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?

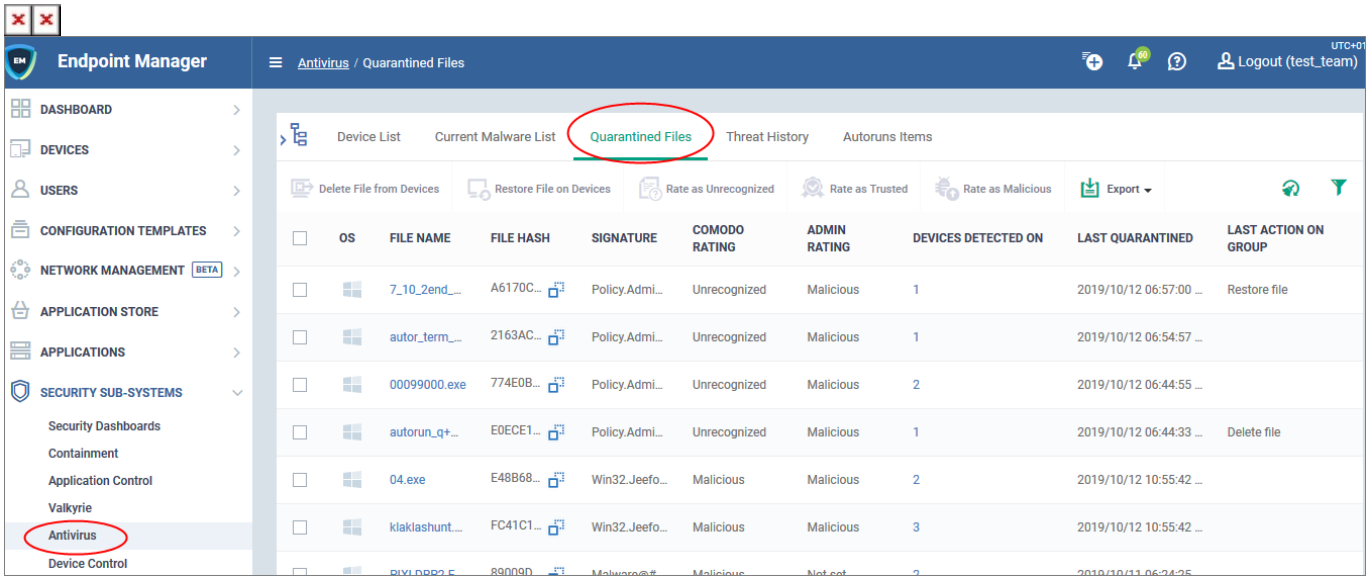
1. Because of settings in the ‘Antivirus’ section of the device profile
    - Real Time Scan Settings - ‘Show antivirus alerts' is *disabled* with 'Quarantine Threats' set as the default action

      … 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.

