Doctor Web. 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 CureIt!
User Manual
9/23/2021

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. Conventions	5
2. About Product	6
2.1. System Requirements	7
2.2. Testing Your Anti-Virus	8
2.3. Detection Methods	8
2.4. Sending Statistics	10
3. Quick Start	11
3.1. Dr.Web CureIt! Update	11
3.2. Express Scan	12
3.3. Quarantine Manager	15
4. Advanced Options	17
4.1. Custom Scan	17
4.2. Configuring Threat Neutralization	20
4.3. Configuring Scanning	21
4.3.1. Main Tab	21
4.3.2. Actions Tab	22
4.3.3. Exclusions Tab	24
4.3.4. Log Tab	25
4.4. Launching From Command Line	26



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.



2. About Product

Dr.Web CureIt! is an anti-virus scanner based on Dr.Web Scanning Engine, the standard virus scanning engine of Dr.Web products. Although Dr.Web CureIt! has limited performance capabilities in comparison to Dr.Web Anti-virus for Windows (no resident monitor, no command line scanner, no updater, etc.), it is able to effectively scan the system and perform necessary actions for detected threats.

You can use Dr.Web CureIt! free of charge to scan your personal computer. However, a license is required for any commercial use of Dr.Web CureIt!. To learn more about licensing and purchasing the product, visit the Dr.Web CureIt! [official website](#).

Dr.Web CureIt! detects and neutralizes the following types of malicious programs:

- worms;
- viruses;
- trojans;
- rootkits;
- spyware;
- dialers;
- adware;
- hacktools;
- jokes;
- riskware.

Dr.Web CureIt! is an ideal solution for situations when installation of an anti-virus is impossible due to virus activity or some other reason. It does not require installation, operates under Windows® (from Microsoft Windows XP up to Microsoft Windows 11) and Windows Server® operating systems for 32 or 64-bit platforms and is constantly supplemented with the latest Dr.Web virus databases to ensure its effectiveness against all virus threats and other malicious programs. It also automatically detects the language used by your operating system. If your language is not supported, Dr.Web CureIt! will use English by default.

During scans Dr.Web CureIt! sends [general information](#) on your computer and its state of information security to Doctor Web. If you use Dr.Web CureIt! Commercial Edition, you can deny statistics gathering.



To use Dr.Web CureIt! Free Edition, you need to have root privileges and connection to the internet.



2.1. System Requirements

To use Dr.Web CureIt!, your computer should meet the following requirements:

Specification	Requirement
OS	<p>For 32-bit platforms:</p> <ul style="list-style-type: none">• Windows XP Service Pack 2 or later;• Windows Vista Service Pack 2 or later;• Windows 7 Service Pack 1 or later;• Windows 8;• Windows 8.1;• Windows 10;• Windows Server 2003 Service Pack 1;• Windows Server 2008 Service Pack 2 or later. <p>For 64-bit platforms:</p> <ul style="list-style-type: none">• Windows Vista Service Pack 2 or later;• Windows 7 Service Pack 1 or later;• Windows 8;• Windows 8.1;• Windows 10;• Windows 11;• Windows Server 2008 Service Pack 2 or later;• Windows Server 2008 R2 Service Pack 1 or later;• Windows Server 2012;• Windows Server 2012 R2;• Windows Server 2016;• Windows Server 2019.
Hard disk space	160 MB of disk space.
Free RAM	Minimum 360 MB of RAM.
CPU	i686-compatible processor and SSE2 instruction set.



Since Microsoft has stopped supporting SHA-1 hashing algorithm, make sure that your operating system supports SHA-256 hashing algorithm before installing Dr.Web CureIt! on Windows Vista or Windows 7, Windows Server 2008 or Windows Server 2008 R2. To do so, install all the recommended updates listed in Windows Update section. For a detailed information, visit [Doctor Web official website](#).



2.2. Testing Your Anti-Virus

You can test Dr. Web CureIt! functionality with the help of a test file EICAR—European Institute for Computer Anti-Virus Research.

For this purpose, you can use a standard `test.com` program. This program was designed in a way that users could test how a newly-installed anti-virus tool reacts when it detects a virus—without compromising security of their computers. Although the `test.com` program is not actually a virus, it is treated by the majority of anti-viruses as if it were a virus. On detection of this "virus", Dr.Web CureIt! reports the following: EICAR Test File (Not a Virus!). Other anti-virus tools alert users in a similar way.

The `test.com` program is a 68-byte COM-file that prints the following line on the console when executed: EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

The `test.com` file contains only textual characters that form the following string:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To get your own test file with the "virus", create a new text file with this line and save it as `test.com`.

2.3. Detection Methods

Doctor Web anti-virus solutions simultaneously use several methods to detect malicious software, which allows to thoroughly check suspicious objects.

Signature analysis

Scanning begins with signature analysis which is performed by comparing segments of code in a scanned file to known virus signatures. *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, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. This helps to reassure correct matching and neutralizing malicious objects. Entry structure of Dr.Web virus databases allows to detect not just specific viruses, but whole classes of threats.

Origins Tracing

After signature analysis is completed, Dr.Web uses a unique Origins Tracing method to detect new and modified viruses, which use known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition, Origins Tracing technology allows to considerably reduce the number of



false triggering of heuristics analyzer. Objects detected through Origins Tracing algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

Technology of program code emulation is used to detect polymorphic and encrypted viruses. It's applied when search through signature checksums is impossible, or is very difficult to perform due to the impossibility of building secure signatures. The method simulates execution of an analyzed code by an *emulator*—a programming model of a processor and runtime environment. The emulator operates with a 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 an infected file, emulation results in a decrypted virus body, which is then easily determined by searching through signature checksums.

Heuristic analysis

Detection method used by the heuristics analyzer is based on *heuristics*—assumptions based on experience—about certain features (attributes) than might be typical for a malicious or a secure executable code. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if a corresponding attribute is indicative of a malicious code or negative if the attribute is not typical for a computer threat. Based on a sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. If this probability threshold is exceeded, the heuristic analyzer concludes that the analyzed object is probably infected with an unknown virus.

The heuristics analyzer also uses the FLY-CODE technology—a versatile algorithm for extracting files. The technology allows to make heuristic assumptions about the presence of malicious objects in files compressed not only by the 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 a characteristic way, in which pieces of code are arranged inside a file; thus, one database entry allows to identify a substantial portion of threats packed with the same polymorphous packager.

Like any system designed to check hypotheses 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 above-mentioned checks, Dr.Web anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web anti-virus laboratory discover new threats, update for virus signatures, behavior characteristics and attributes is issued. In some cases updates can be issued several times per hour.



2.4. Sending Statistics

To obtain data on overall information security state in the world and to improve Dr.Web products with the help of this data, Dr.Web CureIt! offers to send anonymous statistics to the Doctor Web servers while it scans your system. Statistical data is posted during scanning and contains only the following information:

- CPU details including processor name, technical description, current and maximum speed, number of processor cores, and number of logical processors;
- RAM details including amount of physical and virtual memory both total and available at the time of scanning;
- operating system parameters including operating system name, version, build number, installed service packs, boot mode, type of an account (user or root), and locale settings;
- information on installed anti-virus, anti-spy, and firewall software;
- information on each detected threat including threat name and type, name and type of an infected object, action applied to it, and a hash sum of an infected file when necessary;
- summary information about a scan including scanning completion time, number of scanned files and objects, number of suspicious objects, and number of detected threats per type;
- summary information about applied actions including number of unmodified objects as well as number of cured, deleted, moved, renamed, and ignored objects.

You can read Doctor Web privacy policy on the on the official website at <https://company.drweb.com/policy>.



