## **ESET Tech Center**

Kennisbank > Legacy > ESET Security Management Center > 7.x > Ransomware Shield - enable Audit mode and exclude an application from detection (7.x)

# **Ransomware Shield - enable Audit mode and exclude an application from detection (7.x)**

Anish | ESET Nederland - 2019-12-30 - Reacties (0) - 7.x

#### Issue

ESET business products (version 7 and later) include **Ransomware Shield**. This new security feature is a part of HIPS and protects computers from ransomware. When ransomware is detected on a client computer, you can view the detection details in ESMC Web Console in **Threats**.

By default, Ransomware Shield blocks all applications with potential ransomware behavior. If there is a legitimate application or script automatically running on the managed computer and performing operations that are evaluated as ransomware behavior (moving files across folders, encrypting files and folders), you may want to exclude it from being blocked by ESET business product.

#### Solution

ESMC Web Console Policy settings for ESET business products include **Audit mode**. When Audit mode is enabled, applications with ransomware behavior are allowed to run and are only logged in ESMC Web Console in **Threats**. The administrator can decide to block the potential detected threat or allow it permanently by adding it to exclusions.

Follow these steps to exclude applications on a managed computer from being detected as ransomware:

- 1. Open the ESET Security Management Center (ESMC) Web Console.
- 2. Click **Policies**, select the policy for ESET business product, and then click **Policies**  $\rightarrow$  **Edit**.

(ESet)	SECURITY MANAGEMENT	CENTER				G ~								
		Policies	:	ACCESS GR	IOUP Select	SHOW UNA	ISSIGNED 🔽	ि All (29)	Tags	ADD FI		PRESETS 🔝	] 0	
		Policies			NAME		POLICY PROD	UCT	TAGS		DESCRIPTION		0	^
		^ All			Antivirus - Maxi	mum security	ESET Endpoint	for macOS (O			Taking advantage of ad	vance		
		✓ ∅ Custom Policies			Device control -	Maximum se	ESET Endpoint	for Windows			All devices are blocked.	Whe		
 61		✓			Device control -	Read only	ESET Endpoint	for Windows			All devices can only be	read		
<b>a</b>					Firewall - Block	all traffic exce	ESET Endpoint	for Windows			Block all traffic except c	onne		
۲	Policies				Logging - Full d	liagnostic log	ESET Endpoint	for Windows			This template will ensur	e that		
٨					Logging - Log ir	mportant eve	ESET Endpoint	for Windows			Policy ensures that warr	nings,		1
Φ					Antivirus - Balan	nced	ESET Endpoint	for Windows			Security configuration r	ecom		II.
s - 6-			1		Antivirus - Maxi	mum security	ESET Endpoint	for Windows			Taking advantage of ma	schin	-	1
4					Visibility - Balan	ced	ESET Endpoint	for Windows			Default setting for visibi	ility. S		1
			Ľ		Visibility - Invisil	ble mode	ESET Endpoint	for Windows			Disabled notifications, a	lerts,		1
		Tags	Q		Visibility - Redu	ced interactio	ESET Endpoint	for Windows			Disabled statuses, disab	led n		I
		Company 1			Antivirus - Real-	time scanner	ESET File Securi	ity for Windo			Optimized performance	for s		I
		best	-	I Show Detail	ils Aaxir	mum security	ESET File Securi	ity for Windo			Taking advantage of ad	vance		1
		Test Test	<	∂ Tags	ilent	t mode	ESET File Securi	ity for Windo			Suitable for multi-user s	erver		I
		Test 3		/ Edit	d rep	putation and	ESET Endpoint	for Windows			Enables ESET LiveGrid®	clou		1
		Test 4		Change Ass	signments rep	putation and	ESET Mail Secu	rity for Micros			Enables ESET LiveGrid®	clou		I
		Test comapny 2	1	Delete	A 101	putation and	ESET File Securi	ity for Windo			Enables ESET LiveGrid®	clou		1
			Ē	Import	21	- Recommen	ESET Full Disk E	Encryption			Enables full disk encryp	tion f		1
			C	Access Grou	up ⊳t dis	sk only - Reco	ESET Full Disk E	ncryption			Enables full disk encryp	tion f		~
E	COLLAPSE		1	ACTIONS	▼ NE	W POLICY						⊲ ⊚ 1 ↔	9	

Figure 1-1 Click the image to view larger in new window

3. Click Settings  $\rightarrow$  Detection Engine  $\rightarrow$  HIPS.



Figure 1-2 Click the image to view larger in new window

4. Click the slider bar next to **Enable Audit mode** to enable this setting and click **Finish** to apply the Policy settings.

### Use Enable Audit Mode with care

When you apply **Enable Audit mode**, automatic ransomware protection is turned off and the managed computer is not protected against ransomware.

(CSet)	SECURITY MANAGEMENT	CENTER							
		Edit Policy							٦
돠		Policies > Edit Policy							
▲		Pasis	FFFF Fordersite for Mindaue					2	
<b>2</b>		Settings	ESET Endpoint for windows		Q			. ^	
Ð		Assign	DETECTION ENGINE	3 BASIC			••• •		
	Installers	Summary	Real-time file system protection	○ ● ∲ Er	able HIPS			0	
~	Computer Users		Malware scans	50 0 4 Er	able Protected			0	
φ			HIPS		able Advanced Memory Scan	ner		0	
<u>ه ب</u>			UPDATE O 🔶 🗲 Enable Exploit Blocker	<b>v</b>		0			
<u>4</u>			NETWORK PROTECTION		TR RELATIONAL INCRECTU				
			WEB AND EMAIL		able Deep Behavioral				
			DEVICE CONTROL		spection			0	
			TOOLS	0070		(JETE) EUR			
			USER INTERFACE	R/	ANSOMWARE SHIELD				
			OVERRIDE MODE	0 • % Er	able Ransomware Shield	(2) ≥ 7.0 ✓		0	
							U		
				н	PS SETTINGS				
				0 • % Fil	tering mode	Automatic n	node	<b>Y</b> • <b>Y</b>	
				0 0 % Le	arning miles will end at	1970 Jan 1 0	1:00:00	0	
e	COLLAPSE			H SAVE AS	CANCEL				

Figure 1-3 Click the image to view larger in new window

- 5. On the managed computer, run the application with ransomware behavior.
- 6. Return to ESMC Web Console and click Detections. You can see the information about the potential ransomware application detected on the client computer. In the **Action** column, there is a note **allowed by audit**.



