Dr.WEB®
since 1992

Dr.Web Enterprise Security Suite 12.0 Features of the Application Control module

Dr.Web Enterprise Security Suite 12.0

Features of the **Application Control** module

Important! Before initiating the upgrade procedure, it is recommended that you study the relevant sections of the product documentation for Dr.Web Enterprise Security Suite 12.

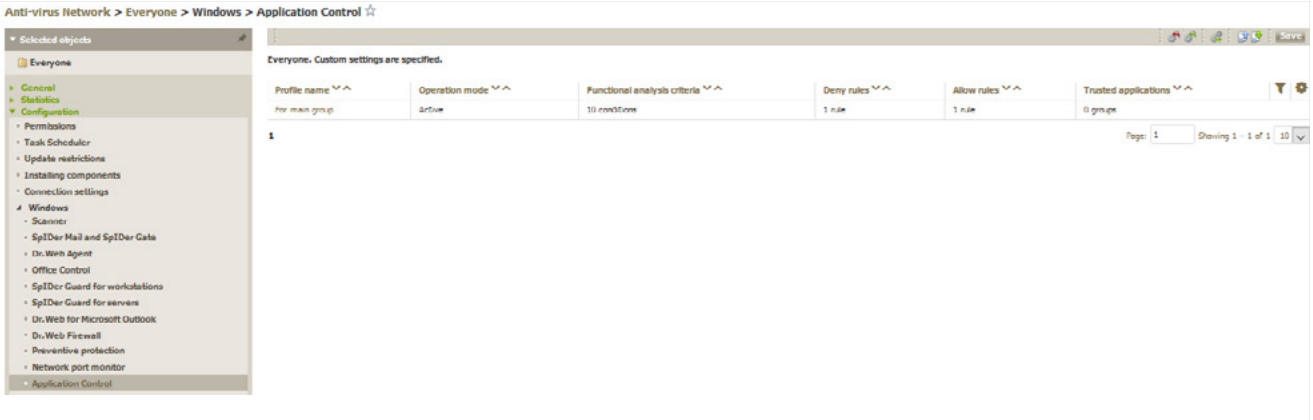
Contents

1. The module’s purpose and configuration procedure

To block malicious files that are known only to be found in mailings, you can use the functionality of the **Application Control** module within **Dr.Web Enterprise Security Suite's Control Center**.

This module monitors the activity of all the processes running on the protected stations in an anti-virus network. **Application Control** lets the system administrator (or the security specialist) allow or deny the launch of applications on stations running Dr.Web Agent for Windows.

The presence of the **Application Control** module depends on the type of operating system being protected.



Anti-virus Network > Everyone > Windows > Application Control

Everyone. Custom settings are specified.

Profile name	Operation mode	Functional analysis criteria	Deny rules	Allow rules	Trusted applications
For main group	Active	10 conditions	1 rule	1 rule	0 groups

1

Important! The **Application Control** module can only be configured via the Control Center—it's impossible to configure the module via the stations running Dr.Web Agent.

To configure **Application Control**, do the following:

1. Create a profile.

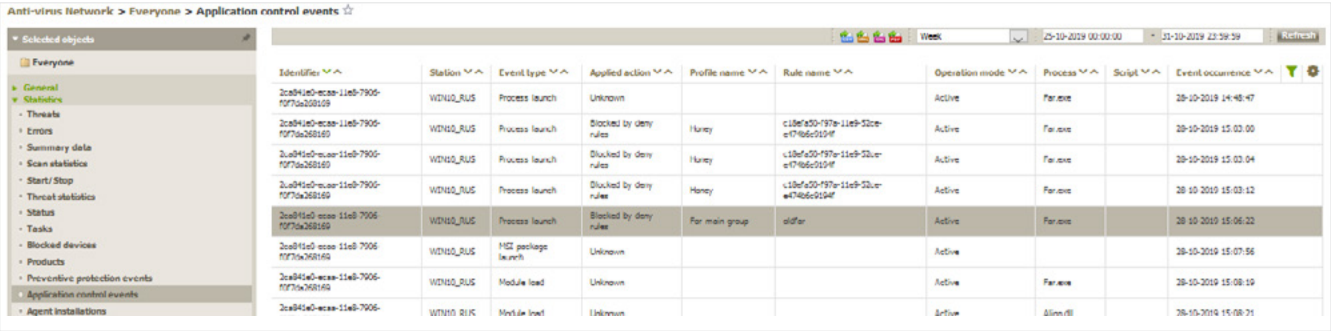
   The launch of all applications is allowed until you create profiles and assign them to anti-virus network stations.

2. Designate the stations, users, and groups to which the settings of the newly created profile will be distributed.
3. Configure the profile.

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 protected stations in the statistics log, but applications are not actually blocked.

1.1. Configuring the contents of the activity statistics on protected stations

Allow the gathering and sending of information from stations for the **Application Control events** section.



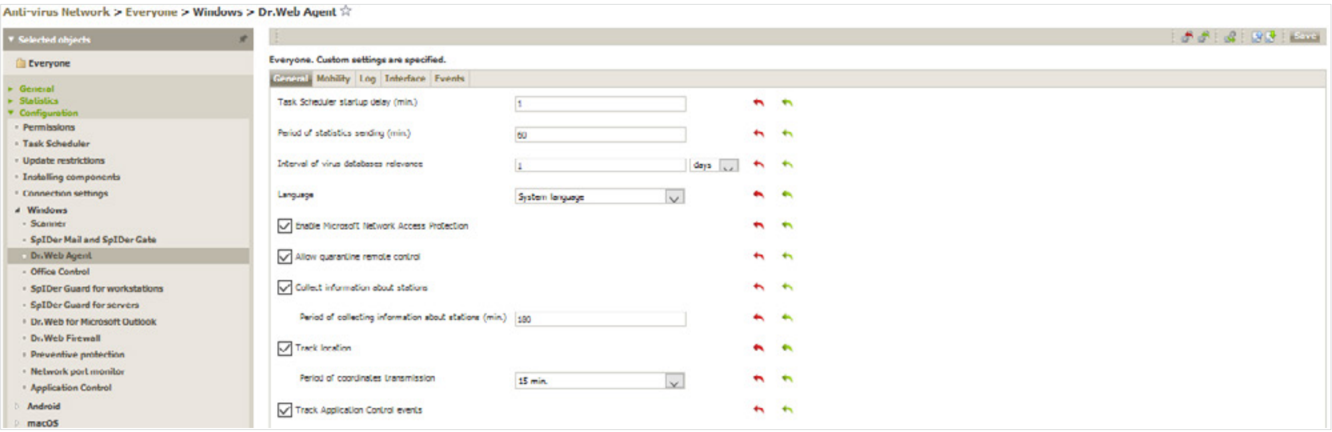
Anti-virus Network > Everyone > Application control events

25-10-2019 00:00:00 - 31-10-2019 23:59:59

Identifier	Station	Event type	Applied action	Profile name	Rule name	Operation mode	Process	Script	Event occurrence
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Process launch	Unknown			Active	Far.exe		28-10-2019 14:48:47
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Process launch	Blocked by deny rules	Honey	c18efa50-f97a-11e9-52ce-e474b6c9104f	Active	Far.exe		28-10-2019 15:03:00
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Process launch	Blocked by deny rules	Honey	c18efa50-f97a-11e9-52ce-e474b6c9104f	Active	Far.exe		28-10-2019 15:03:04
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Process launch	Blocked by deny rules	Honey	c18efa50-f97a-11e9-52ce-e474b6c9104f	Active	Far.exe		28-10-2019 15:03:12
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
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	MSI package launch	Unknown			Active			28-10-2019 15:07:56
2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	Module load	Unknown			Active	Far.exe		28-10-2019 15:08:19
2ca841e0-ecaa-11e8-7906-	WIN10_RUS	Module load	Unknown			Active	Align.dll		28-10-2019 15:08:21

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.



Everyone. Custom settings are specified.

Task Scheduler startup delay (min.) 1

Period of statistics sending (min.) 60

Interval of virus databases relevance 1 days

Language System language

☑ Enable Microsoft Network Access Protection

☑ Allow quarantine remote control

☑ Collect information about stations

Period of collecting information about stations (min.) 180

☑ Track location

Period of coordinates transmission 15 min.

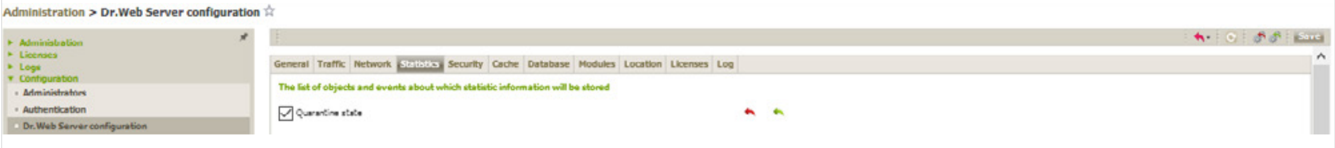
☑ Track Application Control events

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.



The list of objects and events about which statistic information will be stored

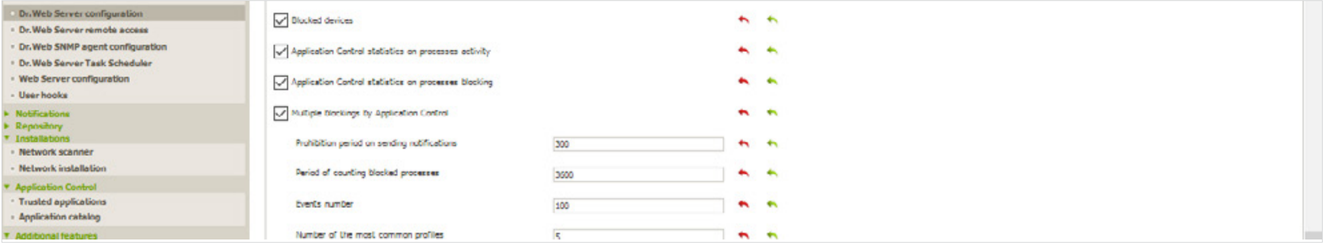
☑ Quarantine state

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.

     Important! 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.



