




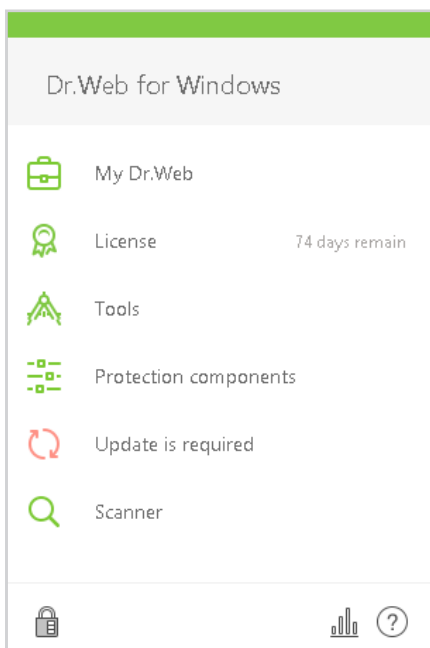
Configure Dr.Web to protect
your computer from miners


To maximally protect your computer against modern malware programs—including miners—you need to configure your anti-virus right after you install it.

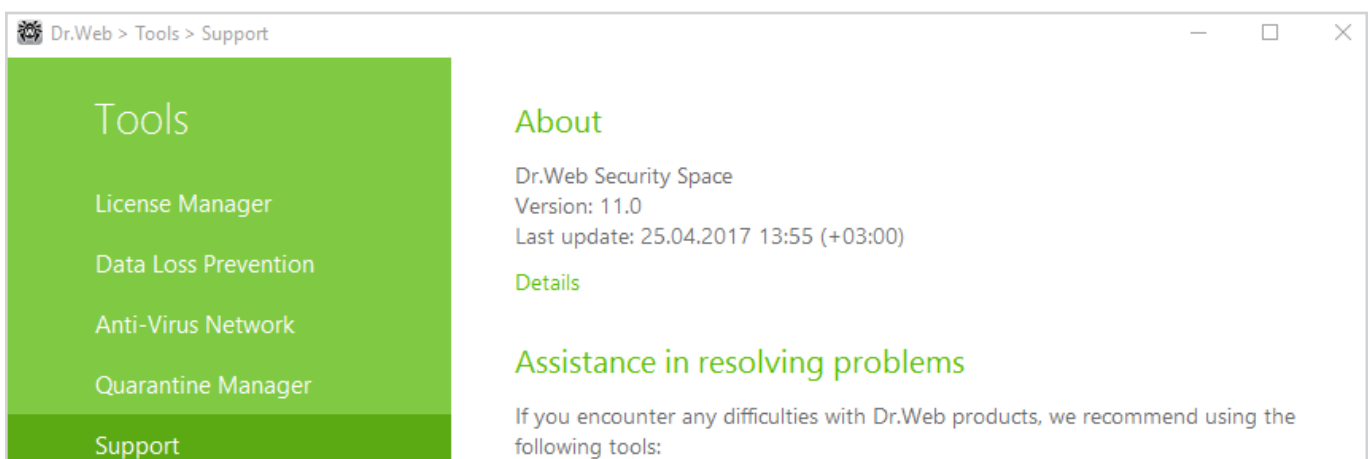
1. Make sure that the anti-virus version you're using is current and that your license is valid

Important! Doctor Web technical support service statistics show that a significant number of infections happen because the anti-virus has been disabled or has gone without being updated for some period of time.

To check your license's status, click on the  icon. Next to **License**, you will see the number of days remaining until your current license expires.



To know what product version you're using, click on the  icon; select **Tools**, and in the newly appeared window, select **Support**.




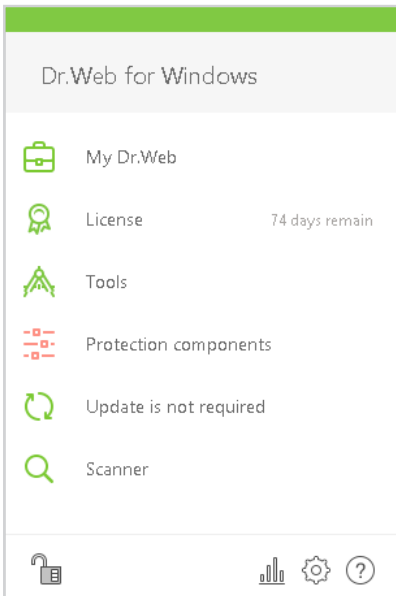
Important! The current version of the Dr.Web Security Suite anti-virus is 11. Outdated versions of anti-viruses increase the risk of infection because they do not incorporate the [latest malware-detection technologies](#).

2. All the anti-virus protection components should be enabled at the moment of infection

This includes the Preventive Protection modules, Dr.Web SplDer Gate, Dr.Web Anti-spam, and Dr.Web Firewall.

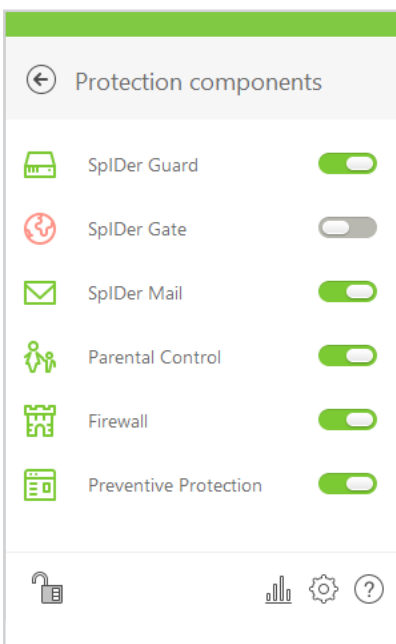
The Dr.Web Anti-virus has no extraneous components! Take, for example, Dr.Web Anti-spam. Testing of this module has shown that it can filter out more than 90% of unknown malicious programs that have all the characteristic hallmarks of cybercriminals. And this is without using the anti-virus engine technologies.

The **SplDer Agent icon** in the system tray shows that one or several components are disabled: . And this is how the agent menu will look:



The agent icon's absence can mean that the anti-virus has been unloaded and the system has been left without any anti-virus protection.

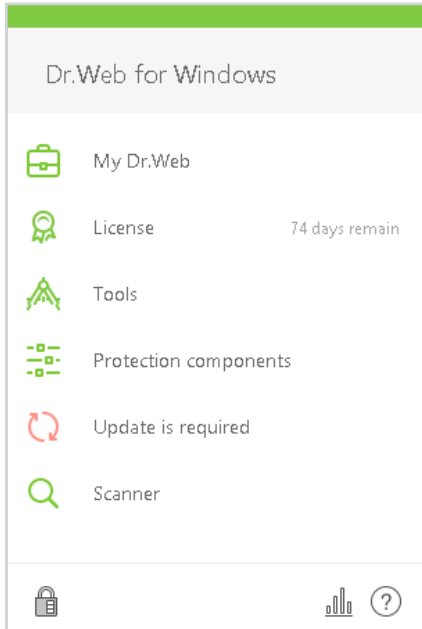
Click on the agent icon and then on **Protection components** to find out what components are disabled.






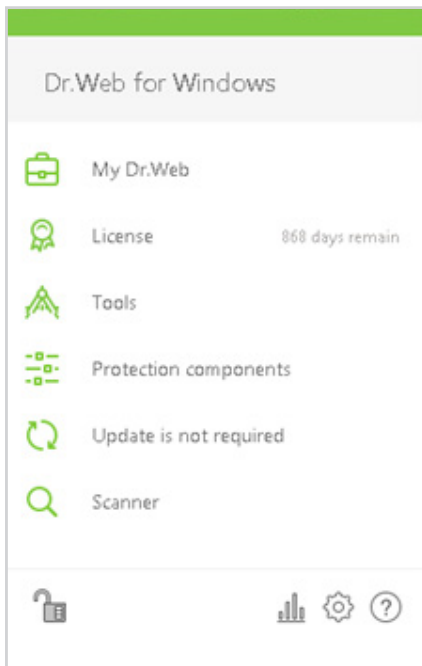
3. All anti-virus updates should be installed, including updates that require a reboot to install new interception drivers and fixes that close potential vulnerabilities.

Every day cybercriminals create hundreds of new miners (in addition to the other malware programs they create). If your anti-virus is disabled or it hasn't been updated for a long time, each of these miners can easily install itself onto your PC or device.

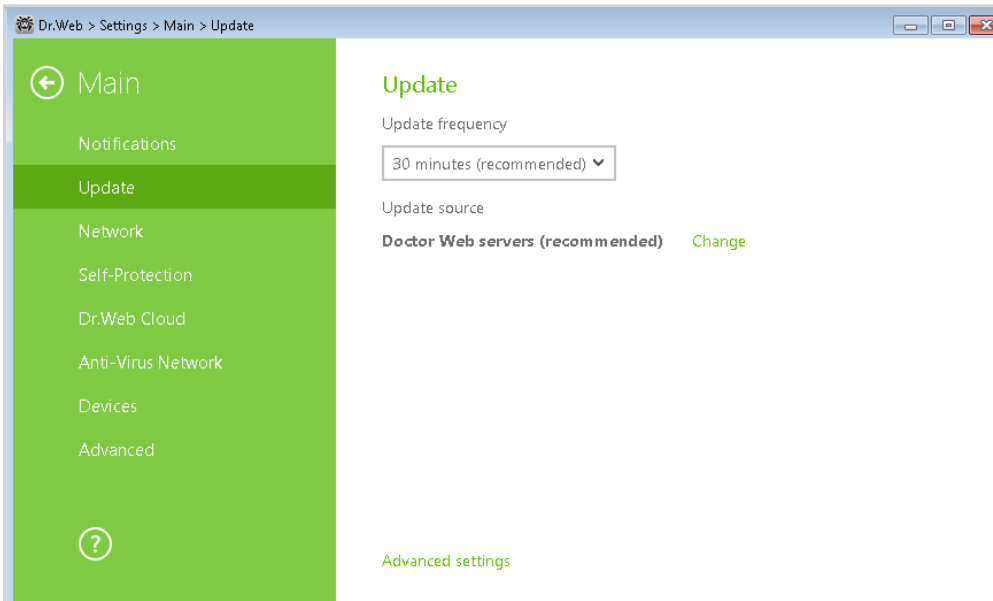
Click on the  icon to check the update status. The status will be displayed in the newly appeared menu.



