Dr.WEB®
since 1992

Dr.Web Enterprise Security Suite 12.0 Using Application Control to block outdated software

Dr.Web Enterprise Security Suite 12.0

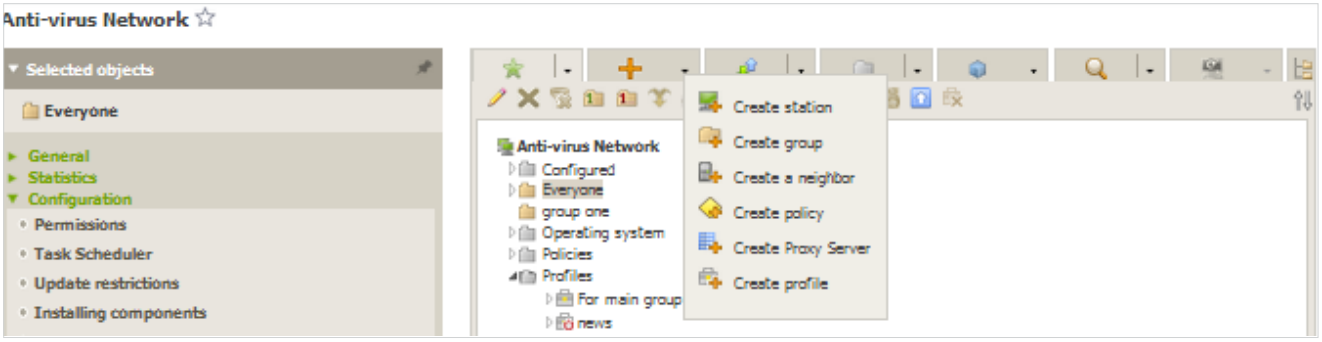
Using Application Control to block outdated software

Outdated software is one of today's security problems. Users do not want to update their systems, and malware programs exploit unclosed vulnerabilities. Fortunately, there is a solution. The **Application Control** module included in the Dr.Web Enterprise Security Suite Control Center can block outdated software.

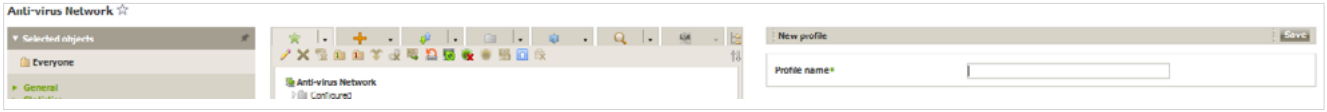
Configure the application control system using profiles—profile settings will dictate which applications will be launched or blocked on stations (or for selected users).

To create a profile

1. Select **Anti-virus Network** in the Control Center's main menu.
2. In the newly appeared window, on the toolbar, click on **Add network object** → **Create profile**.



3. In the subsequent panel, enter the **Profile name**.



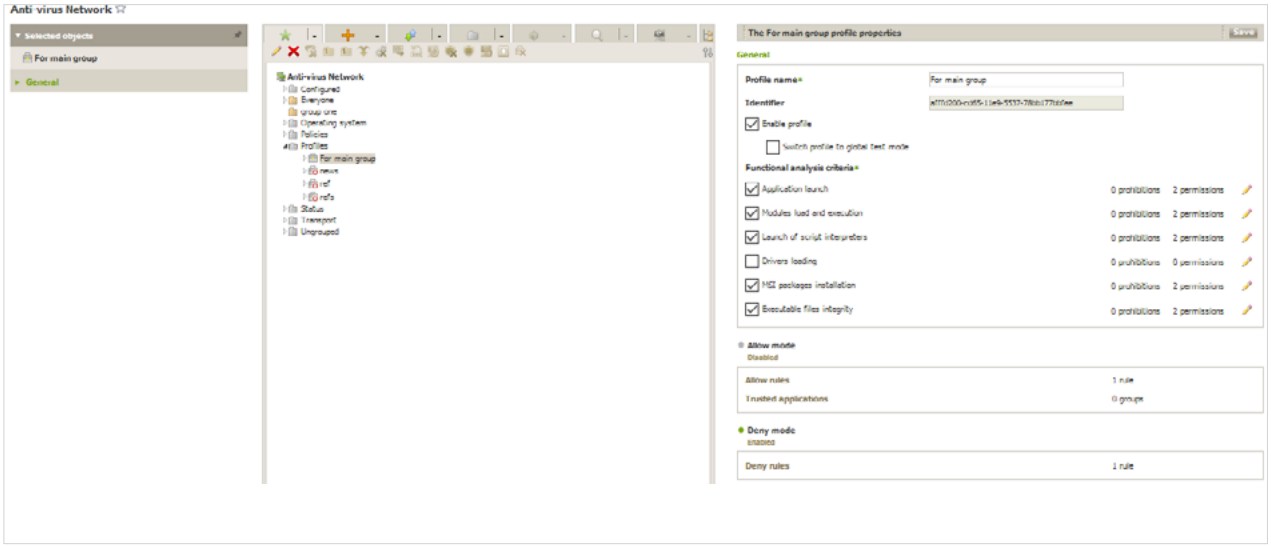
4. Click on **Save**.

