

Dr.Web Enterprise Security Suite 12.0 Using Application Control to block outdated software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## Using Application Control to block outdated software

Outdated software is one of today's security problems.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 The **Application Control** module included in the Dr.Web Enterprise Security Suite Control Center can block outdated software.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**  $\rightarrow$  **Create profile**.



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

Anti-virus Network 🏫		
▼ Selected objects #	🔆  • 🕂 • 🥔  • 👜  • 🌒 • Q,  • 🕺 • 🖯	Save
🛄 Everyone	/ X 型 創 創 学 成 局 型 簡 数 単 当 回 段 10	
<ul> <li>General</li> <li>General</li> </ul>	Anti-virus Network  III Configured	

4. Click on Save.

Anti-virus Network 🛱			
▼ Selected objects	* I• + • \$ I• @ I• @ • Q I• @ • [8		Operation status / error message
🛅 Everyone	/ × ⑤ Ⅲ Ⅲ 平 永 팩 記 9 ● ● ⑤ ◎ ◎ ◎ ◎	ł.	The rols profile successfully created.
<ul> <li>General</li> </ul>	Manti-virus Network		

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).



Image: Section and space profile projections         Image: Section and space profile project	Save
Portmain group       Image: Control of Contro of Control of Control of Contro of Control of	
P General         Portila name*         Portila name*         Portila name*         Portila name*                Provide name*               Bergen	
1 Service     Takendifier       1 Operation ystem     Image: Service	
Image: Comparison of protein     Image: Comparison of the image: Comp	
all brolle	
Point     Functional analysis order/at       1 (B) ref     Image: Control of analysis order/at     0 prolititions     2 permissions       1 (B) ref     Image: Control of analysis order/at     0 prolititions     2 permissions       1 (B) ref     Image: Control of analysis order/at     0 prolititions     2 permissions       1 (B) response     Image: Control of analysis order/at     0 prolititions     2 permissions       1 (B) response     Image: Control of analysis order/at     0 prolititions     2 permissions	
Instance     Instance     Instance     Instance     Instance	
Initial Status     Muldies land and execution     0 protititions     2 permissions       Initianemptified     Initianemptified     Initianemptified     Initianemptified       Initianemptified     Initianemptified     Initianemptified     0 protititions	1
Fill Ungraund	1
	1
Drivers feeding 0 purilibilities 0 permissione	1
🗹 MS2 peckaper installation 0 μυλίλδουs 2 μεινήssiums	1
Seculable files integrity 0 prohibitors 2 permissions	1
© Allow mode Deatod	
Altow notes 1 note	
Trusted applications 0 groups	
Obny mode     Exand	
Deny nules i nule	
Auli-virus Network > For main group > Properties 🕆	
Subschaf objects     P     The Formalis group profile properties	Seve
Permain group General Altow mode Deny mode	
<ul> <li>General</li> <li>Perfile name+</li> <li>rgr man grap</li> </ul>	
Identifies df1000-005-11c9-003-700007704/m	
🖉 brails grafie	
Skilculi pudlje tu glubal test mode	
Functional analysis citeria *	
Z approximations 0 prohibitions 2 premissions	
Violate lost and remain 0 prohotow 2 permasors	
Lunch of stock integrations 0 prohotions 2 permanent	
Drives loading 0 principlems 0 permissions	
V MS packages installation 0 previousions 2 permittions	
Concutable files idea / 0 profiliations 2 permissions	
Allow mode	
Distance Texture	
noverna žina Tratele gapitalions 0 prava	
Deny mode     English	
Deny rules 1 rule	

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**  $\rightarrow$  **Assign profile**.

Anti-virus Network 🖄								
▼ Selected objects	* - + - 🕫	. a . a .	Q.   - 🕺 - 😫	The For main group profile properties				Save
🚍 For main group	✓×型面面单设用器	🦉 🌇 Save data to CSV file	18	General				
> General	Anti-vina Network  Configured  Source of the system  Profile of the	Save data to HTHL file Save data to XML file		Profile name* Identifier Datis profile Suitch profile to global test mode Suitch profile to global test mode	For main group art10200-co25-11e9-5237-788617768/ee			
	) (B) rems ) (B) refs ) (B) refs ) (B) Satur ) (B) Françort ) (B) Ungrouped	Image: Propagate configuration		Application laureh     Modules load and enclution     Laureh of script integraters		0 prohibitions 0 prohibitions 0 prohibitions	2 permissions 2 permissions 2 permissions	111

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):