To check the frequency of updates, click on the  icon in the system tray; and in the context menu, click on the icons  icon in the system tray; and in the context menu, click on the icons .



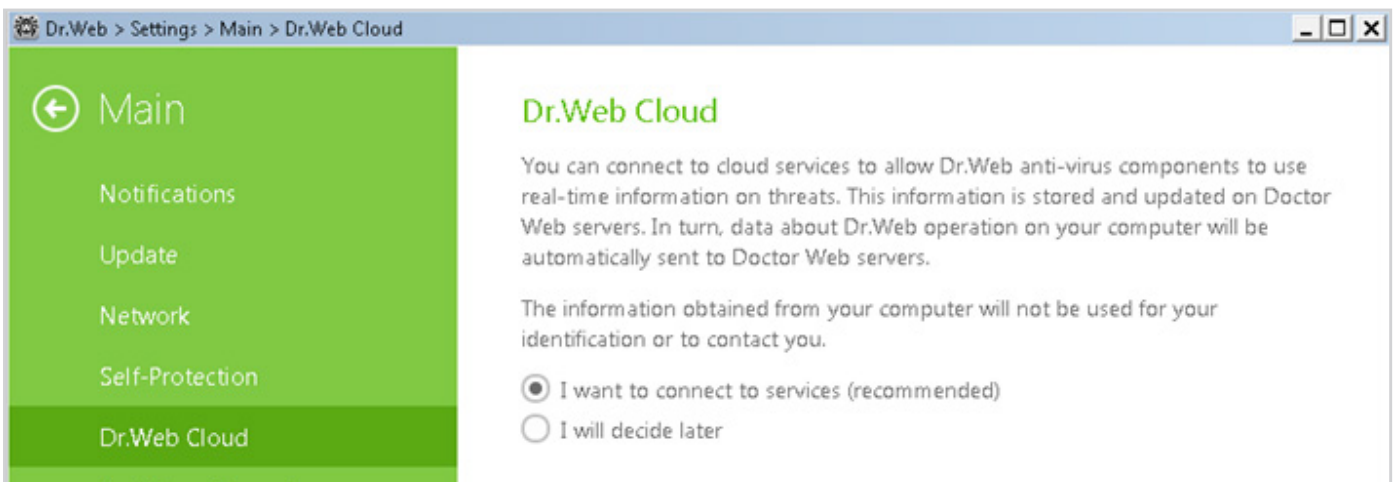
In the newly appeared window, select **Settings** → **Main** → **Update**.



We recommended performing updates no more frequently than once per hour.




- 4. Dr.Web Cloud should be enabled before updates are delivered.** This component reacts instantly to newly emerged threats.

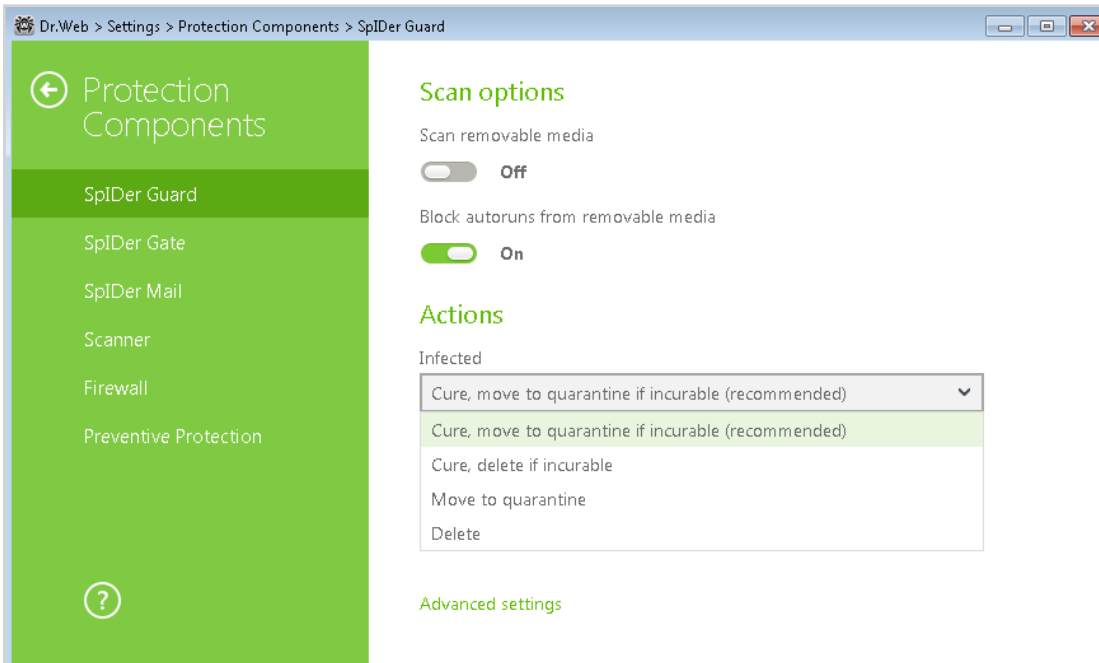
To check the status of the cloud control, click on the  icon (the icon will change to ); click on the newly appeared , and then select **Main** in the **Settings** menu.



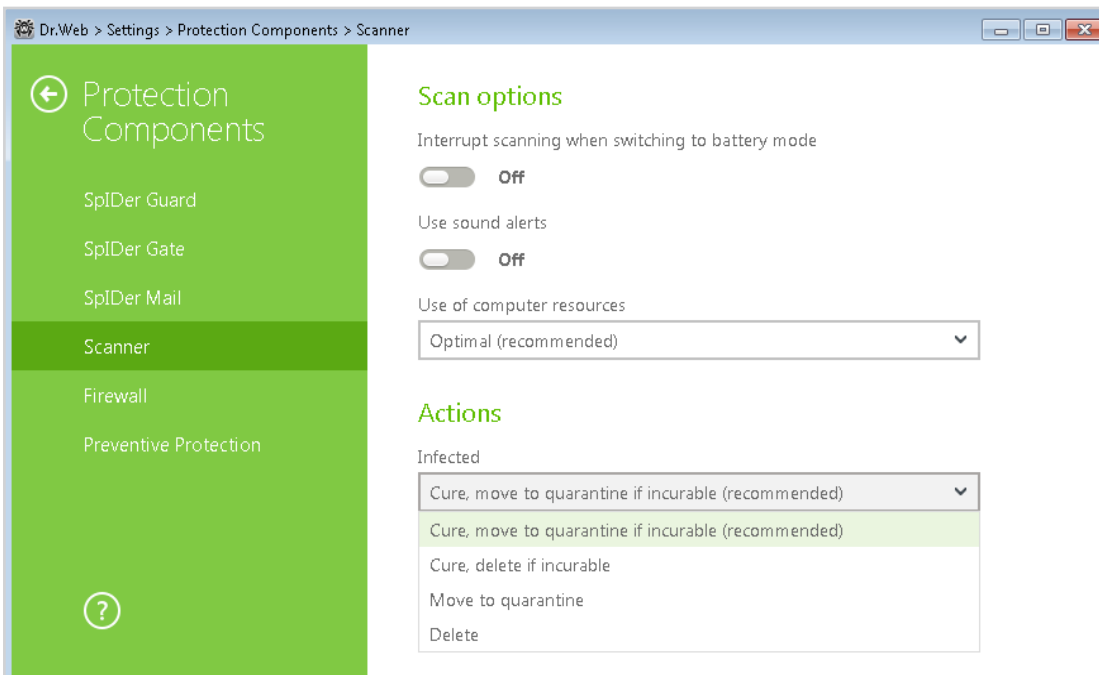
- 5. Dr.Web Security Space should move miners to the quarantine**

In the case of re-infections and targeted attacks and when it is necessary to identify the path of an infection, it can be critical to have the body of the malicious program that's involved. That's why you should choose the option **Move to quarantine** for these programs.

Click on the  icon in the system tray; in the context menu, select  (Administrator Mode), and then click on the gears icon  (Settings). In the **Settings** window, select **Protection Components**, and then select **SpIDer Guard**. Configure actions for the groups **Infected** and **Potentially dangerous**.



The same settings should be applied for other anti-virus modules—e.g., the Anti-virus module and the Dr.Web SpIDer Gate module.