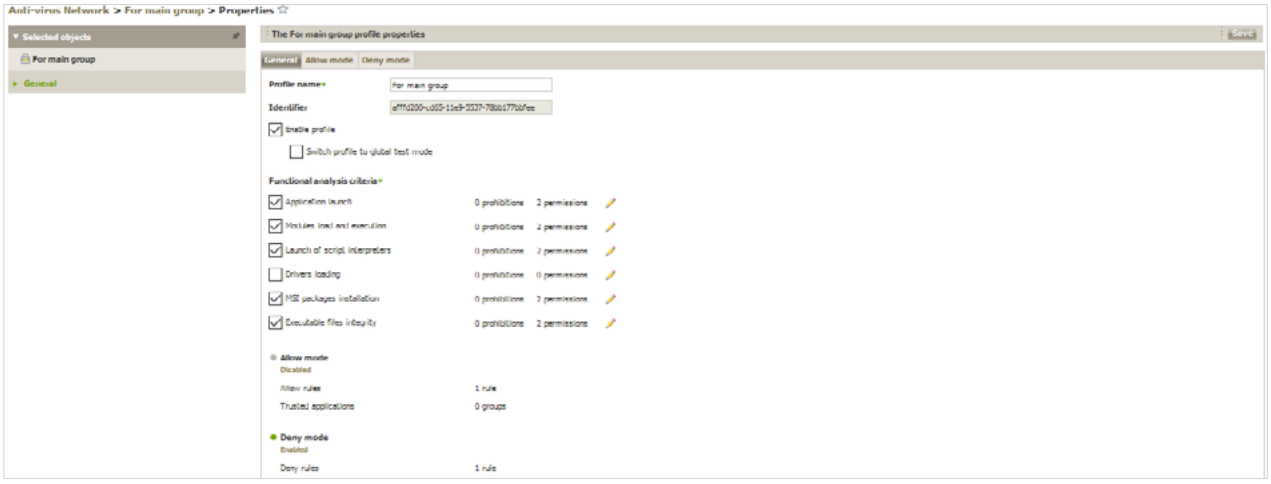
5. The new profile will be created and placed in the **Profiles** group of the anti-virus network tree.

After you create a profile, you need to configure it (specify the necessary restrictions and operating rules) and assign it to anti-virus network stations and users.

Important! It is recommended that you configure profiles in the test mode. The test mode imitates what the Application Control module does, fully logging the activity occurring on all the protected stations in the statistics log, but applications are not actually blocked.