☑ Blocked devices

☑ Application Control statistics on processes activity

☑ Application Control statistics on processes blocking

☑ Multiple blockings by Application Control

Prohibition period on sending notifications 300

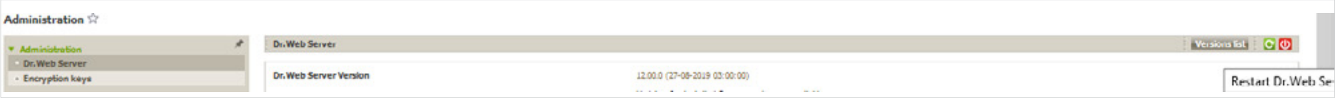
Period of counting blocked processes 3600

Events number 100

Number of the most common profiles 5

3. Click on **Save**.

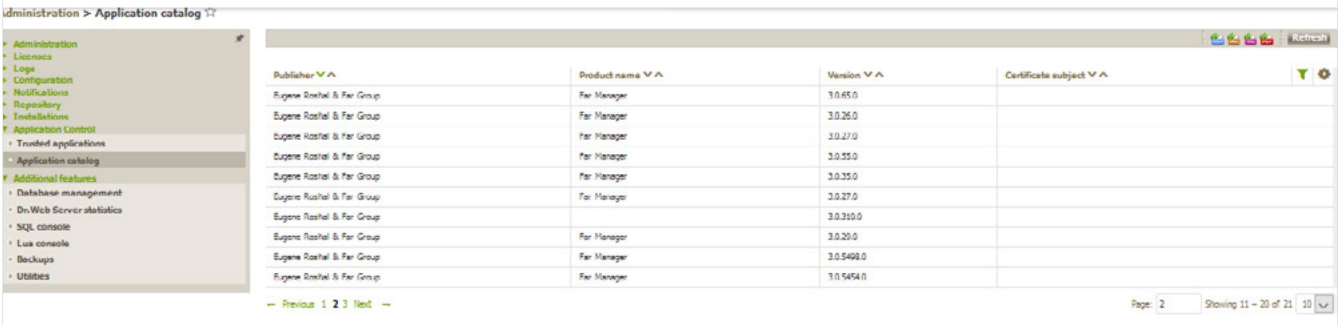
4. Restart the anti-virus server.



Dr.Web Server Version 12.00.0 (27-08-2019 03:00:00)

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.



Publisher	Product name	Version	Certificate subject
Eugene Roshal & Far Group	Far Manager	3.0.65.0	
Eugene Roshal & Far Group	Far Manager	3.0.26.0	
Eugene Roshal & Far Group	Far Manager	3.0.27.0	
Eugene Roshal & Far Group	Far Manager	3.0.55.0	
Eugene Roshal & Far Group	Far Manager	3.0.35.0	
Eugene Roshal & Far Group	Far Manager	3.0.27.0	
Eugene Roshal & Far Group		3.0.310.0	
Eugene Roshal & Far Group	Far Manager	3.0.20.0	
Eugene Roshal & Far Group	Far Manager	3.0.5498.0	
Eugene Roshal & Far Group	Far Manager	3.0.5454.0	

← Previous 1 2 3 Next → Page: 2 Showing 11 – 20 of 21 10

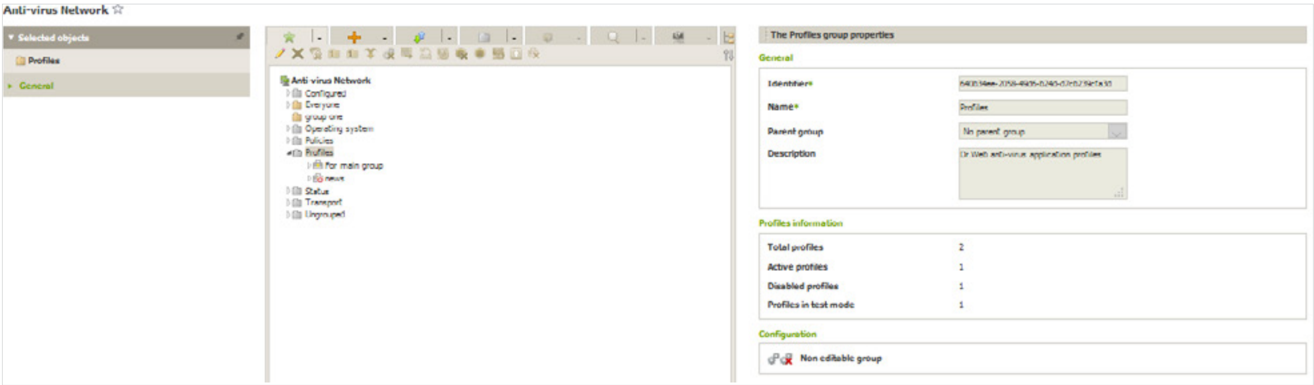
To view the application catalog, go to **Administration → Application Control → Application catalog**.

The catalog can be used to create Application Control module deny and allow rules. The catalog simplifies the process of creating rules because all application information is auto-filled using data about the selected known application.

1.2. Creating an Application Control module Profile

Profiles are used to specify the Application Control module settings that will dictate what applications will be launched or blocked on stations. Profiles define how the Application Control module operates. In this regard, the first step in configuring the **Application Control** module is to create a needed profile — configure what the Application Control module does for the stations, groups of stations, and individual users to which they can be assigned.

All profiles are placed in the pre-defined group **Profiles** in the anti-virus network view.



The Profiles group properties

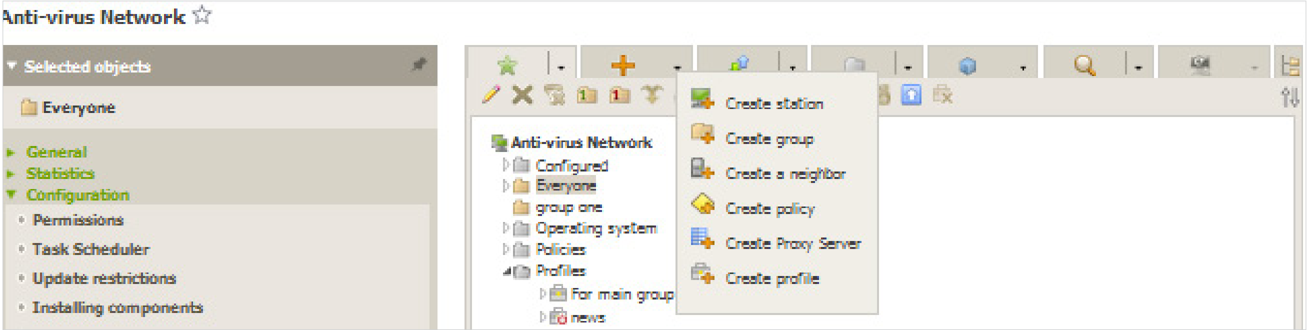
Identifier*	6408534ee-2058-4905-0240-07c023ef a30
Name*	Profiles
Parent group	No parent group
Description	Dr.Web anti-virus application profiles

Total profiles	2
Active profiles	1
Disabled profiles	1
Profiles in test mode	1

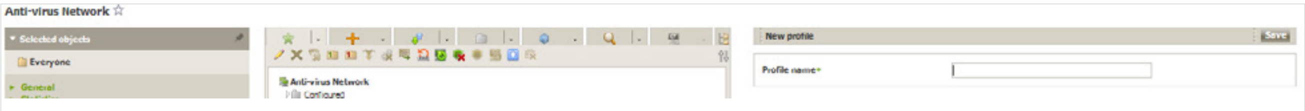
Non editable group

To create a profile

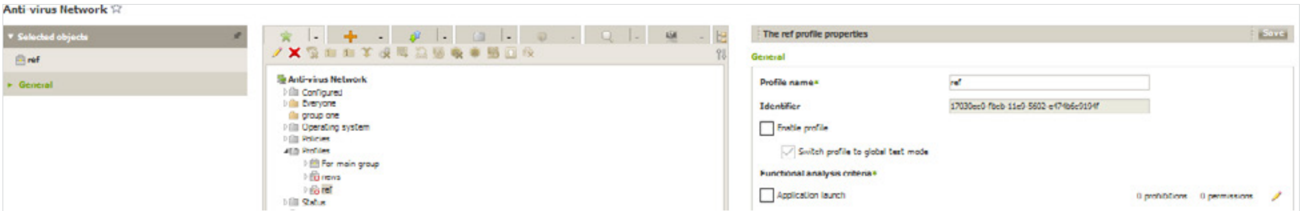
1. Select **Anti-virus Network** in the Control Center's main menu.
2. In the newly appeared window, on the toolbar, select **Add network object** → **Create profile**.



3. On the newly appeared panel, enter the **Profile name**.



In the future, the profile name can be changed in the **General** profile properties settings.



The ref profile properties

Profile name*	ref
Identifier	17030ec0 fbcb 11e0 5602 e474b6c0194f

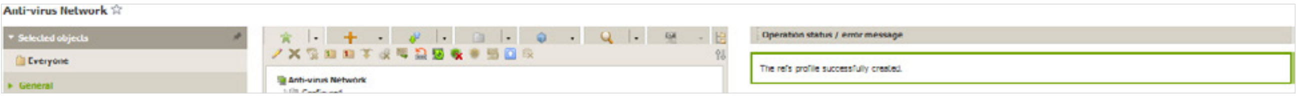
□ Enable profile

☑ Switch profile to global test mode

Functional analysis criteria*

□ Application launch 0 prohibitions 0 permissions

4. Click on **Save**.



The ref's profile successfully created.

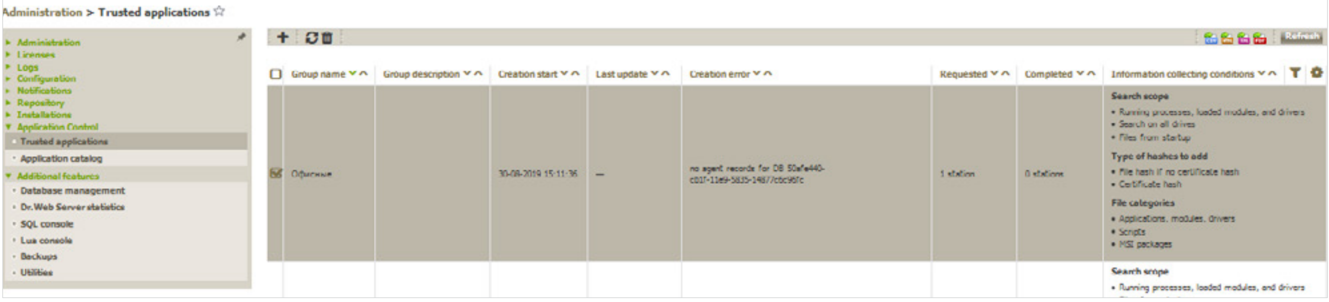
5. The new profile will be created and placed in the **Profiles** group.

