How to manage unknown & malicious files on your endpoints

Open Endpoint Manager > Click ‘Security Sub-Systems’ > ‘Application Control’

- The application control screen lets you view all files on your devices that have a trust rating of ‘Unrecognized’ or ‘Malicious’.
- You can manually change the rating of a file if required. The rating is then sent all managed devices with the file installed.

What is a file trust rating?

A file’s trust rating determines how Xcitium Client Security handles the file on the endpoint.

There are three possible ratings:

- **Trusted** - The file is safe and is allowed to run normally on the endpoint. It will, of course, still be subject to the standard protection mechanisms of Xcitium
  Client Security (behavior monitoring, host intrusion prevention etc).
- **Malicious** - The file is not allowed to run. It will be automatically quarantined or deleted depending on admin preferences.
- **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.

What’s the difference between ‘Comodo’ and ‘Admin’ ratings?

Although only two are covered in this interface, there are actually three possible sources for a file trust rating:

Xcitium **rating** - This is the official Xcitium trust rating for the file. CCS gets this rating from our file-lookup server (FLS) when it runs a virus scan on the file.

Admin rating - Admins can use Endpoint Manager to apply their own rating to a file. You can do this by clicking ‘Change Rating’ in the ‘Application Control’ screen. You can also specify a file’s admin rating in device details > file list. Local verdict server must be enabled in the profile for admin ratings to have any effect.

Local rating - End-users (or local admins) can set a file’s rating in the CCS interface. This can be done in CCS in the file list, in the vendor list, or at a virus alert.

Ratings are prioritized as follows:

1) Admin rating

2) Local rating

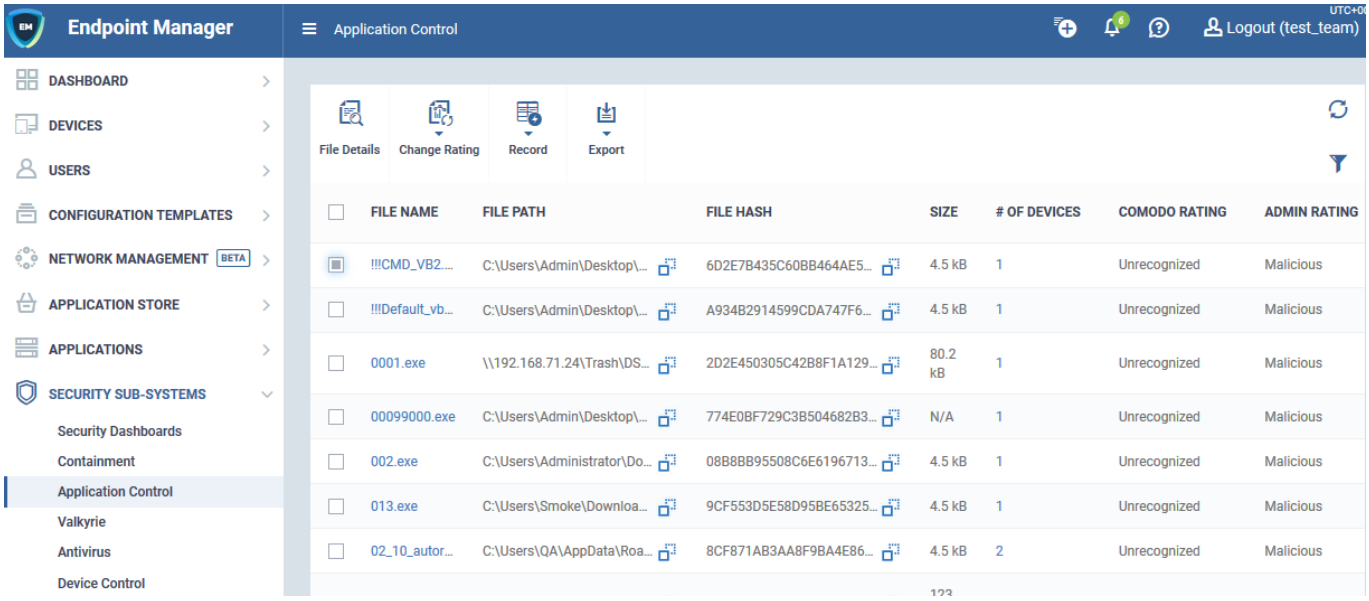
3) Xcitium rating

- Admin ratings over-rule Xcitium and local ratings *IF* local verdict server is enabled (default).
- *Admin ratings are disregarded if the 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'.*