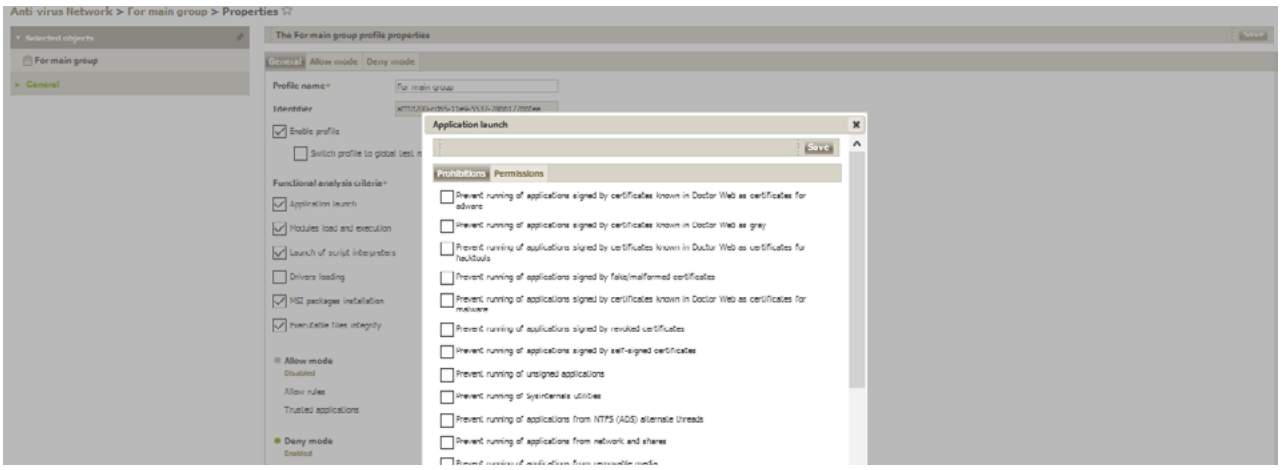
1. In the Control Center's main menu, select **Anti-virus Network**. Click on the profile name in the hierarchical list of the anti-virus network (on the right side of the Control Center's window, the profile properties panel will automatically open), or click on the profile icon in the anti-virus network tree, or select a profile and then select **Properties** in the control menu (a window showing the profile properties will open).





2. Select **Enable profile** to start using this profile. If you select **Switch profile to global test mode**, all the profile settings will not be applied to the stations, but activity will be recorded as if the settings were enabled.
3. In the **Functional analysis criteria** section, select the events that you want to track

To specify advanced settings for each selected event criteria type, click on ✎ (**Edit**) for the corresponding type of event. A window showing a list of settings will open.



Tick the boxes for the settings that you want to be applied.

If you enable an event types but do not specify its advanced settings, launch control will be carried out for all the objects according to this criteria in accordance with the allow or deny modes. If you specify advanced settings but do not enable the event type itself, neither the advanced settings nor the criteria will be executed.

To save the advanced settings, click on **Save** in the window containing the list of advanced settings.

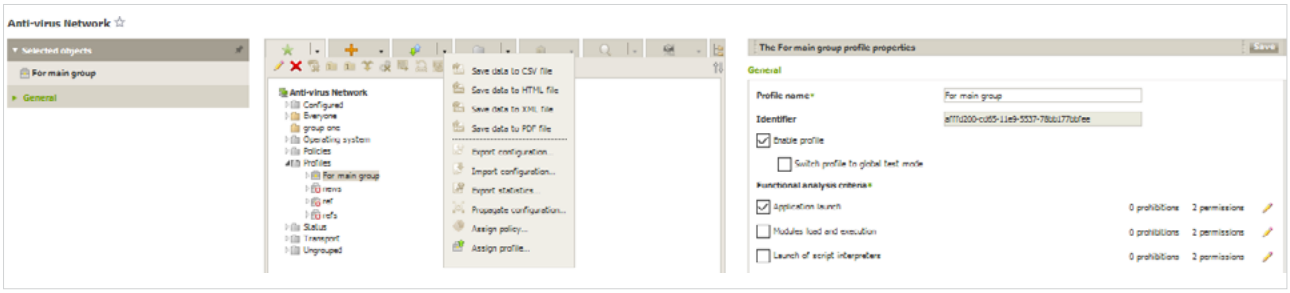
4. To apply the settings specified in the **General** section, click on **Save** in the profile settings.
5. The **Deny mode** assumes that only applications that comply with deny rules are denied on all the controlled stations. All other applications are allowed.

   To enable or disable this mode and to configure rules, go to the **Deny mode** section in order to select the appropriate section.