1.3. Defining the list of trusted applications

Trusted applications — lists of applications that are always allowed to be launched on stations running the Application Control component. The user can select allowed lists of applications in the settings of the profile in the Allow mode settings.

To manage trusted applications on Servers that collect information, go to **Administration** → **Application Control** → **Trusted applications**.

The table in this section contains a list of all the relevant groups of trusted applications (whitelists) — applications that have been collected according to a specified criteria from a selected station or a group of stations.



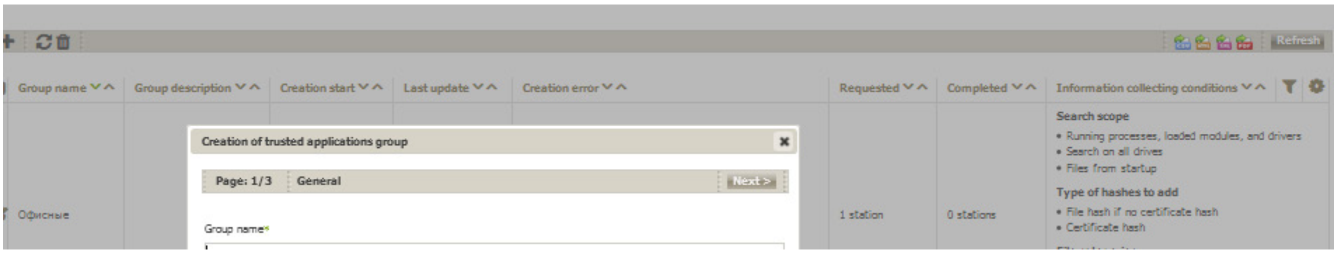
Administration > Trusted applications

- Administration
- Licenses
- Logs
- Configuration
- Notifications
- Repository
- Installations
- Application Control
  - Trusted applications
  - Application catalog
- Additional features
  - Database management
  - Dr.Web Server statistics
  - SQL console
  - Lua console
  - Backups
  - Utilities

□	Group name	Group description	Creation start	Last update	Creation error	Requested	Completed	Information collecting conditions
☑	Офисные		30-08-2019 15:11:36	—	no agent records for DB 50afe440-cb1f-11e9-5835-1487/cbc95fc	1 station	0 stations	**Search scope** • Running processes, loaded modules, and drivers • Search on all drives • Files from startup **Type of hashes to add** • File hash if no certificate hash • Certificate hash **File categories** • Applications, modules, drivers • Scripts • MSI packages
								Search scope • Running processes, loaded modules, and drivers

To create a new group of trusted applications

1. In the Trusted applications section, click on the toolbar button ➕ (**Creation of trusted applications group**).
2. In the newly appeared window, specify a **Group name** (the name of the group of trusted applications you are creating) and a **Description** (an optional description for the created group).



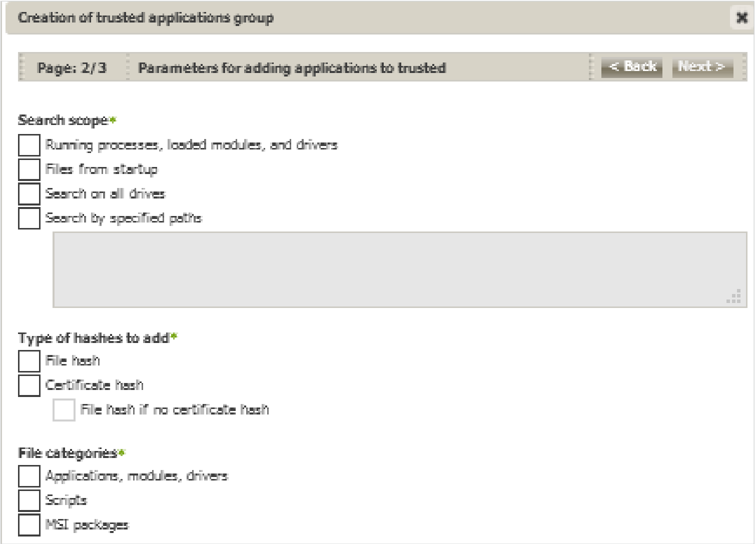
Group name	Group description	Creation start	Last update	Creation error	Requested	Completed	Information collecting conditions
Офисные					1 station	0 stations	Search scope • Running processes, loaded modules, and drivers • Search on all drives • Files from startup Type of hashes to add • File hash if no certificate hash • Certificate hash

Creation of trusted applications group

Page: 1/3 General

Group name*

3. Click on **Next** and set the rules for adding applications to the list of trusted applications by selecting the options according to which the applications on the stations will be added to the newly created group of trusted applications.



Creation of trusted applications group

Page: 2/3 Parameters for adding applications to trusted

Search scope*

□ Running processes, loaded modules, and drivers
□ Files from startup
□ Search on all drives
□ Search by specified paths

Type of hashes to add*

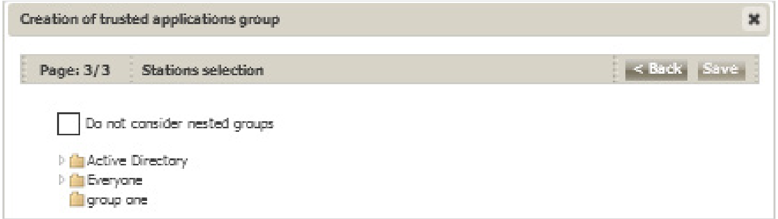
□ File hash
□ Certificate hash
  □ File hash if no certificate hash

File categories*

□ Applications, modules, drivers
□ Scripts
□ MSI packages

In the **Search by specified paths** field, you can specify ways to search for applications. Use ";" as a separator.

4. Click on **Next**, and in the network tree, select the stations and groups of stations on which application information will be collected for inclusion in the trusted lists. To select multiple groups and stations, use the CTRL and SHIFT keys.



Creation of trusted applications group

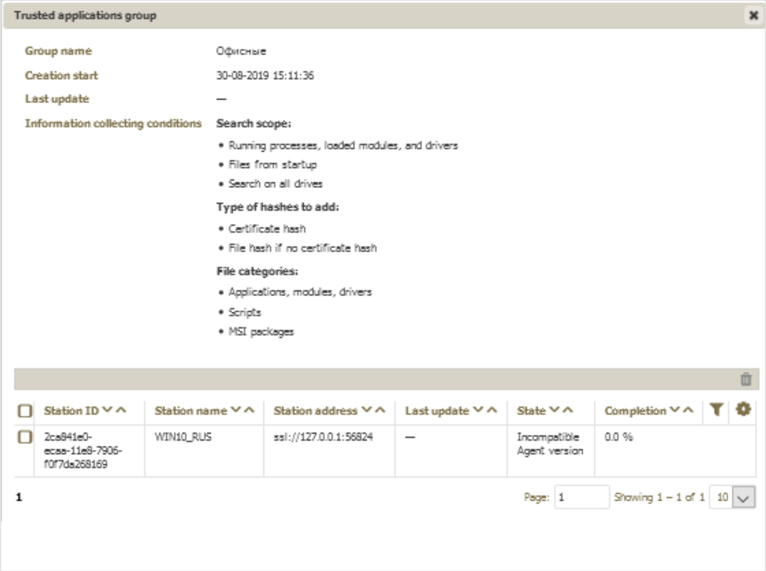
Page: 3/3 Stations selection

□ Do not consider nested groups

- Active Directory
- Everyone
- group one

5. Click on **Save** to begin collecting application information on the stations according to the settings you specified. This process can take a long time.

Status and updating information for a group of trusted application groups can be viewed both in the main table of the **Trusted applications** section and in the additional group information that is available by clicking on the line corresponding to the group in the main table of the **Trusted applications** section.



Trusted applications group

Group name	Офисные
Creation start	30-08-2019 15:11:36
Last update	—
Information collecting conditions	**Search scope:** • Running processes, loaded modules, and drivers • Files from startup • Search on all drives **Type of hashes to add:** • Certificate hash • File hash if no certificate hash **File categories:** • Applications, modules, drivers • Scripts • MSI packages

□	Station ID	Station name	Station address	Last update	State	Completion
□	2ca841e0-ecaa-11e8-7906-f0f7da268169	WIN10_RUS	ssl://127.0.0.1:56824	—	Incompatible Agent version	0.0 %

1

Page: 1 Showing 1 – 1 of 1 10

To update a group of trusted applications

1. In the **Trusted applications** section, in the table, tick the boxes next to the groups that you want to update.
2. On the toolbar, click on 🔄 (**Restart creation of trusted applications group**).

To delete a group of trusted applications

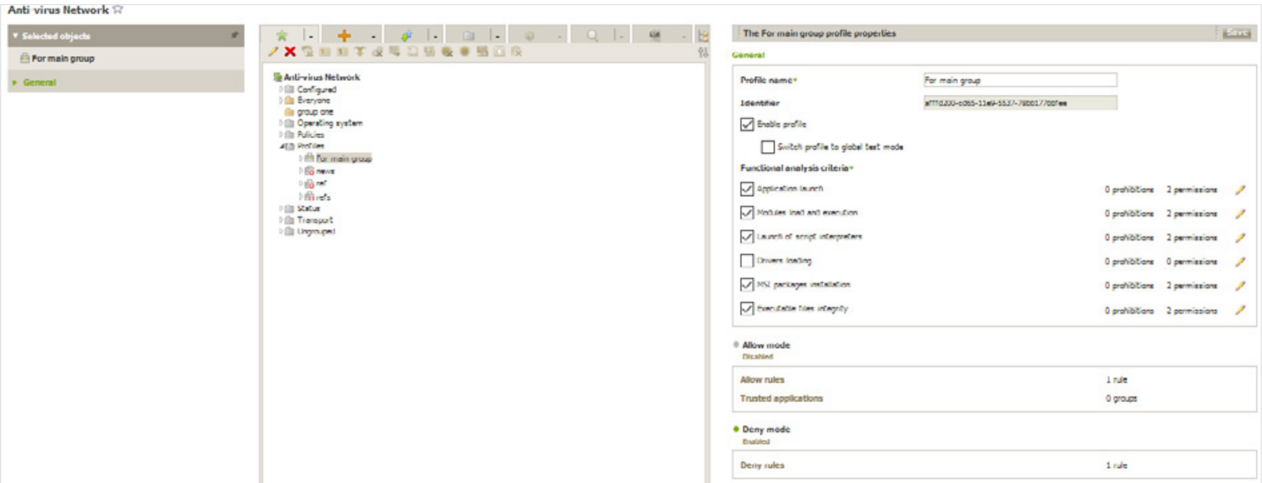
1. In the **Trusted applications** section, in the table, tick the boxes next to the groups that you want to delete.
2. On the toolbar, click on 🗑 (**Delete trusted applications group**).
3. If the group is not assigned to the Application Control profiles, the applications in this group will be deleted from the list of applications allowed to be launched on stations, and no more applications will be added to the list of applications that are to be trusted according to this group’s criteria.

