Open Endpoint Manager > Click 'Security Sub-Systems' > 'Antivirus' > 'Autorun Items'

- The autoruns area lets you view and take action on items blocked by the boot protection feature of Comodo Client Security (CCS).
- This includes unrecognized Windows services, items that run at startup, and scheduled tasks.
- Click the following links to learn more

Background - How do unrecognized autoruns get terminated?

Overview of the auto-run interface

Take actions on terminated auto-runs

### Background - How do unrecognized auto-runs get terminated?

Comodo Client Security will terminate unrecognized auto-runs if:

'Apply this action to suspicious auto-run processes' is enabled, with 'Terminate', 'Terminate and Disable' or 'Quarantine and Disable' set as the action.

You can implement this setting in two places:

1. Miscellaneous Settings - The 'Miscellaneous' section of a profile. This applies the action to the realtime/background virus scanner.

General	Containment	Firewall	HIPS	Antivirus	Miscellaneous	
Miscel	aneous					
Appl When this Windows	y the selected ac option is enabled, the services, autostart ent	tion to unrec registry will be ries or schedule	cognized a monitored fo ed tasks.	utorun entries r modifications a	s related to new/modified registry items: CCS 10.7+ nd the selected protective action will be applied to detected unrecognized	7
Actio	n					_
Т	erminate and Disa	able			~	
Dete	ct shellcode injec	tions Ex	clusions			

2. Custom scan options – This is the 'Options' section when you create a custom virus scan in a profile. This applies the action to any on-demand or scheduled virus scans which use your custom scan.

Profiles / New test / Antivirus		
	Add Scan Profile	×
New test	Define items to be scanned, scanning options and running schedule.	
Add Profile Export Profile Clone Profile Delete Profile Mak	Scan name Scan name	
General Maintenance Window BETA Antivirus	Items Options	
Antivirus Realtime Scan Scans Exclusions	<ul> <li>Enable scanning optimizations up to CCS 8.3 This option increases the scanning speed significantly.</li> <li>Decompress and scan compressed files This option allows scanner to decompress archive files e.g., zip., rar, etc., during scanning.</li> </ul>	
This section hows you to add, remove and edit scan profiles and Add	<ul> <li>Use cloud while scanning This option allows scanner to connect to cloud to query file ratings.</li> <li>Automatically clean threats When the threats are identified, perform the selected action automatically.</li> </ul>	
NAME ¢	Disinfect	~
Full Scan	Show scan results window Show results of scheduled scans and scans launched from a remote management portal. Use heuristics scanning	
Quick Scan	Use the selected level or sensitivity while scanning neuristically.	$\sim$
Unrecognized and Quarantined Files Scanning	Apply this action to suspicious autorun entries Ccs 10.7+ The selected action will be automatically applied if unrecognized Windows services, autostart entries scheduled tasks are detected.	or
	Ignore	~

# Overview of the auto-run interface

- Open Endpoint Manager
- Click 'Security Sub-Systems' > 'Antivirus' > 'Autoruns Items'

Endpoint Manager	Antivirus / Autoruns Items		🔁 👔 🕹 Logout (:	UTC+03:00 1)
DASHBOARD >				
DEVICES	Search group name	Current Malware List Quarantined Files Threat History Autoruns Items		
A users →	B Show all	📴 Delete Autorun from Devices 🛛 📮 Restore Autorun on Devices 🖉 Rate as Unrecognized 🧟 Rate as Trusted 🗞 Rate as Malicious 🖆	Export 🗸	<b>@ T</b>
CONFIGURATION TEMPLATES	<ul> <li>→ ● 0NewCustomer</li> <li>→ ● 1111</li> </ul>	DATE TYPE ACTION # OF DEVICES FILE NAME FILE HASH FILE PATH RATING	ADMIN LAST ACTION ON RATING GROUP	AUTORUN STATUS
€00 NETWORK MANAGEMENT BETA >	· · · · · · · · · · · · · · · · · · ·	2019/10/08Autostart EnTerminated2     autorum_08EB6CF4 C\Users\AdUnrecognized	Not set Rate as trusted	Disabled
APPLICATION STORE	+ 🖨 222		Not est Data se melieleue	Disabled
APPLICATIONS >	+ 🖶 54545345	2019/10/08 Autostart En Terminated T autor_08_10 400b20 0.1 C. (Users QA Unrecognized	Not set Rate as malicious	Disabled
SECURITY SUB-SYSTEMS	+ 🖨 aasd	2019/10/07 Autostart En Quarantined 1 amd64" 0161DE 🛱 C:\WINDOW Unrecognized	Not set	Disabled
Security Dashboards	🔸 🖨 asdaa adad1	2019/10/07 Autostart En Quarantined 1     OneDriveSet 394568 d      C.\WINDOW Unrecognized	Unrecognized	Disabled
Containment	+ 🖶 Bad_company	2019/10/07 Autostart En Quarantined 1 OneDriveSet D9AB25 C:\WINDOW Unrecognized	Unrecognized	Disabled
Application Control Valkyrie	Default Customer	2019/10/04 Autostart En Quarantined 1     7vX6zJFW.e 1C6A4A	Unrecognized Rate as unrecognized	Disabled
Antivirus Device Control	<ul> <li>→ ➡ ds11234</li> </ul>	2019/10/04	Not set	Disabled
LICENSE MANAGEMENT >		2019/10/04	Malicious Rate as malicious	Disabled
☆ settings >	<ul> <li></li></ul>	□ 2019/10/04 _ Autostart En Quarantined _ 1 upi0Z5rw.exe 52130A _ 3 C.\Users\Ad. Unrecognized	Unrecognized Rate as unrecognized	Disabled
> DEVELOPER TOOLS >	+ 🖶 ebash2	2019/10/04	Malicious Rate as malicious	Disabled
	+ e ebash3	2019/10/04	Unrecognized	Disabled
	🔹 🖶 Good_company	2019/10/04 Autostart EnQuarantined1     zbn1T2Pa.exe     D3631E3     C.\Users\AdUnrecognized	Malicious Rate as malicious	Disabled
	🔹 🖶 Mert Saribasak	2019/10/04	Unrecognized	Disabled
	к « <u>1</u> 2 » н	2019/10/04	Malicious Rate as malicious	Disabled
		2019/10/04 Autostart En Quarantined 1     G3lhigNo.exe 57CB2D HI C:\Users\Ad Unrecognized	Malicious Rate as malicious	Disabled

