

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

© Doctor Web 2003–2019



Dr.Web Enterprise Security Suite 12.0

Features of the Application Control module

Functional analysis

No one knows what processes are running on a controlled computer. It's entirely possible to use special utilities to view the list of downloaded programs (if, of course, one doesn't know that malicious programs track the launch of these utilities and stop working as soon as they detect them). But while obtaining a list of running programs is fairly feasible, figuring out what a program or script does is no longer always possible.

With the Application Control module included in the Dr.Web Enterprise Security Suite Control Center, you can create rules that prohibit the launch of certain categories of software. This prevents suspicious programs from being able to run from the risk zone—anti-virus software developers certainly know what features usually count as malicious when examining such programs!

Configure the application control system by using profiles—the 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**.

Anti-virus Network 🏠							
▼ Selected objects	* - + -	🖉 l. 🗠		• Q	-	191	- 18
🗎 Everyone	/×3000 ¥	Create station	5 🖸 🕸				创
General Statistics Configuration Permissions Task Scheduler Update restrictions Installing components	Anti-virus Network Configured Configured Configured Configured Configured Configured Configured Configured Configured Configured Configured Configured	Create group Create a neighbor Create policy Create Proxy Server Create profile					

3. In the newly opened panel, enter the **Profile name**.

Anti-virus Network 🖄		
▼ Selected objects #	🔆 - 🕂 - 🥔 - 🔯 - Q, - 👯 - 🗠 New große	Seve
Cveryone	✓× 空田 和 平 永 号 益 極 象 単 当 直 除 約	
General	I∰ Anti-vinus Network 1-01 Confounesi	

4. Click on Save.

Anti-virus Network 🕸		
* Selected objects	* • + • # • 🖾 • 🛊 • Q • 🕺 • 🗎	Operation status / error message
🗀 Everyone	✓ X 12 m m 平 成 型 量 量 数 数 単 55 00 m	The refs profile successfully created.
► General	anti-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 (set 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).

Anti-virus Network 🕸							
* Selected objects	* I• + • \$P I• @ I• @ • Q I	· 🕺 - 🗄	The For main group profile properties			-	Save
🗎 For main group	✓ X 型曲曲 苯 改唱 品 短 載 ● 题 凹 映	15	General				
General	Anti-visus Network Fill Configured		Profile name*	For main group			
) 🏠 Everyone		Identifier	af110200-e065-11#9-5537-780017700fee			
	b (iii Operating system b (iii Policies		Enable profile				
	A Profiles		Switch profile to global test mode				
	E Coneve		Functional analysis criteria*				
	ි ලි ක් වි ලි ක්		Application launch		0 prohibitions 2	permissions	1
	> ⊡ Ratus > ⊡ Transport		Modules load and execution		0 prohibitions 2	permissions	1
	Fill Ungrouped		Leunch of script interpreters		0 prohibitions 2	permissions	1
			Drivers landing		0 prohibitions 0	permissions	1
			MSI packages installation		0 prohibitions 2	permissions	1
			Executable files integrity		0 prohibitions 2	permissions	1
			Allow mode Disobled				
			Allow rules		1 rule		
			Trusted applications		0 groups		
			Deny mode Enabled				
			Deny rules		1 rule		
	1						

Anti virus Network > For main group > Properties 🕆					
* Selected objects	The Formain group profile projectiles	Save			
🗎 For main group	General Allow mode Deny mode				
▶ General	Profile name* for man group				
	Identifier dff10200-e855 11c0 5537 708037708/re				
	V Instite profile				
	Skitch profile to global test mode				
	Functional analysis critesia*				
	Application Isurch 0 prehibitions 2 permissions				
	✓ Mobiles tood and execution 0 prehibitions 2 permissions				
	✓ Laurch of script interpreters 0 prehibitions 2 premissions				
	Drivers loading 0 prehibitions 0 premissions				
	✓ MS peckages installation 0 prohibitors 2 permissions /				
	✓ becutatie files integrity 0 prohibitors 2 permissions /				
	* Allow mode Deadlod				
	Altow rules i rule Turbel sufficient Duran				
	Deny mode touted				
	Demy rules i 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.

