

- A file's trust rating determines how Comodo Client Security (CCS) handles the file.
- These are the possible file ratings:
 - **Trusted** - The file is safe and is allowed to run normally on the endpoint
 - **Malicious** - The file is malware and is quarantined or deleted on the endpoint.
 - **Unrecognized** - No trust rating is available for the file. Unrecognized files are automatically run in the container because there is the possibility they are malicious. Contained applications write to a virtual file system and registry, and cannot access other processes or user data. You have the option to auto-upload these files to Valkyrie for behavior testing. The tests will identify whether the file is trustworthy or malicious.
- Going one step further, a file can be rated by three sources:
 - **FLS rating** - This is the official Comodo rating of the file. CCS gets this rating from our file-lookup server when it runs a virus scan on the file.
 - **Admin rating** - Admins can use Endpoint Manager to apply their own rating to a file.
 - **Local rating** - End-users (or admins) can set a file's rating in the CCS interface.

Ratings are prioritized as follows:

1) Admin rating

2) Local rating

3) Comodo rating

- Admin ratings over-rule Comodo and local ratings *IF local verdict server* is enabled (default).
- Admin ratings are disregarded if local verdict server is disabled.
- To prevent local users from rating files, you can [password protect CCS](#) on the endpoint, and disable '[Show antivirus alerts](#)'.

There are two ways admins can set a trust rating in Endpoint Manager:

- [Application Control interface](#)
- [Device Details interface](#)

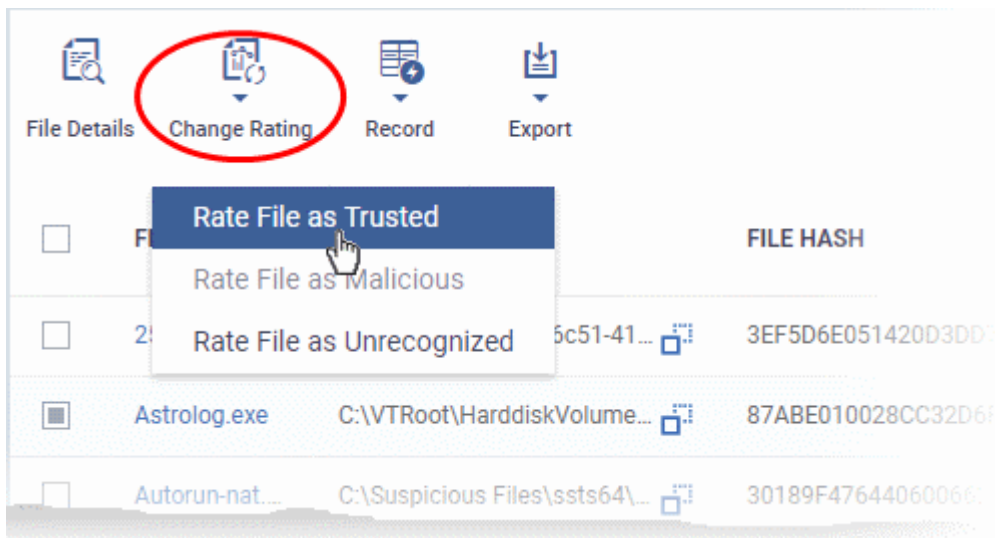
Application Control interface

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Application Control'

The interface shows a list of all files discovered from all managed endpoints with their trust ratings:

| FILE NAME | FILE PATH | FILE HASH | SIZE | # OF DEVICES | COMODO RATING | ADMIN RATING |
|----------------|-------------------------------|--------------------------|----------|--------------|---------------|--------------|
| FileWri3.exe | C:\Suspicious Files\ssts64... | B6F4F723771292EF4DF12... | 133.5 kB | 1 | Unrecognized | Not set |
| FireHole.exe | C:\Suspicious Files\ssts64... | 0D252493BE65734D229F2... | 133 kB | 1 | Unrecognized | Not set |
| FireHole2.exe | C:\Suspicious Files\ssts64... | EAECA080C1F6341B4749... | 140 kB | 1 | Unrecognized | Not set |
| FireHoleDLL... | C:\Suspicious Files\ssts64... | 0B38E861550375BC9817C... | 86.5 kB | 1 | Unrecognized | Not set |
| Flank.exe | C:\Suspicious Files\ssts64... | 5DA83EE42A2B53A5E4D1... | 124.5 kB | 1 | Unrecognized | Not set |
| Ghost.exe | C:\Suspicious Files\Bewar... | DF3328F9944867C3C5E14... | 11 kB | 1 | Unrecognized | Malicious |
| HostsBlock... | C:\Suspicious Files\ssts64... | 72C0830D1EDB29C2CA7C... | 125 kB | 1 | Unrecognized | Not set |
| Inject1.exe | C:\Suspicious Files\ssts64... | 5798DE6F20FDD8EB5EA1... | 129.5 kB | 1 | Unrecognized | Not set |