3. Quick Start

Dr.Web CureIt! scans boot sectors, random access memory (RAM), and both separate files and objects enclosed within complex objects (archives, e-mail attachments, file containers). During scanning, Dr.Web CureIt! uses all [detection methods](#).



License agreement of Dr.Web CureIt! Free Edition does not allow scanning of email files.

By default, Dr.Web CureIt! does not check archived files. You can enable scanning this option in Dr.Web CureIt! [settings](#).

Dr.Web CureIt! just informs you when a threat is detected. Information on scan results is displayed in a table where you can select a necessary action. You can either apply default actions to all the detected threats at a time or you can select a necessary action for individual objects.

Default settings are optimal for most cases. However, if necessary, you can change them in Dr.Web CureIt! [settings](#). Please note that you can set a custom action for an individual object after a scan is completed, but general settings for neutralizing a particular type of threats should be configured before you start a scan.



During scans, Dr.Web CureIt! sends [general information](#) on your computer and its state of information security to Doctor Web. If you use Dr.Web CureIt! Commercial Edition, you can deny statistics gathering.

Display language

To select display language, click **Language**  on the toolbar and then select the necessary language.

3.1. Dr.Web CureIt! Update

Dr.Web CureIt! does not contain an automatic updating module, therefore it remains fully efficient only until the next database update (which occurs approximately every hour). After that, to ensure anti-virus operation efficiency, download the latest version of Dr.Web CureIt!. You can find the latest Dr.Web CureIt! version on Dr.Web CureIt! [official website](#). The latest version of Dr.Web CureIt! is supplied with the latest virus databases and an advanced virus detection engine.

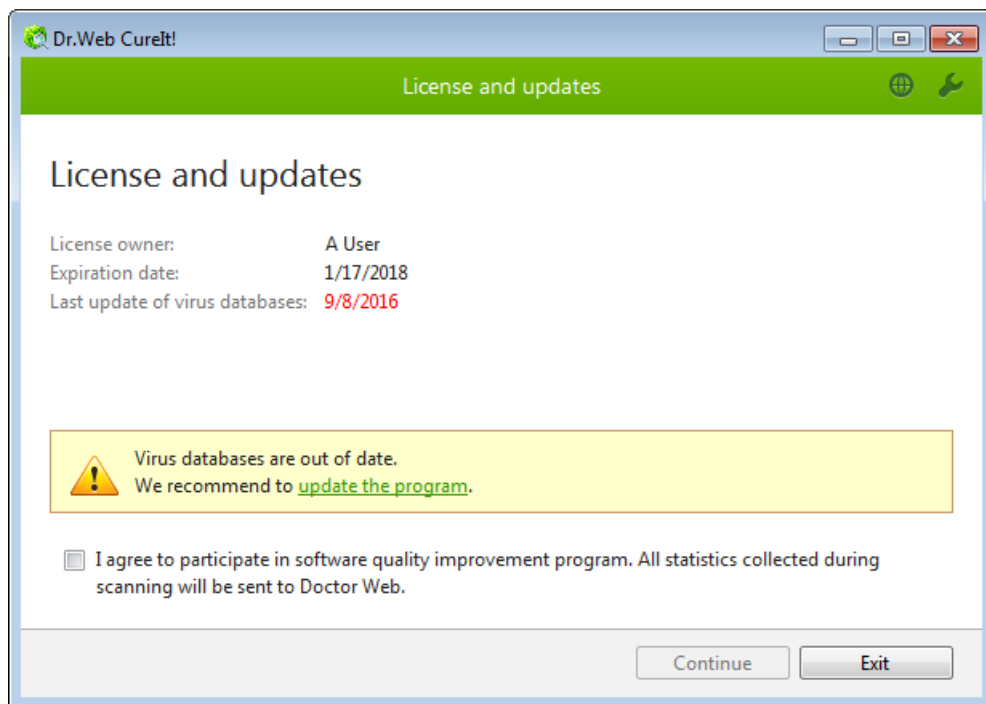
To download the latest version of Dr.Web CureIt!

1. Run Dr.Web CureIt!.



2. If Dr.Web CureIt! is out of date, the first window **License and updates** will display a notification. To update, click **Update the program** in the notification area.

This opens Dr.Web CureIt! official website in your default internet browser where you can download the latest version of Dr.Web CureIt!.



Picture 1. Updating Dr.Web.

3.2. Express Scan

Dr.Web CureIt! provides a pre-installed template for scanning the most vulnerable objects of your operating system.

In this mode, the following objects are scanned:

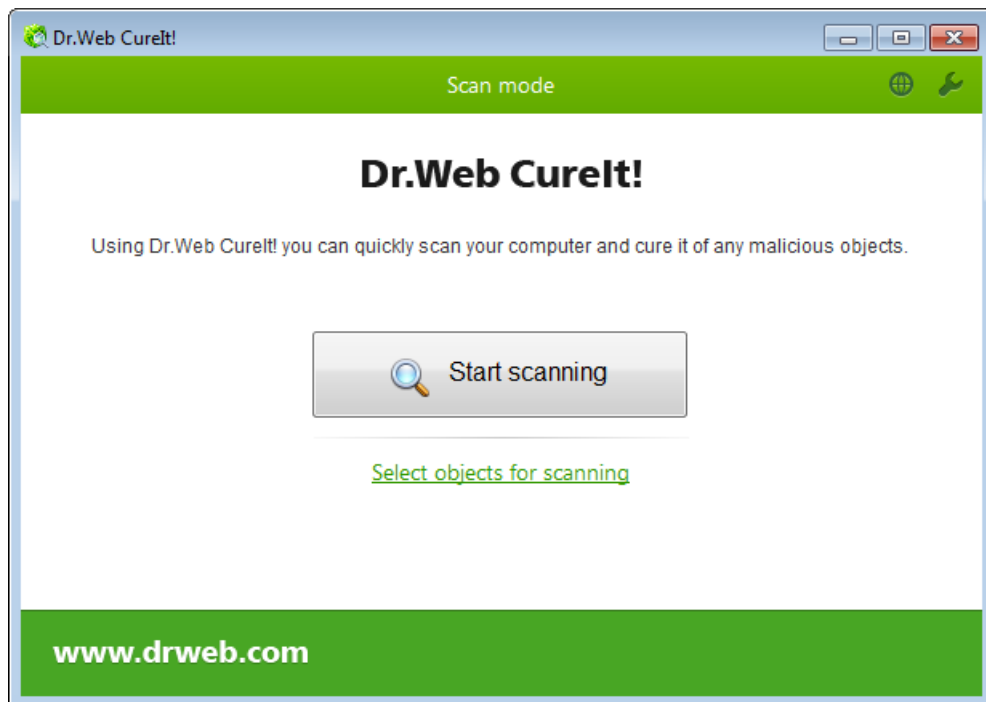
- random access memory;
- boot sectors of all disks;
- root folder on boot disks;
- root folder on the disk where Windows is installed;
- Windows system folder;
- My documents folder;
- temporary system folder;
- user's temporary folder;
- rootkits.

If a more flexible configuration of anti-virus scanning is required, you can run a [custom scan](#).



To run express scan

1. Run Dr.Web CureIt!.
2. In the **License and updates** window, read the conditions of [statistics gathering](#). Click **Continue**.
3. In the scan type selection window, click **Start scanning**.



Picture 2. Selecting scan mode Dr.Web.