Use the Application Control interface

- Log into Xcitium
- Click ‘Applications’ > ‘Endpoint Manager’
- Click 'Security Sub-Systems' > ‘Application Control'

The interface lists all files discovered on managed endpoints along with their trust rating.

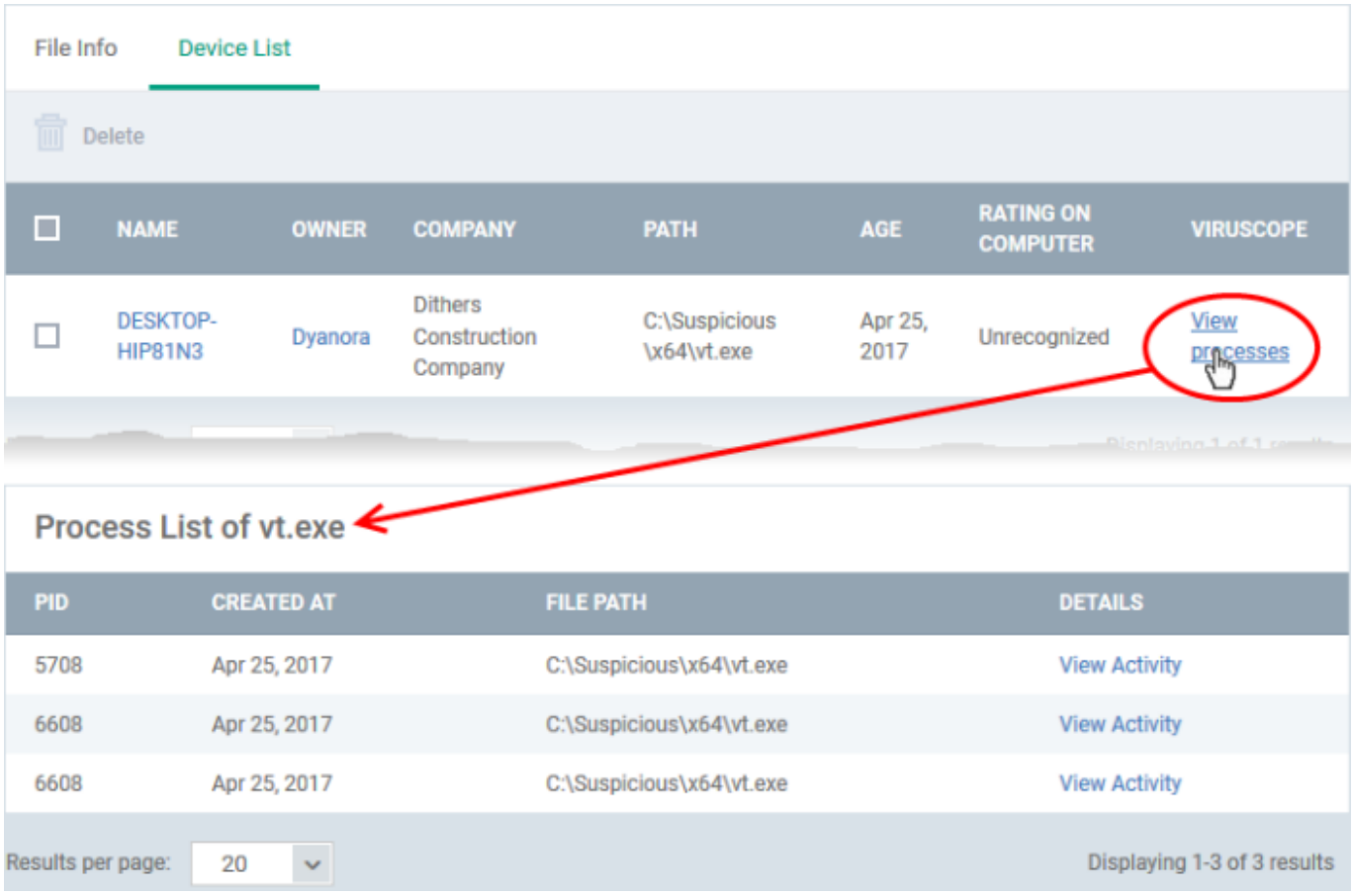


The following information is shown for each file:

