

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.

Anti-virus Network > Everyone > Application control events 🏦										
* Selected objects 🏓						****	Week	25-10-2019 00:0	00:00 * 3	1-10-2019 23:59:59 Refresh
📋 Everyone	Identifier MA	Station MA	Event type MA	Applied action V A	Profile name MA	Rule name MA	Operation mode MA	Process	Script MA	Event occurrence VA
 General Statistics 	2ca841e0-ecaa-11e8-7905- f0f7da268169	WINIQ_RUS	Process launch	Unknown			Active	Farlexe		25-10-2019 14:45:47
Errors	2ca841e0-ecaa-11e5-7905- f0f7da268160	WIN10_RUS	Process launch	Blocked by deny rules	Honey	c18efa50-f97a-11e9-52ce- e174b6c0104f	Active	For Joke		28-10-2019 15:03:00
 Summary data Scan statistics 	2:a041e0-e:aa-11e0-7900- f0f7da268160	WIN10_RUS	Process launch	Blocked by deny rules	Honey	c10efa50-f97a-11e9-52ce- e174b6c0104f	Active	Foruese		28-10-2019 15:03:04
Start/Stop Threat statistics	200941e0-e000-11e0-7900- f0f7ds268169	WINLO_RUS	Process lounch	Blocked by deny rules	Напеу	c10efa50-f97a-11e9-52ce- e47456c9194f	Active	Fervexe		28 10 2019 15:03:12
• Status • Teska	2cc841c0-ccc0 11c8 7006- f0f7ds268169	WIN10_RUS	Process Jourch	Blocked by deny rules	For main group	oldfar	Active	For Joke		28 10 2019 15:06:22
Blocked devices Products	2cc841c0-cccc-11c8-7906- f0f7ds268169	WIN10_RUS	MSI pockoge launch	Unknown			Active			29-10-2019 15:07:56
Preventive protection events Application control events	2cs841e0-ecss-11e8-7906- f0f7ds268169	WIN10_RUS	Module load	Unknown			Active	Farland		29-10-2019 15:08:19
Agent installations	2cm841e0-ecms-11e8-7906-	WINIO RUS	Notice Inst	Unknown			Active	Alion (II		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** \rightarrow **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.

Anti-virus Network > Everyone > Windows > I	Dr.Web Agent 🏠					
* Selected objects						0 0 i 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
🔛 Everyone	Everyone, Custom settings are specified.					
 Control 	General Mobility Log Interface Events					
Statistics Configuration	Task Scheduler startup delay (min.)	1		•	•	
Permissions Task Scheduler	Period of statistics sending (min.)	60		•	•	
Update restrictions	Interval of virus databases relevance	1	Cerys 🗸	•	•	
Connection settings	Language	System language	,	•	•	
4 Windows - Scanner	Enable Microsoft Network Access Protection			•	•	
SpIDer Mail and SpIDer Gate						
Dr.Web Agent	Mlow quarantine remote control			•	•	
Office Control SpIDer Guard for workstations	Collect information about stations			•	•	
SpIDer Guard for servers Dr.Web for Microsoft Outlook	Period of collecting information about stations (min.)	190		•	*	
On:Web Firewall Preventive protection	Track location			•	•	
Network port monitor Application Control	Period of coordinates transmission	15 min.		*	*	
Android mecOS	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 \rightarrow Dr.Web Server configuration, go to the Statistics tab.

Administration > Dr.Web Server configuration		
► Administration		🔸 🕤 🖉 🖉 🔤
 Logs Confouration 	General Traffic Network Statistics Security Cache Database Modules Location Licenses Log	<u>^</u>
Administrators	The list of objects and events about which statistic information will be stored	
Authentication Dr. Web Server configuration	Quaractive 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.

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 antivirus network stations.