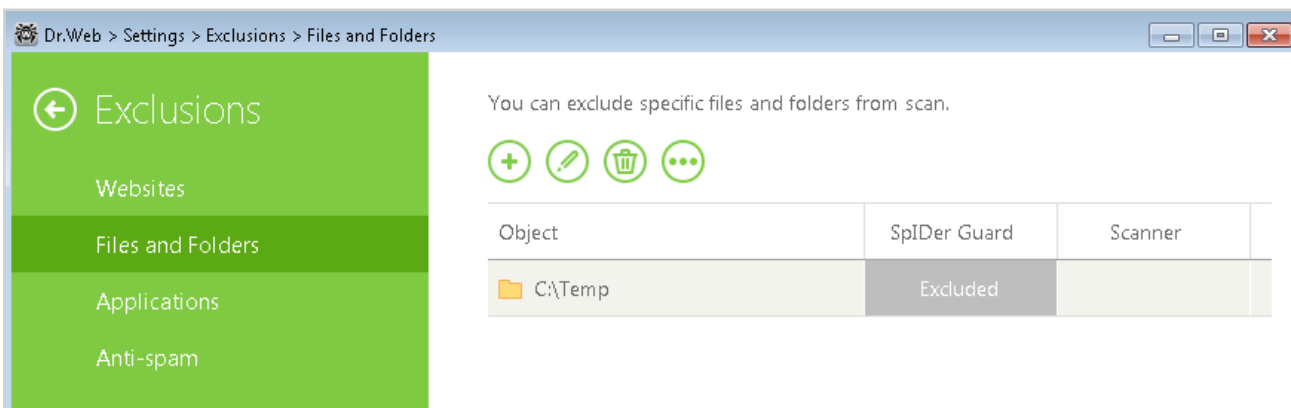
Important! «Miners» is the general name for some malicious programs. They can specifically be detected as Trojans (Trojan.BtcMine), Java scripts (JS.BtcMine), and utilities (Tool.BtcMine). Using Dr.Web Security Space's settings, you can choose the default action for all these types of miners.

To ensure Tool miners are detected, it is recommended that you select the action **Potentially dangerous in Move to quarantine**.

6. Use the anti-virus scanning exclusion rules very carefully. If necessary, add the files you don't want the anti-virus to scan onto the exclusion list.

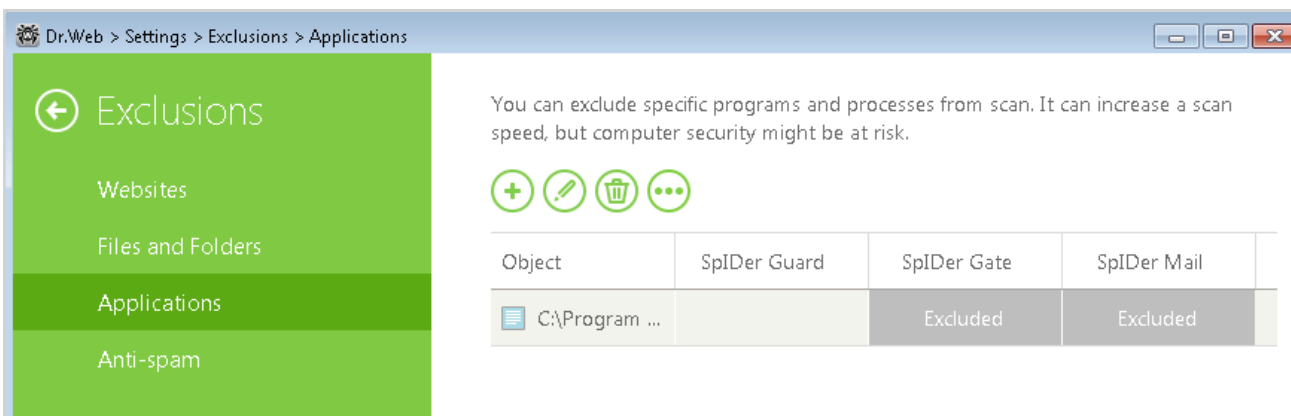
Often malicious programs use legitimate programs for mining. Such programs are detected by anti-viruses as potentially dangerous. If you are sure that the miner you installed is legal and not malicious, you can use the settings' **Exclusions** section to allow it.

To add your mining application onto the scan exclusion list, click on the  icon (it will now look like this: ); then click on the , icon, and go to **Exclusions** in the **Settings** menu.




Внимание! Исключения по маскам типа *.exe или *.dll будут служить причиной того, что никакие объекты, подходящие под такую маску, не будут и будут пропущены. В случае маски *.exe будут пропущены все исполняемые файлы.



Внимание! Не рекомендуется исключать проверку трафика для используемых программ — в таком случае никакое вредоносное ПО, загруженное данными программами, проверяться не будет.

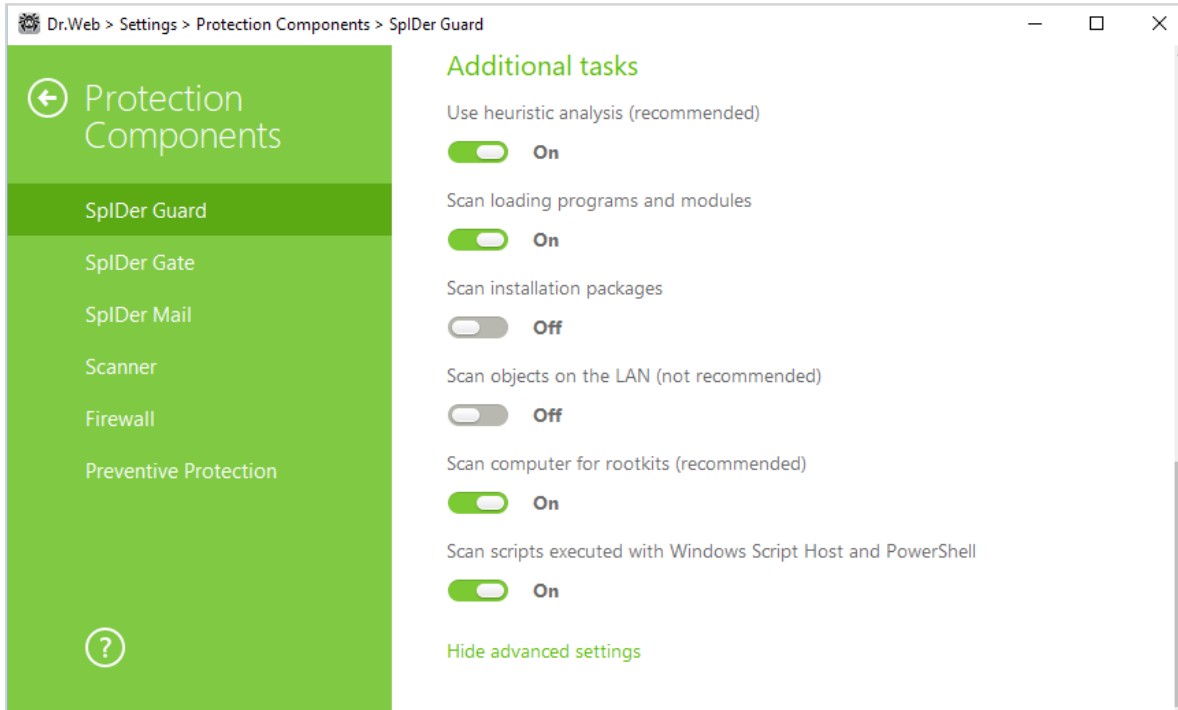


7. A routine for detecting malicious scripts should be used

Dr.Web uses ScriptHeuristic—a technology that prevents malicious browser scripts (including miners) from being executed without disabling the functionality of legitimate scripts. In addition to that technology, Dr.Web uses the Amsi-client protection module. Its task is to check running scripts—JScript, JavaScript, VBScript, and PowerShell.

The anti-virus scan performed by the Dr.Web Amsi-client module can be enabled in the **SpIDer Guard** settings section. By default, this scanning option is enabled. To check the module's status, click on the  icon in the




system tray, and in the context menu, select  (**Administrator Mode**). Then click on the gears icon  (**Settings**). In the **Settings** window, select **Protection Components**. Then select **SplDer Guard**, and click on **Advanced settings**. The option **Scan scripts...** should now be enabled.

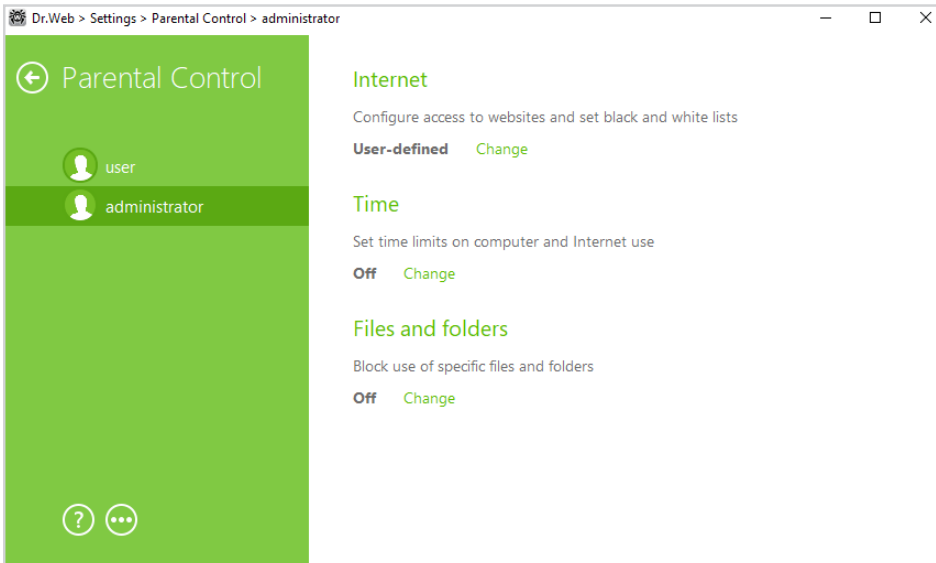


Important! The Dr.Web Amsi-client module is installed and removed simultaneously with the Dr.Web SplDer Guard module. The module is available if you are using Dr.Web Anti-virus and Dr.Web Security Suite in operating systems starting with Windows 10 (x 86, x 64) and in server operating systems starting with Windows Server 2016.

