

## LOGZILLA DOCUMENTATION

# Juniper SRX Configuration

Configure Juniper SRX devices to forward security logs to LogZilla in RFC5424 sd-syslog structured format using stream mode and a source address

Receiving Data in LogZilla · Generated May 3, 2026 · [logzilla.ai/docs/receiving-data/juniper-srx-configuration](https://logzilla.ai/docs/receiving-data/juniper-srx-configuration)

# Juniper SRX Configuration

Juniper SRX devices should send logs in RFC5424 structured format (key-value pairs) rather than legacy RFC3164. The SRX `sd-syslog` format is recommended.

## Prerequisites

- Confirm syslog listener ports on the LogZilla server (see [Syslog Settings](https://www.logzilla.ai/docs/administration/syslog-settings) (https://www.logzilla.ai/docs/administration/syslog-settings)).
- Choose a stable source IP/interface on the SRX for logging.
- Ensure network policy allows the SRX to reach LogZilla on the selected syslog port.

## Configure SRX security logging (structured syslog)

Enter configuration mode and apply settings similar to the following. Replace the sample addresses with the correct SRX source and LogZilla destination.

```
edit
set security log mode stream
set security log format sd-syslog
set security log source-address 1.1.1.1
set security log stream logzilla host 10.1.1.2
show | compare
commit check
commit
```

### Notes:

- `format sd-syslog` enables RFC5424 structured data.
- `source-address` is the SRX interface address used as the syslog source.
- The `stream logzilla host` command sets the LogZilla destination address.

## Verification

Generate traffic or events that produce logs on the SRX.

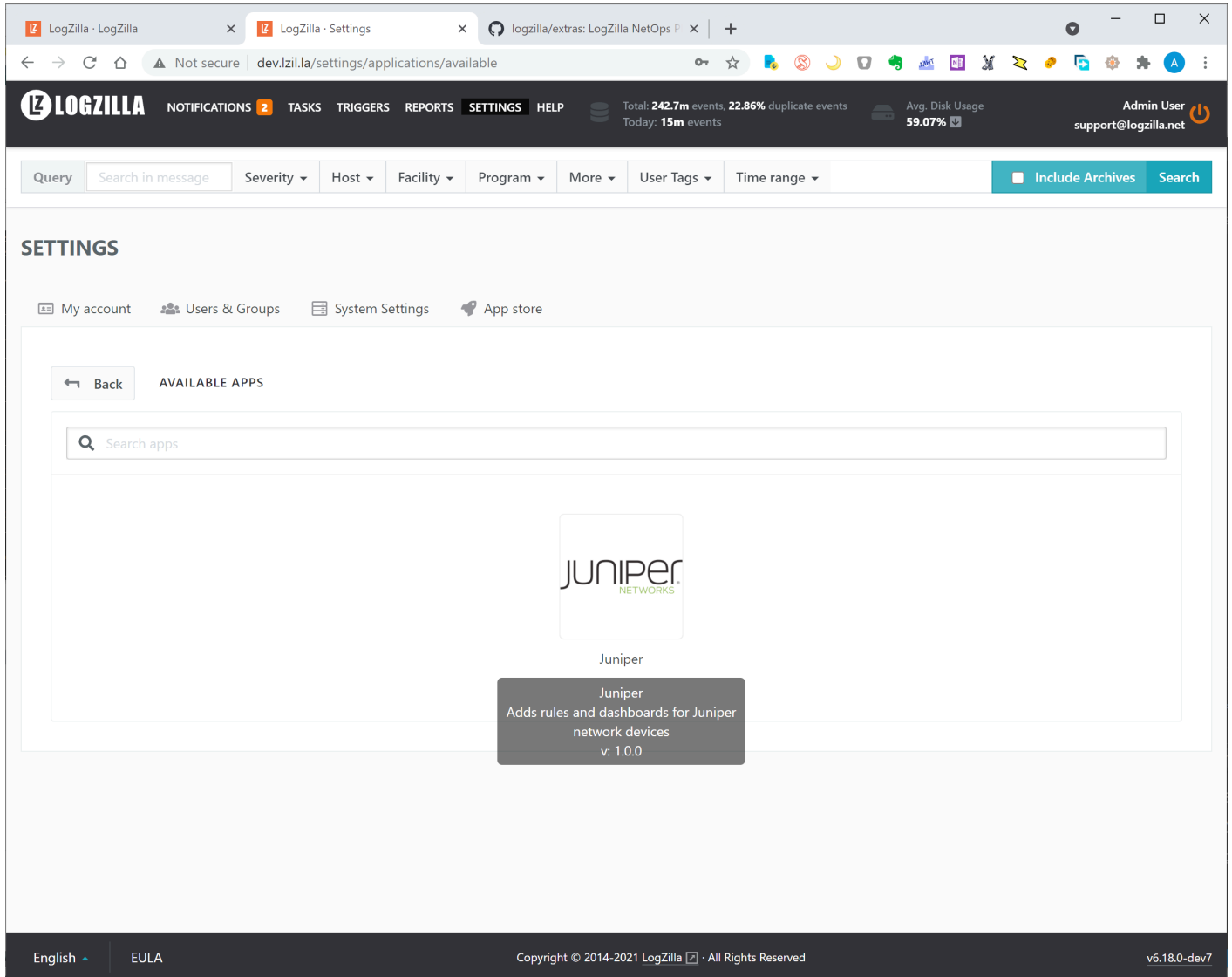
In LogZilla, search by host or program to confirm reception. For example:

- `host : "1.1.1.1"` (the configured SRX source address)
- Text from expected messages

For packet-level checks and capture examples, see [Syslog Troubleshooting](https://www.logzilla.ai/docs/administration/syslog-troubleshooting) (https://www.logzilla.ai/docs/administration/syslog-troubleshooting).

## Juniper appstore rule (optional)

The Juniper appstore rule improves readability and adds user tags for key fields. Install from the [Settings](#) → [App store](#) page.



The screenshot shows the LogZilla web interface. At the top, there's a navigation bar with 'LOGZILLA' and menu items: NOTIFICATIONS (2), TASKS, TRIGGERS, REPORTS, SETTINGS (active), and HELP. System status is shown as 'Total: 242.7m events, 22.86% duplicate events' and 'Today: 15m events'. The user is 'Admin User' with email 'support@logzilla.net'. Below the navigation is a search bar with filters for Query, Search in message, Severity, Host, Facility, Program, More, User Tags, and Time range. The main content area is titled 'SETTINGS' and has sub-menus for My account, Users & Groups, System Settings, and App store (active). The 'App store' page shows 'AVAILABLE APPS' with a search bar. A single app is listed: 'Juniper' with a logo and a description: 'Juniper Adds rules and dashboards for Juniper network devices v: 1.0.0'.

## Related topics

- [Syslog Relays](https://www.logzilla.ai/docs/administration/syslog-relays) (https://www.logzilla.ai/docs/administration/syslog-relays)