# **ESET Tech Center**

Knowledgebase > Legacy > ESET Security Management Center > Exclude files or folders on endpoints from Real-time scanning using ESET Security Management Center (7.x)

# Exclude files or folders on endpoints from Real-time scanning using ESET Security Management Center (7.x)

Anish | ESET Nederland - 2018-09-14 - Comments (0) - ESET Security Management Center

#### lssue

- File-level scanning of some email servers, backup software, Customer Relationship Management (CRM) software, etc. causes abnormal system behavior
- Use ESET Configuration Editor to create a configuration that excludes specific applications or folders from Real-time scanning

# Solution

**PEndpoint users:** <u>Perform these steps on individual client workstations</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 Center Web Console</u> (ESMC Web Console) in your web browser and log in.
- 2. Click **Policies** and select your policy for client computers.
- 3. Click **Policies** → **Edit**.



### Figure 1-1

#### Click the image to view larger in new window

1. Click **Settings**, click **Detection Engine** and then click **Edit** in the **Exclusions** section.

eser	SECURITY MANAGEMENT CE	INTER	G∂ マ Search computer name QUICK LINKS マ	ି HELP ସ ୧ ADMINISTRA	FOR 📑 ≻59 MIN
2 	Edit Policy Policies > Edit Policy				
<b>▲</b> ∞	Basic	ESET Endpoint for Windows		٩	? ^
Þ	Accion	DETECTION ENGINE	E BASIC	1 0	• +
 ⊚	Summary	Real-time file system protection (15) Cloud-based protection (1)	SCANNER OPTIONS		
			O ●	ж	0
~		HIPS	○ ●	ions ×	0
¢			○ ● 🦩 Enable detection of suspicious applications	1 A 1	0
~		UPDATE	○ ● ≁ Enable Initial Scan	≥ 6.6 ✓	0
1 >		NETWORK PROTECTION			
		WEB AND EMAIL	ANTI-STEALTH		0
		DEVICE CONTROL	Fnable Anti-Stealth technology	4	
		TOOLS	PROCESSES EXCLUSIONS		_
		USER INTERFACE	O  Processes to be excluded from scanning	Edit	0
		OVERRIDE MODE	EXCLUSIONS	y .	
			Files and folders to be excluded from scanning	Edit	0
			AMSI		0
			O ● ≠ Enable advanced scanning via AMSI	≥ 10 ✓	~
		BACK CONTINUE FINISH	SAVE AS CANCEL		

#### Figure 1-2

#### Click the image to view larger in new window

 Click Add, type the directory that you want to exclude from scanning into the field under Exclude path and then click OK. Make sure the filepath for your exclusion is in the correct format, for example "C:\Users\[username]\Documents\file.exe".



# Figure 1-3

- 1. Click **Save** when you are finished adding exclusions.
- 2. Click **Finish** to save your changes.

KB Solution ID: KB6766 |Document ID: 25566|Last Revised: August 23, 2018