ESET Tech Center

<u>Kennisbank</u> > <u>ESET PROTECT Cloud</u> > <u>Export logs to Syslog server from ESET PROTECT (8.x-10.x)</u>

Export logs to Syslog server from ESET PROTECT (8.x-10.x)

Mitch | ESET Nederland - 2023-03-10 - Reacties (0) - ESET PROTECT Cloud

Solution

- 1. Open the ESET Protect Web Console in your web browser and log in.
- 1. Click **More** → **Server Settings** and expand **Advanced Settings**.

(ESET)	PROTECT			Gr ⊂ Computer Name	QUICK LINKS 🗢	③ HELP ▼	A ADMINISTRATOR	E LOGOUT
	DETECTIONS Submitted Files	Server Settings Q. Type to search ?						
Ld .	Exclusions							Â
A	COMPUTTERS	UPDATES						
	Computer Users	ADVANCED SETTINGS						
	Dynamic Group Templates							
	LICENSES	Host						
	License Management	Port	3128					
	ACCESS RIGHTS	Username						
	Permission Sets	Password	Cheve parameter					
	CERTIFICATES	Use direct connection if HTTP proxy is not available						- 1
	Peer Certificates Certification Authorities	WAKE-UP CALL		0				
	SERVER	UDPv4 Port	1237					
	Server Settings	UDPv6 Port	1238					
	ACTIVITY AUDIT	WAKE ON LAN						
	Audit Log	Multicast Addresses	Edit multicast addresses	0				
		SMTP SERVER						
		Use SMTP server	×					
		Port	25					
		Username						
		Password						
			Show password					
		Connection security type	Not secured	~				
		Authentication type		¥				-
	CLOSE	SAVE CANCEL						

1. In the **Syslog Server** section:

a. Next to Use Syslog server, click the toggle to enable it.

b. In the **Host** field, type the IP address or hostname for the destination of Syslog messages.

1. In the **Logging** section, click the toggle next to **Export logs to Syslog** to enable it and click **Save**.

rver Settings	ype to search	?						
Host								
Username								
Password								
		Show password						
Root container								
SYSLOG SERVER	SYSLOG SERVER 3							
Use Syslog server		✓						
Host		10.0.0.0						
Port		514						
Format		BSD						
Transport		UDP 🗸						
Octet-counted framing		×						
STATIC GROUPS	STATIC GROUPS							
Automatically pair four	nd computers							
Enables automatic pairing be disabled. If pairing fails	Enables automatic pairing of found computers to computers already present in static groups. Pairing works on reported hostname by agent and if it can not be trusted then it should be disabled. If pairing fails computer will be placed into Lost and Found group.							
REPOSITORY								
Server		AUTOSELECT						
PRODUCT IMPROVEN	PRODUCT IMPROVEMENT PROGRAM							
Participate in product i	mprovement program	× 6						
LOGGING								
Trace log verbosity	4	Warning ~						
Export logs to Syslog	-							
Exported logs format		JSON						

 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 Export logs to Syslog Online Help topic.