Figure 1-4 Click the image to view larger in new window

7. Click the threat and click **Show Details**. Verify the path to the application in **Object URI** and make sure that you want to exclude the threat from detection. Then click **Close**.

### Use Exclusions with caution

Exclusions increase the exposure of managed computer to malware.

(CSer)	SECURITY MANAGEMENT	CENTER										
		Detections :		<b>0</b> i	SHOW SUBGROUPS 🔽	Tags		ADD FILTER		F	RESETS 🗢	0
딮		Groups P		\\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\	DETECTION TYPE	CAU	ACTION	OCCU	RESO	COMPUTER NAME		٢
A	DETECTIONS	^ 🗅 All 🛛 🔞 🖌			Antivirus trojan	Win	allowed by audit	1	0/1			file://
		All MSP     group1     lest & found     vert Middows computers     Vert Activities decurity product,     Vert Activities decurity product,		i	Detection Detection Computers Actions P Scan Path Create Exclusion	Net.		1	0/1	999		111127
e	COLLAPSE		< sc	NN COMPUTE	RS RESOLVE 🗢	Actions 🗢					⊲ ⊙ 1 ⊙	>

Figure 1-5 Click the image to view larger in new window

8. Click the detection and select Create exclusion.



Figure 1-6 Click the image to view larger in new window

9. Select the **Exclusion criteria**. The recommended option is pre-selected based on the detection type. Select the check box **Resolve matching alerts** to automatically resolve the alerts covered by the exclusion. Optionally, you can add a **Comment**.

CSet	SECURITY MANAGEMENT	CENTER							
		Settings	Do not trigger detections	for: -1 hash: (	_				
	DETECTIONS	Preview	i Some versions	of the security products may not support all exclusio	n criteria. <u>More informati</u>	on			
а в е е е е е			9 Exclusion criteria	Path & Detection Exclude each file by path and detection     Exclude each file by its SMA-1 hash     Exclude each file by its SMA-1 hash     Detection Exclude each detection	] ] ]				
<u>4</u>			Auto-resolving	Resolve matching alerts					
			Target Comment (for all exclusions)	A1				< >	
			Target						
E				ICEL FINISH					

Figure 1-7 Click the image to view larger in new window

10. Click Target and select computer(s) or group(s) where the exclusion will be applied and click Finish

eser	SECURITY MANAGEMENT	CENTER		G ▼ Computer Name	QUICK LINKS 🗢 🕜 H	HELP ♥ & ADMINISTRATOR	
==		Sattings					
G		Target	i Exclusion is by default c	created for all user accessible computers (he	ome group of the user creating th	e exclusion). You can change assignme	nts below.
	DETECTIONS	Preview	ADD COMPUTERS ADD	GROUPS REMOVE TARGETS			
		6	TARGET NAME	TARGET DESCRIPTION	TARGET TYPE		
Ŀ		•			Static Group		
					state croop		
۲							
٨							
φ							
<u>ې</u> ۳							
			Preview				
e			CONTINUE	FINISH			

- 11. Ransomware Shield no longer detects the excluded application.
- 12. Edit the Policy for ESET business product and click the slider bar next to **Audit mode** to turn it off and ensure the automatic ransomware protection of the managed computer.

(ISer)	SECURITY MANAGEMENT	CENTER							
		Edit Policy							
교		Policies > Edit Policy							
•		Paris	FFFF Forder int for Mindows					2	
		Settings	ESET Endpoint for Windows			d		• ^	
		Assian	DETECTION ENGINE	63	BASIC		•••		
		Summon	Real-time file system protection	28 0	● 🦩 Enable HIPS	× 1		0	
	Policies	Summary	Cloud-based protection	•		1		0	
~			Malware scans	<u> </u>	<ul> <li>Finable Protected</li> <li>Service</li> </ul>	(€) ≥ 6.6		0	
¢			HIPS	0	• 🗲 Enable Advanced M	emory Scanner		0	
≶_/γ			UPDATE	0		er 🗸		0	
4			NETWORK PROTECTION						
			WEB AND EMAIL	61	DEEP BEHAVIORAI	INSPECTION		- 1	
			DEVICE CONTROL	0	<ul> <li>Finable Deep Behavi Inspection</li> </ul>	oral (0 ≥ 7.2) ✓		0	
			TOOLS	0	Exclusions	(@ ≥ 7.2) Edit		0	
			USER INTERFACE		BANCOMWART CU	100			
			OVERRIDE MODE	- N	Enable Bansomware	Shield	-		
				0	Fnable Audit mode	(0 ≥ 7.0) ×	762	0	
					HIPS SETTINGS				
				0	Filtering mode	Automa	tic mode 🔽	] o	
				0	• 🖩 Learning mode will	end at 1970 Jan	n 1 01:00:00	0	
	COLLAPSE		BACK CONTINUE	FINISH	E AS CANCEL				

Figure 1-8 Click the image to view larger in new window

# **Reacties (0)**