Export logs to Syslog server from ESET Remote Administrator (6.3 and later)

Ondersteuning | ESET Nederland - 2025-03-07 - Reacties (0) - 6.x

https://support.eset.com/kb5777

Issue

ESET Remote Administrator version 6.3 and later is able to send notifications to your Syslog server
Export Threat events, Firewall Aggregated events and HIPS Aggregated events

Solution

To perform the steps in this article, 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. Open ESET Remote Administrator Web Console (ERA Web Console) in your web browser and log in. How do I open ERA Web Console?

2. Click **Admin** → **Server Settings** and expand **Advanced Settings**.



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

3. In the **Syslog Server** section, complete the following steps (see figure 1-2):

a. Click the slider bar next to **Use Syslog server**

a. **Host:** Type the IP address or hostname for the destination of Syslog messages

b. **Port:** Default value is 514

4. In the **Logging** section, click the slider bar next to **Export logs to Syslog** and click **Save**.



Figure 1-2
Click the image to view larger in new window

5. For a detailed list of the format and meaning of attributes of all exported events (Threat events, ESET Firewall events and HIPS events), visit the Export logs to Syslog Online Help topic.

- Tags
- ERA 6.x
- MSP
- SIEM