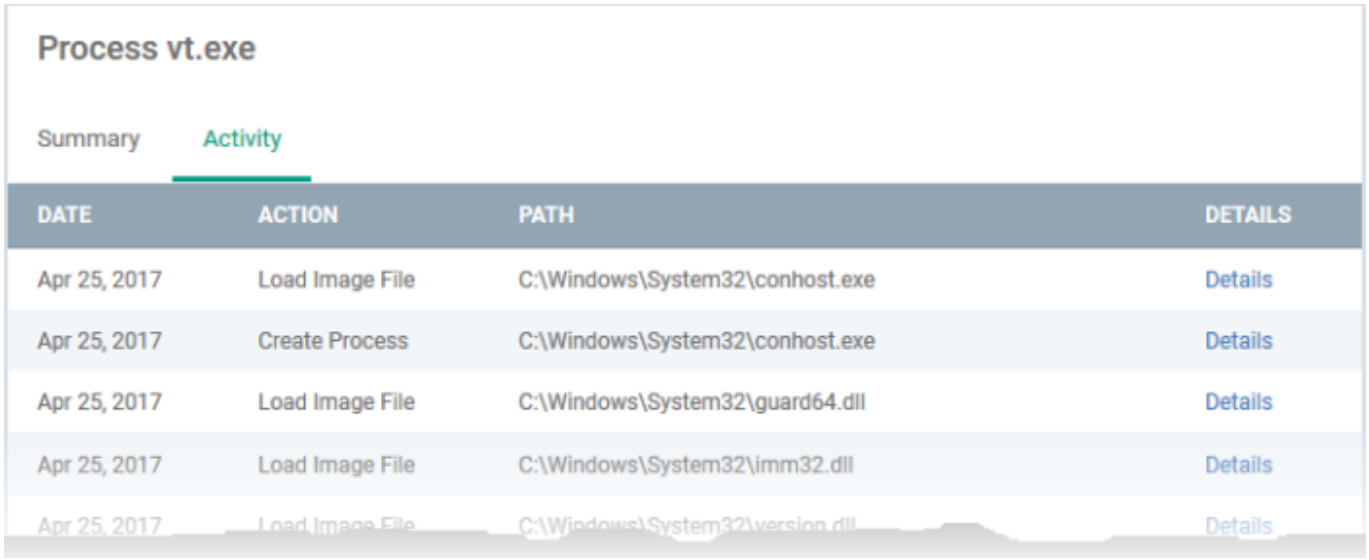
- The name, endpoint location (path) and a hash of the file
- The size of the file and the number of devices on which it was found
- The file’s Xcitium trust rating, and admin rating if set

Click the number in the ‘# of Devices’ column to view devices which feature the file:

- The ‘View Processes’ link in this screen lets you view all processes spawned by the file:

