# How to manage autorun items in Endpoint Manager

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

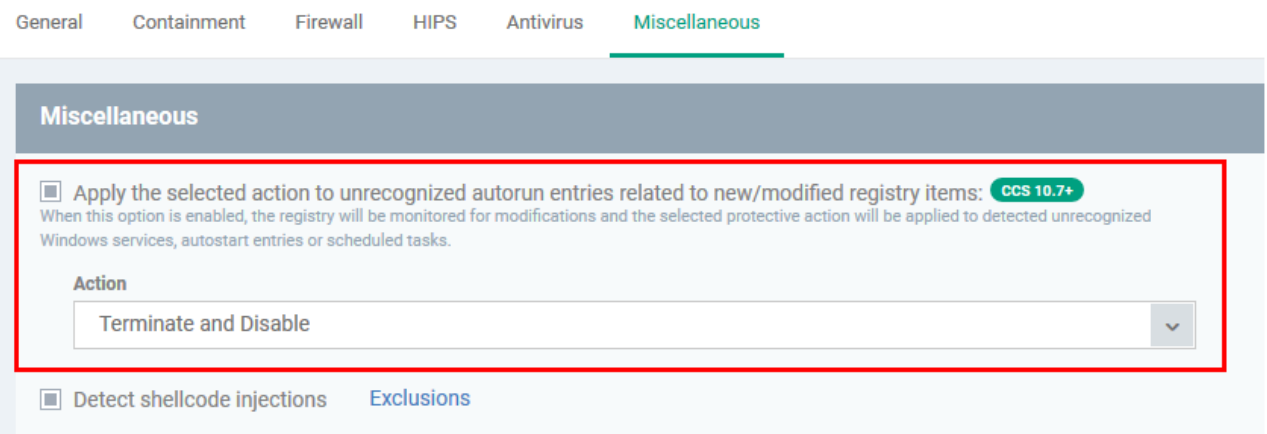
## Background - How do unrecognized auto-runs get terminated?