   When you delete groups of trusted applications, a new revision is created in the repository for the product **Trusted applications** and distributed to neighbouring Servers. This may disrupt the Application Control profile's operation for which this group is assigned on neighbouring Servers.

1.4. Setting an operation mode for the Application Control module Profile

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

profile icon in the anti-virus network tree, or select the profile and then select **Properties** in the control menu (a window showing the profile of the properties will open).



The For main group profile properties

General

Profile name* For main group

Identifier afffd200-cd65-11e9-5537-78bb177bbfee

☑ Enable profile

☐ Switch profile to global test mode

Functional analysis criteria*

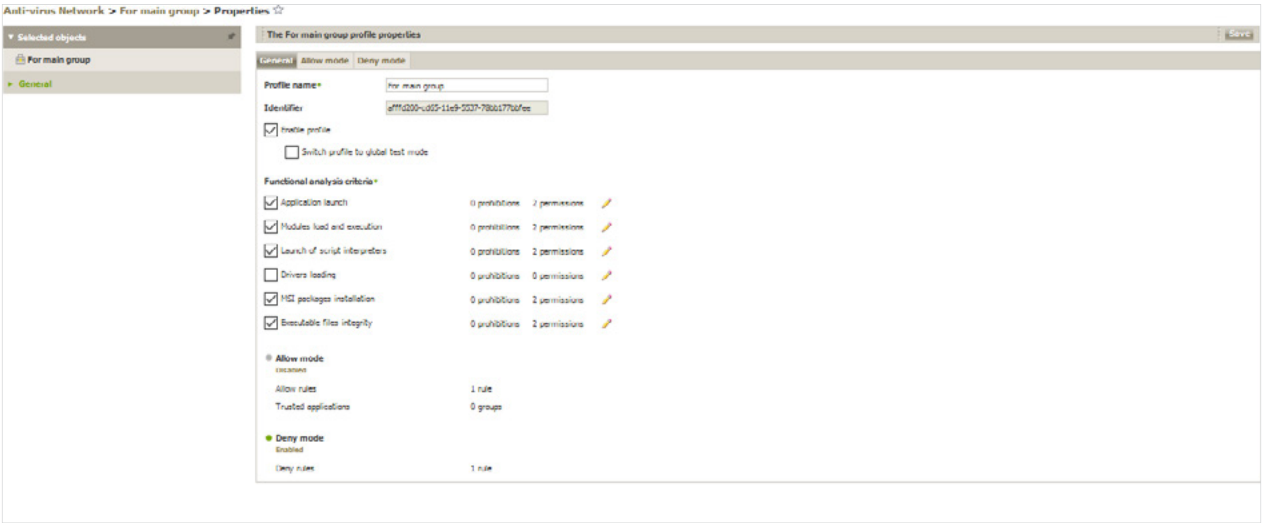
☑	Application launch	0 prohibitions	2 permissions
☑	Modules load and execution	0 prohibitions	2 permissions
☑	Launch of script interpreters	0 prohibitions	2 permissions
☐	Drivers loading	0 prohibitions	0 permissions
☑	MSI packages installation	0 prohibitions	2 permissions
☑	Executable files integrity	0 prohibitions	2 permissions

● Allow mode
Disabled

Allow rules 1 rule
Trusted applications 0 groups

● Deny mode
Enabled

Deny rules 1 rule



The For main group profile properties

Profile name* For main group

Identifier afffd200-cd65-11e9-5537-78bb177bbfee

☑ Enable profile

☐ Switch profile to global test mode

Functional analysis criteria*

☑	Application launch	0 prohibitions	2 permissions
☑	Modules load and execution	0 prohibitions	2 permissions
☑	Launch of script interpreters	0 prohibitions	2 permissions
☐	Drivers loading	0 prohibitions	0 permissions
☑	MSI packages installation	0 prohibitions	2 permissions
☑	Executable files integrity	0 prohibitions	2 permissions

● Allow mode
Disabled

Allow rules 1 rule
Trusted applications 0 groups

● Deny mode
Enabled

Deny rules 1 rule

3. In the **Profile name** field, you can change the profile name.
4. Select **Enable profile** to start using it. 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.

These are the following profile modes:

- **Disabled** — a profile is not active; the profile settings are not applied.
- **Active** — a profile is active; the settings are applied to the objects to which this profile is distributed.
- **Test** *(global)* — a profile is active, but it works in the global test mode.
- **Test** (*for rules*) — a profile is active, but only functional analysis settings are distributed to the objects.

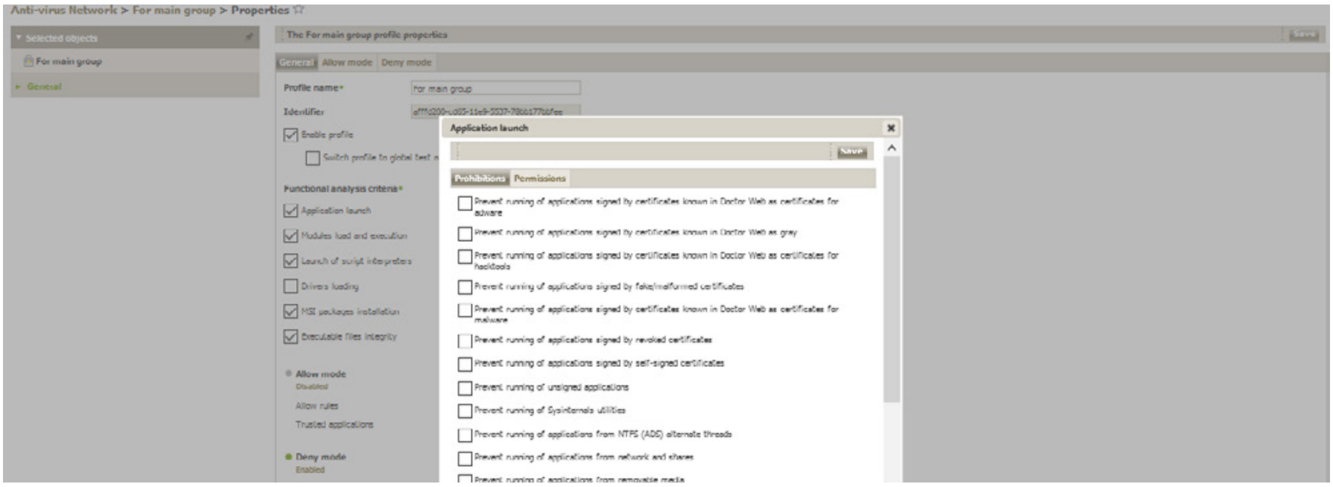
Allow and deny rules work in test mode: their setting are not distributed to objects, but the operation result is recorded in the activity log (the **Application Control events** statistics section).

The test mode for rules is enabled and disabled in the settings section containing the allow and deny rules.

5. In the **Functional analysis criteria** section, select the criteria that you want to use and specify the set of predefined rules that are to be used to allow or deny the launch of applications.

If you are configuring a profile for the first time, when enabling each criteria, the allow categories will automatically be enabled in the advanced settings. In the future, if necessary, you can disable these allow categories in the advanced settings.

To specify advanced settings for the selected criteria, click on **Edit** next to the appropriate criteria. You will see a window with a list of settings.



Profile name* for main group

Identifier afffd200-cd05-11e9-5537-78bb177bbfee

☑ Enable profile

□ Switch profile to global test m

Functional analysis criteria*

☑ Application launch

☑ Modules load and execution

☑ Launch of script interpreters

□ Drivers loading

☑ MSI packages installation

☑ Executable files integrity

□ Prevent running of applications signed by certificates known in Doctor Web as certificates for adware

□ Prevent running of applications signed by certificates known in Doctor Web as gray

□ Prevent running of applications signed by certificates known in Doctor Web as certificates for hacktools

□ Prevent running of applications signed by fake/malformed certificates

□ Prevent running of applications signed by certificates known in Doctor Web as certificates for malware

□ Prevent running of applications signed by revoked certificates

□ Prevent running of applications signed by self-signed certificates

□ Prevent running of unsigned applications

□ Prevent running of Sysinternals utilities

□ Prevent running of applications from NTFS (ADS) alternate threads

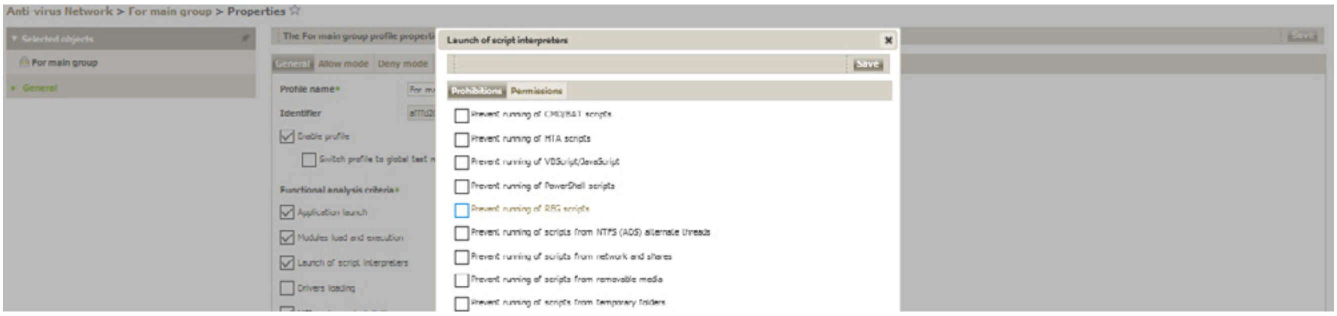
□ Prevent running of applications from network and shares

□ Prevent running of applications from removable media

The functional analysis settings can be either denying or allowing. Tick the boxes for those settings that should be applied.