   1. In the **Deny mode** tab, tick the box next to **Use deny** mode in order to use this mode.
   2. Click on **Save**.

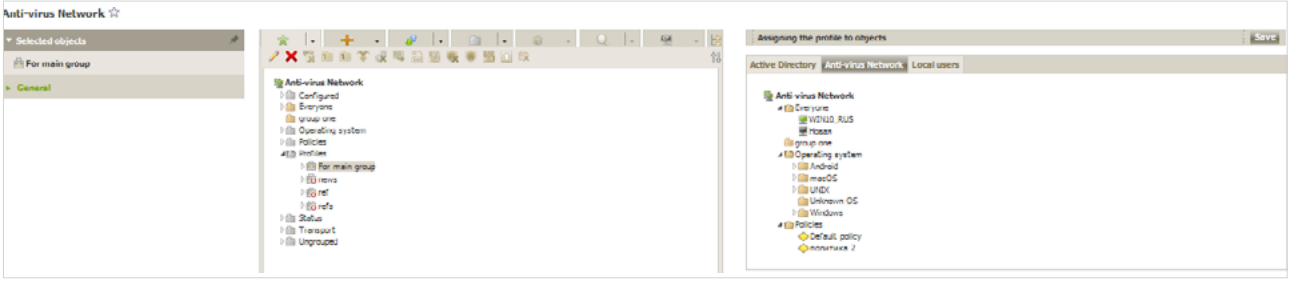
The second stage in configuring the application launch control system involves assigning a created and configured profile to stations or anti-virus network users.

1. Select **Anti-virus Network** in the Control Center's main menu.
2. In the newly appeared window, from the hierarchical list, select the profile that you want to assign.
3. On the toolbar, click on **Export Data** → **Assign profile**.



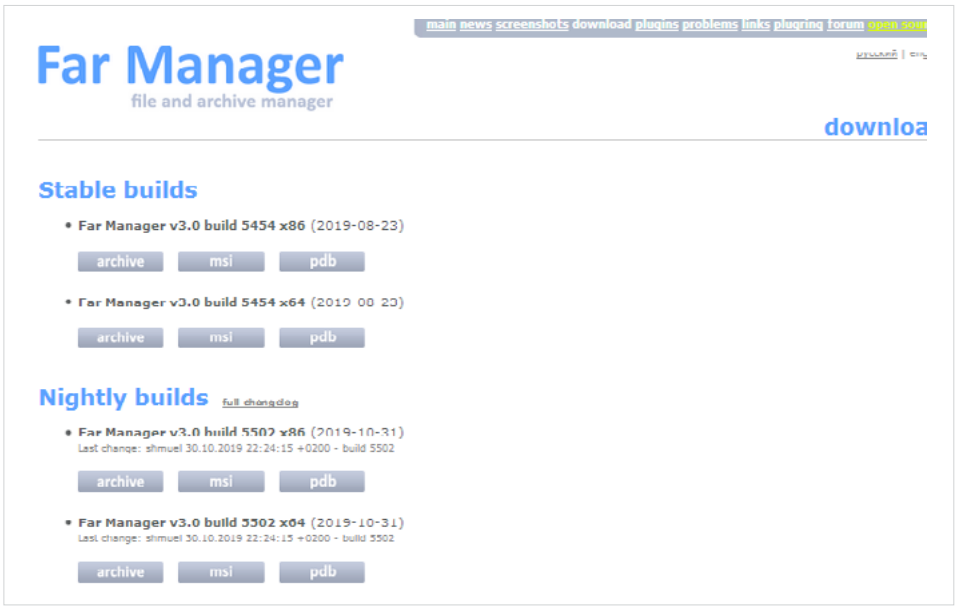
4. In the newly appeared window, select the object to which the settings are to be distributed. In the case of the global deny to execute malicious code option, the most logical thing to do is to assign this restriction to all the stations in the anti-virus network.

