Dr.WEB®
since 1992

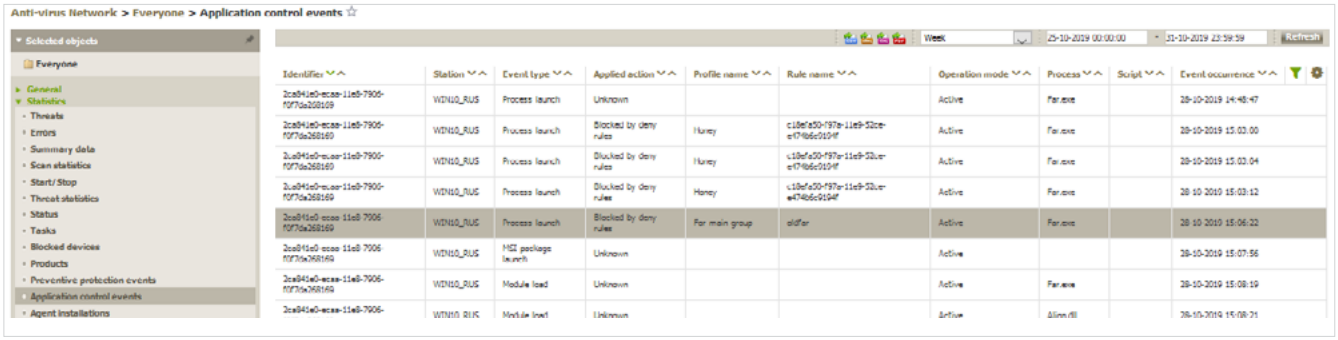
Dr.Web Enterprise Security Suite 12.0 Using Application Control to block programs

Dr.Web Enterprise Security Suite 12.0

Using Application Control to block programs

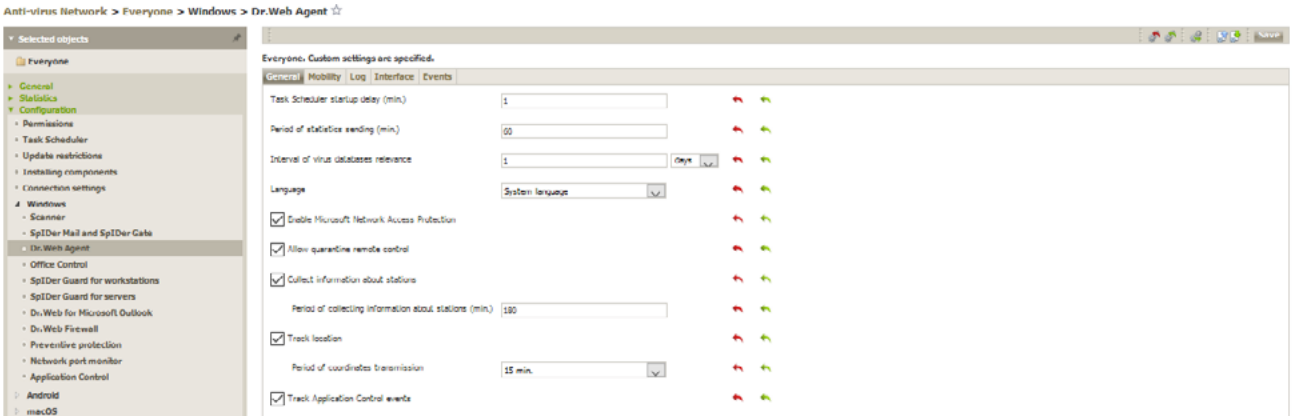
To create a rule for the **Application Control** module within Dr.Web Enterprise Security Suite's Control Center, you need to have information on the file you need to block. This information is easily obtained.

First, allow the gathering and sending of information from stations for the **Application Control events** section.



1. In the tree in the **Anti-virus Network** section, select the station or group of stations the **Application Control** module is installed on from which you want to receive information about the applications being launched.
2. In the control menu, select **Windows** → **Dr.Web Agent**.
3. In the **General** tab, tick the box next to **Track Application Control** events to monitor the station process activity detected by the Application Control module and send the events to the Server.

