

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?](#)

[What's the difference between 'Comodo' and 'Admin' ratings?](#)

[Use the application control interface](#)

[Take actions on files](#)

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

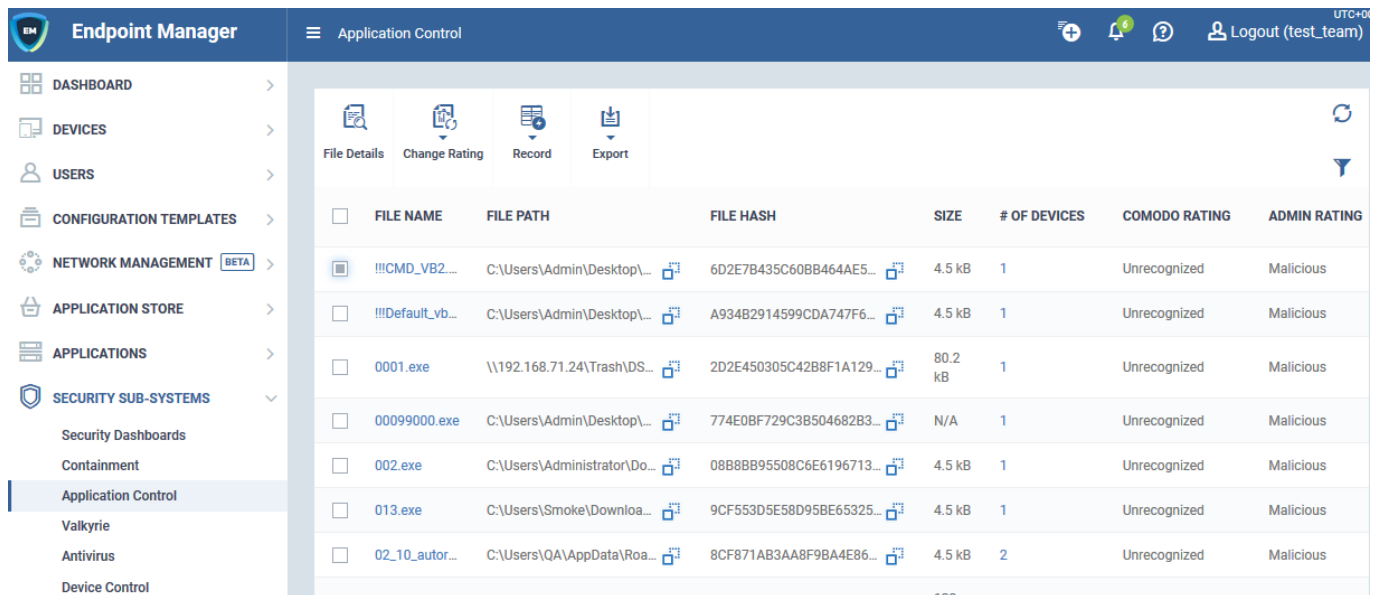
3) Xcitium rating

- 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.



FILE NAME	FILE PATH	FILE HASH	SIZE	# OF DEVICES	COMODO RATING	ADMIN RATING
!!!CMD_VB2...	C:\Users\Admin\Desktop\...	6D2E7B435C60BB464AE5...	4.5 kB	1	Unrecognized	Malicious
!!!Default_vb...	C:\Users\Admin\Desktop\...	A934B2914599CDA747F6...	4.5 kB	1	Unrecognized	Malicious
0001.exe	\\192.168.71.24\Trash\DS...	2D2E450305C42B8F1A129...	80.2 kB	1	Unrecognized	Malicious
00099000.exe	C:\Users\Admin\Desktop\...	774E0BF729C3B504682B3...	N/A	1	Unrecognized	Malicious
002.exe	C:\Users\Administrator\Do...	08B8BB95508C6E196713...	4.5 kB	1	Unrecognized	Malicious
013.exe	C:\Users\Smoke\Downloa...	9CF553D5E58D95BE65325...	4.5 kB	1	Unrecognized	Malicious
02_10_autor...	C:\Users\QA\AppData\Roa...	8CF871AB3AA8F9BA4E86...	4.5 kB	2	Unrecognized	Malicious

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:

File Info **Device List**

Delete

<input type="checkbox"/>	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSCOPE
<input type="checkbox"/>	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious\x64\vt.exe	Apr 25, 2017	Unrecognized	View processes

Results per page: 20 Displaying 1 of 1 results

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

File Info **Device List**

Delete

<input type="checkbox"/>	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSCOPE
<input type="checkbox"/>	DESKTOP-HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious\x64\vt.exe	Apr 25, 2017	Unrecognized	View processes

Displaying 1 of 1 results

Process List of vt.exe

PID	CREATED AT	FILE PATH	DETAILS
5708	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity
6608	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity
6608	Apr 25, 2017	C:\Suspicious\x64\vt.exe	View Activity