If you enable the use of one of the criteria 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 settings that allow or deny. For example:

- If the **Run script interpreters** criteria is specified, but its advanced settings are not specified, you will be able to monitor the launch of all script interpreters in accordance with the settings specified for the allow or deny mode.
- If the **Run script interpreters** criteria and its advanced setting **Prevent running of scripts from removable media** is specified, only the launch of scripts from removable media will be blocked.


Anti-virus Network > For main group > Properties
Selected objects
For main group
General
The For main group profile properti
General
Allow mode
Deny mode
Launch of script interpreters
Save
Prohibitions
Permissions

Profile name* For m

Identifier afffd2

☑ Enable profile

□ Switch profile to global test m

Functional analysis criteria*

☑ Application launch

☑ Modules load and execution

☑ Launch of script interpreters

□ Drivers loading

□ Prevent running of CMD/BAT scripts

□ Prevent running of HTA scripts

□ Prevent running of VBScript/JavaScript

□ Prevent running of PowerShell scripts

□ Prevent running of REG scripts

□ Prevent running of scripts from NTFS (ADS) alternate threads

□ Prevent running of scripts from network and shares

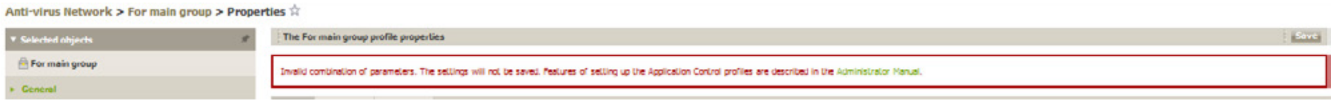
□ Prevent running of scripts from removable media

□ Prevent running of scripts from temporary folders

Important! If you specify advanced settings but do not enable the criteria itself, neither the advanced settings nor the criteria will be executed.

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

Important! If you do not enable a single criterion in the **Functional analysis criteria** section, the profile will be disabled.


Anti-virus Network > For main group > Properties
Selected objects
For main group
General
The For main group profile properties
Save

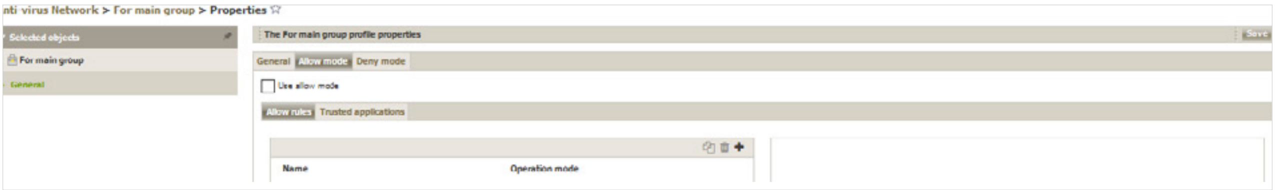
Invalid combination of parameters. The settings will not be saved. Features of setting up the Application Control profiles are described in the Administrator Manual.

Important! If advanced settings are not specified for one of the criteria in the **Functional analysis criteria** section, and the allow and deny modes are disabled, the profile will be disabled.

6. To apply the settings specified in the **General** section, click on **Save** in the profile settings.
7. In the **Allow mode** section, in the profile properties window, you can find a general summary of the mode settings: the number of created allow rules and the groups of trusted applications assigned to this profile.

   The Allow mode assumes that on all the controlled stations, only applications on the list of **Trusted applications** and applications that comply with allow rules are allowed. All other applications are blocked.

   To enable or disable this mode and to configure rules and trusted applications, go to the **Allow mode** section and then go to the relevant section.



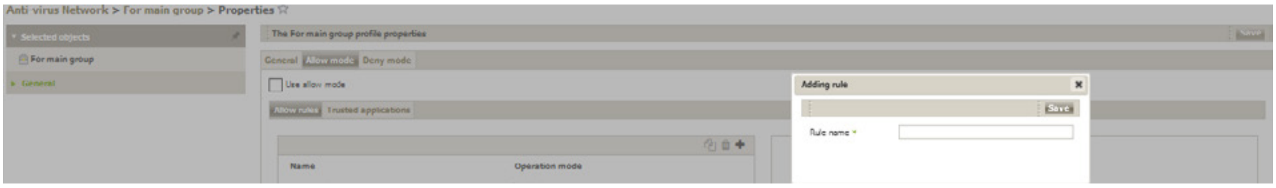
To use the allow mode

1. In the **Allow mode** tab, tick the box next to **Use allow mode**.
2. Specify the settings in the **Allow rules** and/or **Trusted applications** sections.

To create a new allow rule

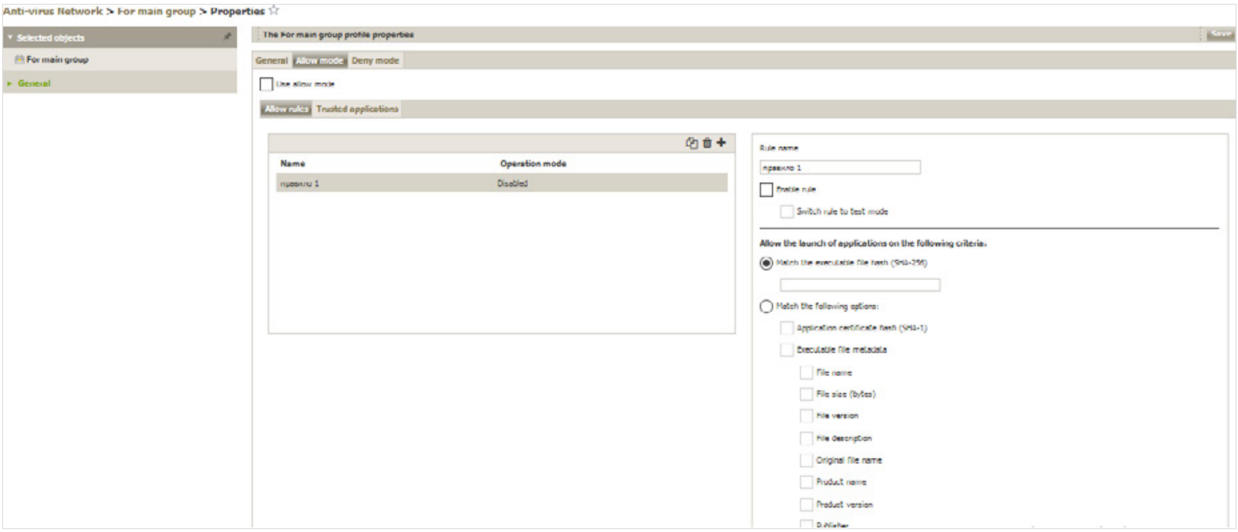
a. In the **Allow rules** section, click on ✚ (**Create a rule**) on the toolbar.

b. In the **Adding rule** window, enter the **Rule name** and click on **Save**.



c. Select the rule from the rules list and specify its settings in the newly appeared property panel:

i. **Select Enable** rule to start using this rule.



Name	Operation mode
правило 1	Disabled

Rule name: правило 1

☐ Enable rule

☐ Switch rule to test mode

Allow the launch of applications on the following criteria:

● Match the executable file hash (SHA-256)

○ Match the following options:

☐ Application certificate hash (SHA-1)

☐ Executable file metadata

☐ File name

☐ File size (bytes)

☐ File version

☐ File description

☐ Original file name

☐ Product name

☐ Product version

☐ Publisher

ii. If you want to check how a rule works without applying it to the stations, tick the box next to **Switch rule to test mode**.

iii. In the **Allow the launch of applications on the following criteria** section, select the options according to which applications will be allowed to launch on the stations. You can also create allow rules from the Control Center's **Application Control events** and **Application catalog** sections based on data received from the stations.

d. Click on **Save**.

To duplicate an allow rule

a. In the **Allow rules** section, in the rules table, select the rule you want to duplicate for this profile.

b. On the toolbar, click on ⧉ (**Duplicate rule**).

c. A new rule will appear in the rules table; its settings will be copied in full from the rule selected in step 1. The figure **1** will be added to the name of the rule.

To remove an allow rule, in the rules table, select the rule that you want to delete from the profile, and on the toolbar, click on 🗑 (**Delete rule**).

To edit a trusted application for a selected profile, go to the **Trusted applications** tab. The tab's table contains a list of all the groups of trusted applications (an application whitelist) that are assigned to that profile. The application whitelist is a list of applications collected from a selected station or a group of stations according to specified criteria.

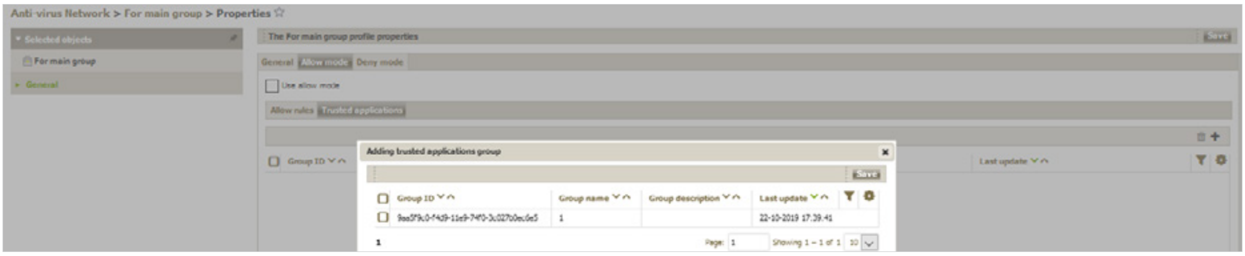
These applications are allowed to run on the anti-virus network stations for which this profile (if working in the allow mode) has been assigned.