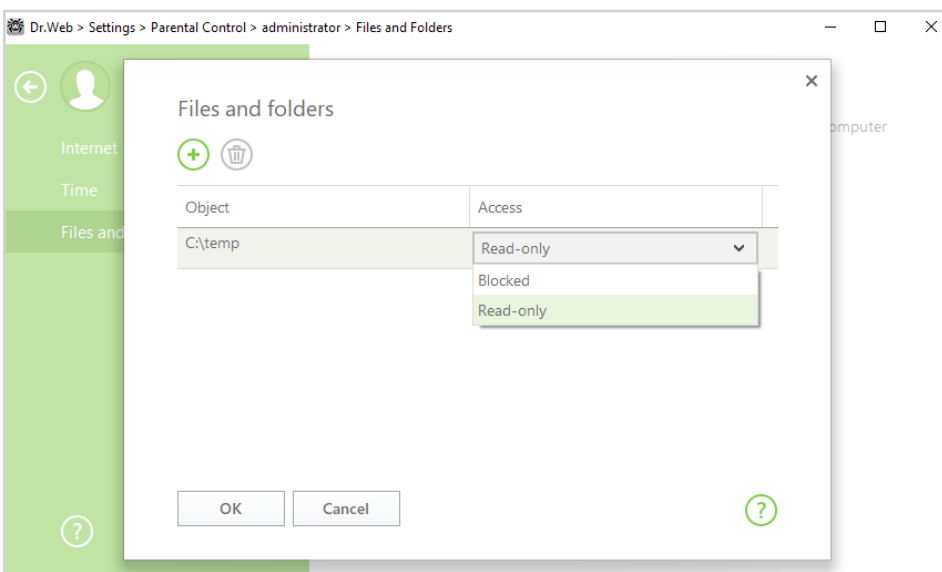
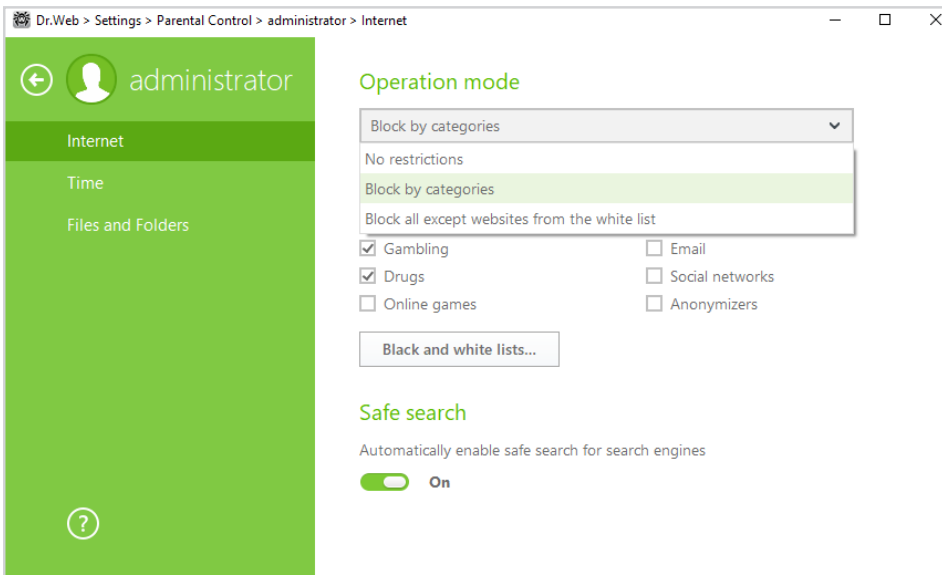
8. Office/Parental Control should be enabled

A Trojan-miner can get into a system via spam (it can be attached to a message or downloaded using a link), IM messages (which also contain a download link), a downloaded file (for example, Java script) or via an infected site or flash drive.

To restrict access to certain sites, files, and folders, click on the  and  icons. Then click on the  icon, and in the **Settings** window, select **Parental Control**.

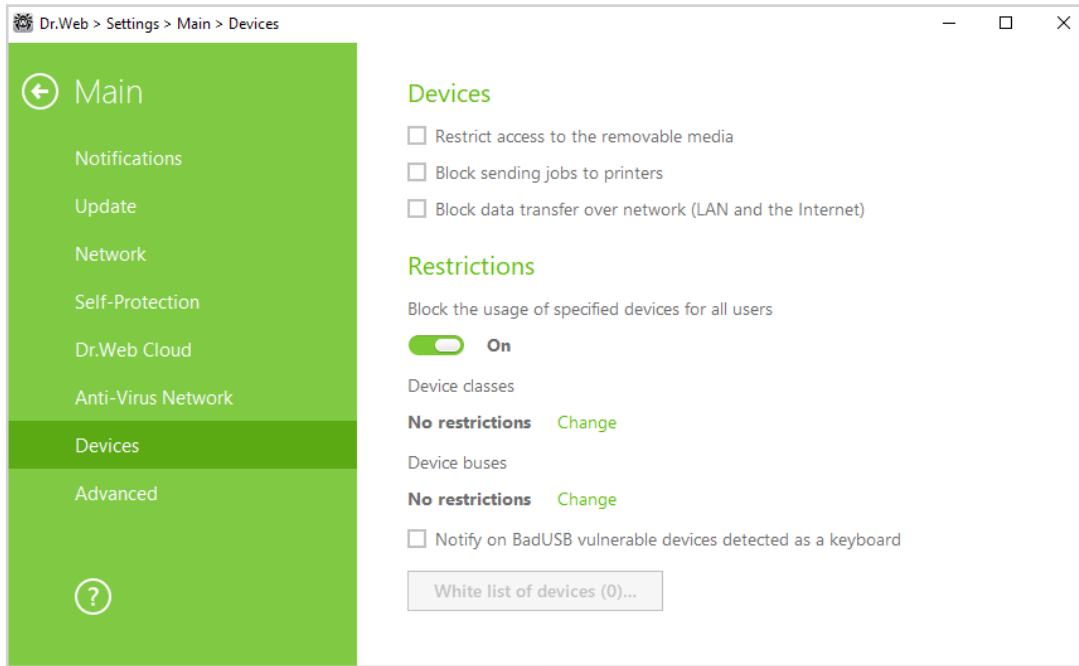


In the next window, select the user account for which you want to set restrictions.

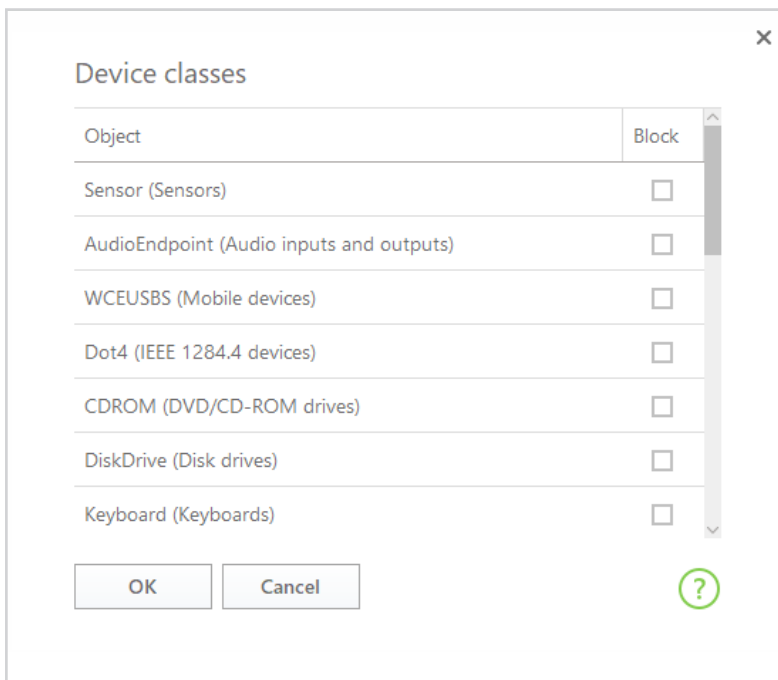



By default, restrictions are disabled.

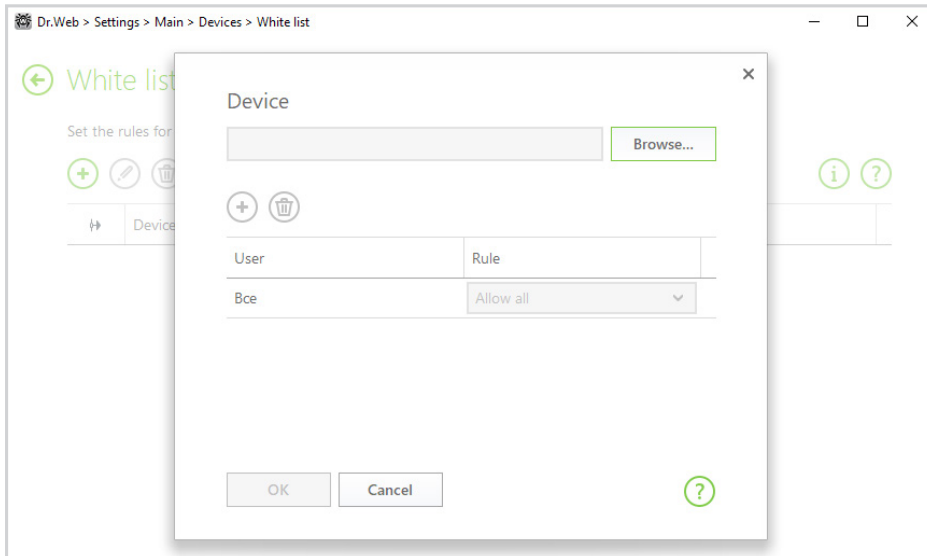
To restrict access to removable media, in the **Settings** window, select **Main** → **Devices**.