Results per page: 20 Displaying 1-3 of 3 results

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

Process vt.exe





Summary Activity


DATE	ACTION	PATH	DETAILS
Apr 25, 2017	Load Image File	C:\Windows\System32\conhost.exe	Details
Apr 25, 2017	Create Process	C:\Windows\System32\conhost.exe	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\guard64.dll	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\imm32.dll	Details
Apr 25, 2017	Load Image File	C:\Windows\System32\version.dll	Details

Take actions on files

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

☰ Application Control

 File Details
 Change Rating
 Record
 Export

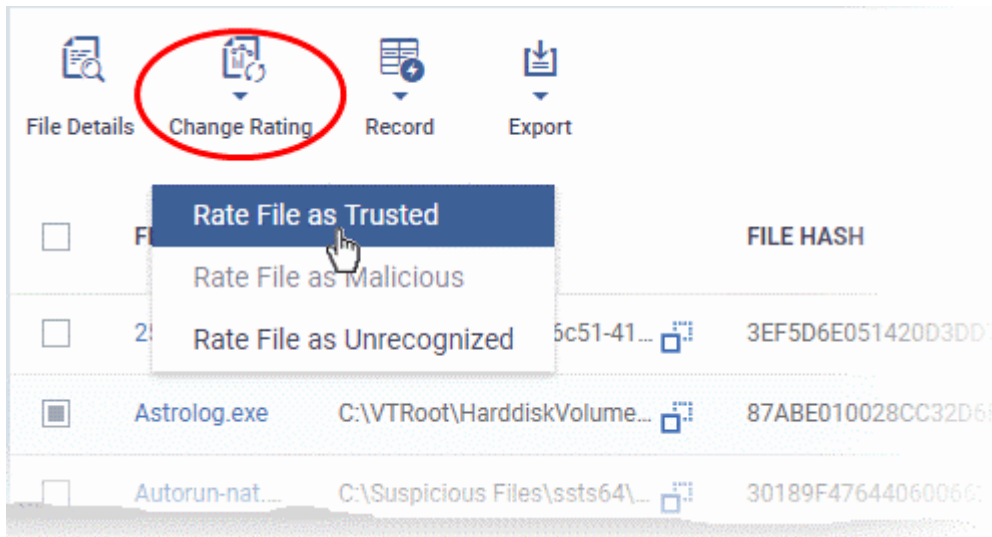
<input type="checkbox"/>	FILE NAME	FILE PATH	
<input checked="" type="checkbox"/>	7z1900-x64.exe	C:\Users\John\Downloads\7z1900-x64.exe	

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.

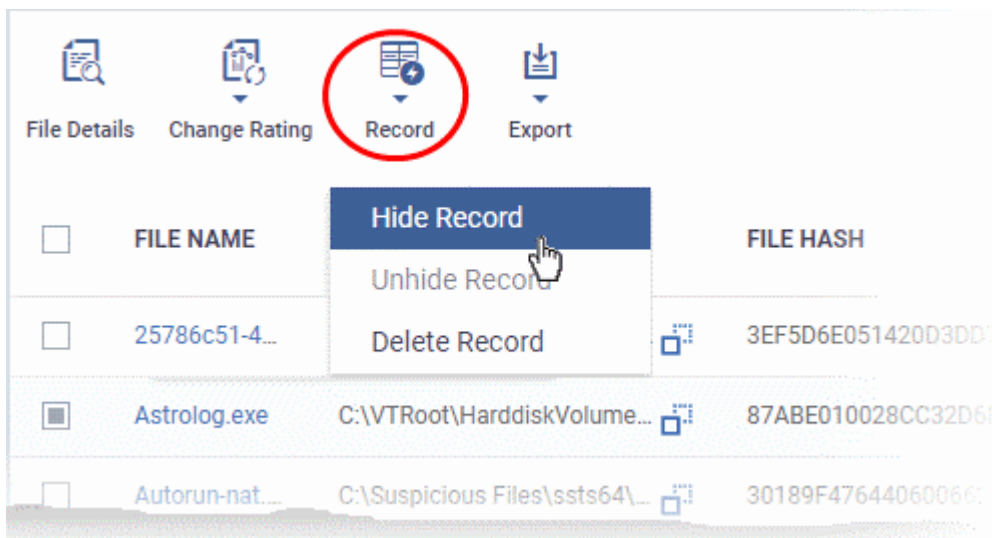
- Select the files whose rating you want to change. Click the funnel on the right to filter the list or search for a specific file.
- Click the 'Change Rating' button, as shown below:



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.

	FILE NAME	FILE PATH	Export to CSV	SIZE	# OF DEVICES
<input type="checkbox"/>	TSServ.exe	E:\suspicious files\TrojanSi...	846C130E115589CF89720A...	145.5 kB	1
<input type="checkbox"/>	TrojanSimul...	E:\suspicious files\TrojanSi...	85789749CE0EC90C8246F6...	337.5 kB	1

- 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](#)