If your Server is receiving trusted applications via an inter-server connection, the group table can contain entries marked with **Trusted applications group is absent in the Server repository**. These entries are relevant for groups of applications that were added from the previous revision of the product **Trusted applications**, after which a new revision, in which this group is not included, was received. To prevent the disruption of the profile’s operation, it is recommended that you remove these groups from its settings.

To add a group of trusted applications to a profile

a. On the toolbar, in the **Trusted applications** section, click on ➕ (**Adding trusted applications group to a profile**).

b. A window containing the list of all the available groups of trusted applications will open.



□ Use allow mode

□ Group ID	Group name	Group description	Last update
□ 9aa5f9c0-f4d9-11e9-74f0-3c027b0ec6e5	1		22-10-2019 17:39:41

c. When configuring the allow mode, groups of trusted applications are selected from the list of groups available in the repository for the product **Trusted applications**.

d. Tick the boxes next to the groups of applications that you want to add to the profile.

e. Click on **Save**.

To remove a group of trusted applications from a profile

a. In the **Trusted applications** section, tick the boxes next to the groups that you want to remove from the profile.

b. On the toolbar, click on 🗑 (**Delete trusted applications group**).

c. The applications of this group will be deleted from the list of those allowed to run on the stations for which this profile was assigned.

When you delete applications from a profile, the group of trusted applications itself is not removed. The group is available in the repository and can be added to this profile and to other profiles.

To use trusted applications, do one of the following:

a. If trusted applications are going to be collected on your Server, activate the collection of trusted applications in the Control Center section **Administration → Application Control → Trusted Applications**.

b. If trusted applications are sent to your Server via an inter-server connection from a neighbouring Server, specify the appropriate settings in the repositories of the Servers that send and receive the product **Trusted applications**.

3. Click on **Save**.

Important! If neither allow rules nor trusted applications are specified, the allow mode will be disabled.

8. In the **Deny mode** section, in the profile properties window, you can find a general summary of the mode settings: the number of deny rules created.

The **Deny mode** assumes that on all the controlled stations, only applications that comply with deny rules are denied. All other applications are allowed.

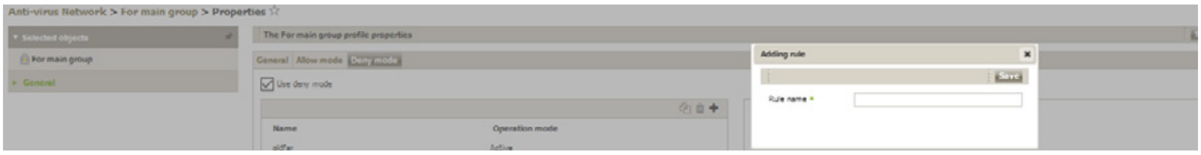
To enable or disable this mode and to configure rules and trusted applications, go to the **Deny mode** section and then go to the relevant section.

1. In the **Deny mode** tab, tick the box next to **Use deny mode**.

2. To create a deny rule

a. Click on ✚ (**Create rule**).

b. In **Adding rule**, enter the **Rule name**.



Anti-virus Network > For main group > Properties ☆

The For main group profile properties

☑ Use deny mode

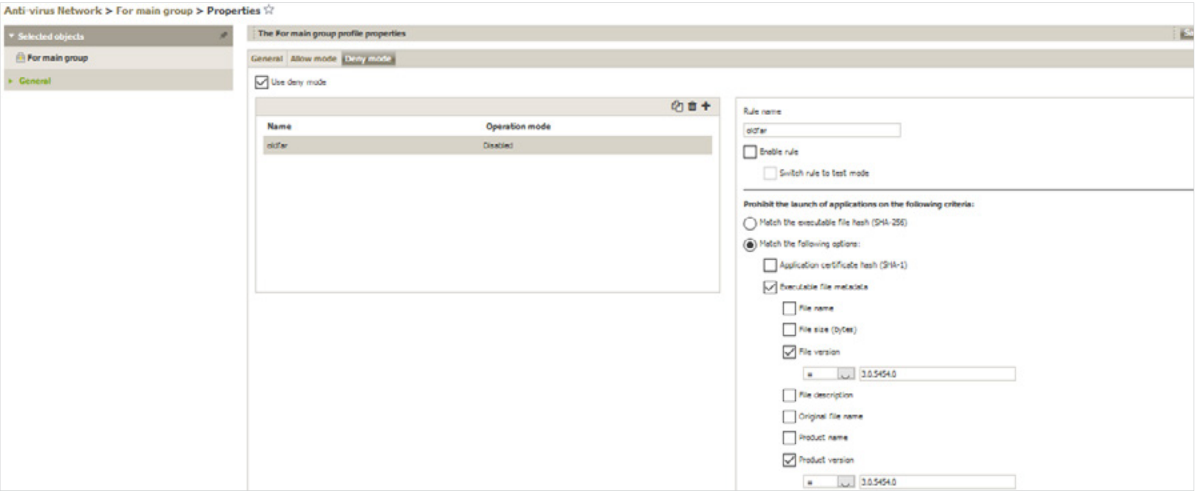
Name	Operation mode
oldfar	Active

Adding rule

Rule name *

c. Click on **Save**.

3. Select the rule from the rules list, and specify its settings in the newly appeared property panel.



Anti-virus Network > For main group > Properties ☆

The For main group profile properties

☑ Use deny mode

Name	Operation mode
oldfar	Disabled

Rule name

oldfar

□ Enable rule

□ Switch rule to test mode

Prohibit the launch of applications on the following criteria:

○ Match the executable file hash (SHA-256)

● Match the following options:

□ Application certificate hash (SHA-1)

☑ Executable file metadata

□ File name

□ File size (bytes)

☑ File version

= 3.0.5454.0

□ File description

□ Original file name

□ Product name

☑ Product version

= 3.0.5454.0

a. Select **Enable rule** to start using this rule.

b. If you want to check how a rule works without applying it to stations, tick the box next to **Switch rule to test mode**. Otherwise, the rule will work in active mode, blocking applications on the stations according to the specified rules settings.

c. In the **Prohibit the launch of applications on the following criteria** section, select the options according to which the launch of applications will be denied on stations.

   You can also create deny rules from the Control Center's Application Control events and Application catalog sections based on the data received from the stations.

d. Click on **Save**.

4. Click on **Save**.

To duplicate a deny rule

1. Select the rule you want to duplicate for this profile.
2. On the toolbar, click on (**Duplicate rule**).
3. A new rule will appear in the rules table; its settings will be copied in full from the rule selected in step 1. The figure 1 will be added to the name of the rule.

   To remove a deny rule, select the rule that you want to delete from the profile, and on the toolbar, click on (**Delete rule**).

   Important! If you do not specify deny rules, the profile will be disabled.

   Important! Allow and deny modes can be enabled or disabled together or separately. Functional analysis should always be enabled. If all the rules of functional analysis are disabled, application launches are not controlled.

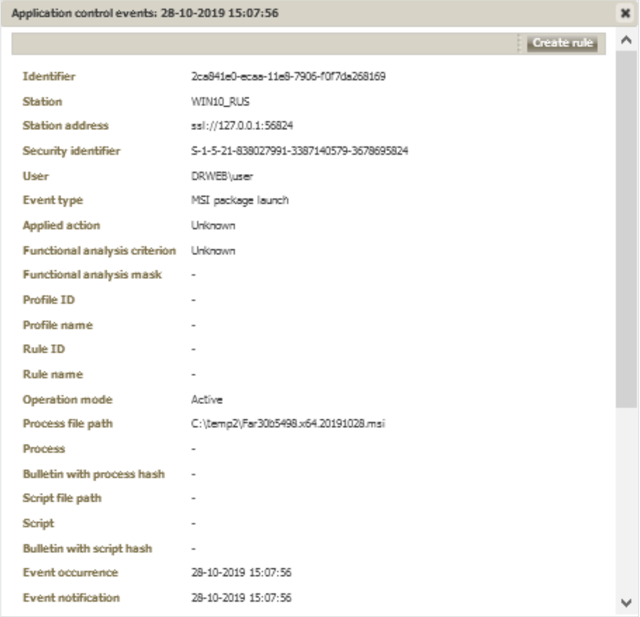
1.5. Configuring the Application Control module Profile

To control the launch of applications on stations, at least one active profile must be assigned to a station or to the user of that station.

Since all profiles are placed in the pre-defined group Profiles, which is accessible in the anti-virus network view, the objects to which a specified profile is assigned are placed in the anti-virus network tree as elements of this profile.

1.5.1. Creating a rule based on activity log data

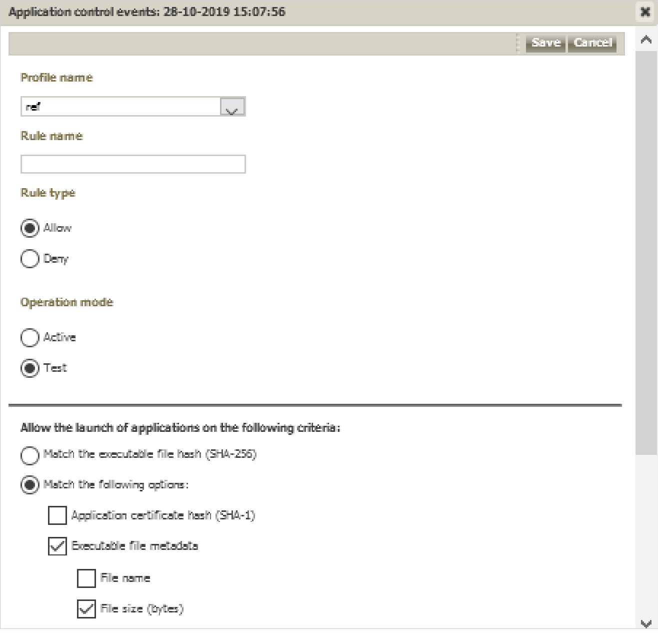
1. In the section **Statistics → Application Control** events, click on the line with the event about an attempt to run the application for which you want to create a rule that will monitor its launch.
2. In the newly appeared window containing information about the selected event, click on **Create rule**.



