

syslog_output

XML section name

```
<syslog_output>
</syslog_output>
```

Configuration options for sending alerts to a syslog server.

Options

- server
- port
- level
- group
- rule_id
- location
- use_fqdn
- format

server

The IP Address of the syslog server.

Default value	n/a
Allowed values	Any valid IP address

port

The port to forward alerts to.

Default value	514
Allowed values	Any valid port

level


The minimum level of the alerts to be forwarded.

Default value	n/a
Allowed values	Any level from 1 to 16

group

Group of the alerts to be forwarded.

Default value	n/a
Allowed values	Any valid group. Separate multiple groups with the pipe (") character.

 Note

Observe that all groups must be finished by comma.

rule_id

The rule_id of the alerts to be forwarded.

Default value	n/a
Allowed values	Any valid rule_id

location

The location of the alerts to be forwarded.

Default value	n/a
Allowed values	Any valid log file location

use_fqdn

Toggle for full or truncated hostname configured on the server. By default, ossec truncates the hostname at the first period (".") when generating syslog messages.

Default value	no
Allowed values	yes, no

format

Format of alert output. When `jsonout_output` in `global` section is enabled, alerts are read from alerts.json instead of alerts.log for JSON format.

Default value	default	
Allowed values	default	
	cef	will output data in the ArcSight Common Event Format.
	splunk	will output data in a Splunk-friendly format.
	json	will output data in the JSON format that can be consumed by a variety of tools.

Example of configuration

```
<syslog_output>
  <server>192.168.1.3</server>
  <level>7</level>
  <format>json</format>
</syslog_output>
```