How to manage quarantined items in Endpoint Manager

Open Endpoint Manager > Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files' tab

- Comodo Client Security (CCS) neutralizes threats it discovers by placing them in quarantine on an endpoint.
- Quarantine is a secure holding area for potentially dangerous files. All quarantined files are encrypted, so they cannot run or cause harm to the computer.
- You can review all quarantined files on your network from the Endpoint Manager interface. You can restore them, delete them, change their trust rating, or submit them to Valkyrie.
 - Valkyrie is an advanced file analysis service designed to establish the trust rating of unknown files. The service runs a battery of dynamic and static tests on a file to determine whether or not it is malware
- This article explains how to use the Endpoint Manager to review and manage quarantined files.

How do items get quarantined?

Open the quarantine area

Restore items to their original location

Delete quarantined items

Assign a new trust rating to an item

Manage quarantine locally instead

How do items get quarantined?

- 1. Because of settings in the 'Antivirus' section of the device profile
 - Real Time Scan Settings 'Show antivirus alerts' is *disabled* with 'Quarantine Threats' set as the default action
 - ... or 'Show antivirus alerts' is *enabled*, and the end-user quarantined the threat at an alert.
 - On-demand scan settings 'Automatically clean threats' are enabled and 'Quarantine' is set as the action.
- 2. Because an admin or end-user manually moved the threat into quarantine. This may have been done in Endpoint Manager, or locally at the endpoint.

Open the quarantined items area

Log into Comodo One / Dragon

- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Quarantine Files'
- The interface shows every quarantined item on all Windows, Linux and Mac devices. Click the funnel icon on the right to filter the list.

××												
Endpoint Manager		<u>Antivirus</u> / Quarantined Files							ē 🗘 🕂	uтс+о Logout (test_team)		
DASHBOARD	>											
DEVICES	>	> B Device List Current Malware List Quarantined Files Threat History Autoruns Items										
	>		Delete File	from Devices	Restore File on D	Devices Rate as Unrecognized		Rate as Truster	d Rate as Malicious	Export 🗸	@ T	
	>		OS	FILE NAME	FILE HASH	SIGNATURE	COMODO RATING	ADMIN RATING	DEVICES DETECTED ON	LAST QUARANTINED	LAST ACTION ON GROUP	
	>			7 10 2end	A6170C	Policy Admi	Unrecognized	Malicious	1	2019/10/12 06:57:00	Restore file	
APPLICATION STORE	>			7_10_L0114		r onoy.r tarria.	onroodginzed	manorodo		2013/10/12 00:07:00		
	>			autor_term	2163AC	Policy.Admi	Unrecognized	Malicious	1	2019/10/12 06:54:57		
SECURITY SUB-SYSTEMS	~			00099000.exe	774E0B	Policy.Admi	Unrecognized	Malicious	2	2019/10/12 06:44:55		
Security Dashboards				autorun_q+	E0ECE1	Policy.Admi	Unrecognized	Malicious	1	2019/10/12 06:44:33	Delete file	
Application Control				04.exe	E48B68	Win32.Jeefo	Malicious	Malicious	2	2019/10/12 10:55:42		
Valkyrie Antivirus				klaklashunt	FC41C1	Win32.Jeefo	Malicious	Malicious	3	2019/10/12 10:55:42		
Device Control			1.0		800000	Malwara@#	Maliaiaua	Not out	0	2010/10/11 06:24:25		

- Each row represents an individual file. The same file might be quarantined on multiple machines.
- Click the number in the 'Devices...' column to view all devices on which the file is quarantined. You can also apply actions to individual devices from this screen, rather than to every device:

File Info		Device List							
Dele	ete File f	from Devices	Restore File on Device	s Rate as Unr	recognized 👰 Rate as Trus	sted 👸 Rate as Malicious		R	T
This list contains only active devices and devices allowed in accordance with access scope settings									
	OS	DEVICE NAME	FILE PATH	DEVICE OWNER	DATE QUARANTINED	USER'S LAST ACTION	USER'S LAST ACTION	STATU	s
	os	DEVICE NAME DS-WIN7x6	FILE PATH	DEVICE OWNER dsok	DATE QUARANTINED	USER'S LAST ACTION	USER'S LAST ACTION	STATU	s

Click the following links for more help:

Restore items to their original location

Delete quarantined items

Assign a new trust rating to an item

Manage quarantine locally instead

Restore items to their original location

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 quarantined as malware.

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files'
- Select the items that you want to restore. Click the funnel icon on right to search for specific files.
- Click 'Restore File(s) on Devices' from the options at the top.