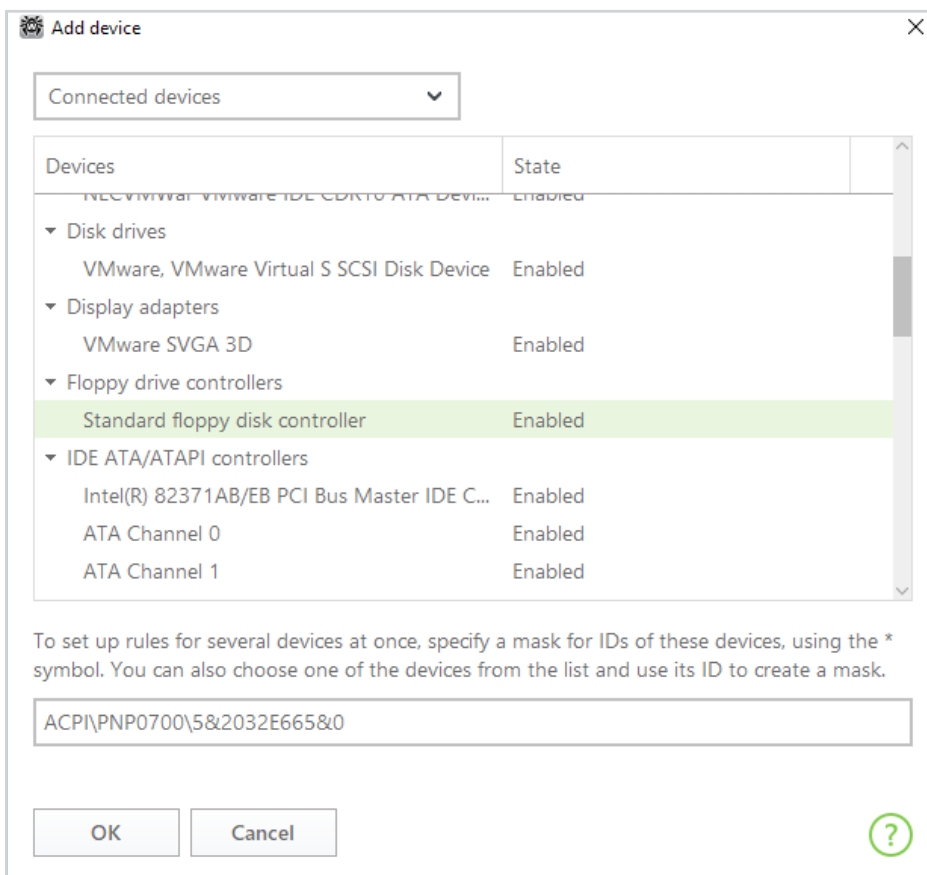
In this window, select **Restrict access to removable media**. Then click **Change** for the device classes, and select the desired device classes.



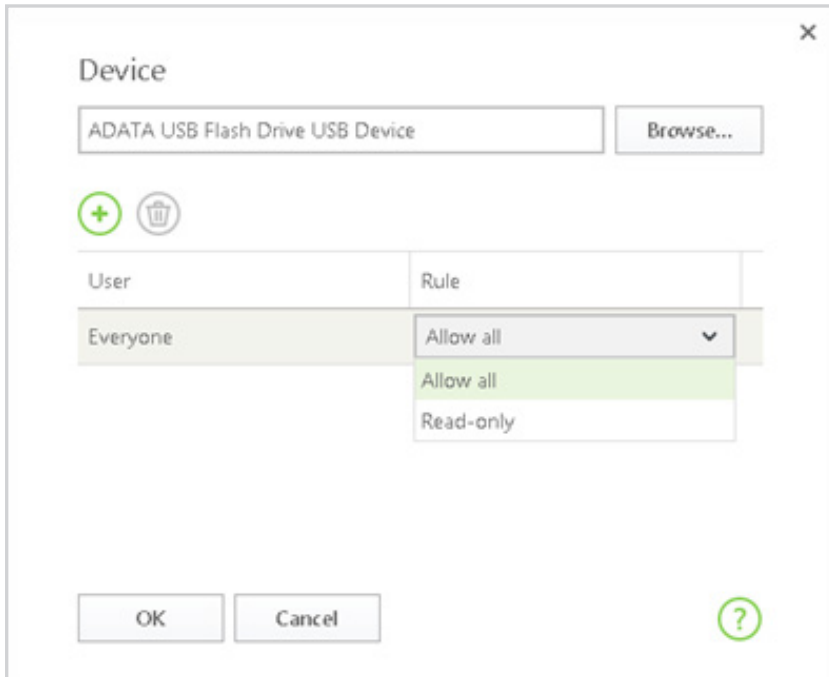
After that you will be able to configure the **Whitelist**. If you only want the devices on the whitelist to be accessible, click **Change** → .




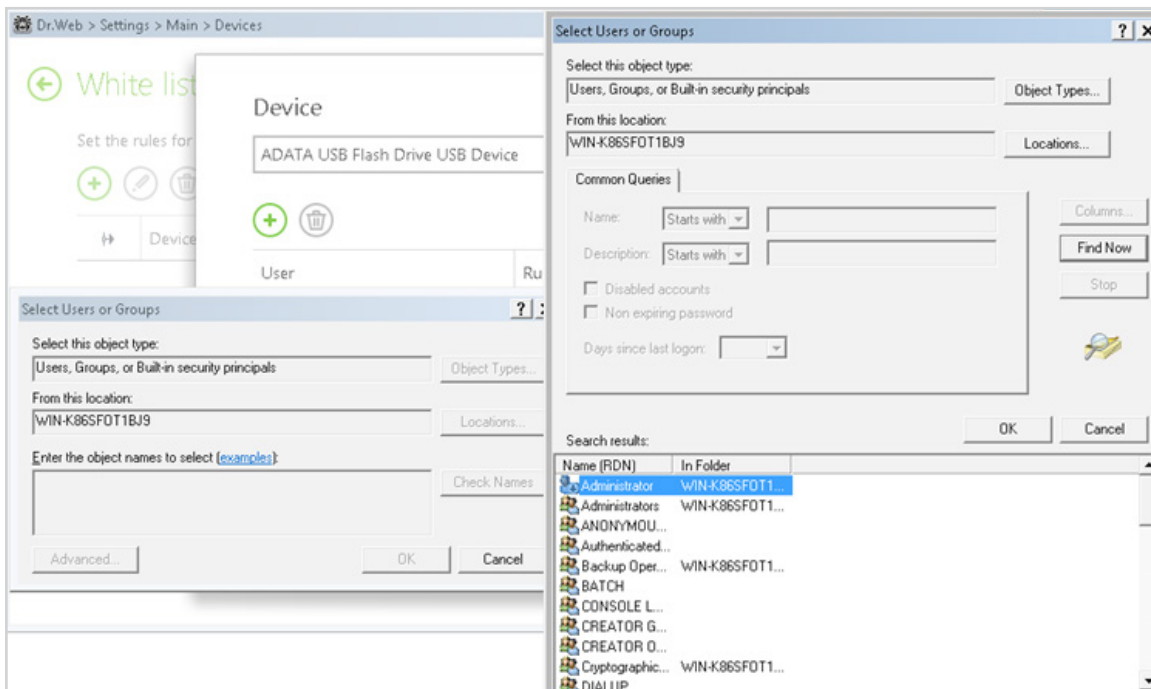
In the subsequent window, click **Browse** and select the desired device.



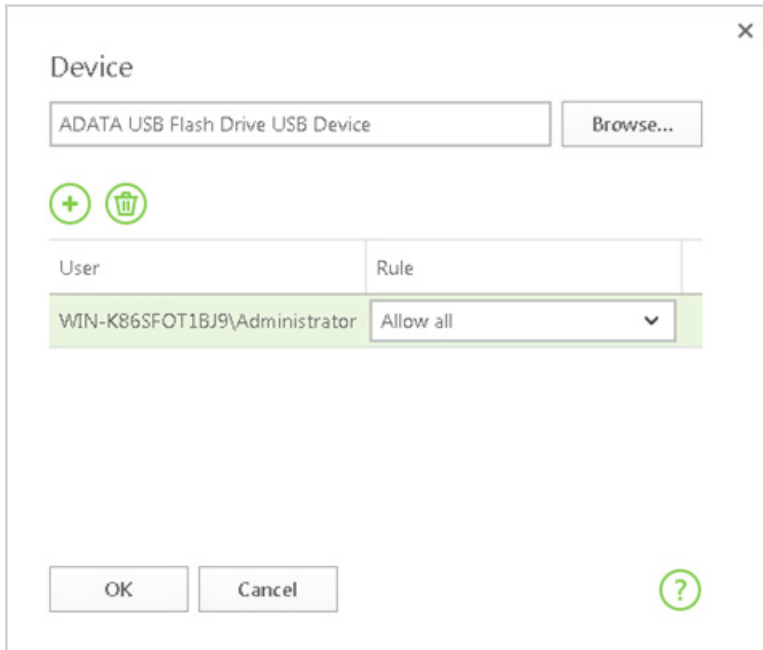
Press **OK** to confirm your choices.