   In the **Anti-virus Network** tab, you can select groups of stations (the settings will be applied to all the user accounts of all the stations included in the group data) or individual stations in groups (the settings will be applied to all the user accounts of the selected stations):



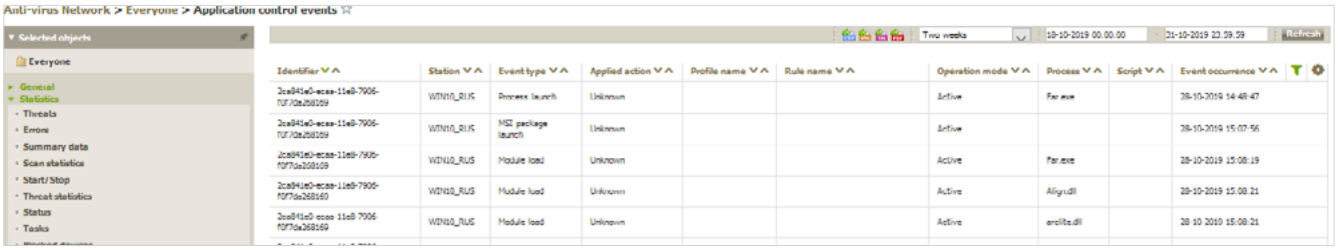
5. Click on **Save**. All the objects selected will be added to the list covered by the configured profile and displayed in the tree as nested objects of the configured profile.

You can now start creating deny rules.
As an example, take one of the popular utilities—Far Manager—and download its two versions.

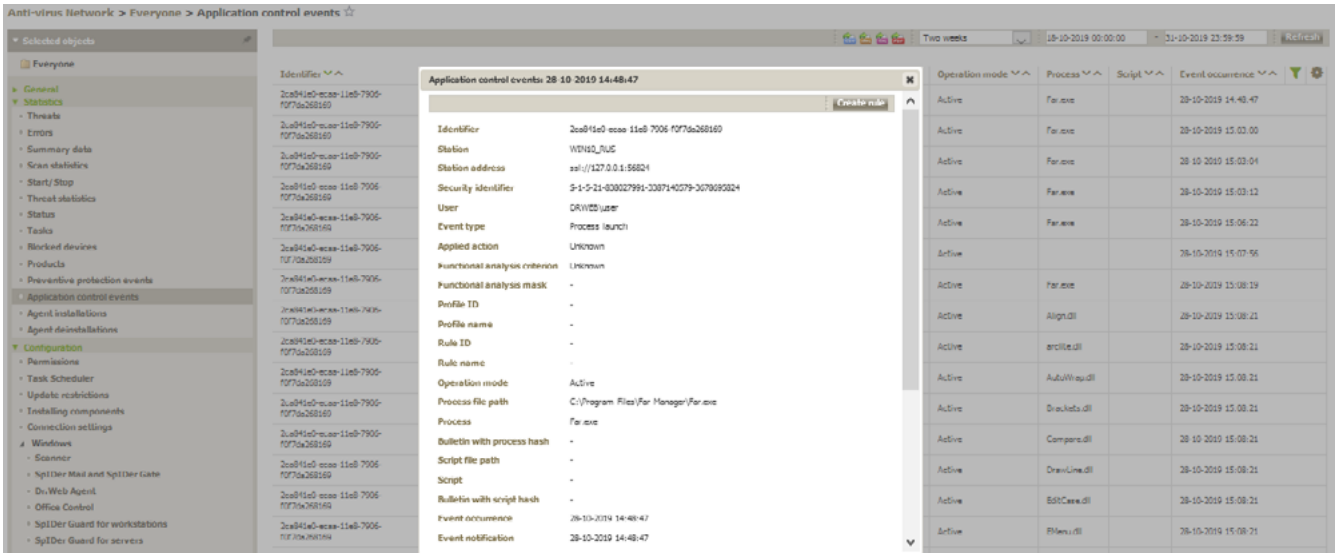


Install the earlier version. Run it.

