ESET Tech Center

Kennisbank > Legacy > ESET Security Management Center > Add a trusted IP address to allow connection to a network device such as a computer or printer in ESET Security Management Center (7.x)

Add a trusted IP address to allow connection to a network device such as a computer or printer in ESET Security Management Center (7.x)

Anish | ESET Nederland - 2022-08-19 - Reacties (0) - ESET Security Management Center

Issue

If you are unable to connect to another computer or device, such as a printer on your network, you can add these devices to the trusted range of IP addresses defined on the computer you are trying to connect from.

Solution

Endpoint users: Perform these steps on individual client workstations

Home users: <u>View instructions to resolve this issue in your ESET home product</u>

- 1. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
- 2. Click **Policies** \rightarrow **New Policy** (or **Policies** \rightarrow **Edit** to edit an existing policy).

eser	SECURITY MANAGEN	VENT	CENTER								E LOGOUT
		Pol	licies	Show unassig	ned	Endpoint Sec	urity - Assign	ed to			0
² 🖵		AC	CESS GROUP Select		∇	Assigned to	Applied on	Settings	Summary		
		~ 0 0	Custom Policies		^	TARGET N	AME		TARGET	DESCRIPTION	٢
		~1	ESET Endpoint for Windo	ows	_			NO DA	TA AVAILABLE		
Ē		V	Lo Endpoint Security								
<u> </u>			uit-in Policies	n.							
6	Policies	~ [Suite in Fondes	id (2+)							
, e	Computer Users	~ t	ESET Endpoint for Windo	ows							
<u></u>	Computer Users		Antivirus - Balanced								
ų.			🗟 Antivirus - Maximum	security - recommended							
ۍ ۲			Cloud-based protect	ion - recommended							
<u> </u>			🕃 Device control - Max	imum security	- 11						
			🕞 Device Control - Rea	d only							
			🕃 Firewall - Block all tra	affic except ESMC & EEI conr	necti						
		(2)	🕃 Logging - Full diagno	ostic logging							
			🔓 Logging - Log impor	tant events only							
		Ν.	🔓 Visibility - Balanced								
			🕻 Visibility - Invisible m	node							
			C Visibility - Reduced in	nteraction with user							
		~ ť	ESET Endpoint for macO	S (OS X) and Linux							
		~ (ESET File Security for Wir	ndows Server (V6+)							
		~ [ESET Mail Security for M	icrosoft Exchange (V6+)	Ň						
		<pre></pre>			,						
ŧ		PO	LICIES 🔻 NEW POI	LICY		ASSIGN GROUP	(5) ASSIGN C	UN/	ASSIGN		

3. Click Settings and select ESET Endpoint for Windows from the product drop-down menu.

eset	SECURITY MANAGEM	IENT CENTER	G マ Search computer na	ame QUICK LINKS 🗢	⊘ HELP ⊽	名 ADMINISTRATOR	🗄 LOGOUT
		New Policy			,		
° 🖵		Policies > New Policy	3				
		Basic	ESET Endpoint for Windows	~	Q		?
		Settings	DETECTION ENGINE				
		Summary	UPDATE				
۲	Policies		NETWORK PROTECTION				
~			WEB AND EMAIL				
			DEVICE CONTROL				
1			TOOLS				
			USER INTERFACE				
			OVERRIDE MODE				
_							
Ð			BACK CONTINUE FINISH	CANCEL			

4. Click **Network Protection**, select **Firewall**, select **Automatic mode** from the **Filtering mode** drop-down menu and then click **Advanced** and click **Edit** next to **Zones**.

(CSeT)	SECURITY MANAGEMENT C	ENTER				
2 	New Policy Policies > New Policy		-			
i A	Basic	ESET Endpoint for Windows		٩		?
6 1	Assign	DETECTION ENGINE UPDATE	 ■ BASIC ○ ●		0 • 4	
© ~	Summery		Also evaluate rules from Wind Firewall O Filtering mode	dows (0 ≥ 6.5) (1 ≥ 7) × Automat	ic mode	0
φ & 		Network attack protection WEB AND EMAIL	Automatic mode is the default one firewall with no need to define rule blocks all non-initiated connection	e. It is suitable for users who preferences an es. Automatic mode allow an outbound tra is from the pair and side unless otherwise d	d convenient use of the iffic for the given system and iefined by custom rules.	
		DEVICE CONTROL TOOLS	+ ADVANCED		0 • 4	
		USER INTERFACE	+ KNOWN NETWORKS		0 • +	0
		OVERRIDE MODE	FIREWALL PROFILES APPLICATION MODIFICATION	DETECTION	○ ● <i>f</i> ○ ● <i>f</i>	0
			LEARNING MODE SETTINGS		0 • 4	
٦		BACK CONTINUE FINISH	CANCEL			

5. Select **Trusted zone** and click **Edit**.

eser	SECURITY MANAGEMENT C								
2	New Policy Policies > New Policy		Firewall zones	? □ ×					
	Basic Settings Assign Summary	ESET Endpoint for Wind DETECTION ENGINE UPDATE NETWORK PROTECT Ficewall Network attack prote WEB AND EMAIL DEVICE CONTROL TOOLS USER INTERFACE OVERRIDE MODE	Name Trusted some Addresses excluded fn TCP/UDP ports visibilit DNS Servers Local addresses Add Edit	m IDS ty zone 5 Remove Save Cancel	CATION DETECTION	Q Edit	0 • 0 • 0 • 0 • 0 •	+ + + + + + +	?
±1		BACK CONTINUE	FINISH						

6.Type the trusted IP adress(es) in the **Remote computer address** field and click **OK**.

Multiple IP addresses	
Use commas to separate multiple IP addresses, for example: 192.168.1.5, 10.1.0.99, 10.1.0.0/255.255.0.0	

Edit zone		? 🗆 X
Name	Trusted zone	
Description	The actual trusted zone is computed from these adresses and adresses specified in networks marked as home or office	$\langle \rangle$
Remote computer address (IPv4, IPv6, range, mask)	192.168.1.1, 10.1.0.25	↔ 6
	6	ОК

7. Click **Save** and assign the policy to the designated host or group. The IP addresses used below are examples; you must enter the actual IP address of the computer/device that you are connecting to.



KB Solution ID: KB6805 |Document ID: 25668|Last Revised: August 29, 2018