Anti-virus Network 😭			
▼ Selected objects	🚖  + 🕂 + 🥔  + 📾  + 💩 - Q  + 🕺 - 🖯	Assigning the profile to objects	Save
🚔 For main group	✓X協動動業成型型等機等器目標	Active Directory Anti-virus Network Local users	
• Ceneral	Afficient Network     Configured     Configured     Configured     Configured     Configured     Configured     Configure     Configure	Acti visus Network	

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.

	main news screenshots download plugins problems links plugring forum opan sour
Far Manager	<u>DATTANU</u>   cur
file and archive manager	
	downloa
Stable builds	
• Far Manager v3.0 build 5454 x86 (2019-08-23)	
archive msi pdb	
• Far Manager v3.0 build 5454 x64 (2010 00 20)	
archive msi pdb	
Nightly builds full changed og	
• Far Manager v3.0 huild 5502 x86 (2019-10-31) Last change: shmuel 30.10.2019 22:24:15 +0200 - build 5502	
archive msi pdb	
<ul> <li>Far Manager v3.0 build 3502 x04 (2019-10-31) Last change: shimuel 30.10.2019 22:24:15 +0200 - build 5502</li> </ul>	
archive msi pdb	

Install the earlier version. Run it.

## Go to Statistics $\rightarrow$ Application control events.

Anti-virus Network > Everyone > Application control events 😪										
▼ Selected objects x*						10 10 10 10 10 10 10 10 10 10 10 10 10 1	ino meeta 🗸	18-10-2019 00.0	0.00 2	1-10-2019 23.59.59 Refresh
Cveryone	Identifier V A	Station VA	Event type VA	Applied action VA	Profile name VA	Rule name VA	Operation mode VA	Process V A	Script V A	Event occurrence VA
► General ▼ Statistics	2cs841e0-ecss-11e8-7906- TUT/0s268169	WIN10_RUS	Process launch	Unknown			Active	Far eve		28-10-2019 14-48-47
Threats     Errons	2cm841e0-ecms-11e8-7006- TUT/05258169	WIN10_RUS	MSI package launch	Unknown			Active			28-10-2019 15-07-56
Summary data     Scan statistics	2ca841e0-ecaa-11e8-7906- f0f7da268169	WIN10_RUS	Module load	Unknown			Active	Far.exe		28-10-2019 15:08:19
<ul> <li>Start/Stop</li> <li>Threat statistics</li> </ul>	2ca84ie0-ecas-11e8-7906- f0f7da268160	WIN10_RUS	Module load	Unknown			Active	Align.dl		28-10-2019 15:08:21
• Status • Taska	2co841e0-ecos-11o8-7006- f0f7da268169	WIN10_RUS	Module load	Unknown			Active	arelite.dl		28 10 2019 15:08:21