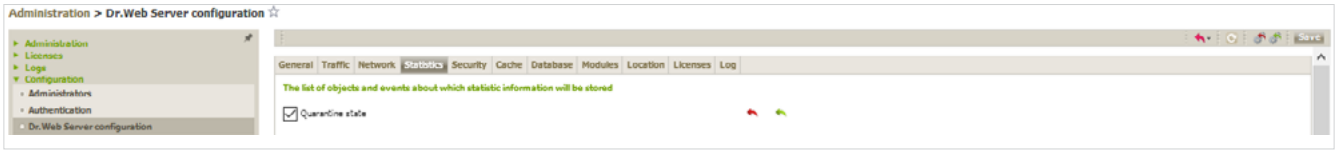
   Important! If the box is cleared, process activity is ignored.



   If there is no connection to the Server, events are collected and sent when a connection appears.
4. Click on **Save**.

Allow the anti-virus server to collect information for the **Application Control events** section.

1. In **Administration** → **Dr.Web Server configuration**, go to the **Statistics** tab.



2. Select one of the following options:

- **Application Control statistics on processes activity** — to receive and record information on the activity of all the processes: both those allowed to be launched and those whose launch is denied by the Application Control module.

  When this option is enabled, all the applications on the stations, regardless of whether or not profiles were created to control the launch of applications, will be added to the catalog.

Importan! Selecting this option can significantly increase the intensity with which resources are consumed as statistics are collected throughout the anti-virus network.

- **Application Control statistics on processes blocking** — to receive and record information on the activity of all the processes that have been blocked by Application Control.

  When this option is enabled, applications will be added to the catalog only after profiles (whose setting are used to block the launch of applications) have been created and assigned to the anti-virus network stations.

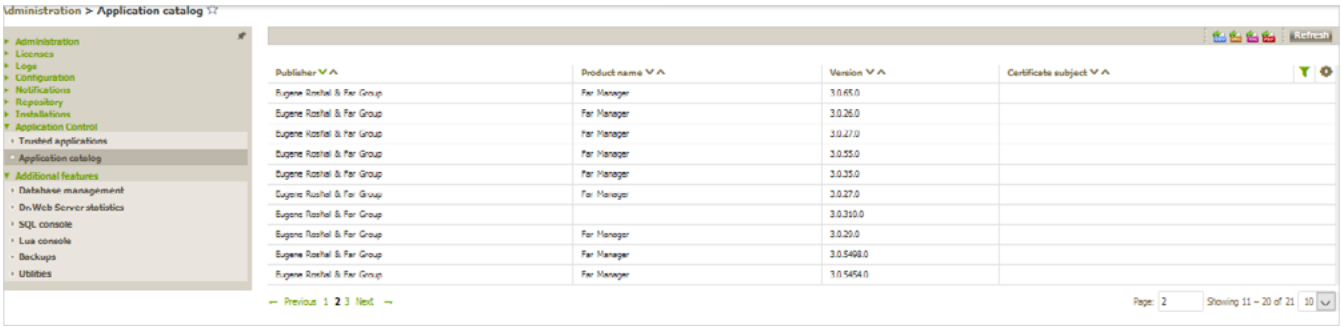
3. Click on **Save**.

4. Restart the anti-virus server.

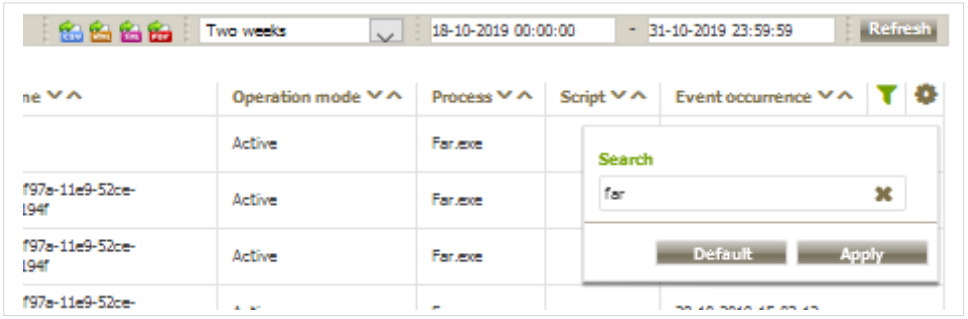
After rebooting, the server will start recording all application launch-related statistics from all the stations that have Application Control installed on them. The Agent sends information about each application to the server only once, when an application first becomes active.