In this section, you can specify the features that are unwanted or desirable for the programs launched on the protected computers. To specify advanced settings for each selected event criteria type, click on \checkmark (**Edit**) for the corresponding type of event. A window showing a list of settings will open.

Let's consider the advanced settings in more detail.

There are 6 criteria types of functional analysis:

- Application launch
- Module load and execution



- Launch of script interpreters
- Driver loading
- MSI package installation
- Executable file integrity

Each group has its own set of criteria; let's consider them in detail.

Application launch

Application launch X
Save
Prohibitions Permissions
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
Prevent running of applications from temporary folders
\square Prevent running of Windows/Microsoft Store applications (only for Windows 8 and later) $~~$ \checkmark
Application launch
Save
Prohibitions Parmissions
Allow running of system applications and Microsoft company applications
Allow running of system appreciations and increasing company appreciations
Al variate requiring or introduction of normal action abhardroups

The list of permissions is easy to understand, so let's proceed to the prohibitions. Most items do not even need any commentary—it is obvious what kind of programs fall within them and whether you need to launch them:

- Prevent the running of applications signed by certificates known in Doctor Web as certificates for adware
- Prevent the running of applications signed by certificates known in Doctor Web as gray
- Prevent the running of applications signed by certificates known in Doctor Web as certificates for hacktools
- Prevent the running of applications signed by fake/malformed certificates
- Prevent the running of applications signed by certificates known in Doctor Web as certificates for malware
- Prevent the running of applications signed by revoked certificates
- Prevent the running of Sysinternals utilities
- Prevent the running of applications from NTFS (ADS) alternate threads



- Prevent the running of Windows/Microsoft Store applications (only for Windows 8 and later)
- Prevent the running of applications with a double/atypical extension

It's well understood that Linux programs run under Windows are not used in most systems, so we can also select **Prevent running of bash shells and WSL applications (only for Windows 10 and above)**.

It's also not a bad idea to prohibit the launch of applications from removable media (Prevent the running of applications from removable media) and over the network (Prevent the running of applications from the network and shared resources). Flash cards are a well-known source of viruses.

Quite often, malware is used to run folders for temporary files. If you are not going to deploy new software that can also use those folders—select the option **Prevent the running of applications from temporary folders**.

Modules load and execution × Save Prohibitions Permissions Control all modules load and execution Control modules load and execution in host applications Prevent loading and execution of modules signed by certificates known in Doctor Web as certificates for adware Prevent loading and execution of modules signed by certificates known in Doctor Web as gray Prevent loading and execution of modules signed by certificates known in Doctor Web as certificates for hacktools Prevent loading and execution of modules signed by fake/malformed certificates Prevent loading and execution of modules signed by certificates known in Doctor Web as certificates for malware Prevent loading and execution of modules signed by revoked certificates Prevent loading and execution of modules signed by self-signed certificates Prevent running of unsigned modules Prevent loading and execution of modules from NTFS (ADS) alternate threads Prevent loading and execution of modules from network and shares Prevent loading and execution of modules from removable media Modules load and execution × Save Prohibitions Permissions Allow loading and execution of system modules and Microsoft company modules Allow loading and execution of known/trusted by Doctor Web modules

Module load and execution

Control the loading and execution of all modules

Control the loading and execution of modules in host applications

The list of permissions is also straightforward; the prohibitions are similar to the previous section.



Launch of script interpreters

Launch of script interpreters X
Save
Prohibitions Permissions
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
Launch of script interpreters X
Save
Prohibitions Permissions
Allow running of system scripts and Microsoft company scripts
Allow running of known/trusted by Doctor Web scripts

In this section, you can prohibit the types of scripts (and also registry modification) that are definitely not used in your system and their launch from removable media or from temporary directories.