Comodo Client Security will terminate unrecognized auto-runs if:

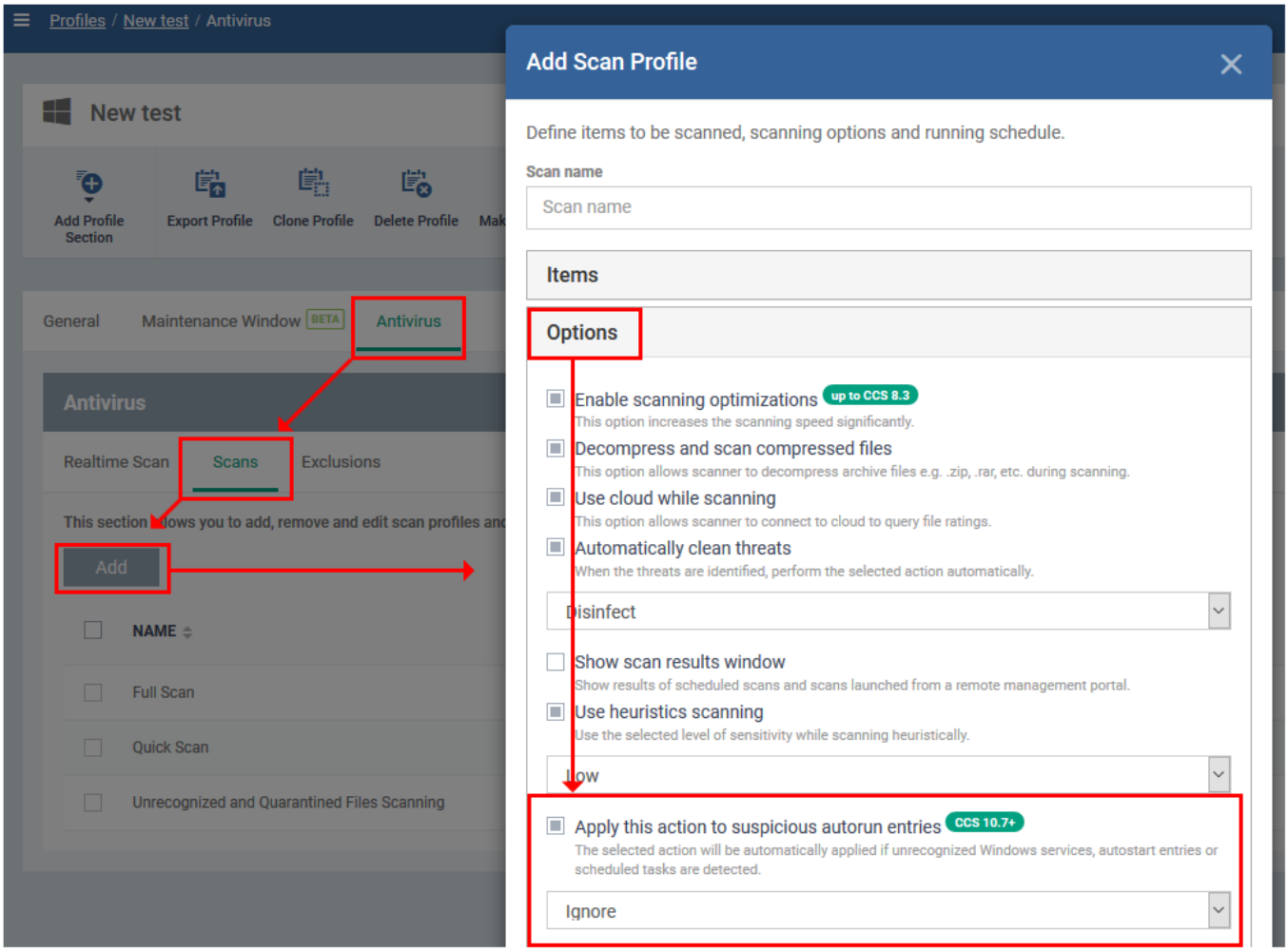
‘***Apply this action to suspicious auto-run processes***’ is enabled, with ‘Terminate’, ‘Terminate and Disable’ or 'Quarantine and Disable’ set as the action.

