How to configure the virus scope in a profile

Introduction:-

This section explains as how to modify VirusScope

- VirusScope monitors the behavior of running processes to detect and block malicious activities. VirusScope can also undo any changes made by the malware.
- You can set VirusScope to take one of the following actions if it finds a threat:
 - $\circ\,$ Generate an alert. The user can decide whether to allow or block it. OR
 - Automatically quarantine the threat and reverse any actions that it took.
- By default, VirusScope only monitors processes which are running in the container. You can enable whole-host protection if required.
- VirusScope is a feature of CCS, and can be configured as part of a security profile.

Process in brief

- Log into ITarian then click 'Applications' > 'Endpoint Manager'
- Click 'Configuration Templates' > 'Profiles'
- Click on the name of the Windows profile that you want to configure, then:
 - Click the 'VirusScope' tab if it has already been added to the profile OR
 - Click 'Add Profile Section' > 'VirusScope'
- You can set the following options:
 - Enable VirusScope Switch the feature on or off
 - Show popup alerts:
 - Enabled VirusScope will show an alert on the endpoint when if finds a threat. This gives the end-user the option to block the threat or ignore it.
 - Disabled No alert is shown on the endpoint. VirusScope will quarantine the threat and reverse any actions that were taken by it.
 - Monitor contained applications only:
 - Enabled VirusScope only monitors processes running in the sandbox/container.
 - Disabled VirusScope will monitor all running processes on the endpoint. Those inside the container, and those outside.

Process in detail

- Open Endpoint Manager
- Click 'Configuration Templates' > 'Profiles'

Endpoint Manager	≡	Profiles					~⊕ ②	
DASHBOARD >								_
DEVICES >		Profiles Default Profiles						
△ USERS >		Ę	Ę,					
CONFIGURATION TEMPLATES		Create	Import	Export Profile Clone Profile Delete Profile				T
Profiles Alerts		OS	NAM	E	CREATED BY	CREATED -	UPDATED AT	
Procedures	- [virsus	scope	competition/protices	2018/06/19 06:31:17 AM	2018/06/19 06:31:17 AM	
APPLICATION STORE >			Alert	profile		2018/05/16 10:45:42 AM	2018/05/16 10:45:42 AM	
APPLICATIONS >			Enabl	le_Proxy		2018/05/16 10:45:19 AM	2018/05/16 10:45:19 AM	
SECURITY SUB-SYSTEMS			port	settings		2018/05/16 10:45:04 AM	2018/05/16 10:45:04 AM	
<pre> settings > </pre>			Proce	edure Execution		2018/05/16 10:44:14 AM	2018/05/16 10:44:14 AM	
			Event	logging		2018/05/16 10:43:29 AM	2018/05/16 10:43:29 AM	
			Secui	iry profile		2018/05/16 10:42:56 AM	2018/05/16 10:42:56 AM	
			Exclu	sion_files		2018/05/16 10:42:38 AM	2018/05/16 10:42:38 AM	
			Conta	ainment		2018/05/16 10:42:20 AM	2018/05/16 10:42:20 AM	
			Event	Tracking		2018/05/16 10:41:56 AM	2018/05/16 10:41:56 AM	
			Netw	ork access		2018/05/16 10:39:50 AM	2018/05/16 10:39:50 AM	
			Winde	ows profile		2018/05/16 10:38:52 AM	2018/05/16 10:38:52 AM	
			Optim	num_profile		2018/05/16 10:38:36 AM	2018/05/16 10:38:36 AM	
			Antivi	irus_status		2018/05/16 10:38:06 AM	2018/05/16 10:38:06 AM	
			Monif	toring_Firewall	and a supplying and an	2018/05/16 10:37:40 AM	2018/05/16 10:37:40 AM	

Step 2 :

- Click the name of a Windows profile to open its detail page
- Click the 'Add Profile Section' drop-down > Select 'VirusScope'

virsuscope				
Add Profile Export Profile Cl	one Profile Delete Profile Make Default			
Antivirus				
Updates				
File Rating				
Firewall				🆻 Edit
HIPS				
Containment				
VirusScope				
Valkyrie				
Global Proxy				
Clients Proxy				
Agent Discovering Settings				
UI Settings				
Logging Settings				
Client Access Control				
External Devices Control				
Monitoring				
Procedures				

- Configure the feature as required:
 - **Enable VirusScope** Enable or disable VirusScope. If enabled, VirusScope monitors the activities of running processes and generates alerts if suspicious activity is detected.
 - Show popup alerts:
 - Enabled VirusScope will show an alert on the endpoint when if finds a threat. This gives the end-user the option to block the threat, or ignore it.
 - Disabled No alert is shown on the endpoint. VirusScope will quarantine the threat and

reverse any actions that were taken by it.

- Monitor contained applications only:
 - Enabled VirusScope only monitors processes running in the container.
 - Disabled VirusScope monitors all processes on the endpoint. Those inside the container, and those outside.
- Click 'Save'.

virsus	соре					
Add Profile Section	Export Profile Clone Profile Delete Pr	rofile Make Default				
General V	irusScope					
_						
VirusSco	pe					Save
Enable	VirusScope ables VirusScope subsystem which dynamica	cally analyzes the behavior of running process	s and keeps a record of their activities.			
Show p This option, w	opup alerts hen disabled, automatically quarantines detec	ected threats and reverses their activities.				
Monito This option ap	r contained applications only plies VirusScope monitoring only to containe	ed applications that are run virtually or run res	icted.			

VirusScope Alerts

• If 'Show Popup Alerts' is enabled, end-users will see a notification each time VirusScope discovers a potential threat.



- Clean Move the item to quarantine and reverse any changes that it made. Choose this if you are unsure about the application shown in the alert.
- Ignore Allows the process to continue. You must then choose one of the following options.
 - Ignore Once The process is allowed to run this time only. Another alert will be generated if the process attempts to execute in future.

- Ignore and Add to Exclusions The file is allowed to run and will not be contained in future. See Auto-Containment Rules for help to configure which types of files should be auto-contained.
- Ignore and Report as False Alert The process is allowed to run and a false-positive report is sent to Comodo. Select this if you think the file is safe. If it is verified as a false-positive it will be added to the global white list.