Application control events: 28-10-2019 15:07:56

Identifier	2ca841e0-ecaa-11e8-7906-f0f7da268169
Station	WIN10_RUS
Station address	ssl://127.0.0.1:56824
Security identifier	S-1-5-21-838027991-3387140579-3678695824
User	DRWEB\user
Event type	MSI package launch
Applied action	Unknown
Functional analysis criterion	Unknown
Functional analysis mask	-
Profile ID	-
Profile name	-
Rule ID	-
Rule name	-
Operation mode	Active
Process file path	C:\temp2\Far30b5498.x64.20191028.msi
Process	-
Bulletin with process hash	-
Script file path	-
Script	-
Bulletin with script hash	-
Event occurrence	28-10-2019 15:07:56
Event notification	28-10-2019 15:07:56

3. In the subsequent window, specify:
    a. In the **Profile name** drop-down list, select the Application Control profile in which the rule will be created.



Profile name: ref

Rule name:

Rule type
● Allow
○ Deny

Operation mode
○ Active
● Test

Allow the launch of applications on the following criteria:
○ Match the executable file hash (SHA-256)
● Match the following options:
□ Application certificate hash (SHA-1)
☑ Executable file metadata
□ File name
☑ File size (bytes)

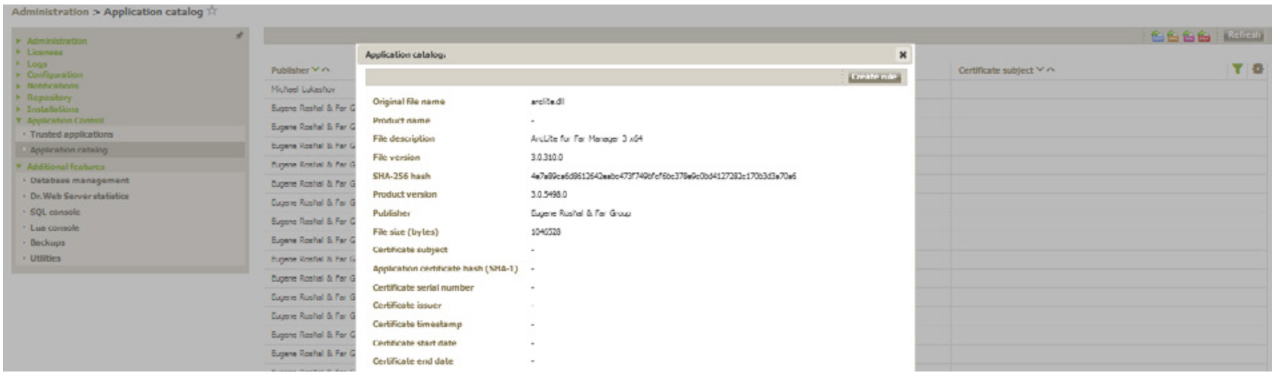
    b. In the **Rule name** field, enter the name for the new rule.
    c. In the **Rule type** section, select the type of rule to be created: allow or deny.
    d. For the **Operation mode** option, select the mode in which the created rule will work.

    In the **Test** mode, applications will not be blocked on stations, but activity will be recorded with the settings enabled. The results of potential application blocking based on the rule you created will be displayed in the **Application Control events** section.

    e. In the **Prohibit the launch of applications on the following criteria / Allow the launch of applications on the following criteria** section, fields are auto-filled in accordance with the application data used to create the rule. You can edit it, if necessary.
4. Click on **Save**. The rule will be created in the specified Application Control Profile.

1.5.2. Creating a rule based on Application catalog data

1. In the **Application catalog** section, select the line about the application for which you want to create a rule that will control its launch.
2. When you click on a line in the table, a window showing information about the selected application will appear.

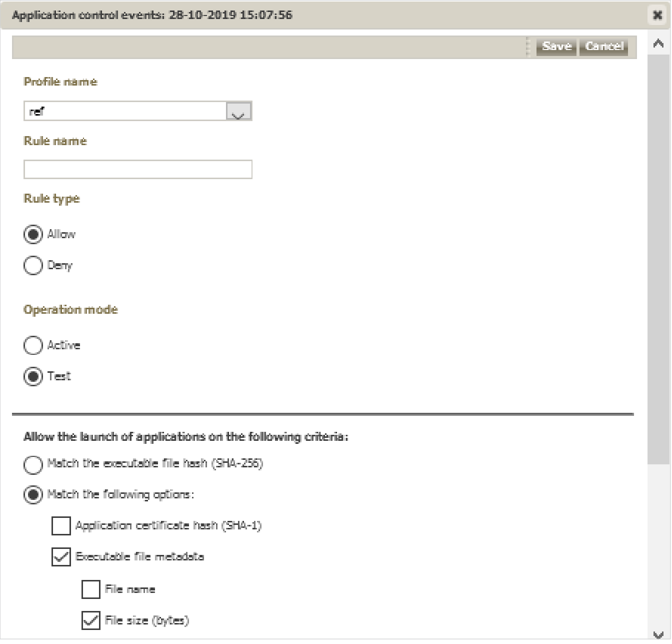


Publisher
Michael Lukashov
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G
Eugene Roshal & Far G

Original file name	arclite.dll
Product name	-
File description	ArcLite for Far Manager 3 x64
File version	3.0.310.0
SHA-256 hash	4e7a89ca6d9612642eabe473f749bfcf6bc378e9c0bd4127282c170b3d3a70a6
Product version	3.0.5498.0
Publisher	Eugene Roshal & Far Group
File size (bytes)	1040528
Certificate subject	-
Application certificate hash (SHA-1)	-
Certificate serial number	-
Certificate issuer	-
Certificate timestamp	-
Certificate start date	-
Certificate end date	-

3. Click on **Create rule**.

4. The window for creating a new rule will open. Configure the following settings:
   a. In the **Profile name** drop-down list, select the Application Control profile where the rule is to be created.



Application control events: 28-10-2019 15:07:56

Profile name: ref

Rule name:

Rule type
● Allow
○ Deny

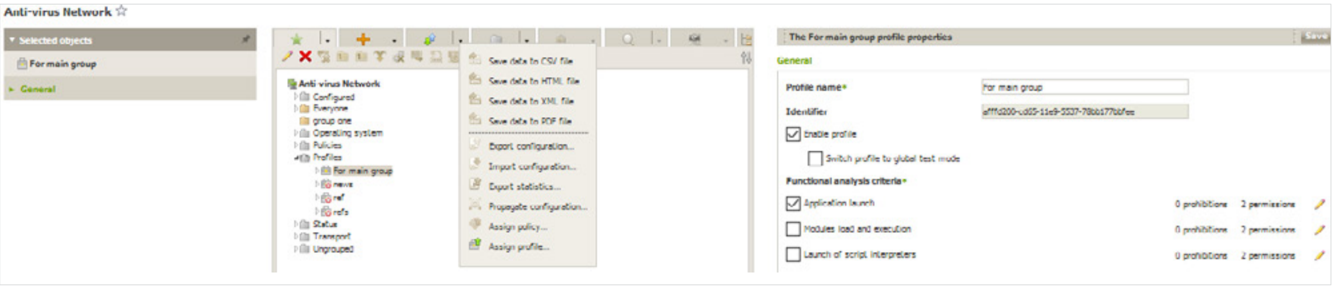
Operation mode
○ Active
● Test

Allow the launch of applications on the following criteria:
○ Match the executable file hash (SHA-256)
● Match the following options:
□ Application certificate hash (SHA-1)
☑ Executable file metadata
□ File name
☑ File size (bytes)

   b. In the **Rule name field**, specify the name for the new rule.
   c. For the **Rule type** option, select the type of rule you are creating: allow or deny.
   d. For the Operation mode option, select the mode for the created rule (this corresponds to the **Switch rule to test mode** checkbox when you are creating a rule from a profile). If you want to check how a rule works without applying it to stations, select the **Test** mode.
   e. In the **Prohibit the launch of applications on the following criteria / Allow the launch of applications on the following criteria** section (depending on the rule type selected in step d), fields will be auto-filled in accordance with the application for which the rule is being created. You can edit the configuration values if necessary.
5. Click on **Save**. The rule will be created in the specified Application Control profile.

1.6. Assigning a Profile to protected objects

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



The For main group profile properties

General

Profile name*: For main group

Identifier: afffd200-cd65-11e9-5537-78bb177bbfee

☑ Enable profile

□ Switch profile to global test mode

Functional analysis criteria*

☑ Application launch	0 prohibitions	2 permissions
□ Modules load and execution	0 prohibitions	2 permissions
□ Launch of script interpreters	0 prohibitions	2 permissions

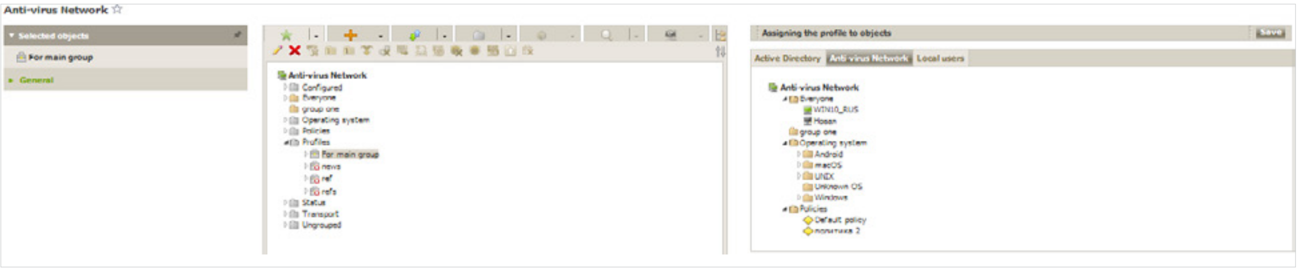
4. In the newly appeared window, select the object to which the settings are to be distributed.
   In the **Active Directory** tab, you can find lists (similar to the list in the anti-virus network tree) that are updated according to a **Synchronize with Active Directory** task from the Server

schedule. Lists contain identical objects but differ in terms of the type of objects to which the profile will be assigned:

- In the **Active Directory stations** list, you can select a group of stations or individual stations registered in the Active Directory domain.
- In the **Active Directory users** list, you can choose user groups and individual users who are registered in the Active Directory domain.