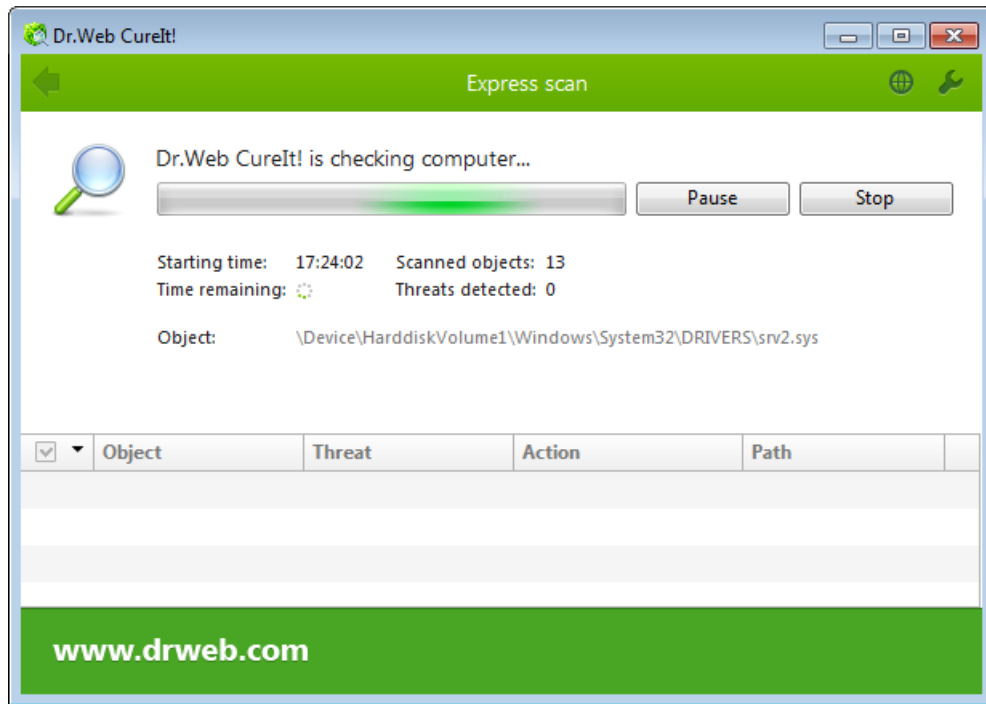
4. During scanning, Dr.Web CureIt! displays general information on scan progress and lists detected threats.

To manage scanning process, use the following options:

- To suspend scanning, click **Pause**.
- To start scanning again after a pause, click **Resume**.
- To terminate scanning, click **Stop**.

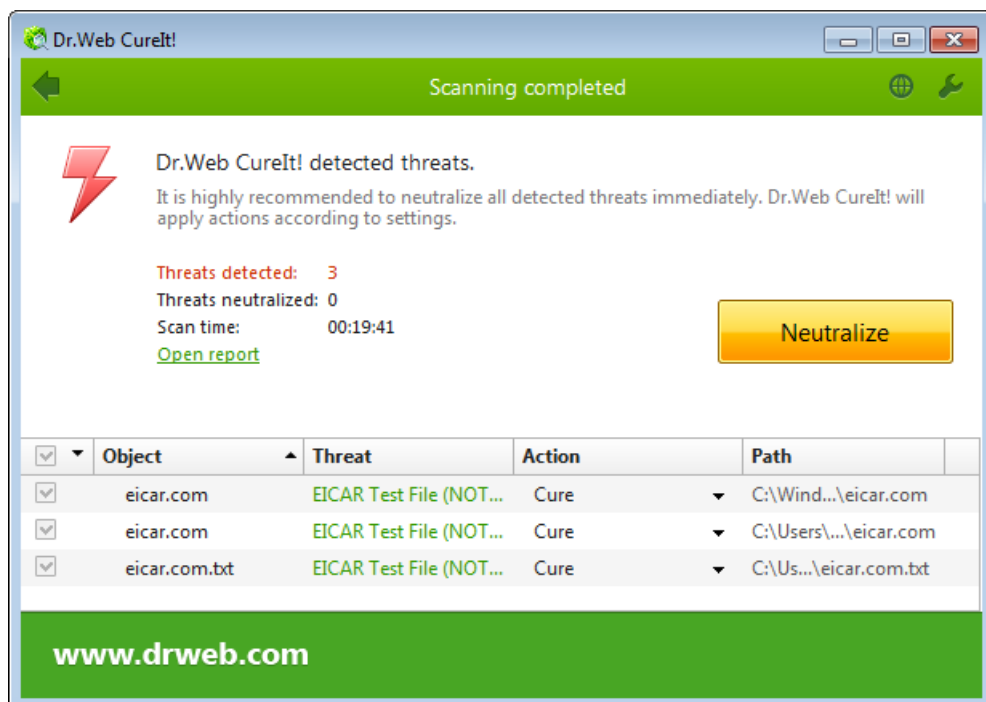


The **Pause** button is not available while processes and RAM are being scanned.



Picture 3. Express scan Dr.Web.

5. Once scanning is complete, Dr.Web CureIt! displays detailed information on detected threats. Review scan results. If necessary, you can also review a [scanning log](#) by clicking **Open report**.



Picture 4. Express scan results Dr.Web.

If viruses or other threats were detected, you need to neutralize them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can [select](#) custom actions for particular threats.

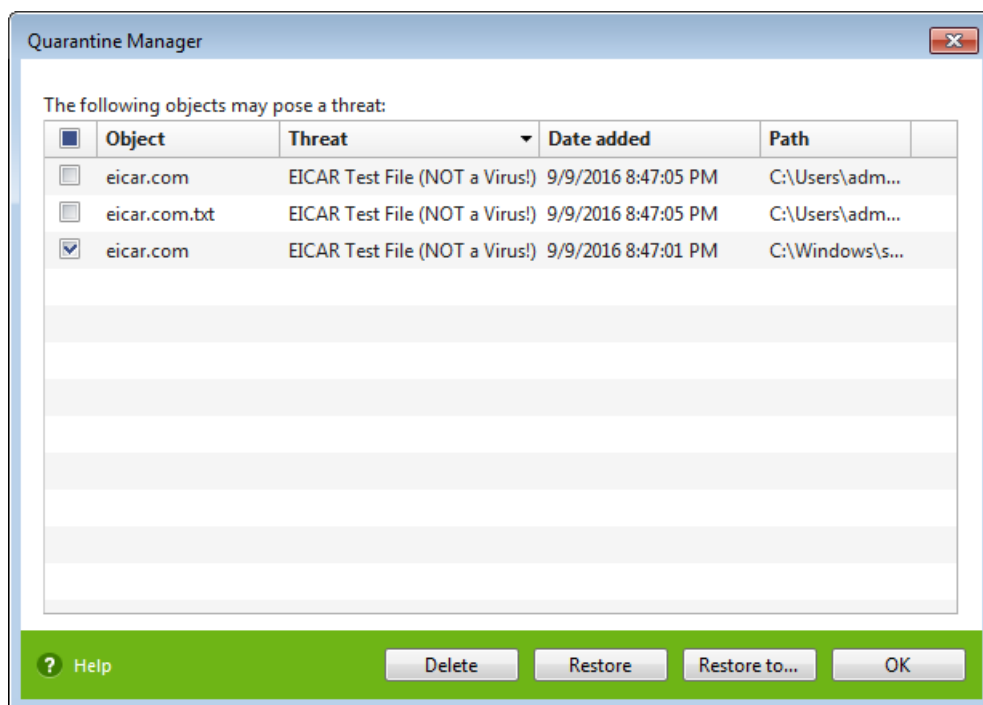


3.3. Quarantine Manager

Quarantine Manager window displays content of Dr.Web CureIt! Quarantine where suspicious files and file backups are kept.

Quarantine is stored in %USERPROFILE%\Doctor Web\DrWeb CureIt! Quarantine. Infected objects are moved to a corresponding subfolder and then, unless the objects are located on a removable drive, quarantined objects are encrypted.