- Select the file for which you want to set a rating
 - Tip – Click the funnel icon at the top right and use the filters to search for a specific item
- Click 'Change Rating'.
- Select the new rating from the options:
 - Rate File as Trusted
 - Rate File as Malicious
 - Rate File as Unrecognized



The new admin rating will be set and sent to all endpoints. The new rating will determine the file's

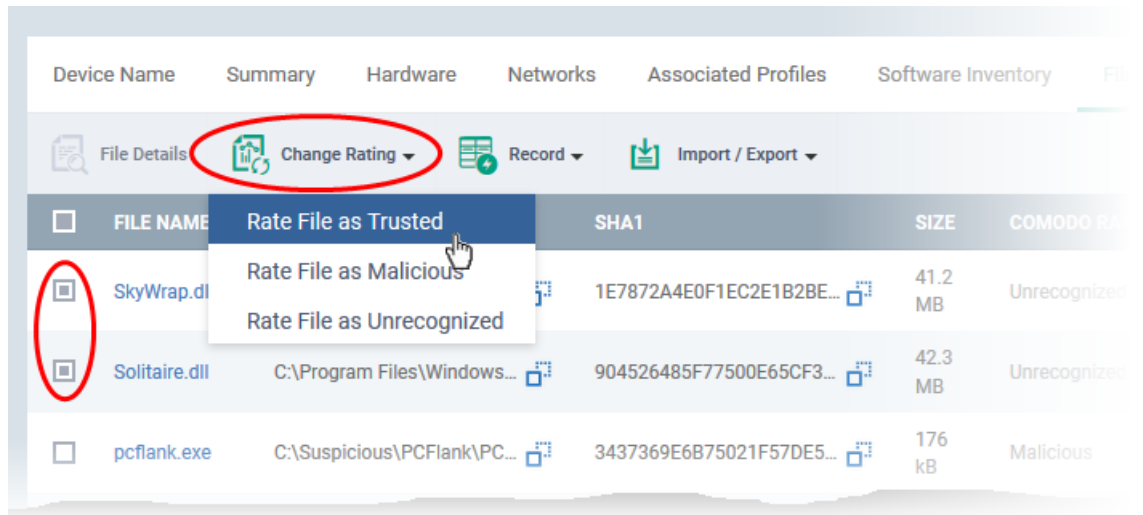
run-time privileges.

Device Details interface

- Login to ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Devices' > 'Device List' > 'Device Management'
 - Select a company or group on the left to view only their devices
- OR
- Select 'Show all' on the left to view every device enrolled to EM
- Click the name of a Windows device then select the 'File List' tab:

| FILE NAME | FILE PATH | FILE HASH | SIZE | COMODO RATING | ADMIN RATING |
|--|---------------------------------|--------------------------|--------|---------------|--------------|
| <input type="checkbox"/> CPILSuite.exe | E:\Suspicious files\All_test... | DCF2DFCB39003683BE2E0... | 1.5 MB | Malicious | Not set |
| <input type="checkbox"/> pcfank.exe | E:\Suspicious files\All_test... | 3437369E6B75021F57DE5... | 176 kB | Malicious | Not set |

- Select the file(s) whose rating you want to change
 - Tip – Click the funnel icon at the top right and use the filters to search for a specific item
- Click the 'Change Rating' button.
- Choose the rating you want to from the drop-down:



The new admin rating will be set and sent to all endpoints. The new rating will determine the file's run-time privileges.

??????