ESET Tech Center

Knowledgebase > Legacy > ESET Security Management Center > Create IDS exclusions for client workstations in ESET Security Management Center (7.x)

Create IDS exclusions for client workstations in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2019-02-04 - Comments (0) - ESET Security Management Center

Create IDS exclusions for client workstations in ESET Security Management Center (7.x)

Applies to: ESET Security Management Center | Product version: 7.x

Solution

Endpoint users: <u>Perform these steps on individual client workstations</u>

<u>Create IDS exclusions in ESET Security Management Center</u>

ESET Security Management Center (ESMC) 7 User Permissions

This article assumes that your ESMC user has the correct access rights and permissions to perform the tasks below.

If you are still using the default Administrator user, or you are unable to perform the tasks below (the option is grayed out), see the following article to create a second administrator user with all access rights (you only need to do this once):

• Create a second administrator user in ESET Security Management Center 7.x

View permissions needed for least privilege user access

- 1. <u>Open ESET Security Management Web Console</u> (ESMC Web Console) in your web browser and log in.
- 2. Click **Policies**, select the policy in the **ESET Endpoint for Windows** section that you want to edit and then click **Policies** \rightarrow **Edit**.

eser	SECURITY MANAGEN	MENT CENTER	a.:			Ga マ Search com	oputer na QUICK LINKS *	. Ø HELP ♥	A ADMINISTRATOR	🖻 >9 MIN
		Policies Show unassigned	Antivirus - Maximum security - recommended -			ended - Assigne	- Assigne			
' G		ACCESS GROUP Select	Assigned to	Applied on	Settings	Summary				
▲		^ ℓ Custom Policies	TARGET N	IAME			TARGET DESCRIPTION	i.		0
ŭ		수 💿 ESET Management Agent 다 10 sec	NO DATA AVAILABLE							
Þ		△								
≞		ESET Endpoint for Android (2+)								
	Policies	C ESET Endpoint for Windows								
*		Lo Antivirus - Balanced								
¢.		Candivirus - Maximum ser (a)								
8-		Co Cloud-based protection - red								
		Co Device Control - Read only								
		C Firewall - Block all traffic exce								
		all diagnostic logs								
		Actions + New >g important ever								
		/ Edit. (2) alanced								
	 `	Duplicate visible mode								
		Change Assignments educed interactio di Delete								
		Import or macOS (OS X)								
	\	Export by for Windows St								
	N									
		POLICIES V NEW POLICY	ASSIGN GROUP	(5) ASSIGN C		ASSIGN				

Figure 1-1

Click the image to view larger in new window

1. Expand Settings → Network Protection → Network attack protection and click Edit next to IDS exceptions.

eser	SECURITY MANAGEN	MENT CENTER		G マ Search computer na	QUICK LINKS 🔻 🦉 HELP 👻	A ADMINISTRATOR 🖂 >9 MIN
• G		Edit Policy				
▲ ≈ 2 0 ¢	THREATS Reports Client Tasks Installers Policies	Basic Settings Assign Summary	ESET Endpoint for Windows DETECTION ENGINE UPDATE UPDATE	NETWORK ATTACK PROTECTION + Enable Network attack protection (DS + Enable Storeg protection	Q Type	to search
			INETWORK PARTICULAR Internal Internal Web and Email OEVICE CONTROL TOOLS USER INTERFACE OVERRIDE MODE	O O D Exceptions AdvanceD options	Edit	3
	COLLAPSE		BACK CONTINUE FINISH	SAVE AS.		

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

1. Click Add.

IDS exceptions						? 🗆 🗙
The exceptions are evaluated from top to b log) separately.	ottom. They can be used to custom	ize firewall behaviour upon various IDS dete	ections. First matching exception is	applied, for each	action type (blo	xck, notify,
Alert	Application	Remote IP	Block	Notify	Log	Q
4						
Add Edit Remove			2		T	¥
					Save	Cancel

Figure 1-3

1. Select the **Alert**, type the **Remote IP address** (IP address of the machine with the software that scans the network).

Alternatively, to set up an IDS exclusion for a locally installed application, type the full path to the <code>.exe</code> file in **Application** (e.g. C:\Windows\system32\cmd.exe).

2. In the Action section, select No from each drop-down menu. Click $OK \rightarrow Save \rightarrow Finish$ to save the policy. If this is a new policy, assign the policy to the correct groups. After the computers check in, they will get the policy change.

Add IDS exception	? 🗆 X
Alert	Any alert
Threat name (€ ≥ 6.	
Direction	Both
Application	
Remote IP address	192.168.1.5
Profile	Any profile 🔻
ACTION	
Block	No
Notify 6	No
Log	No



KB Solution ID: KB7054 |Document ID: 26426|Last Revised: January 22, 2019