ESET Tech Center

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): Create a second 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. Open ESET Security Management Web Console (ESMC Web Console) in your web browser and log in.
2. Click **More → Server Settings** and expand **Advanced Settings**.

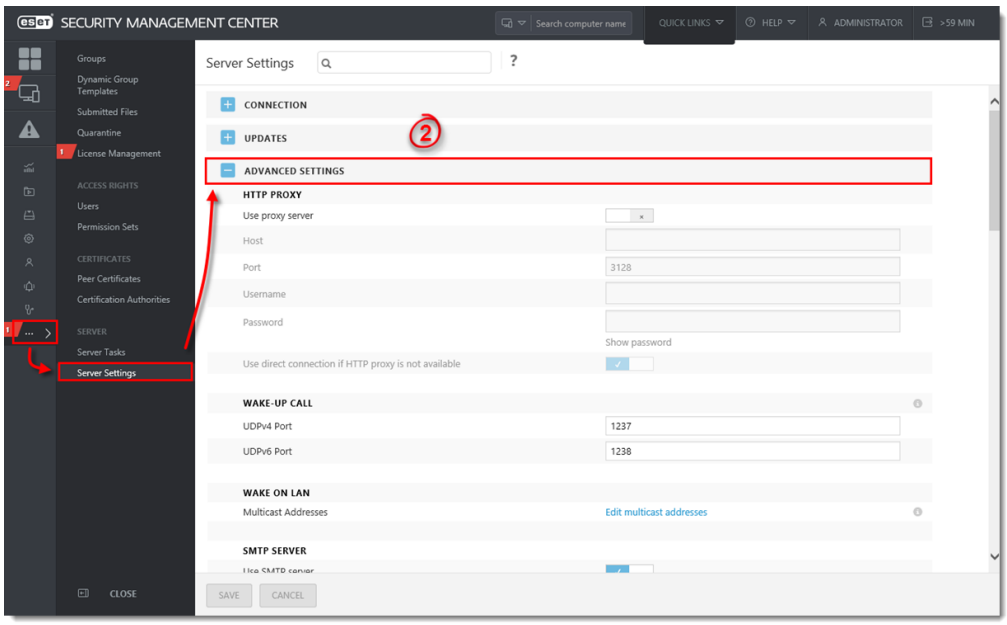

Figure 1-1

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 click **Save**.

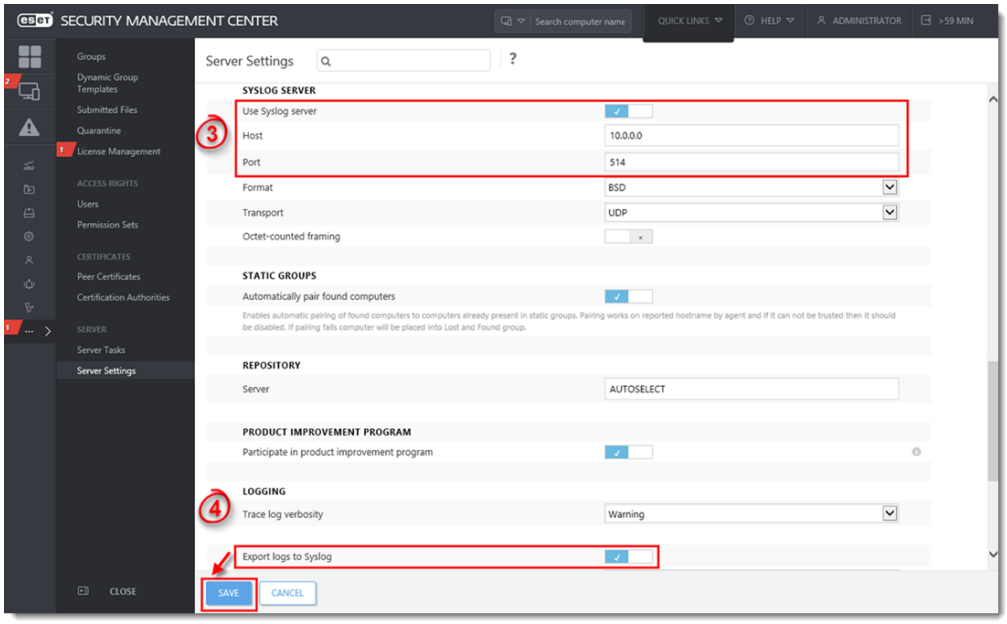

Figure 1-2

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, HIPS events, Audit events, Enterprise Inspector alert events), visit the Export logs to Syslog Online Help topic.