Dr.Web Server configuration	Diocked devices		*	*	
Dr.Web SNMP agent configuration Dr.Web Server Task Scheduler	Application Control statistics on processes activity		•	•	
Web Server configuration User hooks	Application Control statistics on processes blocking		•	*	
Notifications Repository	Multiple blockings by Application Control		*	*	
Installations Network scanner	Prohibition period on sending notifications	300	•	•	
Network Installation Application Control	Period of counting blocked processes	3600	•	•	
Trusted applications Application catalog	Events number	100	•	•	
Additional features	Number of the most common profiles	Ę	•	•	

3. Click on Save.

4. Restart the anti-virus server.

Administration 🛱			
* Administration	# Dr.Web Server		Yersions list 💽 🕖
Dr.Web Server Encryption keys	Dr.Web Server Version	12.00.0 (27-06-2019 02:00:00)	Restart Dr.Web Se

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 \rightarrow Application Control \rightarrow Application catalog.

Idministration > Application catalog 🏦											
Administration											
Configuration	Publisher V A	Product name VA	Version VA	Certificate subject V A	τ ο						
Notifications	Eugene Roshal & Far Group	Far Manager	30.650								
Installations	Eugene Roshal & Far Group	Far Manager	3.0.26.0								
Application Control Trusted applications	Eugene Rosifal & Far Group	Far Manager	3.0.27.0								
Application catalog	Eugene Roshal & Far Group	Par Manager	3.0.55.0								
Additional features	Eugene Roshal & Far Group	Par Manager	3.0.35.0								
Database management	Eugene Roshal & Far Group	For Monoyer	3.0.27.0								
Dr. Web Server statistics SPI consols	Eugene Rashel & For Group		3.0.310.0								
Lua consola	Eugene Rashel & For Group	For Monogor	3.0.29.0								
Backups	Eugene Rochal & Far Group	Far Manager	3.0.5498.0								
Utilities	Eugene Roshal & Far Group	Far Manager	3.0.5454.0								
	- Previous 1 2 3 Next -			Page: 2	Showing 11 - 20 of 21 10 🗸						



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

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 	Two weeks	18-10-2019 00:0	0:00 - 3	31-10-2019 23:59:59 Refresh
ne 🔨 🔨	Operation mode VA	Process V A	Script V ^	Event occurrence 🔨 🍸 🧔
	Active	Farlexe	Search	
f97a-11e9-52ce- 194f	Active	Farlexe	far	x
197a-11e9-52ce- 194f	Active	Farlexe		Default Apply
197a-11e9-52ce-		-		

Click on **Apply**.

Anti-virus Network > Everyone > Application	control events 🛱										
* Selected objects						1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Veek 🗸	25-10-2019 00:00	00 - 3	1-10-2019 23:59:59	Refresh
🔝 Everyone	Identifier V A	Station VA	Event type MA	Applied action V A	Profile name VA	Rule name MA	Operation mode MA	Process	Script V A	Event occurrence MA	T 0
 General Statistics Taxada 	2ca841e0-ecas-11e8-7906- f0f7ca268569	WIN10_RUS	Process leurch	Unknown			Active	Fer.exe		20-10-2019 14:40:47	

