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 to 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 Comodo 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 Comodo 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:

**Comodo rating** - This is the official Comodo 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) Comodo rating

- Admin ratings over-rule Comodo 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 ITarian
- Click 'Applications' > 'Endpoint Manager'
- Click 'Security Sub-Systems' > 'Application Control'

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

Endpoint Manager	≡ Ap	plication (	Control						<b>*</b>	¢ 0	итс+о Logout (test_team)
DASHBOARD >											
DEVICES >	6		ange Rating	Record	Export						O
A USERS >	File D	etalis Ch	ange kaung	Record	Export						T
CONFIGURATION TEMPLATES		FILE NA	AME I	FILE PATH			FILE HASH	SIZE	# OF DEVICES	COMODO RAT	TING ADMIN RATING
0 NETWORK MANAGEMENT BETA >		!!!CMD_	VB2	C:\Users\Admi	n\Desktop\	di i	6D2E7B435C60BB464AE5	4.5 kB	1	Unrecognized	Malicious
APPLICATION STORE		!!!Defau	ilt_vb (	C:\Users\Admi	n\Desktop\	ġ3	A934B2914599CDA747F6	4.5 kB	1	Unrecognized	Malicious
APPLICATIONS >		0001.ex	ke v	\192.168.71.2	4\Trash\DS	di	2D2E450305C42B8F1A129	80.2 kB	1	Unrecognized	Malicious
Security SUB-SYSTEMS V Security Dashboards		000990	100.exe	C:\Users\Admi	n\Desktop\	ġ,	774E0BF729C3B504682B3	N/A	1	Unrecognized	Malicious
Containment		002.exe	e (	C:\Users\Admi	nistrator\Do	ġ,	08B8BB95508C6E6196713	4.5 kB	1	Unrecognized	Malicious
Application Control Valkyrie		013.exe	e (	C:\Users\Smok	e\Downloa	ġ3	9CF553D5E58D95BE65325	4.5 kB	1	Unrecognized	Malicious
Antivirus		02_10_	autor (	C:\Users\QA\A	ppData\Roa	- <b>6</b> 3	8CF871AB3AA8F9BA4E86	4.5 kB	2	Unrecognized	Malicious
Device Control								122			

#### 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 Comodo 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							
	NAME	OWNER	COMPANY	PATH	AGE	RATING ON COMPUTER	VIRUSCOPE
	DESKTOP- HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious \x64\vt.exe	Apr 25, 2017	Unrecognized	View processes
Results p	er page: 20	~				Disp	laying 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							
	NAME	OWNER	COMPANY	РАТН	AGE	RATING ON COMPUTER	VIRUSCOPE
	DESKTOP- HIP81N3	Dyanora	Dithers Construction Company	C:\Suspicious \x64\vt.exe	Apr 25, 2017	Unrecognized	View processes
						Disp	laving 1 of 1 re-
Proc	cess List of	vt.exe 🗲					
PID	CREA	ATED AT	FILE	PATH		DETAILS	
5708	Apr 2	25, 2017	C:\S	cuspicious\x64\vt.exe		View Act	vity
6608	6608 Apr 25, 2017			Suspicious\x64\vt.exe	View Act	View Activity	
6608	Apr 2	25, 2017	C:\S	cuspicious\x64\vt.exe		View Act	vity
esults p	er page: 20	~				Displa	ying 1-3 of 3 result

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

Process vt.exe					
Summary	Activity				
DATE	ACTION	РАТН	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:

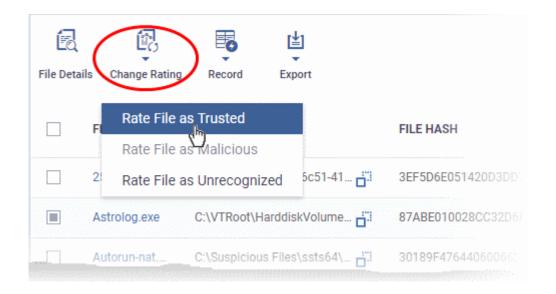
=	Applicat	tion Control				
	File Details	Change Rating	Record	Export		
1	_ F	ILE NAME		FILE PATH		
	. 7	z1900-x64.exe		C:\Users\Joh	n\Downloads\7z1900-x64.exe	ġ,

**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.

File Info	Device List		<ul> <li>Back to Application Control</li> </ul>
Change Rating	Record		
Name: 0001.exe Path: C:\Users\/	Administrator\Desk	top\0001.exe	
<b>Type:</b> Unknown			
SHA1: 2D2E4503	05C42B8F1A1291F	-6C4343401D7DAED1C	
MD5: N/A			
Version: Not availa	ble		
<b>Size:</b> 80.2 kB			

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.

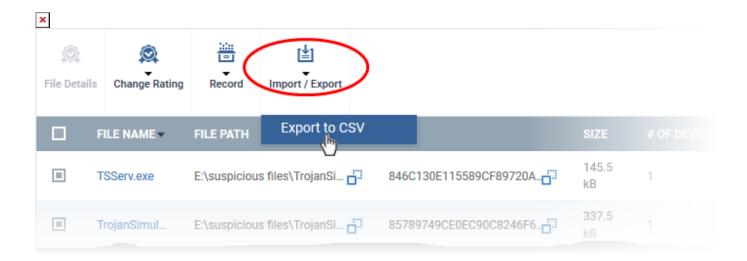
Your new rating is automatically applied to all devices on which it is present.

×

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 on 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