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.

Endpoint Manager		■ Applica	tion Control						+	\$ 2	<mark>گ</mark> ۱	uтс+o ogout (test_team)
DASHBOARD	>											
DEVICES	>	E	Ē,	G	Ť.							O
A USERS	>	File Details	Change Rating	Record	Export							Ţ
CONFIGURATION TEMPLATES	>		ILE NAME	FILE PATH			FILE HASH	SIZE	# OF DEVICES	COMODO	RATING	ADMIN RATING
O NETWORK MANAGEMENT BETA	>		CMD_VB2	C:\Users\Adr	min\Desktop\	ġ3	6D2E7B435C60BB464AE5	4.5 kB	1	Unrecogn	ized	Malicious
	>		Default_vb	C:\Users\Adr	min\Desktop\	ġ3	A934B2914599CDA747F6	4.5 kB	1	Unrecogn	ized	Malicious
	>		001.exe	\\192.168.71	.24\Trash\DS	Ċ,	2D2E450305C42B8F1A129	80.2 kB	1	Unrecogn	ized	Malicious
Security Dashboards	Ň		0099000.exe	C:\Users\Adr	min\Desktop\	ġ3	774E0BF729C3B504682B3	N/A	1	Unrecogn	ized	Malicious
Containment			02.exe	C:\Users\Adr	ninistrator\Do	- 6 3	08B8BB95508C6E6196713	4.5 kB	1	Unrecogn	ized	Malicious
Application Control		0	13.exe	C:\Users\Sm	oke\Downloa	ġ3	9CF553D5E58D95BE65325	4.5 kB	1	Unrecogn	ized	Malicious
Antivirus		. 0:	2_10_autor	C:\Users\QA	\AppData\Roa.	- 63	8CF871AB3AA8F9BA4E86	4.5 kB	2	Unrecogn	ized	Malicious
Device Control								123				

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 Ir	nfo Device L	.ist					
1	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	per page: 20	~				Disp	aying 1 of 1 results

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

File Info Device List								
1	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	
						Olar	laving 1 of 1 re-	
Proc	cess List of	vt.exe 🗲						
PID	CRE	ATED AT	FILE	PATH		DETAILS		
5708	5708 Apr 25, 2017			Suspicious\x64\vt.exe		View Activity		
6608	Apr	25, 2017	C:\S	Suspicious\x64\vt.exe		View Act	ivity	
6608	Apr	25, 2017	C:\S	cuspicious\x64\vt.exe		View Act	ivity	
Results p	er page: 20	~				Displa	iying 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	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:

=	E Applicat	tion Control				
ſ	File Details	Change Rating	Record	Export		
	F	FILE NAME		FILE PATH		
		7z1900-x64.exe		C:\Users\Joh	n\Downloads\7z1900-x64.exe	Ē3

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:

File Deta	ils	Change Rating	Record Ex	≟] ▼ port	
	FI	Rate File	as Trusted		FILE HASH
	2	Rate File	as Unrecognized	5c51-41	3EF5D6E051420D3DD
	Ast	rolog.exe	C:\VTRoot\Harddi	skVolume 📑	87ABE010028CC32D6i
	Aut	orun-nat	C:\Suspicious File	s\ssts64\ 💾	30189F47644060066

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.

File Deta	ils Change Rating	Record Export		
	FILE NAME	Hide Record		FILE HASH
		Unhide Recol		
	25786c51-4	Delete Record	ė,	3EF5D6E051420D3DD
	Astrolog.exe	C:\VTRoot\HarddiskVolume	L	87ABE010028CC32D6
	Autorun-nat	C:\Suspicious Files\ssts64\	d'il	30189F47644060066

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