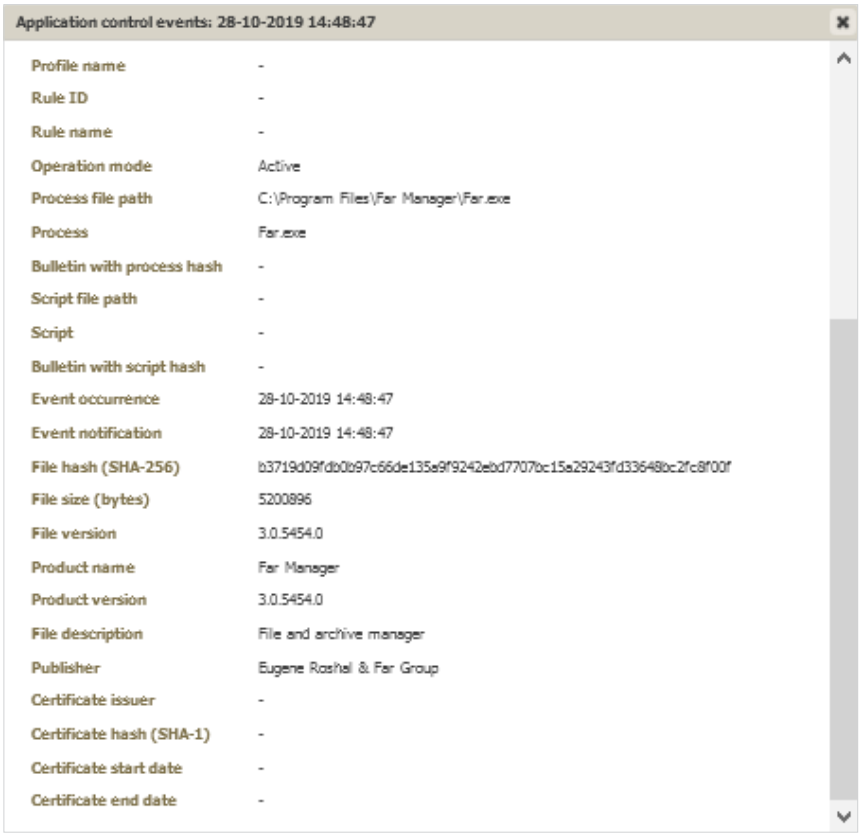
Go to **Statistics → Application control events**.



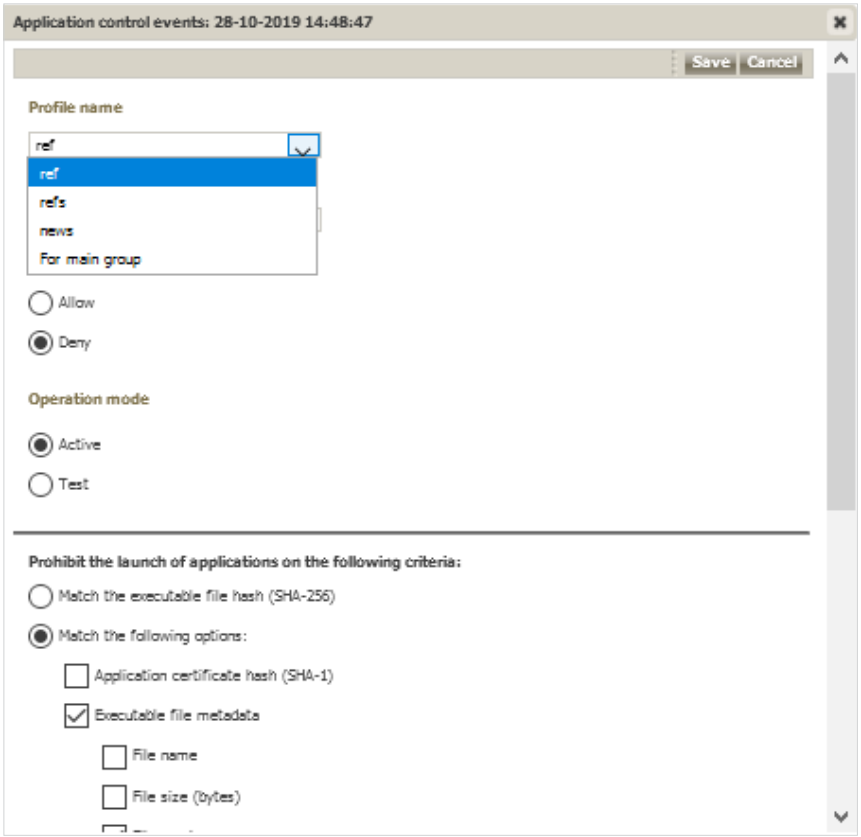
Click on the line that has information about the running program.