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

Anti-virus Network > Everyone > Application	control events $\stackrel{\wedge}{\simeq}$									
* Selected objects					т	wo weeks	18-10-2019 00:00	:00 - 3.	1-10-2019 23:59:59	Refresh
🛄 Everyone	Identifier MA	Analization control events 28	0.2010 14.48.47		×	Operation mode MA	Process MA	Script MA	Event occurrence MA	<b>T</b> 0
<ul> <li>General</li> <li>Statistics</li> </ul>	2ca841e0-ecas-11e8-7906- f0f7da268160	Appreciation control events to .	10 2023 24140147	Create rule	^	Active	For love		28-10-2019 14.48.47	
Errors	200941e0-e000-11e0-7900- f0f7do268160	Identifier	2co841c0 ecco 11c8 7005 f0f7do268160			Active	Farleve		20-10-2019 15.03.00	
Summary data     Scan statistics	210941e0-e100-11e9-7900- f0f7d#268169	Station address	wthis_rus sel://127.0.0.1:56824			Active	For love		28-10-2019 15:03:04	
<ul> <li>Start/Stop</li> <li>Threat statistics</li> </ul>	2co841c0-ccos 11c8 7905- f0f7dw268169	Security identifier	5-1-5-21-838027991-3387140579-3678695824			Active	Farlexe		28-10-2019 15:03:12	
• Status • Tasks	2cm941e0-ecms-11e9-7906- f0f7dx268169	Event type	Process launch			Active	Farlace		28-10-2019 15:06:22	
Rincked devices     Products	2cs941e0-ecss-11e9-7906- FUF708258169	Applied action Functional analysis criterion	Unknown			Active			28-10-2019 15-07-56	
Preventive protection events     Annoration control events	2ca841e0-ecas-11e8-7905- r0r7ua268169	Functional analysis mask				Active	Far.exe		28-10-2019 15:08:19	
Agent installations	2ca941e0-ecas-11e8-7905- f0f7ds268169	Profile ID Profile name				Active	Align.dl		28-10-2019 15:08:21	
Configuration     Demission	2ca941e0-ecas-11e8-7905- f0f7ds268169	Rule ID				Active	arclite.dl		28-10-2019 15:08:21	
Task Scheduler	2ca841e0-ecas-11e8-7905- f0f7da268109	Operation mode	Active			Active	AutoWrep.dll		28-10-2019 15.08.21	
Opdete restrictions     Installing components	200941e0-e000-11e0-7900- f0f7da268160	Process file path Process	C:\/ragram Files\/Far Manager\/Far.exe Far.exe			Active	Breckets.dl		28-10-2019 15.08.21	
/ Windows	2La941e0-eLas-11e9-7900- f0f7da268169	Bulletin with process hash				Active	Compare.dl		28-10-2019 15:08:21	
SpiDer Mail and SpiDer Gate	2co841e0 ccos 11c8 7906 f0f7dx268169	Script file path Script				Active	DrawGre.dl		28-10-2019 15:08:21	
DriWeb Agent     Office Control	2co841c0 cccc 11c8 7906- f0f7dx268169	Bulletin with script hash				Active	EditCese.dl		28-10-2019 15:08:21	
<ul> <li>SpIDer Guard for workstations</li> <li>SpIDer Guard for servers</li> </ul>	2cs84ie0-ecss-11e8-7906- TCF7cs268t69	Event notification	28-10-2019 14:48:47		~	Active	Ellenudl		28-10-2019 15:08:21	

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



Application control events: 28-3	10-2019 14:48:47	×
Profile name		
Rule ID		
Rule name		
Operation mode	Active	
Process file path	C:\Program Files\Far Manager\Far.exe	
Process	Farlexe	
Bulletin with process hash	-	
Script file path		
Script	-	
Bulletin with script hash	-	
Event occurrence	28-10-2019 14:48:47	
Event notification	28-10-2019 14:48:47	
File hash (SHA-256)	b3719d09fdb0b97c66de135a9f9242ebd7707bc15a29243fd33648bc2fc8f00f	
File size (bytes)	5200896	
File version	3.0.5454.0	
Product name	Far Manager	
Product version	3.0.5454.0	
File description	File and archive manager	
Publisher	Eugene Roshal & Far Group	
Certificate issuer		
Certificate hash (SHA-1)		
Certificate start date	-	
Certificate end date		-

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

Application control events: 28-10-2019 14:48:47	×
Save Cancel	^
Profile name  ref ref refs news For main group Allow  Deny	
Operation mode	
Active	
○ Test	
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 name File size (bytes)	
	¥

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	
Brokiki iko lavaria of analizatione on iko followina orkaria.	-
Match the executable file hash (SHA-256)	
Match the fallowing options:	- 8
Application certificate hash (SHA-1)	- 8
Executable file metadata	- 8
File name	- 8
File size (bytes)	- 8
File version	- 8
= 3.0.5454.0	- 8
File description	- 8
Original file name	- 8
Product name	- 8
Product version	- 8
= 3.0.5454.0	
Publisher	~

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

* Selected objects	🔀 🔂 🔂 Time weeks 🔍 18-10-2019 00:00:00 + 13-10-2019 23 59-59	dh
🔛 Everyone	Deminals in profile ref successfully created.	٦
<ul> <li>General</li> </ul>		_
<ul> <li>Statistics</li> </ul>		

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 > Prope	rties 🖄							
* Selected objects	The For main group profile	Save						
🗎 För main gröup	General Allow mode Den	General Allow mode Deny mode						
► General	Profile name*	For main group						
	Identifier	afffd200-cd65-11e9-5537-780017700fee						
	Enable profile							
	Switch profile to glo	Suitch profile to global text words						
Anti-virus Network > For main group > Proper	ties 🖄							
* Selected objects	The For main group profile	The For main group profile properties						
🗎 For main group	General Allow mode Deny	Seneral Allow mode Deny mode						
<ul> <li>General</li> </ul>	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 For main proop profile properties	Save					
🗎 For main group	Operation completed successfully	×					
▶ General							

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

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

However, if we update the utility, it will run correctly. 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 | hhttps://free.drweb.com | https://ru.av-desk.com | https://curenet.drweb.com