To open Quarantine Manager, in the Dr.Web CureIt! toolbar, click **Preferences**  and select **Quarantine Manager**.



Picture 5. Quarantine Manager Dr.Web.

A table in the center of the window lists the following information on quarantined objects:

- **Object**—name of a quarantined object.
- **Threat**—type of a malware, which is assigned by Dr.Web CureIt! when an object is quarantined.
- **Date added**—date and time when an object was moved to quarantine.
- **Path**—full path to where an object was located before being quarantined.



Users can only view those quarantined files, to which they have access to.

To view hidden objects, run Dr.Web CureIt! under an account with root privileges.



Quarantine window provides the following buttons:

- **Restore**—remove selected files from Quarantine and restore them to their original location (restore files with the same name and to the same folder they were located in before being moved to Quarantine).
- **Restore to**—remove selected files from Quarantine with a specified name to a specified folder.



Use this option only when you are sure that selected files are not harmful.

- **Delete**—delete selected files from Quarantine and from the system.

To apply actions to multiple files at a time, select checkboxes next to necessary files and then select the action.



4. Advanced Options

In most cases, express scan is enough to neutralize threats on your computer. In some cases, when flexible configuration is needed you can use the following options:

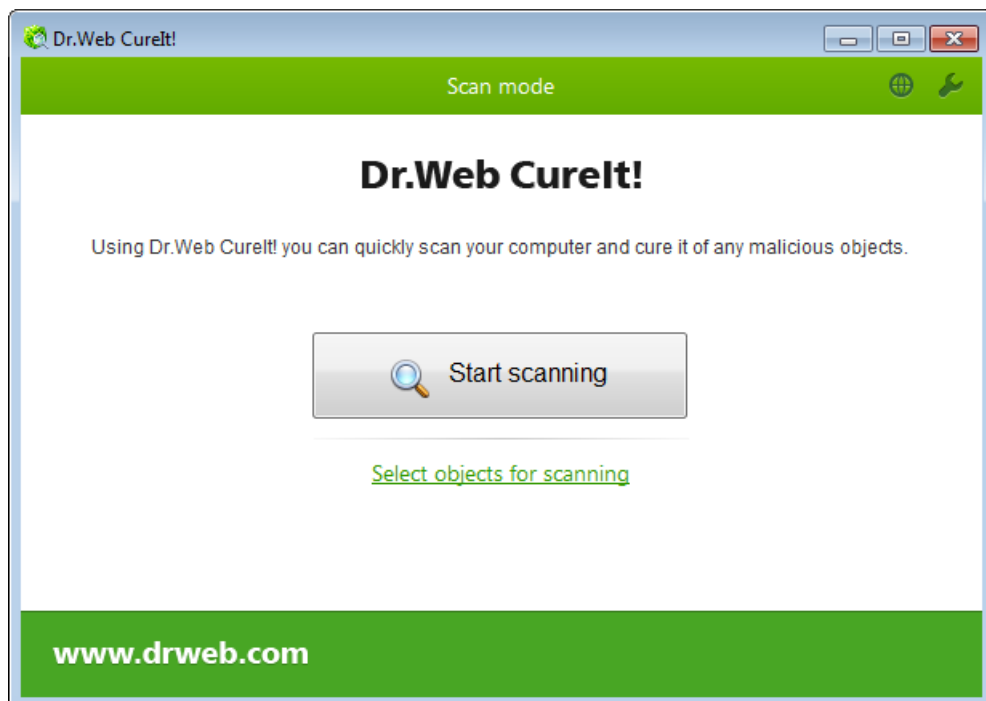
- Perform [custom scan](#), which allows you to select particular operating system objects or files and folders to scan.
- [Select custom actions](#) to neutralize detected threats.
- [Configure](#) general settings of anti-virus scanning.
- Run Dr.Web CureIt! with [command line parameters](#).

4.1. Custom Scan

Apart from the pre-installed scanning template that runs express scan of the most vulnerable objects of the operating system, Dr.Web CureIt! also provides you with custom scan mode. In this mode, you can configure scanning to your purposes.

In this mode, before you configure scanning, you can select objects to be scanned. You can select any folders and files, and such objects as random access memory, boot sectors, etc. Click **Start scanning** to scan selected objects. In full or express scan modes, you do not need to select any objects.

You can select scan type in the **Scan mode** window with every new launch of Dr.Web CureIt!.



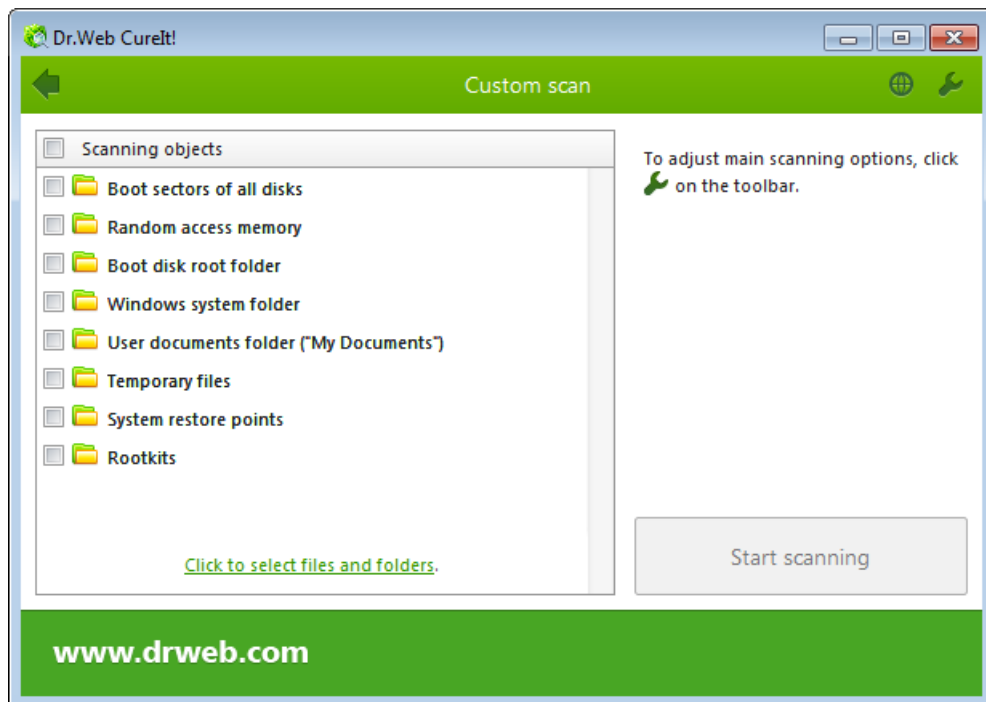
Picture 6. Selecting scan mode Dr.Web.




To run custom scan

1. Run Dr.Web CureIt!.
2. In the **License and updates** window, read the conditions of [statistics gathering](#). Click **Continue**.
3. In the scan type selection window, click **Select objects for scanning**.
4. The table in the center of this window lists objects for scanning. To add a file or a folder to the list, click the link at the bottom of the table and then select objects for scanning in the **Browse** window.

To select all the objects in the table, select the **Scanning objects** checkbox in the table heading.



Picture 7. Selecting files for scan Dr.Web.

If necessary, configure Dr.Web CureIt! settings before starting a scan. To do this, click **Preferences**  on the toolbar.