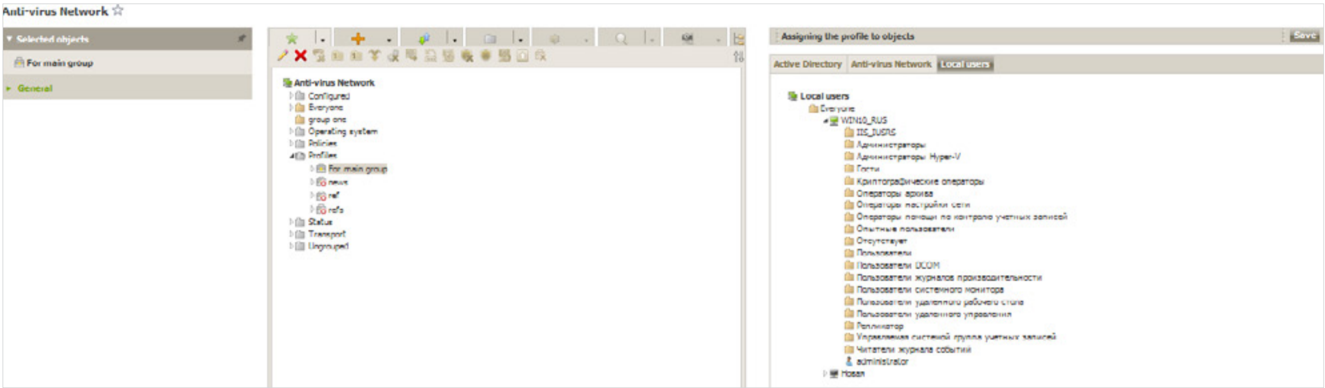
The same objects should not be chosen in different lists.

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



In the **Local users** tab, you can select the following objects:

- Stations. In this case, the settings will be applied to all the user accounts of the selected stations.
- Individual users on stations. In this case, settings will only be applied to the selected user accounts on these stations.



The settings of the Application Control profiles can be assigned not only to stations and groups of stations, but also to individual users and groups of users. In this respect:

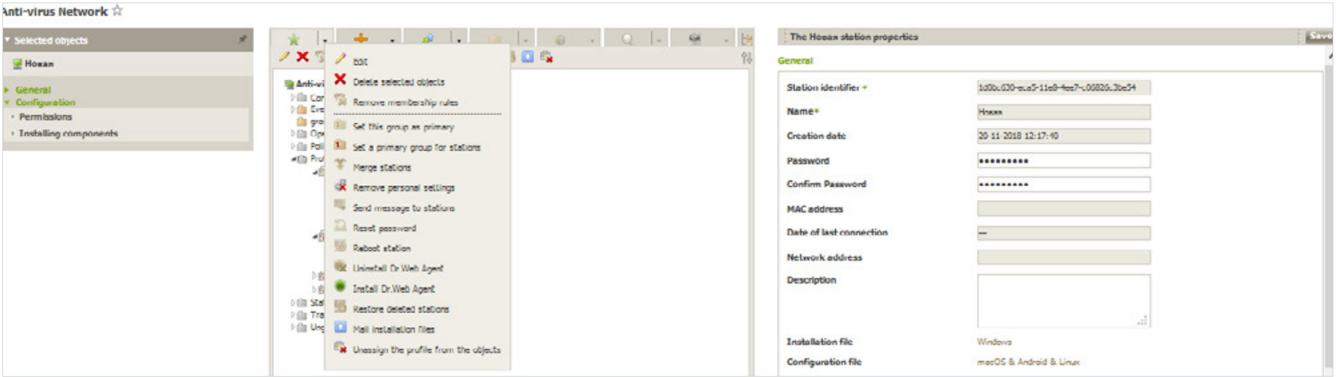
1. If there are custom settings, they have the highest priority.
2. If there are no custom settings, priority is given to the user group settings.
3. If no settings are specified for users and the user group, the inheritance is carried out according to the priority of settings that have been applied to stations.

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

To cancel assigning profile settings to an object

1. Select **Anti-virus Network** in the Control Center's main menu.
2. In the newly appeared window, in the hierarchical list, expand the list of objects attached to the profile, and select the object for which you want to cancel the profile assignment.

3. On the toolbar, click on **General** → **Unassign the profile to objects**.

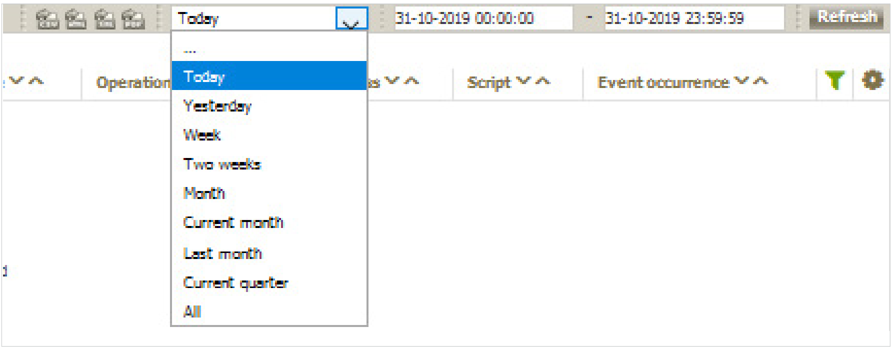


Station identifier * 1d0bc630-eca5-11e8-4ee7-c06826c3be54
Name* Hoeax
Creation date 20 11 2018 12:17:40
Password •••••••••
Confirm Password •••••••••
MAC address
Date of last connection —
Network address
Description
Installation file Windows
Configuration file macOS & Android & Linux

2. Viewing activity statistics on protected stations

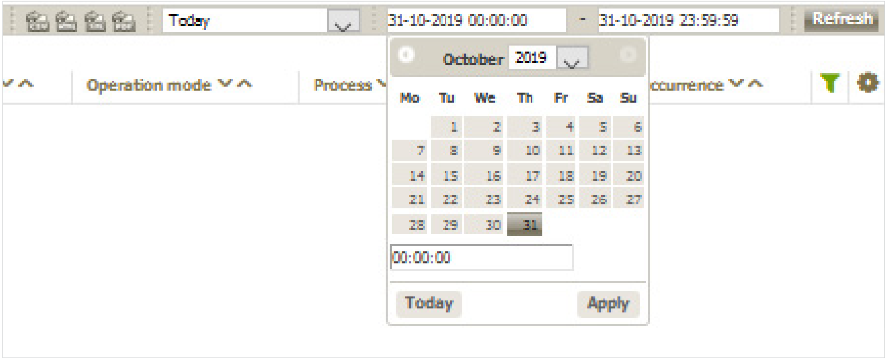
1. In the hierarchical list, select a station or a group.
2. In the **Statistics** section's control menu, select **Application Control events**.
3. A window will appear containing the list of applications that were denied or allowed on the selected stations.

   Statistics for the last 24 hours are displayed by default. To display data for a certain period, specify a date range with respect to the present day from the drop-down list.



31-10-2019 00:00:00 - 31-10-2019 23:59:59

To specify an arbitrary date range, enter the desired dates or click the calendar icon next to the date fields.

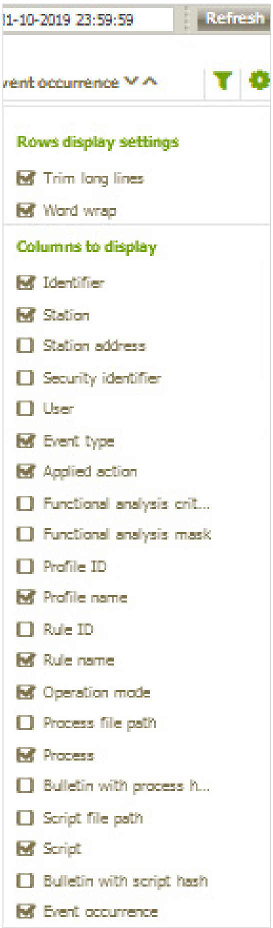


31-10-2019 00:00:00 - 31-10-2019 23:59:59

00:00:00

To display data, click on **Refresh**.

The contents of the displayed information is also configurable. To select what table fields you want displayed, click on ▼.



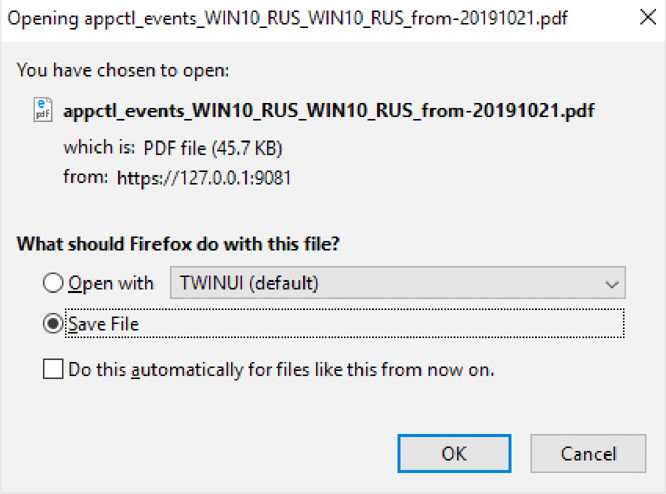
Rows display settings

- ☑ Trim long lines
- ☑ Word wrap

Columns to display

- ☑ Identifier
- ☑ Station
- □ Station address
- □ Security identifier
- □ User
- ☑ Event type
- ☑ Applied action
- □ Functional analysis crit...
- □ Functional analysis mask
- □ Profile ID
- ☑ Profile name
- □ Rule ID
- ☑ Rule name
- ☑ Operation mode
- □ Process file path
- ☑ Process
- □ Bulletin with process h...
- □ Script file path
- ☑ Script
- □ Bulletin with script hash
- ☑ Event occurrence

If you want to save the statistics table for printing or future processing, click on one of these buttons CSV HTML XML PDF (**Save as a CSV file, Save as an HTML file, Save as an XML file, Save as a PDF file**).



Opening appctl_events_WIN10_RUS_WIN10_RUS_from-20191021.pdf

You have chosen to open:

appctl_events_WIN10_RUS_WIN10_RUS_from-20191021.pdf

which is: PDF file (45.7 KB)
from: https://127.0.0.1:9081

What should Firefox do with this file?

○ Open with TWINUI (default)

● Save File

□ Do this automatically for files like this from now on.

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