You can implement this setting in two places:

1. Miscellaneous Settings - The ‘Miscellaneous’ section of a profile. This applies the action to the real-time/background virus scanner.

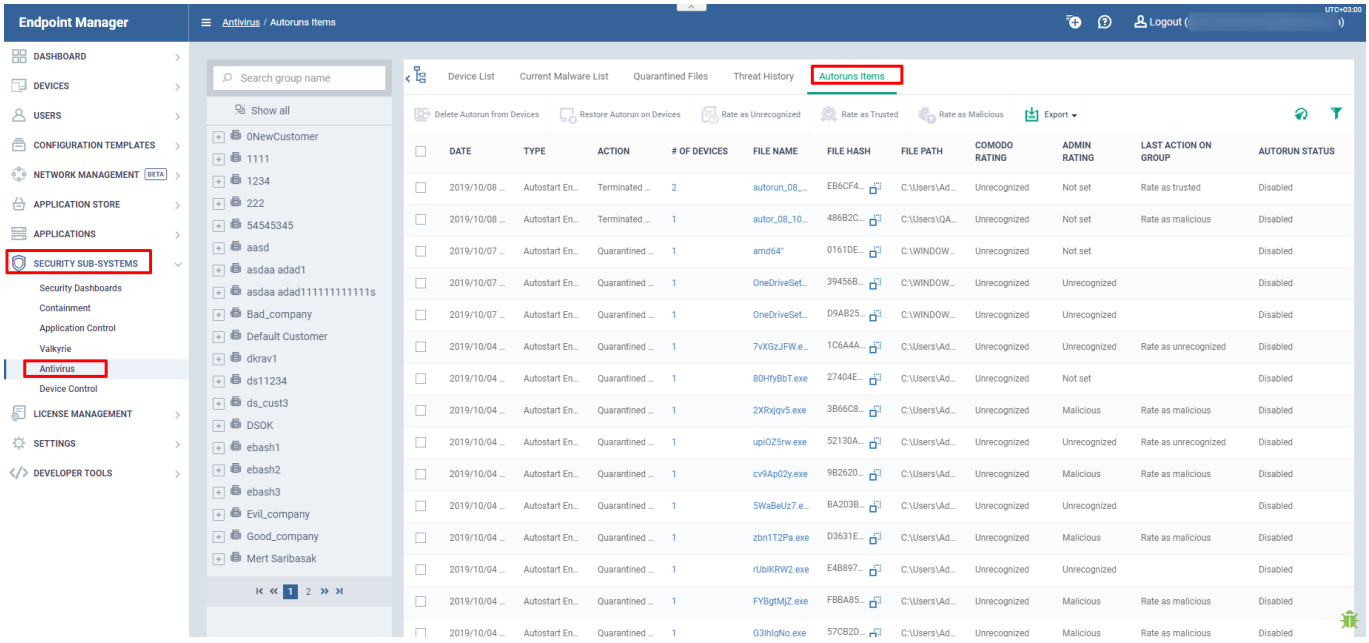



2. Custom scan options – This is the ‘Options’ section when you create a custom virus scan in a profile. This applies the action to any on-demand or scheduled virus scans which use your custom scan.




## Overview of the auto-run interface

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




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.

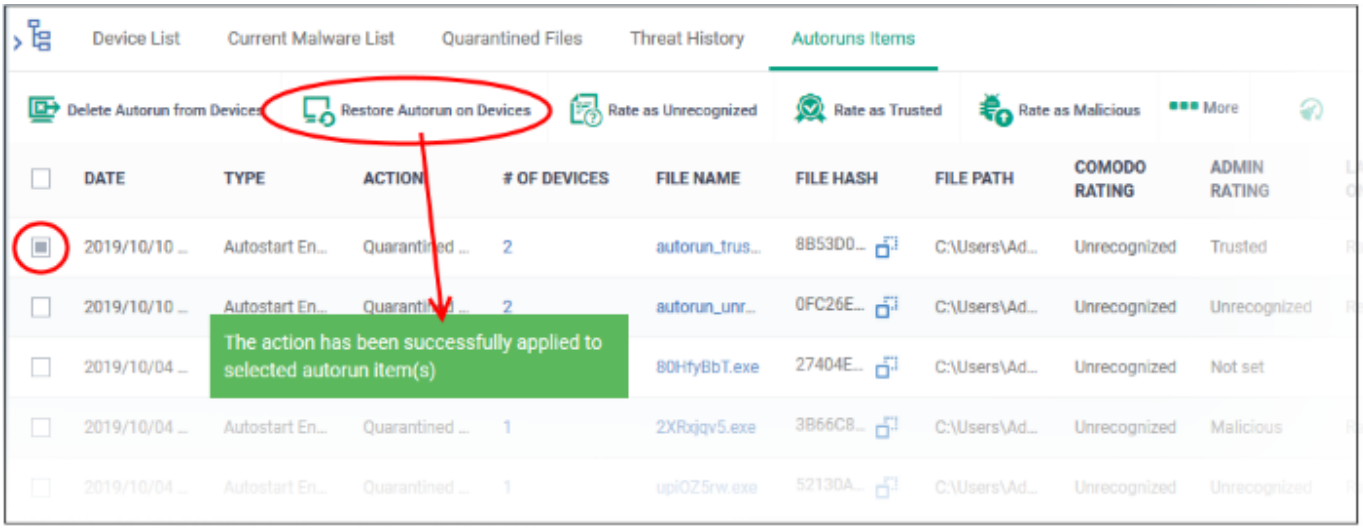
## Take actions on auto-run items

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.