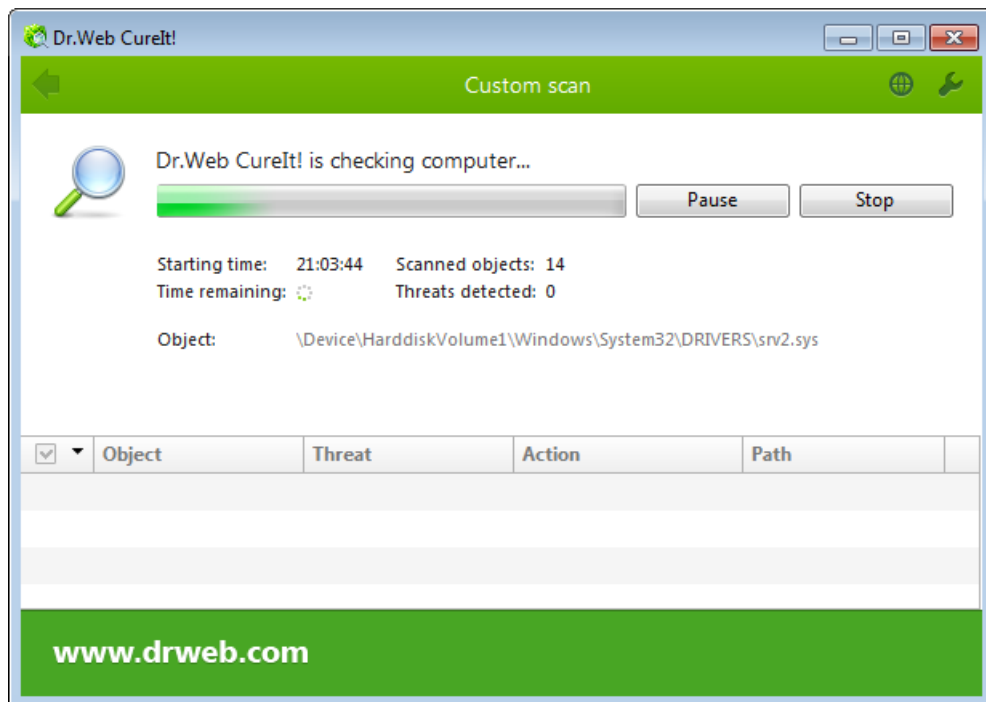
5. Click **Start scanning**.
6. During scanning, Dr.Web CureIt! displays general information on its progress and lists detected threats.

To manage scanning process, use the following options:

- to suspend scanning, click **Pause**;
- to start scanning again after a pause, click **Resume**;
- to terminate scanning, click **Stop**.

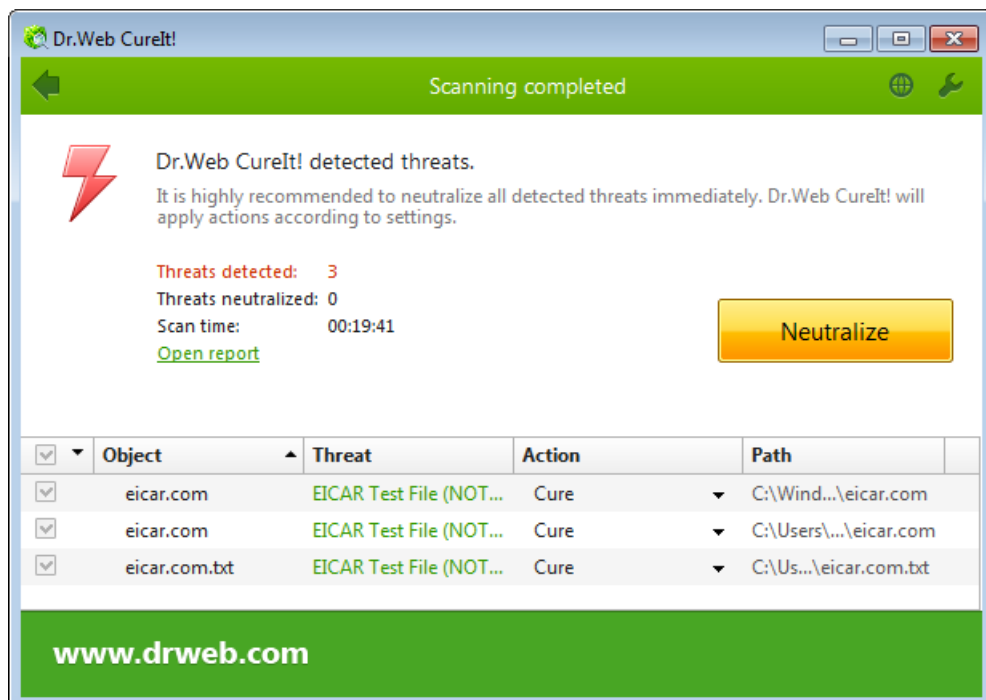


The **Pause** button is not available while processes and RAM are being scanned.



Picture 8. Custom scan Dr.Web.

8. Once scanning is complete, Dr.Web CureIt! displays detailed information on detected threats. Review the scan results. If necessary, you can also review a [scanning log](#) by clicking **Open report**.



Picture 9. Custom scan results Dr.Web.



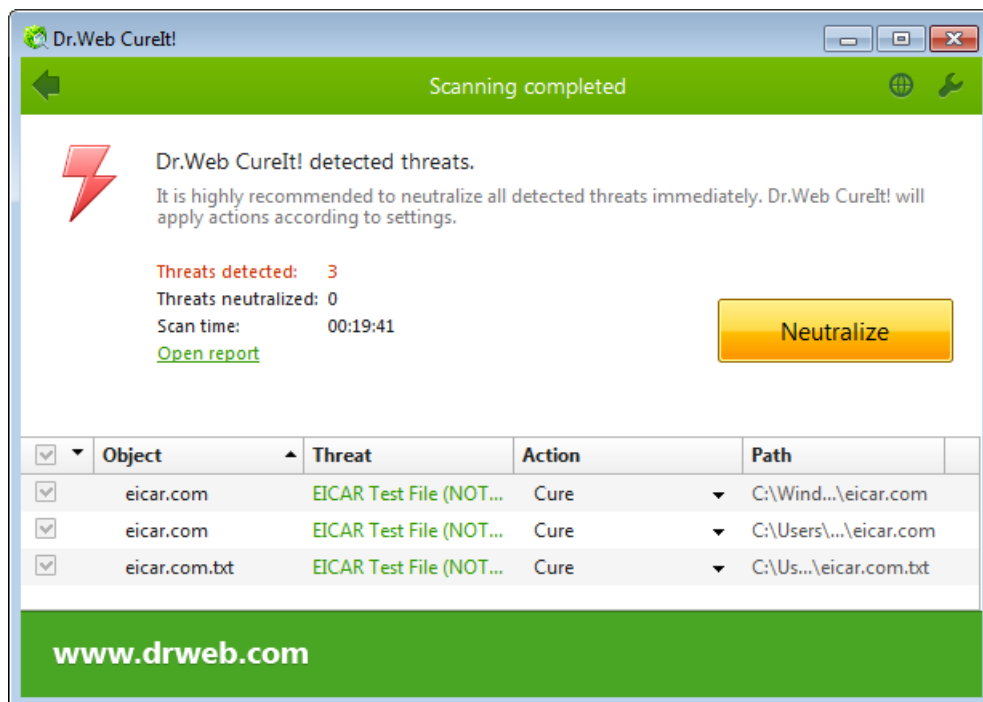
If viruses or other threats were detected, you need to neutralize them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can [select](#) custom actions for particular threats.

4.2. Configuring Threat Neutralization

Once scanning is complete, Dr.Web CureIt! just informs you on threat detection and prompts you to neutralize them by applying suitable actions. You can neutralize all detected threats at a time. To do so, once scanning is completed, click **Neutralize**. Dr.Web CureIt! will apply default actions to all detected threats.



By clicking **Neutralize**, you apply actions to the objects selected in the table. By default, Dr.Web CureIt! selects all objects to neutralize once scanning is completed. If necessary, you can select individual objects or group of objects, which will be neutralized once you click **Neutralize**. Use checkboxes next to an object name a drop-down list in the table header.