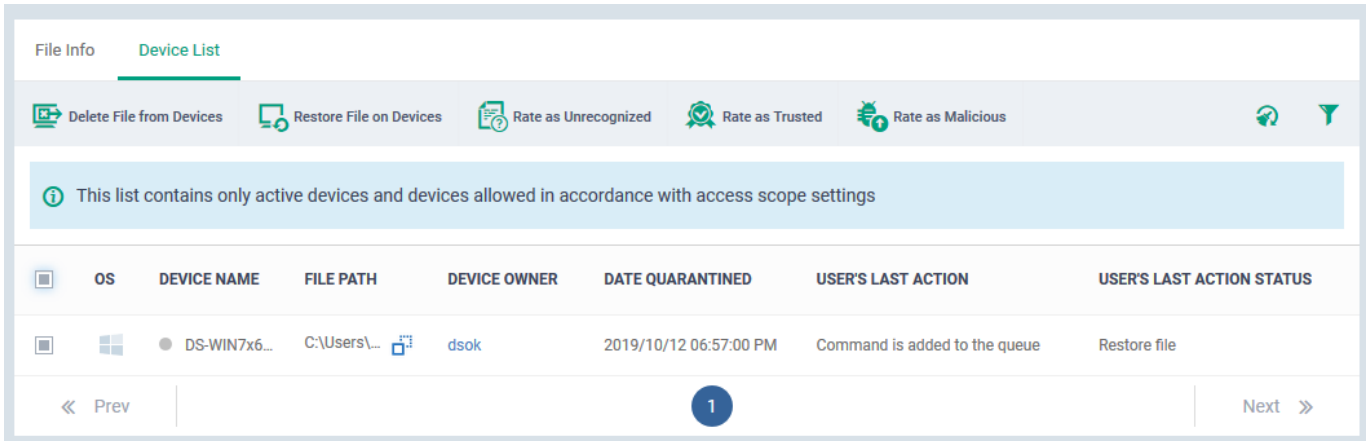
Open the quarantined items area

- 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.



- 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:



Click the following links for more help:

Restore items to their original location

Delete quarantined items

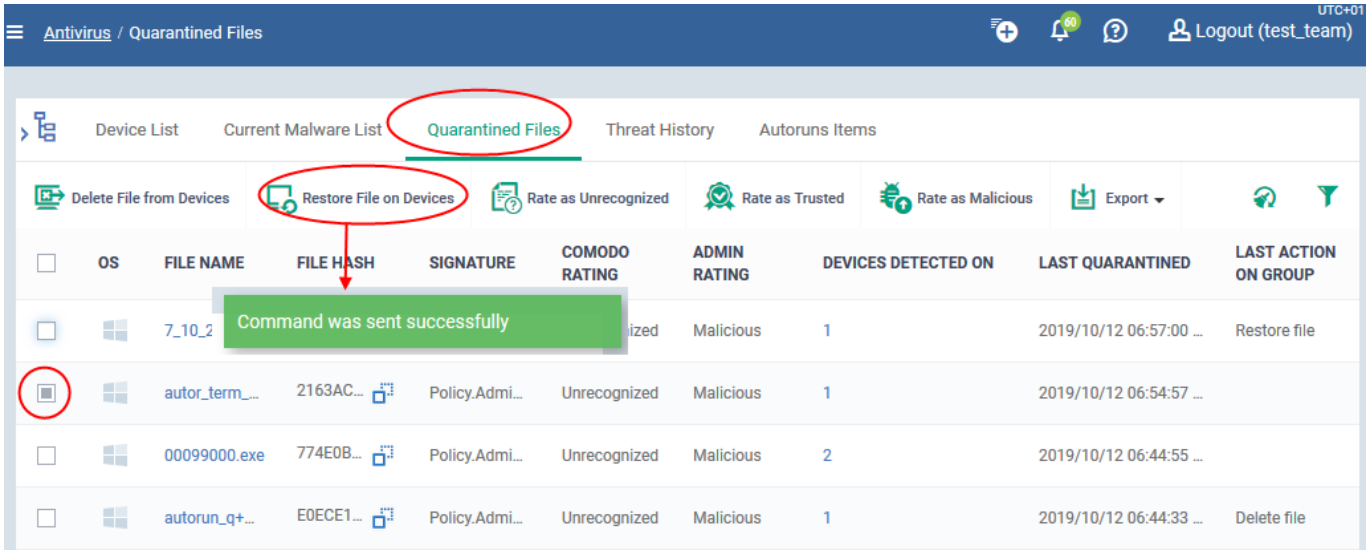
Assign a new trust rating to an item

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.

