LOGZILLA DOCUMENTATION

Palo Alto PAN-OS Configuration

Configure Palo Alto PAN-OS syslog server profiles, custom log formats for traffic and threat logs, and log forwarding to LogZilla

Receiving Data in LogZilla · Generated June 11, 2026 · logzilla.ai/docs/receiving-data/paloalto-pan-os-configuration

© LogZilla Corporation · logzilla.ai

Configure PAN-OS Syslog

Prerequisites

- Include the device IPv4 address in the syslog header: `Panorama/Device > Setup > Management` → `Logging and Reporting Settings` → `Log Export and Reporting` → set `Syslog HOSTNAME Format` to `ipv4-address`.
- Confirm syslog listener ports in LogZilla (see Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)).

Create a syslog server profile

Opens `Server Profiles > Syslog` and select `Add`.
A profile Name and Location is specified (Location refers to the virtual system when VSYS is enabled).
On the `Servers` tab, an entry is added with:

- Syslog Server (LogZilla IP or hostname)
- Transport (UDP/TCP as required)
- Port (default 514 for UDP)
- Facility (for example, `LOG_USER`)

Custom log formats

Threat logs

```
PaloAlto_Threat type="$type" src="$src" dst="$dst" rule="$rule" srcuser="$srcuser"
sessionid="$sessionid" action="$action" misc="$misc" dstloc="$dstloc" referer="$referer"
http_method="$http_method" http_headers="$http_headers"
```

Traffic logs

```
PaloAlto_Traffic type="$type" src="$src" dst="$dst" natsrc="$natsrc" natdst="$natdst" rule="$rule"
srcuser="$srcuser" from="$from" to="$to" sessionid="$sessionid" sport="$sport" dport="$dport"
natsport="$natsport" natdport="$natdport" proto="$proto" action="$action" bytes="$bytes"
packets="$packets" dstloc="$dstloc" action_source="$action_source"
```

Attach log forwarding

A `Log Forwarding` profile is created or updated to reference the syslog server profile (Objects → Log Forwarding).
The forwarding profile is applied to the required security policies: Policies → Security → select a rule → Actions → set `Log Forwarding` to the created profile. `Log at Session End` can be enabled as required.

Commit changes

Commit the configuration (Changes → Commit).

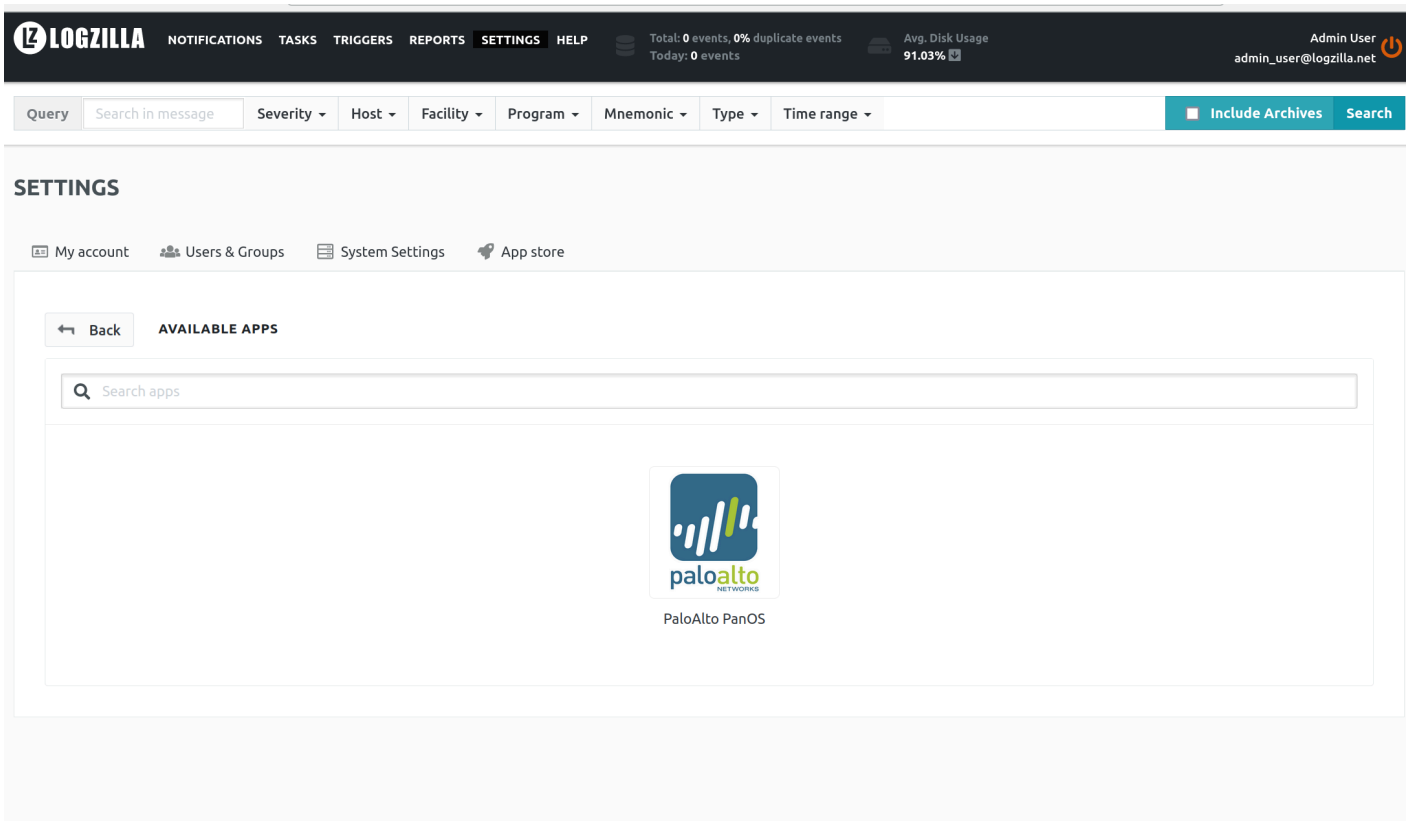
Verify in LogZilla

- Reception can be confirmed by searching for the device host or expected text in LogZilla.
- For packet-level checks, use Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).