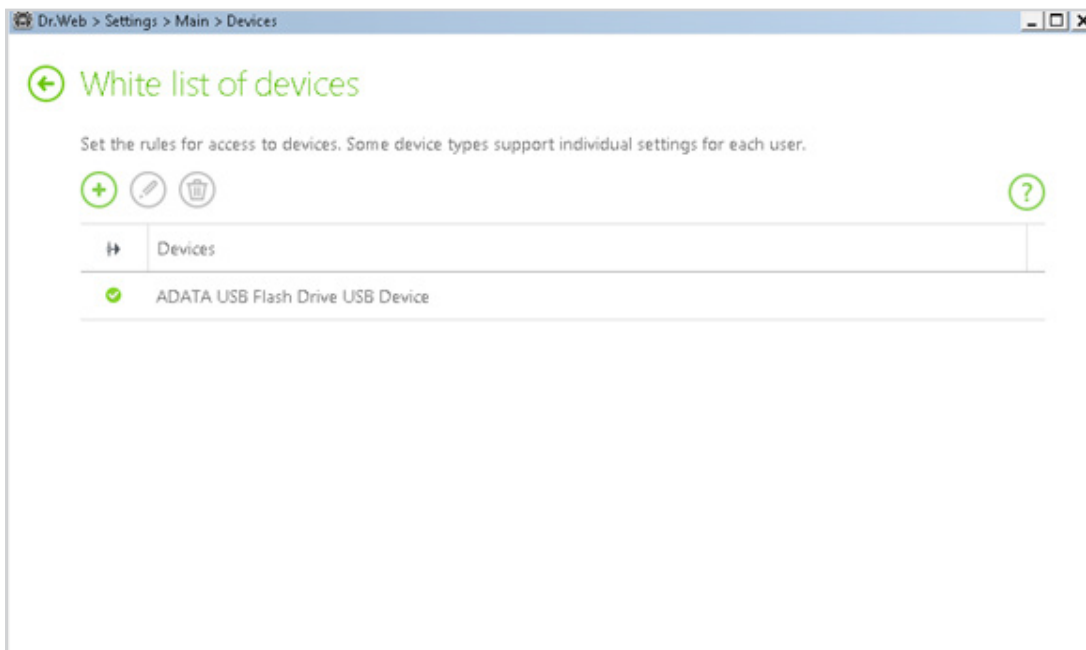
If you want to grant specific users access to certain media, click on the  icon, and select the user accounts for which you need to grant access.







Specify permissions for the device.

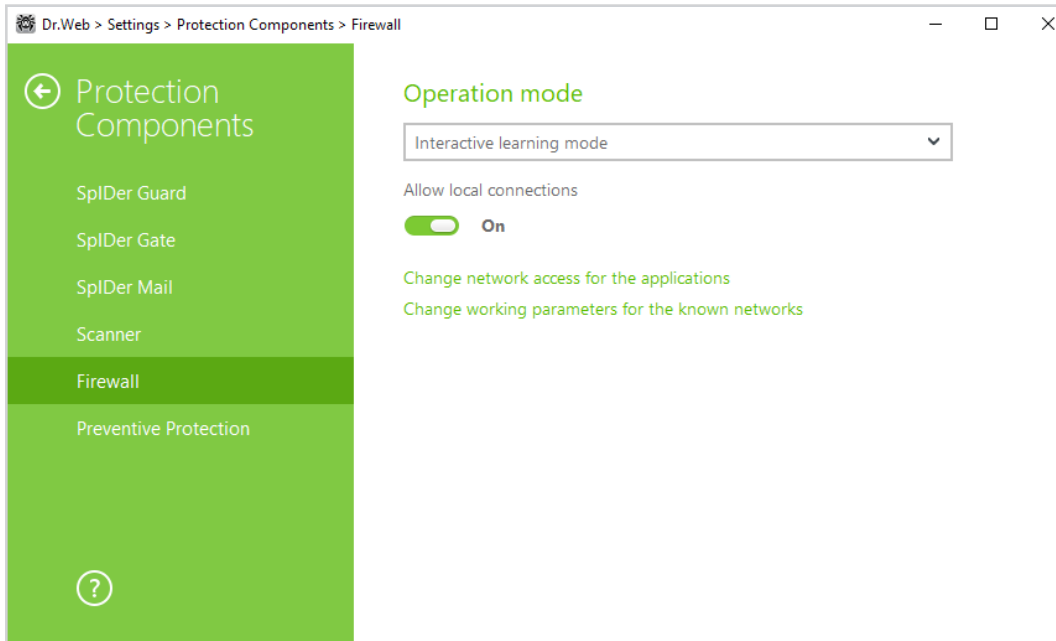


Specify permissions for the device.

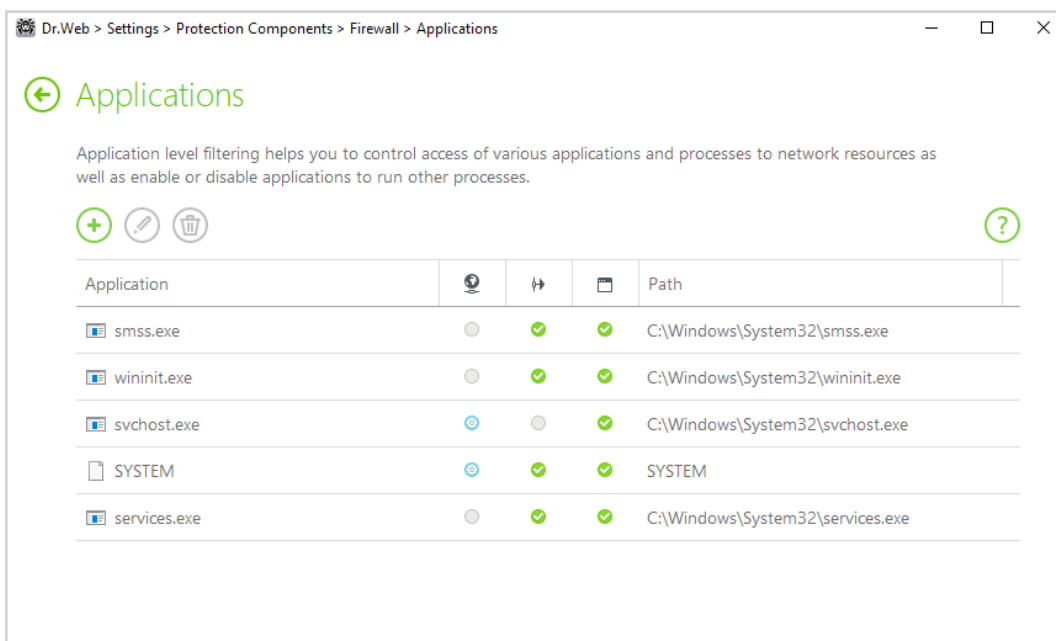


9. You should restrict Internet access for the programs you use — you can do this with the help of the Firewall component.

To configure **the Firewall**, click on the icon  in the system tray; click on the padlock icon  to make the settings accessible (the icon will now look like ). Then click on the gear icon . In the settings window, select **Protection Components** → **Firewall**.






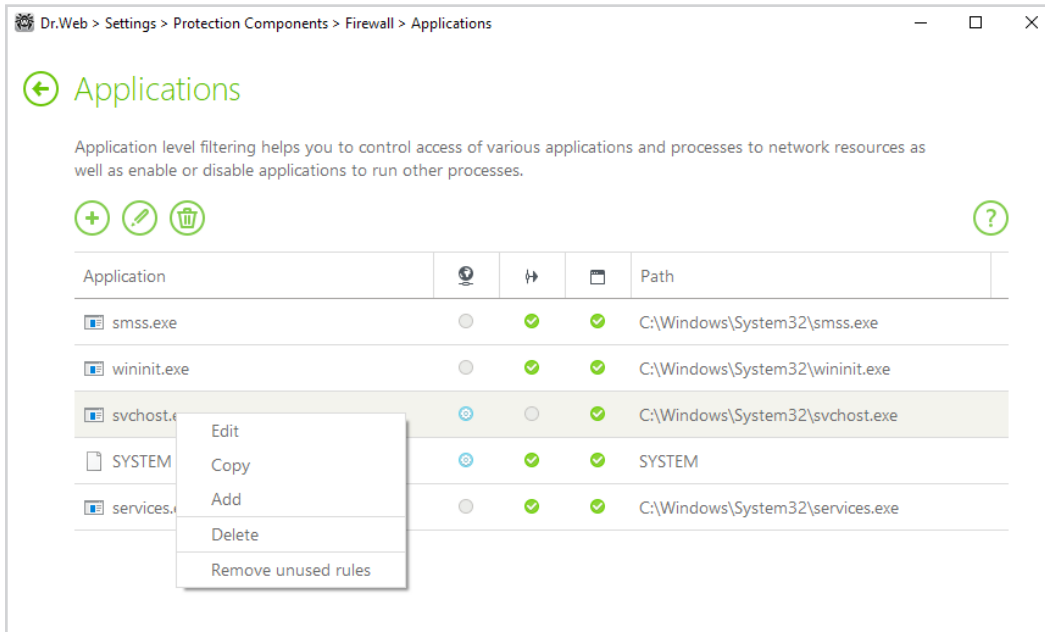
Application filtering lets users control access to network resources for specific programs and processes. Each program can have only one filtering rule set.



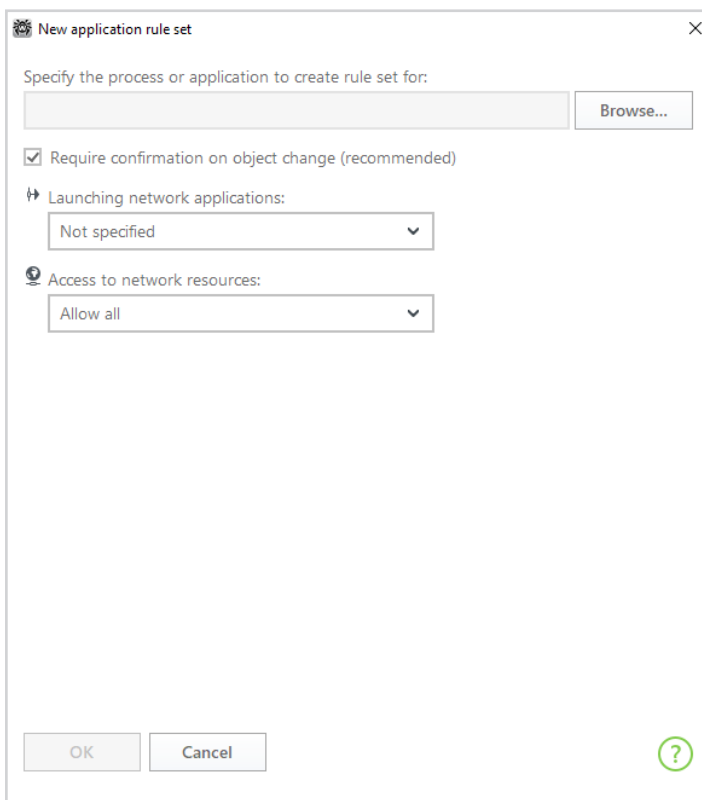
To access this window, in the **Firewall** settings, select **Change network access for applications** and click on , or select an application and click on .