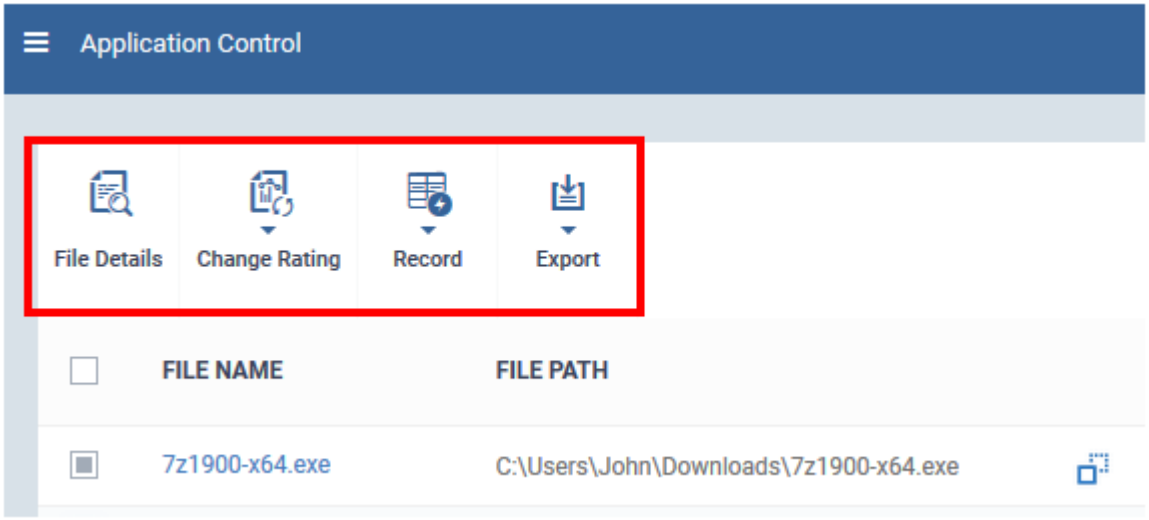


- Going even further, the ‘View Activity’ link lets you view the actions of those processes:



Take actions on files

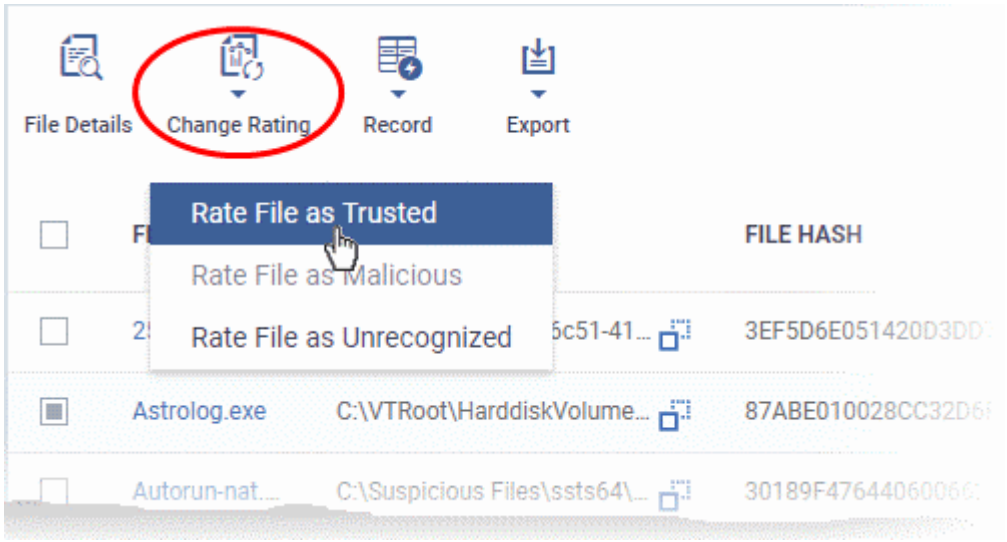
The controls above the list let you take various actions on selected files:



File Details - View basic file details and the devices on which the file is present. You can also change the trust rating of the file in this area.

Change rating – As covered earlier, a file's trust rating determines how CCS handles the file on the endpoint.