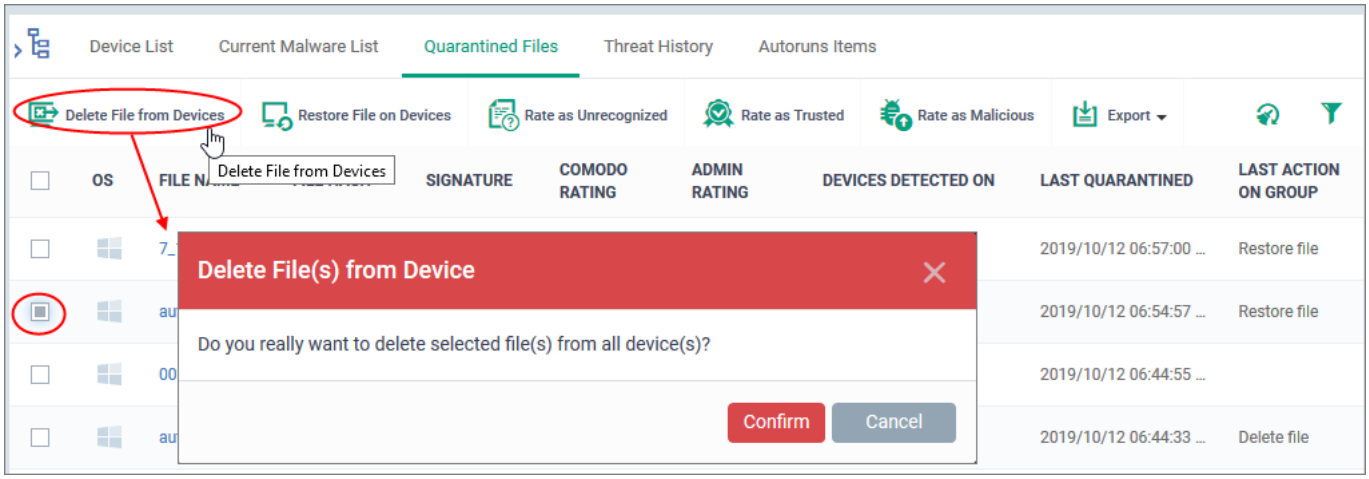


- This will restore the item to its original location on every device.
- If you only want to restore the file on specific devices, then click the number in the ‘Devices...’ column. The device list screen lets you restore items on individual devices.
- Note – Even though you have restored the file, it 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:



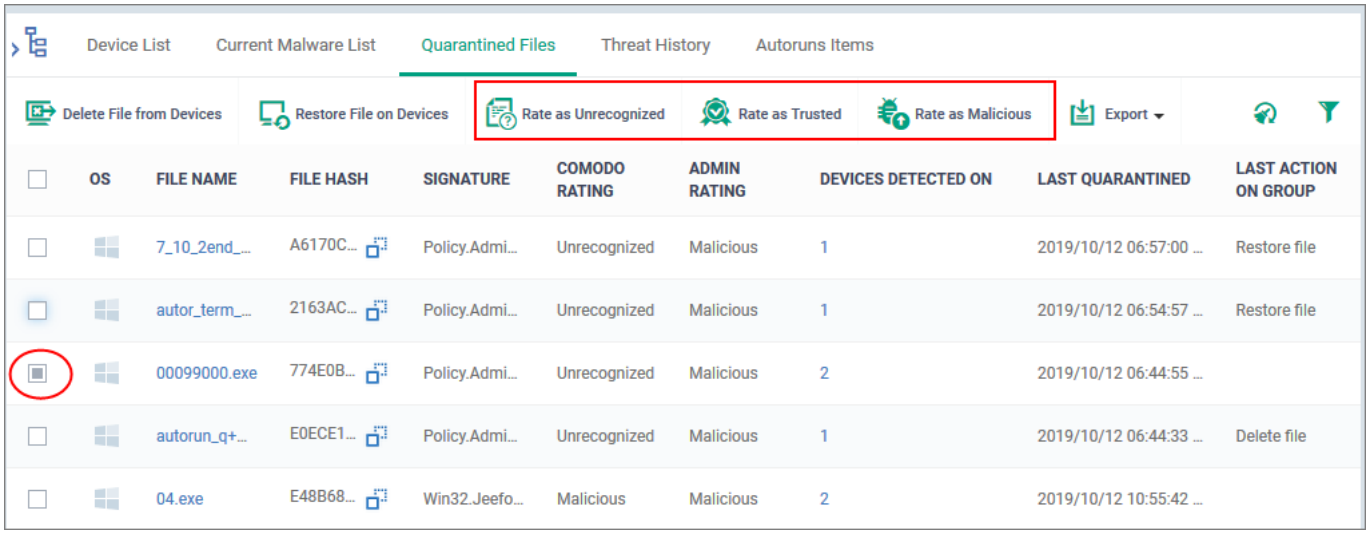
Click 'Confirm' in the confirmation dialog.

- 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:



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