Picture 10. Selecting action after scan Dr.Web.

You can also apply an individual action for a particular threat. You can restore the original state of an infected object (i.e., *cure* it), or when curing is impossible you can remove an infected object completely from your operating system (i.e., *delete* it).

To select an action for a threat

1. Select a necessary action for each object from the drop-down list in the **Action** field. By default, Dr.Web CureIt! suggest the most effective actions.
2. Click **Neutralize**. Dr.Web CureIt! will apply selected actions to all threats at once.



It is recommended that you send suspicious quarantined files for analysis to the Doctor Web anti-virus laboratory.

There are some limitations:



- Suspicious objects cannot be cured.
- Objects which are not files (e.g., boot sectors) cannot be moved or deleted.
- Any actions are impossible for individual files inside archives, containers, or attachments. You can only apply an action to a whole object.

Detailed report on Dr.Web CureIt! activity is saved in `CureIt.log` that is located in `%USERPROFILE%\Doctor Web`.

4.3. Configuring Scanning

Default settings are optimal for most uses. Do not change them unnecessarily.

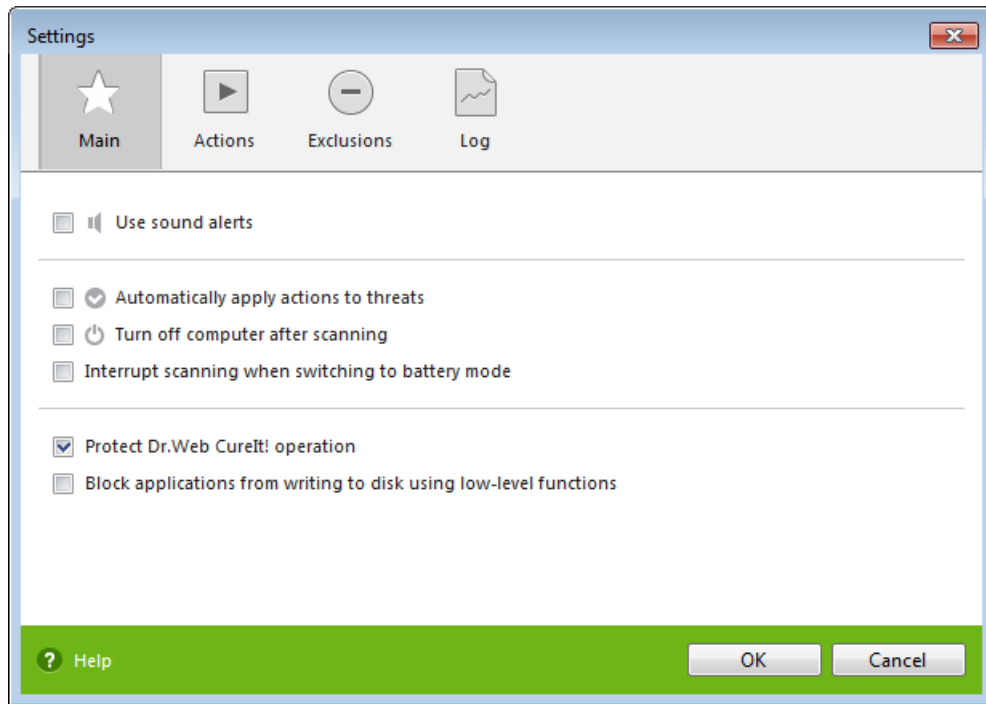
To change Dr.Web CureIt! settings

1. Run Dr.Web CureIt!. This opens Dr.Web CureIt! main window.
2. Click **Preferences**  on the toolbar and then select **Settings**. This opens a window that contains the following tabs:
 - [Main](#) tab where you can configure general parameters of Dr.Web CureIt! operation.
 - [Actions](#) tab where you can configure how Dr.Web CureIt! will react upon detection of infected or suspicious files and archives or other malicious objects.
 - [Exclusions](#) tab where you can specify files and folders to be excluded from scanning.
 - [Log](#) tab where you can set logging options for Dr.Web CureIt!.
3. To get information on options in the tab, click **Help** .
4. Once you finish editing the settings, click **OK** to save the changes or **Cancel** to cancel them.

Changes in the settings of Dr.Web CureIt! are retained only in your current program session. New session resets program settings to default values.

4.3.1. Main Tab

On this tab, you can set general parameters of Dr.Web CureIt! operation.



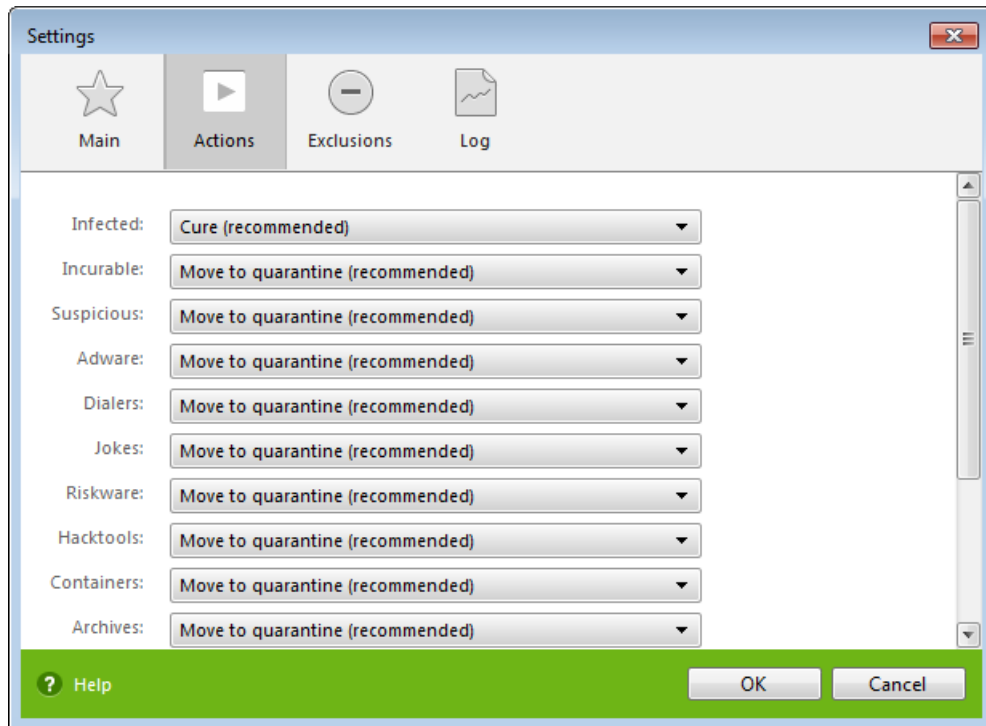
Picture 11. Dr.Web Settings. Main tab.

You can enable sound notifications on particular events, set Dr.Web CureIt! to apply recommended actions to detected threats automatically, and configure Dr.Web CureIt! interaction with the operating system.

On this page, you can also specify self-protection parameters and disable miscellaneous operations that may compromise security of your computer.

4.3.2. Actions Tab

Once scanning is completed, Dr.Web CureIt! just informs you on threat detection and prompts you to neutralize them by applying suitable actions. These actions are suggested in accordance with the settings on this tab.



Picture 12. Dr.Web Settings. Actions tab.

The most suitable action for curable threats (e.g., files infected with known viruses) is curing, since it allows to restore the infected file completely. It is recommended to move other types of threats to quarantine for further analysis in order to prevent loss of potentially valuable data.