Information concerning the launch of applications installed on protected Windows stations and connected to the Dr.Web anti-virus server is recorded in the Application catalog.

To view the application catalog, go to **Administration** → **Application Control** → **Application catalog**.

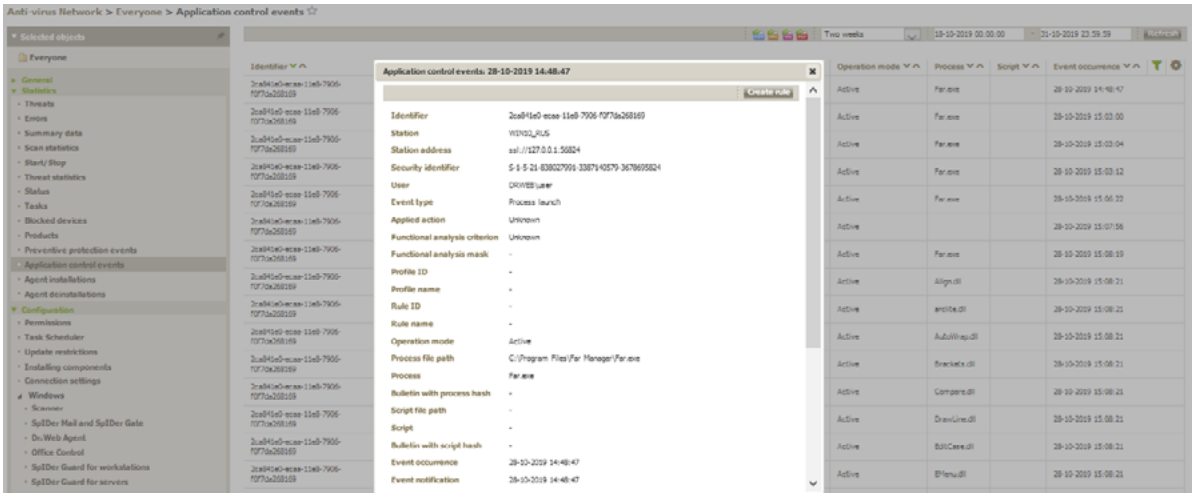


Now, let's use the search on the statistics page.

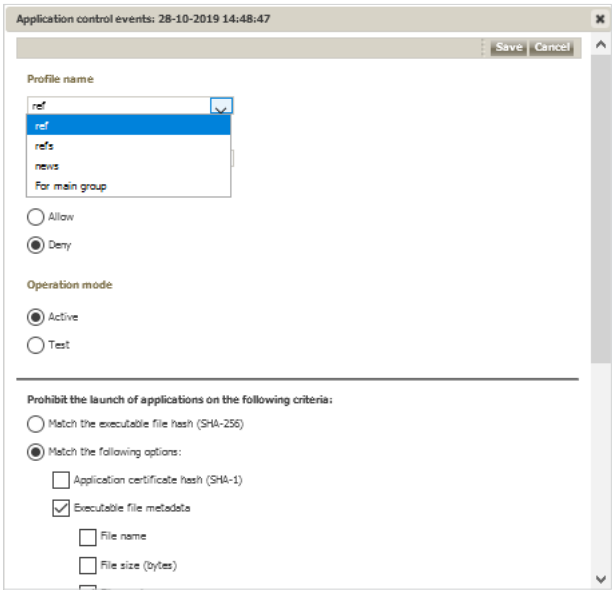


Click on **Apply**.