The interface shows all blocked auto-runs on Windows devices. Autoruns are items which start at Windows

boot-up or are scheduled tasks. Click the funnel icon on the right to filter the list.

The interface columns are as follows:

Date - The date and time the auto-run was terminated on the device.

Type - The auto-run category. Can be one of the following:

- Windows service
- Scheduled task
- Auto-start entry

Action - How the unrecognized autorun was handled by CCS. The possible responses are:

- Terminated
- Terminated and Disabled
- Quarantined and Disabled

**# of Devices** - The number of devices on which the item was found. Click the number to view the actual devices.

File Name - The file whose auto-run entry was terminated. Click the name of a file to view its details.

**File Hash** - The SHA1 hash value of the quarantined file. The hash value uniquely identifies the file, even if the filename is changed.

File Path - The location of the file on the endpoint.

Comodo Rating - The file's official trust level in Comodo's database.

Admin Rating - The trust rating of the file as set by the administrator. Files can be rated as trusted, malicious or unrecognized

Last Action Group - The most recent action taken on the item by an admin.

Auto-run Status - Shows whether the auto-run is enabled or disabled on the endpoint.

### Take actions on auto-run items

The controls above the table let you take various actions on selected items:



#### **Restore an autorun**

You may want to restore an item if you think it is a false-positive. False-positives are files that you deem as safe, but which CCS has blocked, terminated or quarantined.

- · Select the items you want to restore
- Click 'Restore Autorun on Devices':

› <sup>녾</sup>	Device List	Current Malwa	re List Quara	antined Files	Threat History	Autoruns Items			
e	Delete Autorun from	Device:	Restore Autorun on D	evices 🐻 R	ate as Unrecognized	👰 Rate as Trus	ted 😽 Rate :	as Malicious	••• More
	DATE	ТҮРЕ	ACTION	# OF DEVICES	FILE NAME	FILE HASH	FILE PATH	COMODO RATING	ADMIN L RATING 0
	2019/10/10	Autostart En	Quarantined	2	autorun_trus	8853D0	C:\Users\Ad	Unrecognize	nd Trusted R
	2019/10/10	Autostart En	Quaranti	2	autorun_unr	0FC26E	C:\Users\Ad	Unrecognize	ed Unrecognized R
	2019/10/04	The action has selected autor	s been successfi run item(s)	ully applied to	80HfyBbT.exe	27404E	C:\Users\Ad	Unrecognize	ed Not set
	2019/10/04	Autostart En	Quarantined	1	2XRxjqv5.exe	3B66C8 占!!	C:\Users\Ad	Unrecognize	ed Malicious R

### Delete an autorun

Deleting an item will completely remove the file from all devices on which it resides.

- Select the items you want to restore
- Click 'Delete Autorun from Devices':

<mark>،</mark> ۴	Device List	Current Malware Lis	t Quarantined	Files 1	Threat History	Autoruns Items		
¢	Delete Autorun fro	m Devices	e Autorun on Devices	Rate	as Unrecognized	👰 Rate as Truste	ed  🐻 F	tate as Malicio
	DATE	TYPE ACT	TION # OF	DEVICES	FILE NAME	FILE HASH	FILE PATH	COMOU RATING
	2019/10/10	Autostart En Qua	arantined 2		autorun_trus	8B53D0	C:\Users\Ad	
Ο	2019/10/10	Delete Autorun fi	rom device				×	
	2019/10/04 .							
	2019/10/04.	Do you really want to	delete selected au	utorun from	all device(s)?		d	
	2019/10/04.					Confirm Car	ncel	
	2019/10/04	Autostart En Qua	rantined 1		cv9Ap02y.exe	982620	C:\Users\Ad	

### Assign a new trust rating to autorun items

A trust rating determines how Comodo Client Security interacts with a file. The three 'Rate as...' buttons let you assign a new rating to selected autoruns:

×

This is the impact of each rating:

#### **Rate as Unrecognized**

• Files rated as unrecognized are restored to their original locations on the device.

- Under default settings, unrecognized files are run in the container each time they execute.
- Contained files are isolated from the rest of the host so it cannot cause any damage.

# **Rate as Malicious**

- Files rated as malicious remain in quarantine on the device.
- If you want to remove the item entirely, then choose 'Delete Autorun from Devices' instead.

# **Rate as Trusted**

- The file will be removed from quarantine and restored to its original location on the device.
- The files will be white-listed and skipped by future antivirus scans.

# Further Reading

How to run virus scans on devices from the security sub-systems menu

How to manage quarantined items in Endpoint Manager

How to view and manage unprocessed malware on your endpoints