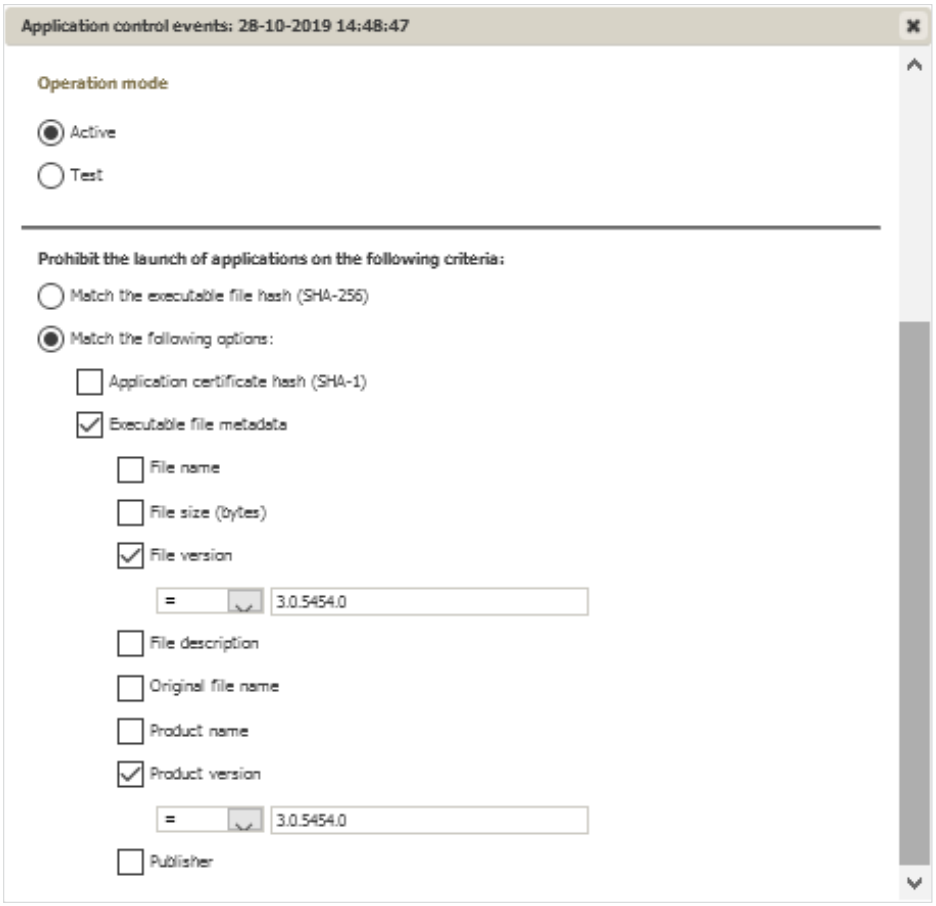
If you scroll down the newly appeared window, you will see information about the program version.



Scroll back and click on **Create rule**.

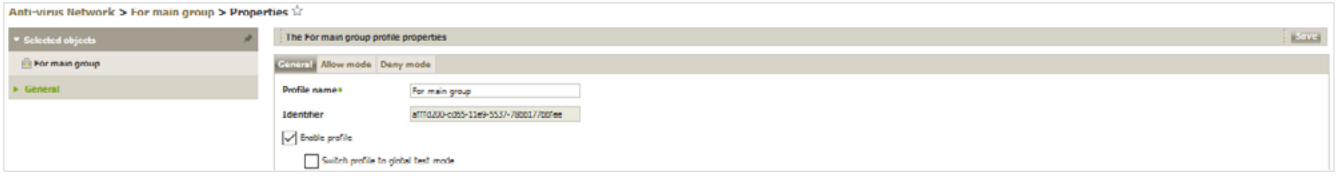


In the profile drop-down list, select the profiles where you will create the deny rule.



Select the type of rule (**Deny**) and the operating mode (to keep things simple, let's select **Active**). 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**.

Start the utility. To be more precise, try to start it. The start failed, and the record about this appears in the statistics:

2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Process launch	Blocked by deny rules	For main group	oldfar	Active	Far.exe		28-10-2019 15:06:22

However, if we update the utility, it will run correctly.

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