You can select one of the following actions:

Action	Description
Cure	<p>Restores the original state of an object before infection. If an object is incurable or an attempt to cure it fails, the action set for incurable viruses is applied.</p> <p>Available for known viruses only except Trojan programs and files within complex objects (archives, email attachments, file containers). Trojan programs are deleted on detection.</p> <p>Curing is the only action available for infected boot sectors.</p>
Move to quarantine	<p>Moves an object to a specific folder for storing suspicious files. By default, Quarantine is located in the hidden folder %USERPROFILE%\Doctor Web\DrWeb CureIt Quarantine\. You can view Quarantine once scanning is completed.</p> <p>No action is applied to malicious objects detected in a boot sector.</p>
Delete	<p>Deletes an object completely.</p> <p>No action is applied to malicious objects detected in a boot sector.</p>



Action	Description
Ignore	<p>Skip an object without applying any action. No logging.</p> <p>Available for potentially dangerous files only, which includes adware, dialers, jokes, hacktools and riskware.</p>



Threats detected within complex objects (archives, email attachments, file containers) cannot be processed individually. By default, all such objects are moved to Quarantine.

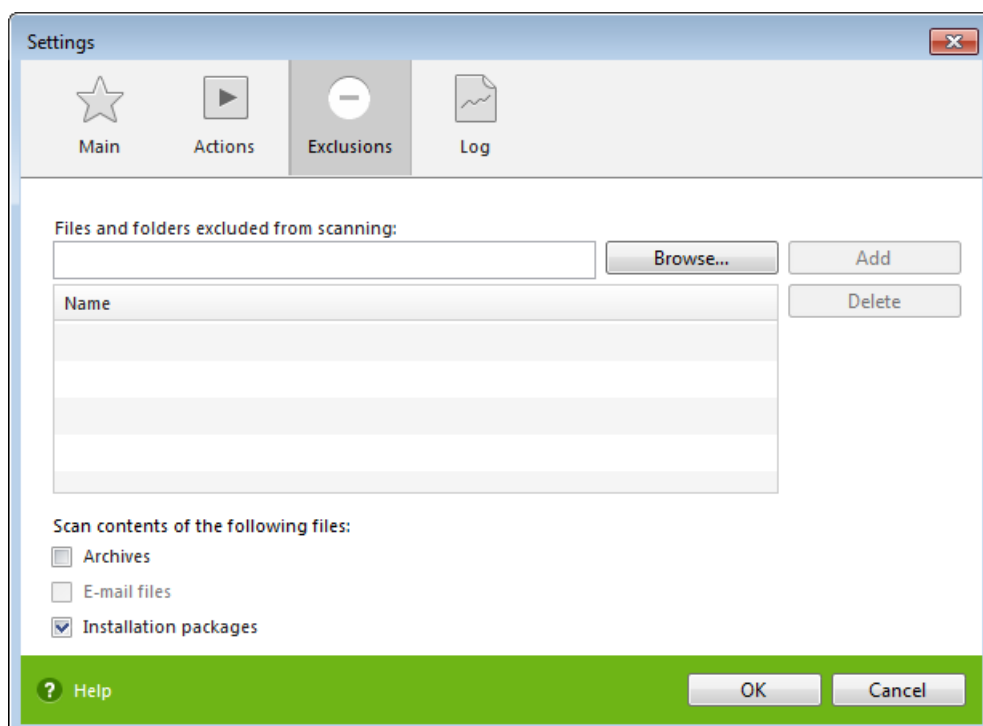
To complete curing some infected files, it is necessary to reboot your operating system. You can choose one of the following:

- **Prompt restart.**
- **Restart computer automatically.** It can lead to loss of unsaved data.

4.3.3. Exclusions Tab

On this tab, you can specify files and folders that should be excluded from scanning and determine whether to scan contents of archives and installation packages.

License agreement of Dr.Web CureIt! Free Edition does not allow scanning of email files. Use Dr.Web CureIt! Commercial Edition or other Dr.Web products to check contents of email files.



Picture 13. Dr.Web Settings. Exclusions tab.



Excluded files list

Here you can list all files (or file masks) that will be excluded from scanning (i.e. the action is applied to all files with the same name). This option is appropriate for temporary files, swap files, etc.

To configure excluded files list

Do one of the following:

- Add name or mask of a file that should be excluded from scanning. If the file already exists, click **Browse** and select the file. You can also use masks.

Mask specifies a common part of an object name:

- the asterisk * character replaces any, possibly empty, sequence of characters;
- the question mark ? replaces only one character;
- other mask characters do not replace anything and mean that the name must contain this particular character in this place.

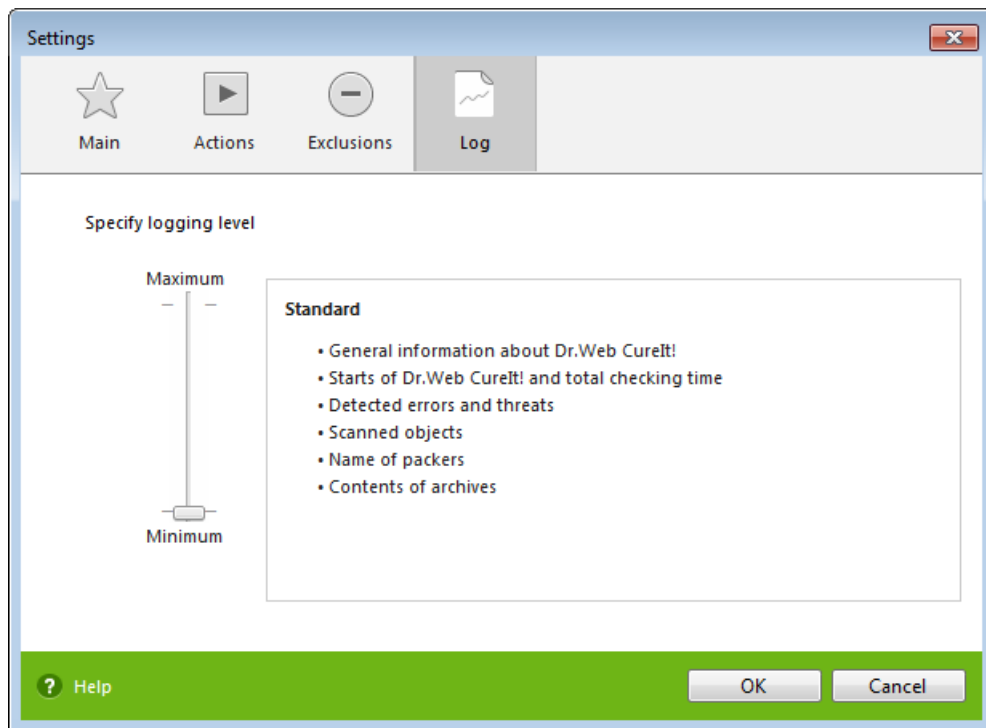
Examples:

- **Report*.doc** stands for all Microsoft Word documents, which names start with the word "Report", for example, `ReportFebruary.doc`, `Report121209.doc`, etc.);
 - ***.exe** stands for all executable files with the EXE extension, for example, `setup.exe`, `iTunes.exe`, etc.);
 - **photo????09.jpg** stands for all JPG images, which names start with the word "photo" and end with "09" and contain exact number of 4 other characters in the middle, for example, `photo121209.jpg`, `photoJude09.jpg`, `photo---09.jpg`, etc..
- Click the **Add** button on the right. File (or its mask) will be added to the list below.
 - To remove a file from the list, select it and click **Delete**. The file will be checked on the next scan.

4.3.4. Log Tab

On the Log tab, you can set up parameters of log file.

Dr.Web CureIt! log is stored in `CureIt.log` that is located in `%USERPROFILE%\Doctor Web`. It is recommended to analyze your log file from time to time.