To form this rule set, try doing one of the following:

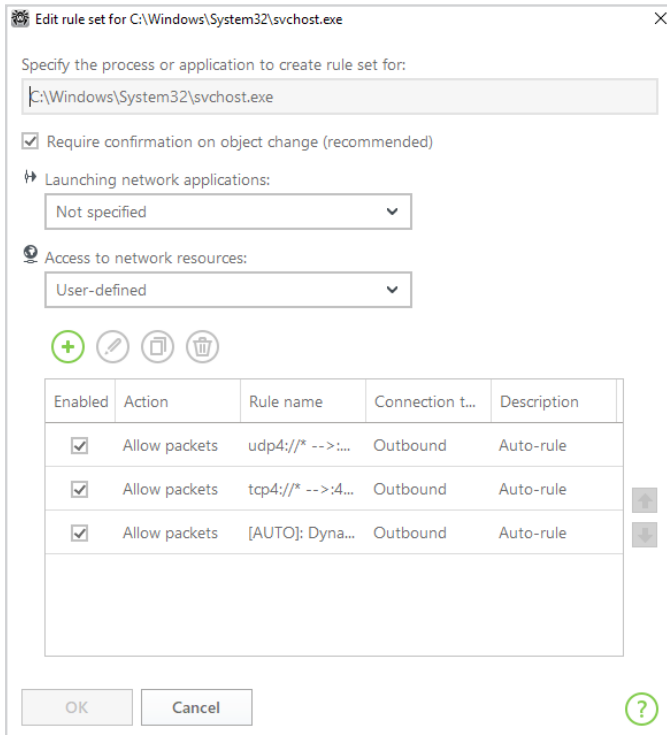
- To create a set of rules for a new program, click on  (Create).
- To edit the existing rule set, select it in the list, and click on  (Change).
- To add a copy of an existing rule set, select **Copy** in the context menu. A copy will be added below the selected set.
- To remove all the rules for a program, select the set from the list, and click on  (Remove).



The window **New application rule set** (or **Edit rule set**) displays the rule type for a particular application or process, and a list of rules. You can change the rule type and create a list by adding new filtering rules or editing existing ones, and by changing the order in which they are executed. The rules are applied consistently according to the list.






You can create a rule using the **Firewall** settings window. When working in the training mode, you can create rules directly from the unauthorised connection attempt notification window.

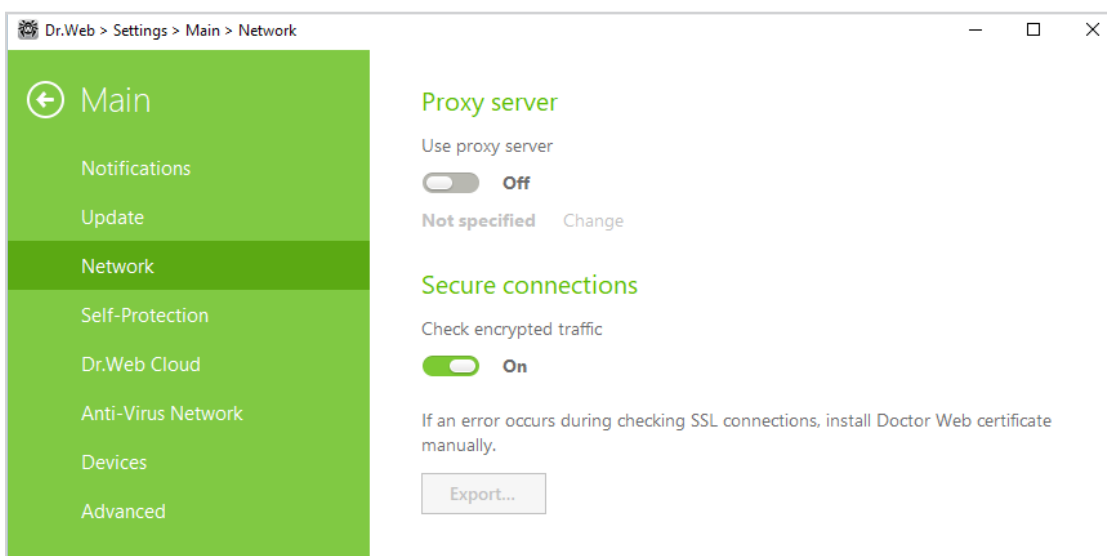


10. Encrypted traffic scanning should be enabled. Currently almost half the traffic on the Internet is decrypted, and cybercriminals can take advantage of that.




As a rule, miners perform their tasks as part of botnets—groups of infected computers. This lets them substantially increase the odds that the mining will be profitable.

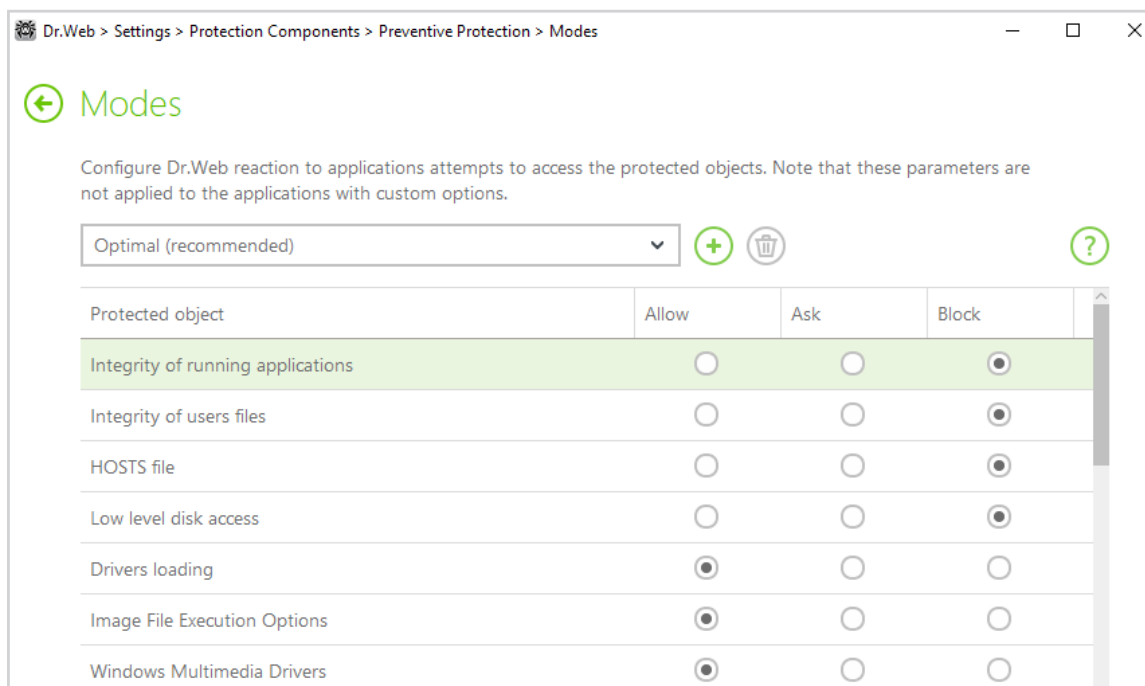
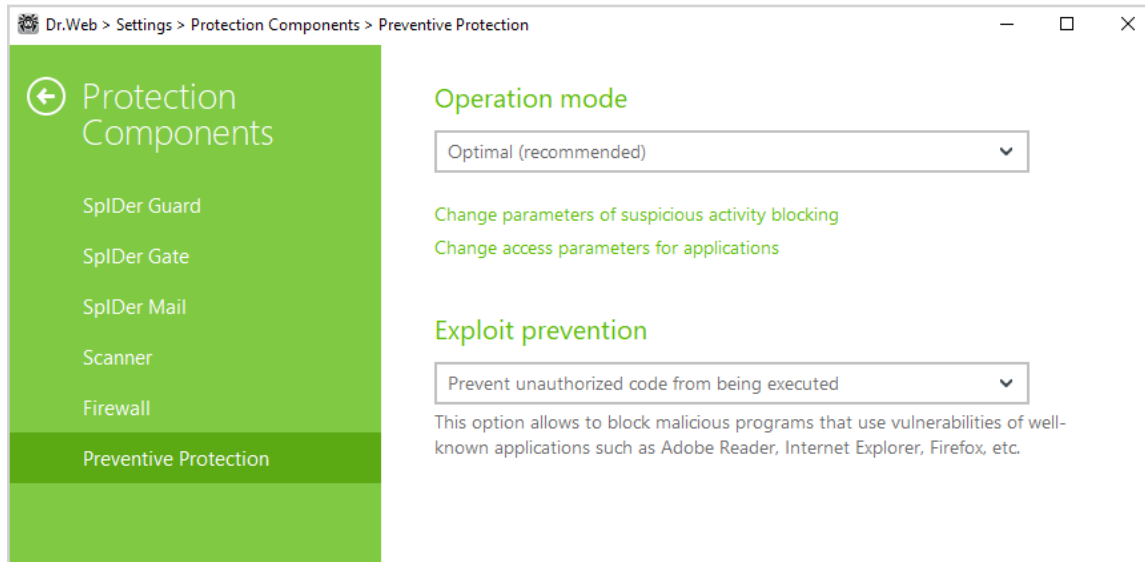
In addition, miners are useless for cybercriminals unless they have Internet connectivity.