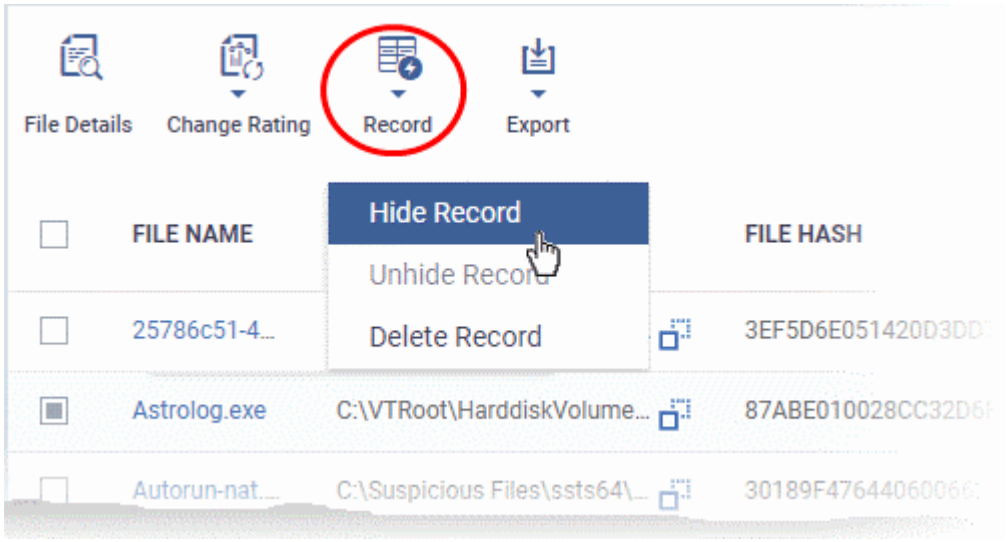
- Select the files whose rating you want to change. Click the funnel on the right to filter the list or search for a specific file.
- Click the 'Change Rating' button, as shown below:



You can choose from the following ratings:

- **Trusted** – The file is allowed to run as normal on the endpoint.
- **Malicious** – The file is quarantined or deleted and not allowed to run.
- **Unrecognized** – The file is run inside the container, a secure, isolated operating environment. Contained applications are not permitted to access files or user data on the host machine.

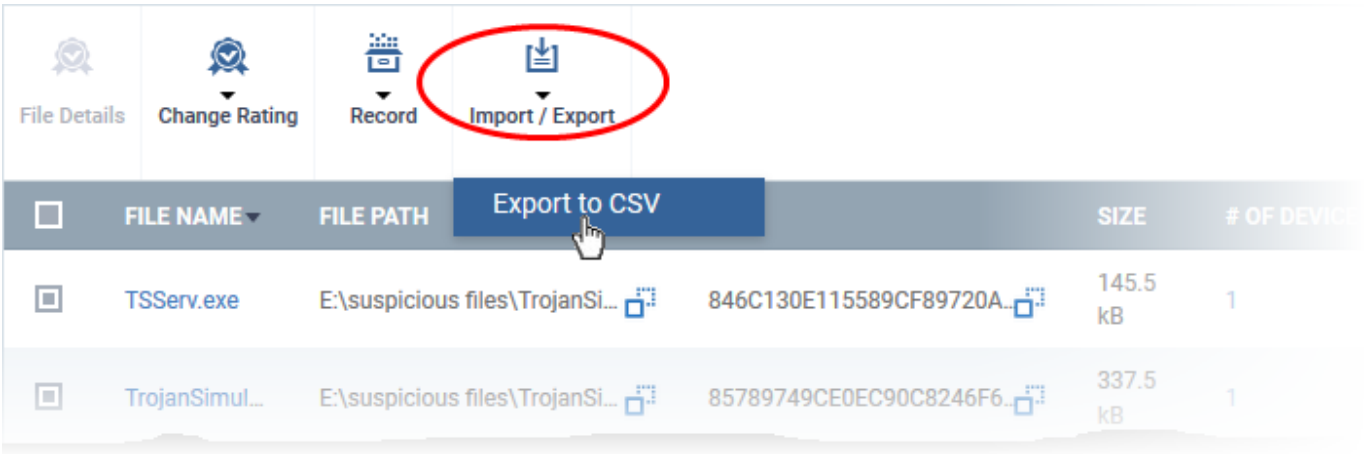
Your new rating is automatically applied to all devices on which it is present.



Record – The record button lets you hide, unhide or delete files in the application control list.

- The action you choose here only affects the visibility of the item in this list. It does not have any effect on the actual file on the endpoint.

Export - Export the current file list to a .csv file.



- Click 'Dashboard' > 'Reports' to access the exported report
- See Reports if you need more help with this interface.

Further reading

How to view security events on Windows endpoints

How to manage programs running in containment on your endpoints

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

How to view connection attempts from external devices to your endpoints