LogZilla Rules and Dashboards

Rules and dashboards for Palo Alto are available in the LogZilla appstore (`Settings` → `App store`).

Install the Palo Alto app to enable the rule.



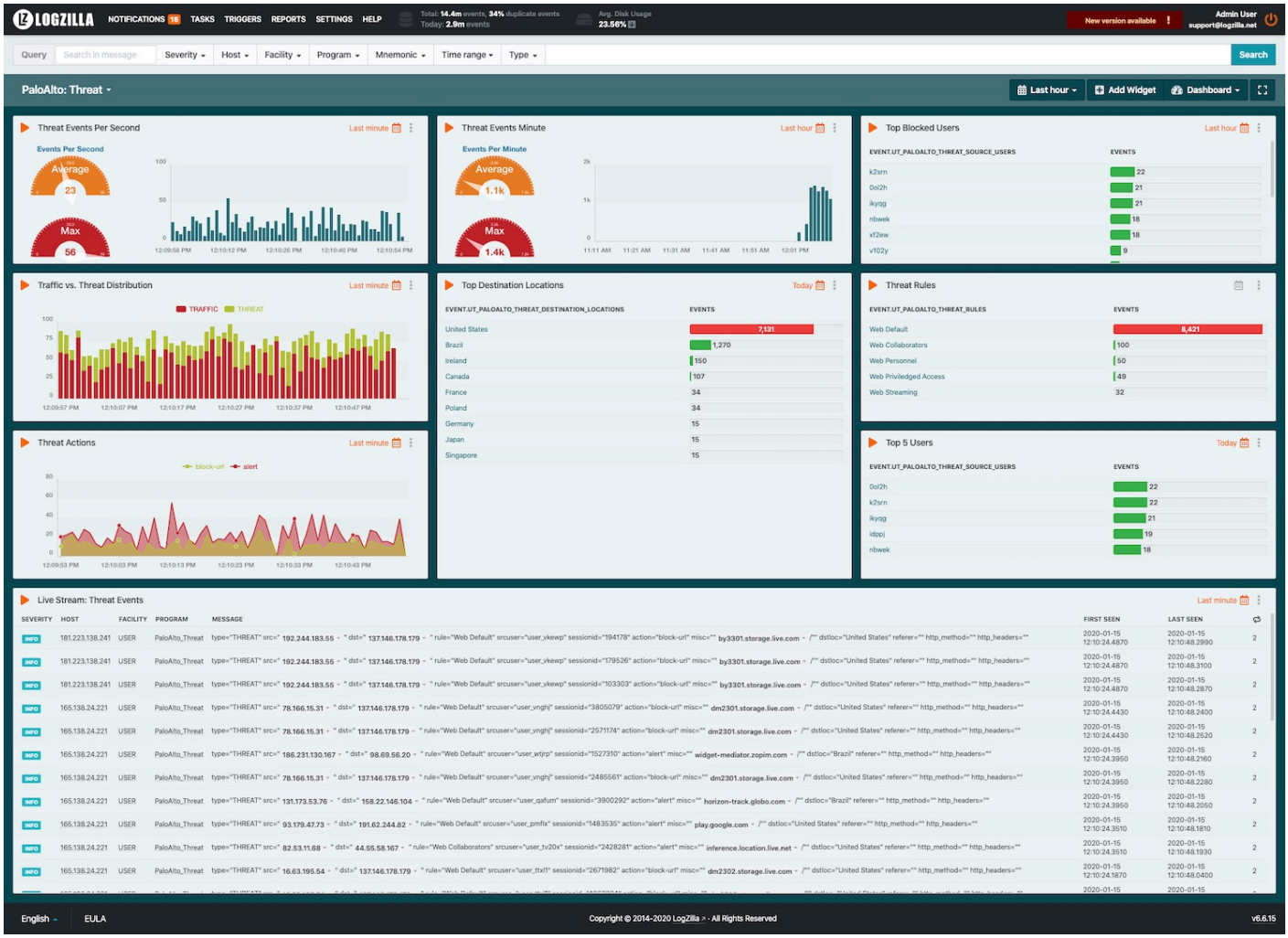
Related topics

- Syslog Settings (https://www.logzilla.ai/docs/administration/syslog-settings)
- Syslog Troubleshooting (https://www.logzilla.ai/docs/administration/syslog-troubleshooting)

Example dashboards

After installation, the dashboards will look similar to these examples.

Threat dashboard



Traffic dashboard


LOGZILLA
NOTIFICATIONS
TASKS
TRIGGERS
REPORTS
SETTINGS
HELP
Search
PaloAlto: Traffic
Last minute
Add Widget
Dashboard
Traffic Events Per Second
Traffic Events Per Day
Top Source Users
Top NAT Sources
Top Destination Locations
Traffic Action Sources
Top Traffic Sources
Top Hosts
Traffic Rules
Traffic Actions
Live Stream: Traffic Events
English
EULA
Copyright © 2014-2020 LogZilla
v6.6.15