Picture 14. Dr.Web Settings. Log tab.

You can set one of the following modes for log file:

- **Standard**—logs only the most important events (start and stop of Dr.Web CureIt! and detected threats);
- **Debugging**—logs maximum data about Dr.Web CureIt! activity. This may result in considerable growth of a log file. It is recommended to use this mode only when errors occur or at request of Doctor Web technical support.

4.4. Launching From Command Line

You can run Dr.Web CureIt! in the command line mode. This allows you to specify additional settings of the current scanning session and a list of objects for scanning as additional parameters.



To use the command line interface in the Free Edition of Dr.Web CureIt!, you are required to confirm that you agree to automatically send anonymous statistics to Doctor Web. When using the Commercial Edition of Dr.Web CureIt!, such confirmation is not necessary.

Run command syntax:

```
[<path_to_program>] [<CureIt!_file_name>] [<objects>] [<switches>]
```

You can leave the list of objects to be scanned empty or specify several elements separated by whitespaces. If no path to the objects is specified, Dr.Web CureIt! will search for objects in the Dr.Web CureIt! folder.



The most commonly used types of scans:

- **/LITE**—performs a basic scan of random access memory and boot sectors of all disks. This mode also detects rootkits.
- **/FAST**—performs [express scan](#) of the system.
- **/FULL**—performs full scan of all hard drives and removable media (including boot sectors).

Switches are command line parameters that specify program settings. If no switches are defined, scanning is performed with the settings specified earlier (or with default settings if you have not changed them). Each switch begins with / and is separated with a whitespace from other switches. If parameter contains a whitespace, you have to put quotation marks around this parameter. For example:

- 636frs47.exe /tm-
- 45hlke49.exe /tm- D:\test\
- 10sfr56g.exe /OK- "D:\Program Files\"

The most commonly used examples of specifying objects for scanning:

- *—scan all files on all disks;
- C:—scan all files on disk C;
- D:\games—scan all files in the specified folder;
- C:\games*—scan all files and subfolders in C:\games*.

Command Line Switches

The list of all command line switches.

/AA—apply actions to detected threats automatically.

/AR—check archives. Option is disabled by default.



To enable archive scanning, you have to specify **/AR** explicitly.

To check files in archives when running a scan from GUI, select **Archives** on the [Exclusions](#) tab of the Dr.Web CureIt! settings.

/AC—check installation packages. Option is disabled by default.



To enable installation package scanning, you have to specify **/AC** explicitly.

To check files in installation packages when running a scan from GUI, select the **Installation packages** checkbox on the [Exclusions](#) tab of the Dr.Web CureIt! settings.

/AFS—use forward slash to specify nesting within an archive. Option is disabled by default.

/ARC:<number>—maximum archive compression level. If compression ratio of an archive exceeds the limit, scanner neither unpacks, nor scans the archive. By default, no ratio limit is set.



- /ARL:***<number>*—maximum nesting level of an archive to be checked. Unlimited by default.
- /ARS:***<number>*—maximum size of an archive to be checked (in KB). If the size of an archive exceeds the limit, Dr.Web CureIt! neither unpacks, nor scans the archive. Unlimited by default.
- /ART:***<number>*—defines what level of compression will be the first one to be scanned (minimum size of a file inside an archive beginning from which compression ratio will be checked (in KB). Unlimited by default.
- /ARX:***<number>*—maximum size of archive objects to be checked (in KB). Unlimited by default.
- /BI**—show information about Dr.Web virus databases. Option is enabled by default.
- /DR**—scan folders recursively (i.e., scan subfolders). Option is enabled by default.
- /E:***<number>*—use specified number of Dr.Web Engines.
- /FAST**—perform [express scan](#) of the system.
- /FL:***<file_name>*—scan paths listed in a specified file.
- /FM:***<mask>*—scan files matching a specified mask. By default, all files are scanned.
- /FR:***<regexpr>*—scan files matching a specified regular expression. By default all files are scanned.
- /FULL**—perform full scan of all hard drives and removable media (including boot sectors).
- /HA**—perform heuristic analysis of files and search for unknown threats. Option is enabled by default.
- /LITE**—perform basic scan of random access memory and boot sectors of all disks and search for rootkits. This parameter disables the **/FAST** and **/FULL** modes.
- /LN**—scan labeled files. Option is disabled by default.
- /MC:***<number>*—set maximum number of cure attempts. Unlimited by default.
- /NB**—do not backup cured or deleted files. Option is disabled by default.
- /NI[:X]**—shows system resource usage in percent. Defines what amount of memory is used for scanning and scanning task priority Unlimited by default.
- /NOREBOOT**—cancel system reboot and shut down after scanning.
- /NT**—check NTFS streams. Option is enabled by default.
- /OK**—display full list of scanned objects. Clean files are marked with OK. Option is disabled by default.
- /P:***<priority>*—priority of a current scanning task in a queue:
- 0*—the lowest;
 - L*—low;
 - N*—general (used by default);
 - H*—the highest;
 - M*—maximal.
- /PAL:***<number>*—maximum number of nesting levels for packer (1000 by default).



/RA:<file_name>—append scanning report to a specified file. By default, report is not generated.

/RP:<file_name>—record scanning report to a specified file. By default, report is not generated.

/QNA—double quote file names.

/QUIT—terminate Dr.Web CureIt! once scanning is completed (whether or not actions were applied to detected threats).

/REP—follow symbolic links while scanning. Option is disabled by default.

/SCC—show contents of complex objects (archives, email attachments, file containers). Option is disabled by default.

/SCN—show installation package name. Option is disabled by default.

/SPN—show packer name. Option is disabled by default.

/SST—display file scan time. Option is disabled by default.

/TB—check boot sectors including master boot record (MBR) of the hard drive. Option is disabled by default.

/TM—search for threats in memory including Windows system control area. Option is disabled by default.

/TR—check system restore points. Option is disabled by default.

/W:<time>—maximum scan time in seconds. Unlimited by default.

/X:S[:R]—after scanning, shutdown, reboot, suspend, or hibernate the computer.

Configuring actions for threats

Use the following modifiers to select actions for different types of threats (C—cure; Q—move to quarantine; D—delete; I—ignore):

- **/AAD:**<action>—action for adware (possible actions: DQI).
- **/AAR:**<action>—action for infected archives (possible actions: DQI).
- **/ACN:**<action>—action for infected installation packages (possible actions: DQI).
- **/ADL:**<action>—action for dialers (possible actions: DQI).
- **/AHT:**<action>—action for hacktools (possible actions: DQI).
- **/AIC:**<action>—action for incurable files (possible actions: DQ).
- **/AIN:**<action>—action for infected files (possible actions: CDQ).
- **/AJK:**<action>—action for jokes (possible actions: DQI).
- **/ARW:**<action>—action for riskware (possible actions: DQI).
- **/ASU:**<action>—action for suspicious files (possible actions: DQI).



Switch modifiers

Some switches may have modifiers that explicitly enable or disable options specified by these switches. For example:

/AC—explicitly disable this mode.

/AC or **/AC+**—explicitly enable this mode.

These modifiers can be useful when the necessary option is enabled or disabled by default.

The following parameters accept these modifiers:

**/AR, /AC, /AFS, /BI, /DR, /HA, /LN, /NB, /NT, /OK, /QNA, /REP, /SCC, /SCN, /SPN,
/SST, /TB, /TM, /TR.**

For the **/FL** switch, the - modifier directs to scan paths listed in a specified file and then delete this file.

For the **/ARC, /ARL, /ARS, /ART, /ARX, /NI[:X], /PAL**, and **/W** switches if **0** is specified as a value for the *<number>*, no limit for the switch is set.

If several mutually exclusive switches are found in a command line, the last of them takes effect.