Driver loading

Drivers loading	×
	Save
Prohibitions Permissions	
Prevent loading of drivers signed by certificates known in Doctor Web as certificates for adware	
Prevent loading of drivers signed by certificates known in Doctor Web as gray	
Prevent loading of drivers signed by certificates known in Doctor Web as certificates for hacktools	
Prevent loading of drivers signed by fake/malformed certificates	
Prevent loading of drivers signed by certificates known in Doctor Web as certificates for malware	
Prevent loading of drivers signed by revoked certificates	
Prevent loading of drivers signed by self-signed certificates	
Prevent loading of unsigned drivers	
Prevent loading of drivers from NTFS (ADS) alternate threads	
Prevent loading of drivers from network and shares	
Prevent loading of drivers from removable media	
Prevent loading of drivers from temporary folders	
Prevent loading of vulnerable driver versions of popular software	



Drivers loading	×
	Save
Prohibitions Permissions	
Allow loading of system drivers and Microsoft company drivers	
Allow loading of known/trusted by Doctor Web drivers	

In addition to the prohibitions described above in this section, there is a unique option—**Prevent the loading of vulnerable driver versions of popular software**. We think that its importance is clear.

MSI package installation

MSI packages installation
Save
Prohibitions Permissions
Prevent installation of packages signed by certificates known in Doctor Web as certificates for adware
Prevent installation of packages signed by certificates known in Doctor Web as gray
Prevent installation of packages signed by certificates known in Doctor Web as certificates for hacktools
Prevent installation of packages signed by fake/malformed certificates
Prevent installation of packages signed by certificates known in Doctor Web as certificates for malware
Prevent installation of packages signed by revoked certificates
Prevent installation of packages signed by self-signed certificates
Prevent installation of unsigned packages
Prevent installation of packages from NTFS (ADS) alternate threads
Prevent installation of packages from network and shares
Prevent installation of packages from removable media
Prevent installation of packages from temporary folders
MSI packages installation
Save
Prohibitions Permissions
Allow installation of system packages and Microsoft company packages
Allow installation of known/trusted by Doctor Web packages

Malicious packages are often used by malicious software. You can use the options in this section to prevent the launch of installation packages.



Executable file integrity

Executable files integrity
Save
Prohibitions Permissions
Prevent creating new executable files
Prevent modification of executable files
For each life file to be all to
Executable files integrity
Save
Prohibitions Permissions
Allow creation and modification of executable files by signed system applications and Microsoft company applications
Allow creation and modification of executable files by signed known/trusted by Doctor Web applications

This is probably the most simple and attractive option. An anti-virus must cure, so it's logical for it to have the right to modify objects. But the updating system can also modify objects. So, if you are using a Microsoft updating system, you can prevent the modification of executable files for all other sources by ticking the boxes on the **Prohibitions** page.

Tick the boxes for the settings that you want to be applied, and don't forget—before enabling the new operation mode on stations, it should be tested.

If you enable an event type 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.

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 🙀			0 0 00 00	The for main arous profile properties				Sare
🖷 For main group	×SHHY& SH	🏝 Save data to CSV file	98 - Caller	General			+ 1	
 General 	Anti-virus Network Configured Group one Group one Configured Profiles Profiles Configured Con	Seve data to HTML file Seve data to XML file Seve data to XML file Seve data to PDF file Depart configuration		Profile name+ Identifier Diable profile Switch profile to global Lest mode	f'αr mein group erffrazzo-co55-11e9-5537-78οb177bb/ee			
	> 6 merce > 6 merce > 6 merce > 2 stue > 2 stue > 2 mercept > 2 mercept	Duort statistics Propagate configuration Assign pullicy Assign profile		Punctional analysis criteria* Application learch Modules load and execution Learch of assist interaction		0 prohibilions 0 prohibilions	2 permissions 2 permissions	1
						0,010000	a permanente	1



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	🚖 l+ 🕂 + 🥔 l+ 📾 l+ 💩 + Q_ l+ 🕺 +	18	Assigning the profile to objects	Save
🖶 For main group	✓ X 强 相 和 筆 读 骂 益 感 ● 题 臼 块	18 Ac	ctive Directory Anti-virus Network Local users	
> Ceneral	All Conjunct Description Descript		Anti Vinzi Notorofi Corrunt Yotu 2 Notorofi Yotu 2 Noto Yotu 2 Noto Yotu 2 Notorofi Yotu 2 Notorofi Yotu 2 Notorofi Uniferent 0 Uniferent	

 Click on Save. All the selected objects will be added to the list to which the profile is being applied. Furthermore, the objects will appear as nested items for the configured profile.
 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