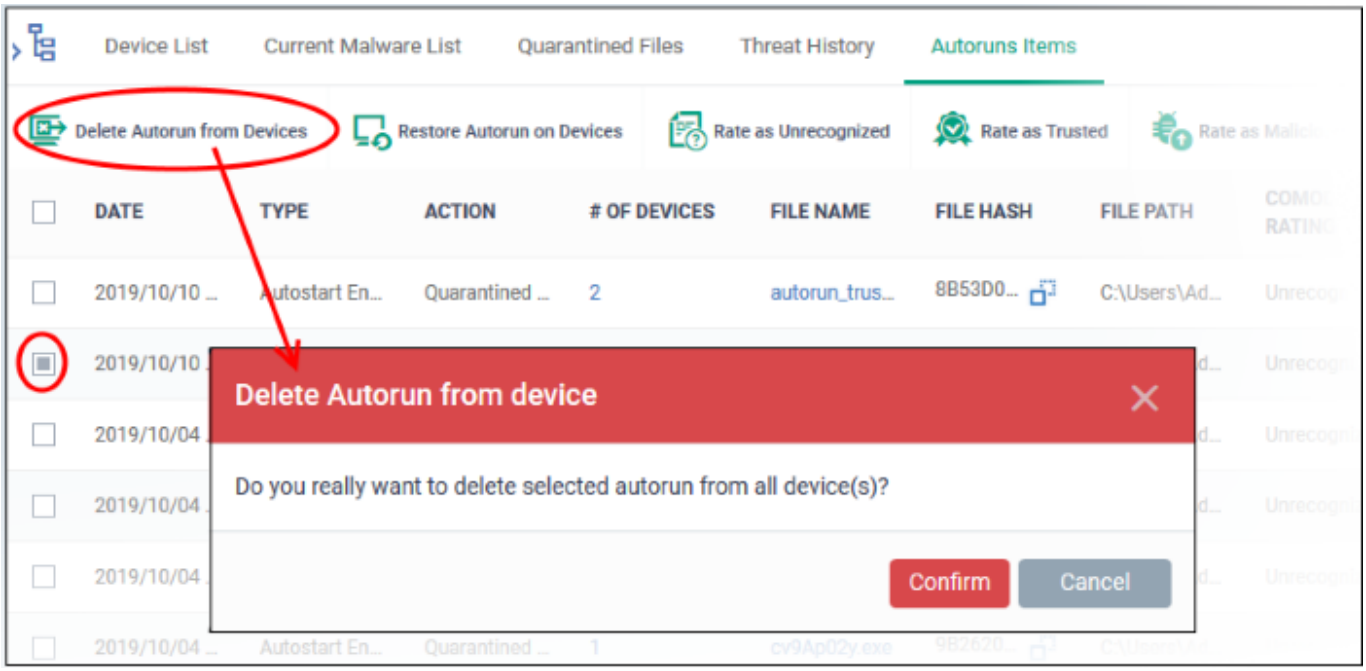
- Select the items you want to restore
- Click 'Restore Autorun on Devices':




### Delete an autorun

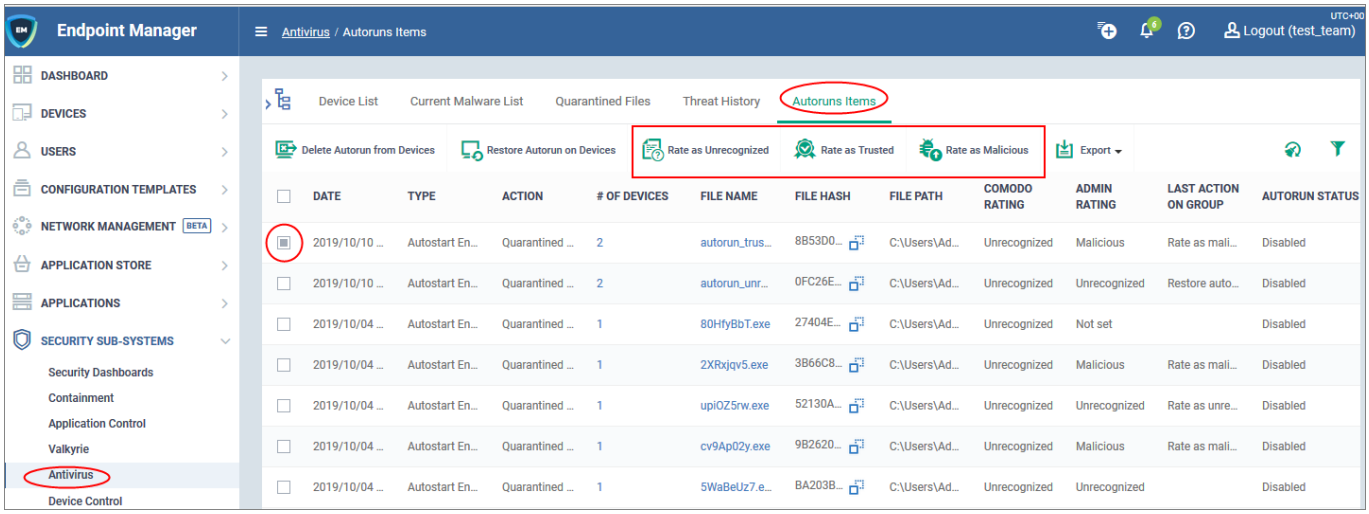
Deleting an item will completely remove the file from all devices on which it resides.

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




### 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