

ESET Tech Center

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

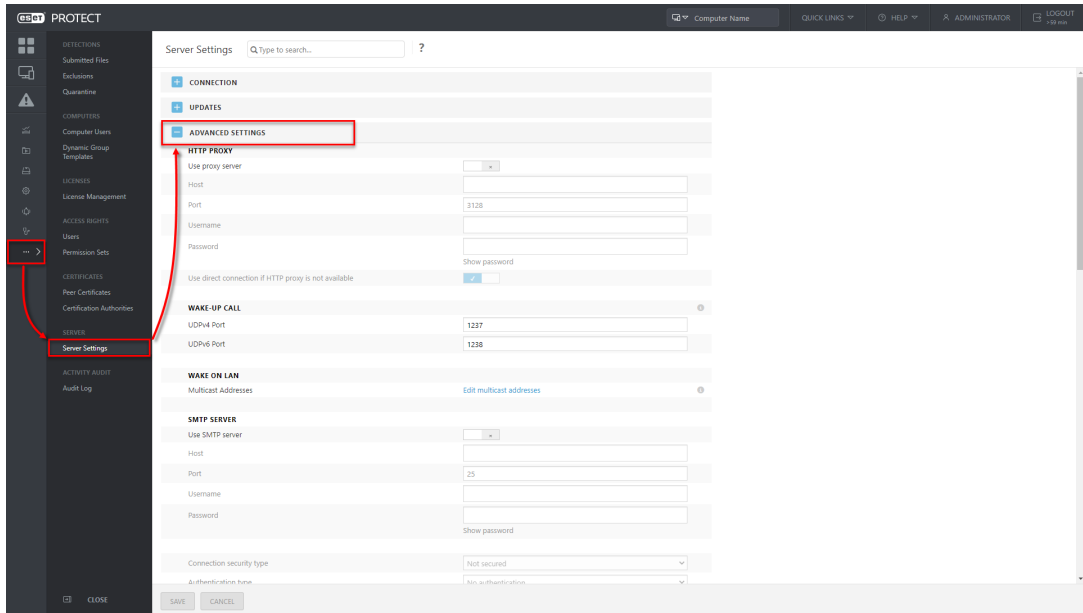
Export logs to Syslog server from ESET PROTECT (8.x-10.x)

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**.



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.

c. In the **Port** field, the default value is set to 514.

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

Server Settings ?

Host	<input type="text"/>
Username	<input type="text"/>
Password	<input type="password"/>
	Show password
Root container	<input type="text"/>

SYSLOG SERVER

Use Syslog server	<input checked="" type="checkbox"/>
Host	<input type="text" value="10.0.0.0"/>
Port	<input type="text" value="514"/>
Format	<input type="text" value="BSD"/>
Transport	<input type="text" value="UDP"/>
Octet-counted framing	<input type="checkbox"/>

STATIC GROUPS

Automatically pair found computers	<input checked="" type="checkbox"/>
------------------------------------	-------------------------------------

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	<input type="text" value="AUTOSELECT"/>
--------	---

PRODUCT IMPROVEMENT PROGRAM

Participate in product improvement program	<input type="checkbox"/>
--	--------------------------

LOGGING

Trace log verbosity	<input type="text" value="Warning"/>
Export logs to Syslog	<input checked="" type="checkbox"/>
Exported logs format	<input type="text" value="JSON"/>

1. 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.