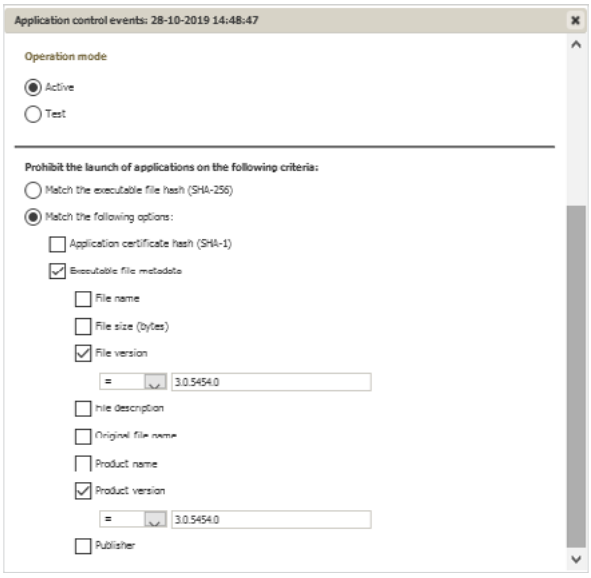
Click on the line that has information about the running program.



Click on **Create rule**.

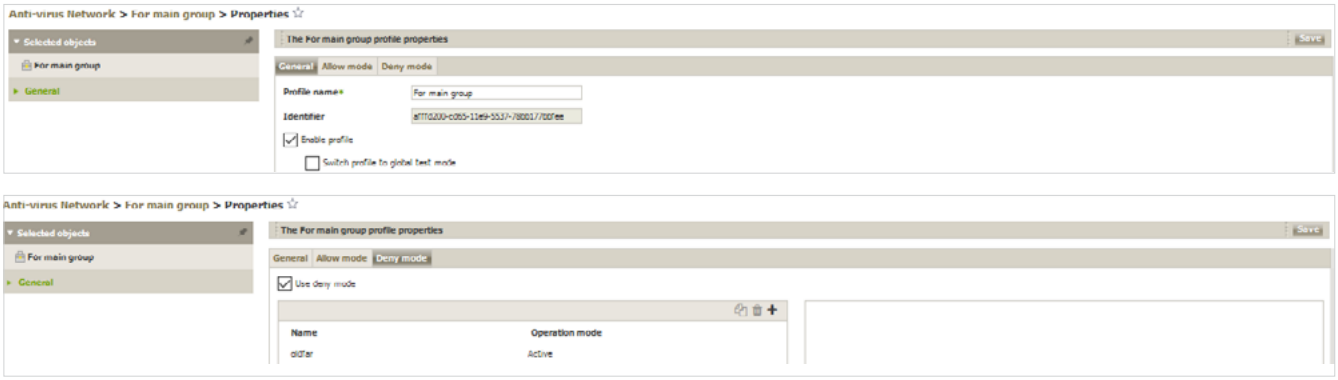


In the profile drop-down list, select the profiles where you will create the deny rule.

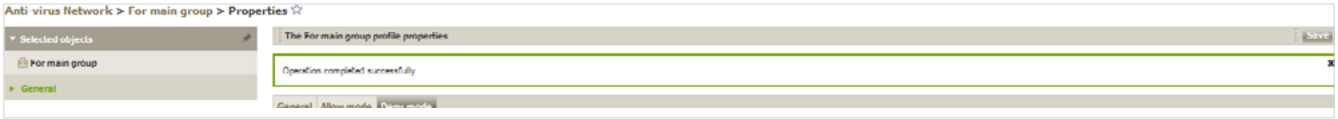


Select the type of rule (**Deny**) and the operating mode (to keep things simple, let's select **Active**). Select the options according to which the rule will work. In our case, this is the version of the program. Finish the rule creation process.

Do not forget that to activate deny rules, you must disable the test mode for a profile and enable the deny rule operation.



If these properties are not specified, select them and click on **Save**.



The problem solved.

Doctor Web
2003–2019

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040
Tel.: +7 (495) 789–45–87
Fax: +7 (495) 789–45–97

https://www.drweb.com | hhttps://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com