Enable encrypted traffic scanning (this feature is only available in Dr.Web Security Space): click on the  icon in the system tray; in the next menu, click on  (**Administrator Mode**) and then on the gear icon  (**Settings**) when it appears. In the **Settings** window, select **Main** and then **Network**. The toggle for **Encrypted connections** should be on.



11. Dr.Web Process Heuristic settings should prevent miners from embedding exploits into running applications




Check the settings by clicking on the  icon (the icon will change to ) and then on the newly appeared  icon; select **Protection components** in the **Settings** menu, and then select **Change parameters of suspicious activity blocking**.

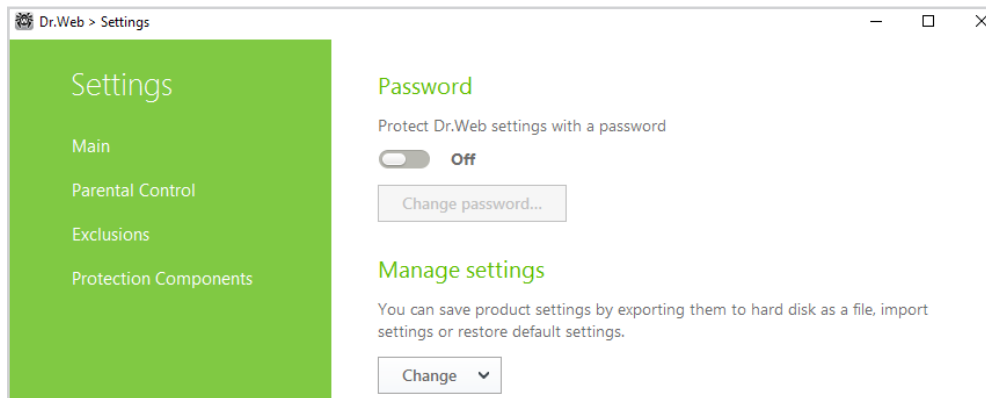


The **Allow** status lets users and cybercriminals make the corresponding changes.

12. Setting a password ensures that your protection won't be disabled by cybercriminals — even if your PC gets hacked.

Malicious programs, including miners, strive to disable anti-viruses. Don't make it easier for them to do that.

To set a password, click on the  icon (its appearance will change to ). Click on the  icon, and in the **Settings** menu, select **Main**. Toggle on the corresponding option, and click on **Change password**.





Important! It is recommended that you do not use the same password you use to access your computer or device.

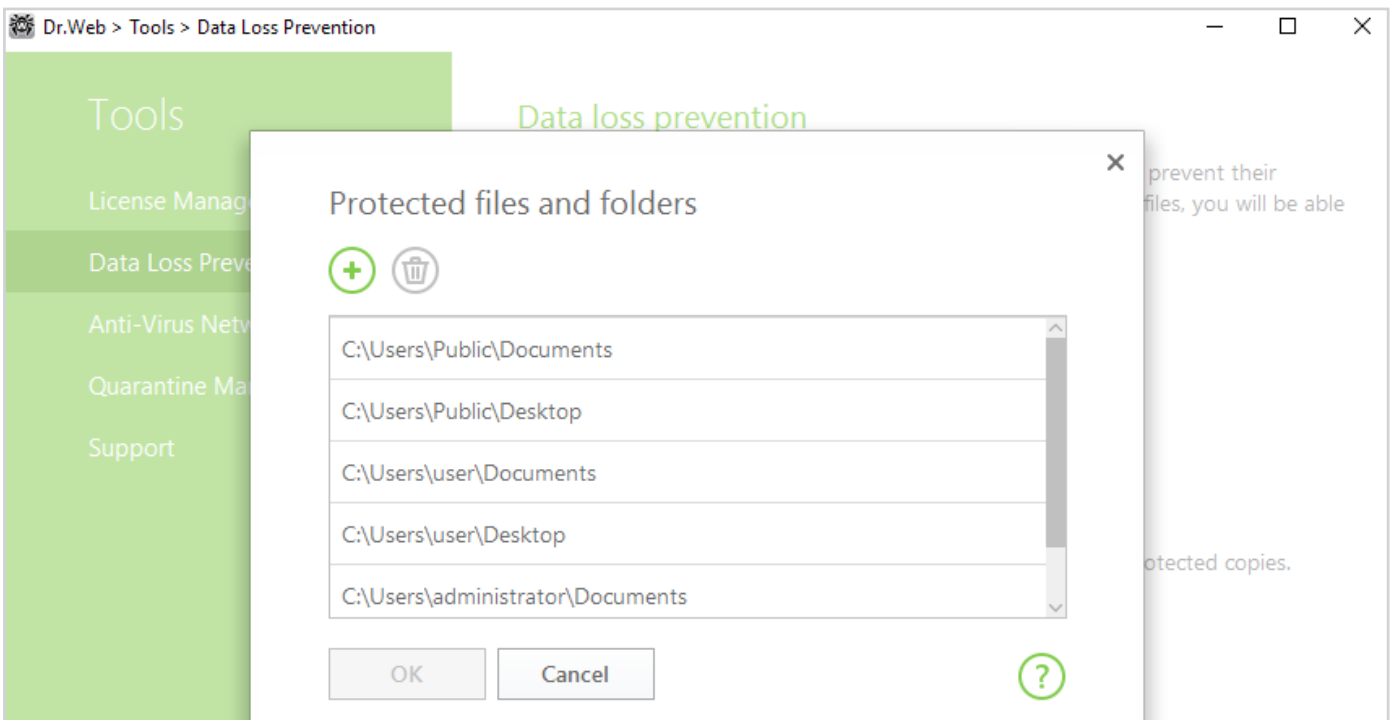
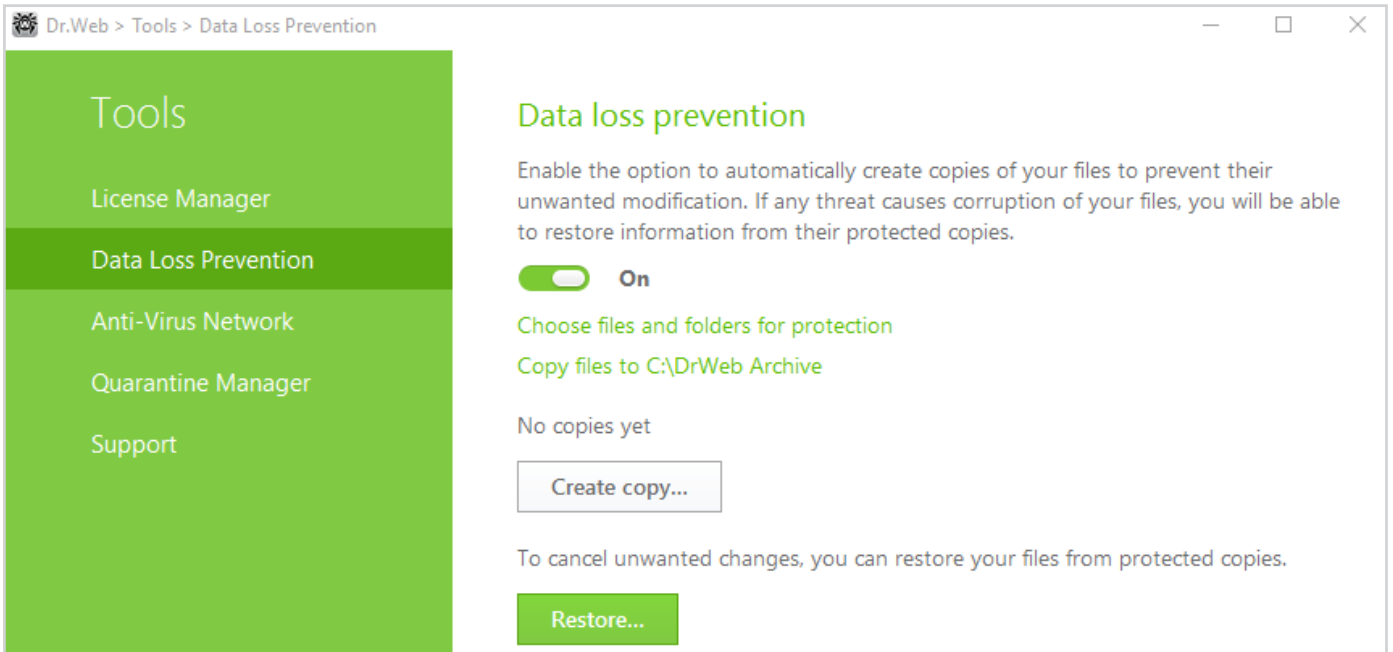
We also recommend that you:

1. Enable and configure the Data Loss Prevention component.

Some miners are not so harmless. For example, [Trojan.BtcMine.1978](#). If anyone tries to shut down this process manually, Windows performs an emergency shutdown and displays the «blue screen of death» (BSOD).

We must not forget that not all virus writers are professionals in the field of programming, and their «creations» can damage the data on your computer.

To configure **Data Loss Prevention**, click on the  icon in the system menu, and then in the newly appeared window, click on , and select **Tools**.



The **Data Loss Prevention** feature is available in Dr.Web Security Space, the Dr.Web Premium package of the Dr.Web Anti-virus service, and under the Dr.Web Desktop Security Suite Comprehensive Protection license. If you inadvertently purchased a product that does not contain this module, you can contact Doctor Web's partners and expand your license to include it.

No anti-virus can detect all malicious programs at the moment they attempt to penetrate your computer, but using Dr.Web [technologies](#), you can ensure the maximum protection possible for your data.



© Doctor Web
2003 — 2018

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992.

3d street Yamskogo polya 2–12A, Moscow, Russia, 125040

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

Fax: +7 495 **789-45-97**

www.drweb.com | www.av-desk.com | free.drweb.com