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

* Selected objects *				***	Two weeks	18-10-2019 00.0	1.00 - 31	-10-2019 23:59:59	- Accresh
🔝 Everyone	Identifier Y A	Application control events, 28-	10-2019 14-48-47	*	Operation mode Y A	Process Y A	Script Y A	Event occurrence V	~ T 0
General Statistics	2ca041e0-ecas-11e0-7906- f0f7da268169			Access and	Active	For Joint		28-10-2019 14:48:47	
Threats Errors	2cs841e0-ecse-11e8-7906-	Identifier	2ca841e0 ecas 11e8 7906 f0f7da268169		Active	far.exe		28-10-2019 15:03:00	
Summary data Scan statistics	2ca841e0-ecae-11e8-7906- f0f7de268169	Station Station address	WINSO_RUS selu//127.0.0.1.56824		Active	Par.ava		28-10-2019 15:03:04	
Start/Stop Threat statistics	2cs041eO-ecse-11e0-7906- 7077ds208109	Security identifier	5-1-5-21-838027901-3387140579-3678695824		Active	Parlana		28-10-2019 15:03:12	
- Status - Tasks	2ca841e0-ecce-11e8-7906- 1077ca268169	Event type	Process launch		Active	Parese		28-10-2019 15 06 22	
Blocked devices Products	2ca84ie0-ecas-11e8-7906- 7077ds258169	Applied action Functional analysis criterion	Unknown		Active			28-10-2019 15:07:56	
Preventive protection events Application control events	2c#041e0-ec##-11e0-7906- f0f7c#268169	Functional analysis mask			Active	Par.exe		28-10-2019 15:08:19	
Agent installations Agent deinstallations	2:a041e0-ecas-11e0-7906- r0r7ca268169	Profile name			Active	Align.dll		28-10-2019 15-08-21	
Configuration Permissions	2ca041e0-ecas-11e0-7906- f0f7de258109	Rule ID			Active	arcille.dl		28-10-2019 15:08:21	
Task Scheduler Undate matrictions	2cs041e0-ecse-11e0-7906- r0r7cis268169	Operation mode	Active		Active	AutoWrep.dll		28-10-2019 15:08:21	
Installing components Connection obligant	2ca845e0-ecaa-11e8-7906- r0r7da268169	Process file path Process	C:/Program Files/For Manager/For.exe Far.exe		Active	Brackets.dl		28-10-2019 15:08:21	
Windows Second	2ca841e0-ecas-11e8-7906- f0f7ds208109	Bulletin with process hash			Active	Compare.dll		28-10-2019 15:08:21	
SpIDer Mail and SpIDer Gate	2cs841e0-ecse-11e8-7906- r0r7cs268169	Script			Active	DrawLine.dll		28-10-2019 15:08:21	
Online Control	2La941e0-ecaa-11e8-7906- 7077da268169	Bulletin with script hash	-		Active	BoltCase.dl		28-10-2019 15:08:21	
SpIDer Guard for workstations SpIDer Guard for servers	2c#941e0-ec##-11e0-7906- f0f7d#268169	Event notification	28-10-2019 14:48:47		Active	EHenu.dl		28-10-2019 15:08:21	

Click on **Create rule**.

plication control events: 28-10-2019 14:48:47	
	Save Cancel
Profile name	
ref	
refs	
news	
For main group	
Allow	
Ο Βατγ	
Operation mode	
Active	
) Test	
Prohibit the launch of applications on the following criteria:	
Match the even dalke file hash (SH0-255)	
Match the following options:	
Application certificate hash (SHA-1)	
Executable file metadata	
File name	

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



Application control events: 28-10-2019 14:48:47	×
Operation mode	^
Active	
○ Test	
Beckliki Han Saurah of Saurijan Kono on Han Kallauring orikowa	•
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	
= 30.54540	
hie description	
Original file name	
Product name	
✓ Product version	
= 3.0.5454.0	
Publisher	~

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.

and and a substantian sector from a subfunction	6, 6, 6, 6, 7 m mmt (b. (5.7016.07.07.00) - 11.(5.7016.07.07.07.07.07.07.07.07.07.07.07.07.07.	chesh
 Selected objecta 		and and a
🔐 Everyone	Dary rule in profile ref successfully created.	
 General 		
 Statistics 		

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

Anti-virus Network > For main group > Properties 🖄					
* Selected objects	. The For main proup profile properties				
🗎 For main group	Canada Mow mode				
► General	Profile name+	For main group			
	Identher	afff0200-cd65-11e9-5537-780017700fee			
	Enable profile				
	Suitch profile to global test mode				
Anti-virus Network > For main group > Properties 🖄					
▼ Selected objects #	The For main group profile properties				
🚔 For main group	General Allow mode Deny mode				
 General 	Use deny mode				
			21 章 +		
	Name	Operation mode			
	oldfar	Active			

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

Anti virus Network > For main group > Properties 😭				
* Selected objects	The Formain group profile properties			
🚔 For main group	Openations completed successfully			
 General 				

The problem solved.



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