# **ESET Tech Center**

Kennisbank > Legacy > ESET Security Management Center > SIEM Integration > Export logs to Syslog server from ESET Security Management Center (7.x)

# Export logs to Syslog server from ESET Security Management Center (7.x)

Anish | ESET Nederland - 2020-07-14 - Reacties (0) - SIEM Integration

#### Issue

- ESET Security Management Center version 7.x is able to send notifications to your Syslog server
- Export Threat events, Firewall Aggregated events, HIPS Aggregated events, Audit events, Enterprise Inspector alert events

#### Solution

### 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): <u>Create a second</u> administrator user in ESET Security Management Center 7.x

#### View permissions needed for least privilege user access

A user must have the following permissions for their home group:

Functionality	Read	Use	Write
---------------	------	-----	-------

Server Settings 🗸 🗸 🗸

Once these permissions are in place, follow the steps below:

- 1. <u>Open ESET Security Management Web Console</u> (ESMC Web Console) in your web browser and log in.
- 2. Click **More** → **Server Settings** and expand **Advanced Settings**.

eser	SECURITY MANAGEN	ENT CENTER	uter name QUICK LINKS ▽ ③ HELP ▽ Å ADMINISTRATOR	🖂 >59 MIN
	Groups Dynamic Group	Server Settings Q ?		
цġ	Templates Submitted Files			^
A	Quarantine			
uni	License Management	ADVANCED SETTINGS		
٦	ACCESS RIGHTS	HTTP PROXY		
	Users	Use proxy server	×	
۲	Permission Sets	Host		. 1
~	CERTIFICATES	Port	3128	
Φ	Peer Certificates			
Q	Certification Authorities	Username		
1 >	SERVER	Password		
· · ·	Server Tasks		Show password	
<u> </u>	Server Settings	Use direct connection if HTTP proxy is not available		
		WAKE-UP CALL		•
		UDPv4 Port	1237	
		UDPv6 Port	1238	
		WAKE ON LAN		
		Multicast Addresses	Edit multicast addresses	•
_		SMTP SERVER		
				$\sim$
	CLOSE	SAVE CANCEL		

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

- 3. In the **Syslog Server** section:
  - 1. Click the slider bar next to **Use Syslog server**
  - 2. Host: Type the IP address or hostname for the destination of Syslog messages
  - 3. Port: Default value is 514
- 4. In the Logging section, click the slider bar next to Export logs to Syslog and

C	lick	Save.	

(ESer)	SECURITY MANAGEN	IENT C	ENTER								🕞 >59 MIN
2	Groups Dynamic Group Terrolater	Serve	er Settings	Q		?					
느	Submitted Files		Ura Surlaa cania	n.							^
Δ	Quarantina	3	Use syslog serve	21							
	Licence Management	3	Host				10.0.0.0				
	cicense management	_	Port				514				
			Format				BSD			~	
			Transport				UDP			~	
			Octet-counted fr	raming							
			STATIC GROUP	s							
			Automatically pa	air found computers			× .				
۳ <sup>.</sup>			Enables automatic p	pairing of found computers to co	imputers already p	resent in static groups. P	airing works on	reported hostname by ag	gent and if it can not	t be trusted then it should	
· ··· >			be usabled. If pairing	ng rais computer will be placed i	nto cost and roun	a group.					
	Server Lasks		REPOSITORY								
	Jerver Jeungs		Server				AUTOSE	ELECT			
			PRODUCT IMPR	ROVEMENT PROGRAM							
			Participate in pro	oduct improvement program	n		1				0
		3	LOGGING								
		4	Trace log verbos	iity			Warning	2		$\checkmark$	
		-									
		1	Export logs to Sy	yslog			4				~
				1							
		SAV	CANCEL								



 For a detailed list of the format and meaning of attributes of all exported events (Threat events, ESET Firewall events, HIPS events, Audit events, Enterprise Inspector alert events), visit the <u>Export logs to Syslog</u> Online Help topic.