≡ <u>Antiv</u>	<u>/irus</u> / Qu	arantined Files						+	@	Logout (test_team)
, 侣	Device	List Curren	t Malware List	Quarantined Fi	les Threat His	story Auto	runs Iter	ns		
	elete File f	from Devices	Restore File on D	evices 🔭 Ra	ate as Unrecognized	횑 Rate as	Trusted	Rate as Malicious	Export	- 🔬 🍸
	OS	FILE NAME	FILE HASH	SIGNATURE	COMODO RATING	ADMIN RATING	DEVI	CES DETECTED ON	LAST QUARAN	TINED LAST ACTION ON GROUP
		7_10_2 Com	imand was sent s	successfully	ized	Malicious	1		2019/10/12 06:	57:00 Restore file
		autor_term	2163AC 📋	Policy.Admi	Unrecognized	Malicious	1		2019/10/12 06:	54:57
		00099000.exe	774E0B	Policy.Admi	Unrecognized	Malicious	2		2019/10/12 06:	44:55
		autorun_q+	E0ECE1	Policy.Admi	Unrecognized	Malicious	1		2019/10/12 06:	44:33 Delete file

- This will restore the item to its original location on every device.
- If you only want to restore the file on specific devices, then click the number in the 'Devices...' column. The device list screen lets you restore items on individual devices.
- Note Even though you have restored the file, it will still get flagged as a threat by the next virus scan. If you want to avoid this then choose 'Rate as trusted' instead. This will restore the file AND make sure it isn't flagged by future virus scans.

Delete quarantined items

If you have reviewed a quarantined file and confirmed it is malware, then you should delete it from the device.

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files'
- Select the items that you want to delete. Click the funnel icon on right to search for specific items.
- Click 'Delete File(s) on Devices' from the options at the top:

› 造	Devic	e List	Current Malware List Quarantined Files Threat History Autoruns Items		
	elete File	from De	vices Restore File on Devices 👩 Rate as Unrecognized 👰 Rate as Trusted 🗞 Rate as Mali	cious 😫 Export 🗸	n 🕈
	OS	FILE	N Delete File from Devices SIGNATURE COMODO ADMIN DEVICES DETECTED ON RATING RATING	LAST QUARANTINED	LAST ACTION ON GROUP
		7_	Delete File(s) from Device	2019/10/12 06:57:00	Restore file
		au	Do you really want to delate selected file(c) from all device(c)?	2019/10/12 06:54:57	Restore file
		00		2019/10/12 06:44:55	
		au	Confirm Cancel	2019/10/12 06:44:33	Delete file

Click 'Confirm' in the confirmation dialog.

- The file will be removed from every device on which it was quarantined.
- If you only want to delete the file from specific devices, then click the number in the 'Devices...' column instead. The device list screen lets you remove items from individual devices.

Assign a new trust rating to an item

A file rating determines how CCS interacts with a file on an endpoint.

- Click 'Security Sub-Systems' > 'Antivirus' > 'Quarantined Files'
- Select the items whose rating you want to change. Click the funnel icon on right to search for specific items.
- You can change the rating of a file with the buttons highlighted in the following screenshot:

› 뭡	Device List Current Malware List Quarantined Files Threat History Autoruns Items										
D 🔁	elete File	from Devices	Restore File on D	Devices	te as Unrecognized	👰 Rate as	Trusted 👸 Rate as Malicio	us 🔛 Export 🗸	@ T		
	OS	FILE NAME	FILE HASH	SIGNATURE	COMODO RATING	ADMIN RATING	DEVICES DETECTED ON	LAST QUARANTINED	LAST ACTION ON GROUP		
		7_10_2end	A6170C	Policy.Admi	Unrecognized	Malicious	1	2019/10/12 06:57:00	Restore file		
		autor_term	2163AC	Policy.Admi	Unrecognized	Malicious	1	2019/10/12 06:54:57	Restore file		
		00099000.exe	774E0B	Policy.Admi	Unrecognized	Malicious	2	2019/10/12 06:44:55			
		autorun_q+	EOECE1	Policy.Admi	Unrecognized	Malicious	1	2019/10/12 06:44:33	Delete file		
		04.exe	E48B68	Win32.Jeefo	Malicious	Malicious	2	2019/10/12 10:55:42			

Rate as Unrecognized

- The file is restored to its original location on the device and given a trust rating of 'Unrecognized'.
- The file will run in the container the next time it executes. Files in the container are isolated from the rest of the endpoint so it cannot cause any damage.

Rate as Trusted

- The file is restored to its original location on the device and given a trust rating of 'Trusted'.
- Trusted files are considered safe by CCS and are allowed to run as normal. Trusted files will not get flagged as a threat by future virus scans.

Rate as Malicious

• The file will remain in quarantine on the device with a trust rating of 'Malicious'.

The file will remain in the list of quarantined items in Endpoint Manager. If you want to remove the item entirely, then choose 'Delete file from device' instead.

Click 'OK' to apply your changes.

This will apply the trust rating to the file on every device. If you only want to change the file's rating on specific devices, then click the number in the 'Devices...' column. The device list lets you apply ratings to files on individual devices.

Manage quarantine locally instead

As an alternative to managing quarantined files via Endpoint manager, you can manage them locally in the Comodo Client Security (CCS) interface.

- Windows CCS Click 'Tasks' > 'General Tasks' > 'View Quarantine'
- Linux and Mac CCS Click 'Antivirus' > 'Quarantined Items'

CCS lets you perform similar actions on quarantined files as those described in this article.

See https://wiki.comodo.com/frontend/web/topic/how-to-manage-quarantined-files-in-ccs for help on this.

Further reading

Manage quarantine locally in Comodo Client Security

View and Manage Quarantined Items

How to view and manage unprocessed malware on your endpoints