## How to set admin rating for an application in Endpoint Manager

- 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 filelookup 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 Comodo One / Xcitium
- 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:

Endpoint Manager		File Rating / File Rating									
B DASHBOARD	>										
DEVICES	>	File Rat	ting Detected	l Scripts	Obsolete F	iles					
A USERS	>	R	Ē.	6	Ľ∎	国					
	>	File Detail	s Change Rating	Record	Export	Import					
	~		FILE NAME		FILE PATH				FILE HASH	SIZE	# OF DEVICES
Endpoint Security Status Security Events			000file_005_1dtpp	c.exe	C:\Users\Adr	ninistrator\Do	wnloads\tmp\000file_00.	63	6851AC0C32D0D6148B8F2F31E7CAC625EEA60D75	1 MB	1
Blocked Threats			0011111.exe		C:\Users\Adr	ninistrator\Do	ownloads\0011111.exe	ġ3	80DC53996149CF51968F32CEB18BD9FEAC74234D	4.5 kB	0
Quarantined Threats Contained Threats			0011112.exe		C:\Users\Adr	ninistrator\Do	ownloads\0011112.exe	ġ3	5C63C2C09BD8416908B9A83E5A3ED6033AF07836	4.5 kB	0
Autorun Alerts			0011113.exe		C:\Users\Adr	ninistrator\Do	wnloads\0011113.exe	ġ3	5C20E5A7FCA286F897B08AC0A6813C03BE1D93CC	4.5 kB	0
File Rating File Verdicts			0011114.exe		C:\Users\Adr	ninistrator\Do	ownloads\0011114.exe	ġ3	FCD505E3FEB31EE430F634A3B4F41CAE1847F09C	4.5 kB	0
Device Control			01.exe		C:\Users\Sm	ok7win\Deskt	top\01.exe	ġ3	021D4A2CED90BD70153838B9ACC797FCDAEDB47B	88.5 kB	0
Data Loss Prevention			0101.exe		C:\Users\Adr	ninistrator\De	esktop\Cont\0101.exe	ġ3	CACE4C793A582ED77C79E9F05E1EF7FA317D6AFE	4.5 kB	0
	2		010101_001_nuza	qb.exe	C:\Users\Adr	ninistrator\Do	ownloads\tmp\010101_00	- 63	F8E834FAE1F31998A9AF4939B7F9087B4988C218	1 MB	1
	2		010101_002_iihwv	y.exe	C:\Users\Adr	ninistrator\Do	wnloads\tmp\010101_00	- 63	077DFB24A1E86DB4321B068020D33531FEA21945	1 MB	1
	ĺ.		010101_003_oca7	d5.exe	C:\Users\Adr	ninistrator\Do	ownloads\tmp\010101_00	- 63	FB70CEB20EF7936EA0F1052C9B7C082AECC47897	1 MB	1
	ĺ		010101_004_xjbov	vq.exe	C:\Users\Adr	ninistrator\Do	ownloads\tmp\010101_00	- 63	F73717C2F0655F539D7187A9523012E75A43589B	1 MB	1
			010101_005_4eoc	ui.exe	C:\Users\Adr	ninistrator\Do	wnloads\tmp\010101_00	- 63	90BA6E44693160E137C69AE0FF4F3C994417D085	1 MB	1
W F DEVELOPER TOOLS			010101_006_2r02	nv.exe	C:\Users\Adr	ninistrator\Do	wnloads\tmp\010101_00	- 63	64C1AD2136B37089FCDB62F113E8D09FB49DCD69	1 MB	1
×											

• Select the file for which you want to set a rating

 $\circ~$  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

File Deta	ils Change Rating	Record Ex	<b>≟]</b> ▼ port	
	Rate File	as Trusted as Malicious		FILE HASH
	2 Rate File	as Unrecognized	5c51-41	3EF5D6E051420D3DD
	Astrolog.exe	C:\VTRoot\Harddi	skVolume	87ABE010028CC32D6
	Autorun-nat	C:\Suspicious File	s\ssts64\ 📋	30189F47644060066

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 Comodo One
- 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:

×										
DES Owne	KTOP- r: John Sn	HI950BN								
Manage	Profiles	Control	File Transfer	Remote Tools	F Run Procedure	Install or Update Packages	C Refresh Devic Information	e Reboot	More	
Devic	e Name	Summary	Networks	Associa	ted Profiles	Software Invento	ry File Lis	st Exported	d Configurations	MÞ
	FILE N	AME FILE	PATH	ecord •	FILE HASH		SIZE	COMODO RATINO	G ADMIN RA	TING
	CPILSU	uite.exe E:\Su	spicious files\A	All_test 📋	DCF2DFCB3900	03683BE2E0 📑	1.5 MB	Malicious	Not set	
	pcflank	c.exe E:\Su	spicious files∖A	All_test 📋	3437369E6B75	021F57DE5	176 kB I	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:

×	]									
	Device Name		Summary Hardware		Networks Associated Pr		sociated Profiles	ofiles Software Inventory F		
	B	File Details	Change R	Rating 🗸 📑	Record 🗸	(±	Import / Export 🗸			
I		FILE NAME	Rate File a	s Trusted		SHA1			SIZE	
		SkyWrap.dl	Rate File a	s Malicious	53	1E7872A	4E0F1EC2E1B2BE.	- 63	41.2 MB	Unrecognized
		Solitaire.dll	C:\Progra	Im Files\Windows	s 📋	9045264	85F77500E65CF3	- 63	42.3 MB	Unrecognized
		pcflank.exe	C:\Suspic	ious\PCFlank\P(	C 🗂	34373691	E6B75021F57DE5	- 63	<b>176</b> kB	Malicious

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

??????