

How-To Guide

Configuring Palo Alto Networks[®] Cortex Data Lake to Forward Logs to EventTracker

EventTracker v9.3 and above

Publication Date:

October 6, 2021

Abstract

This guide provides instructions to retrieve the **Palo Alto Networks® Cortex Data Lake** events via remote syslog. Once the logs start coming into EventTracker, the reports, dashboards, alerts, and saved searches can be configured.

Scope

The configuration details in this guide are consistent with EventTracker version 9.3 or above and **Palo Alto Networks® Cortex Data Lake**.

Audience

Administrators who are assigned the task to monitor **Palo Alto Networks® Cortex Data Lake** events using EventTracker.

Table of Contents

Table of Contents	3
1. Overview	4
2. Prerequisites.....	4
3. Configuring Palo Alto Networks® Cortex Data Lake to Forward Logs to EventTracker.....	4
3.1 Forwarding syslog data to EventTracker.....	4
About Netsurion	7
Contact Us.....	7

1. Overview

The **Palo Alto Networks® Cortex Data Lake** stores the context-rich enhanced network logs generated by the security products, including the next-generation firewalls, Prisma Access, and Cortex XDR.

EventTracker helps to monitor events from Palo Alto Networks® Cortex Data Lake. Its dashboard, alerts, and reports will help you to track authentication activities, threat activities, traffic activities, and configuration changes. It will trigger an alert whenever user authentication fails, a threat is detected, configuration is successfully changed, and an unauthorized configuration change is attempted.

2. Prerequisites

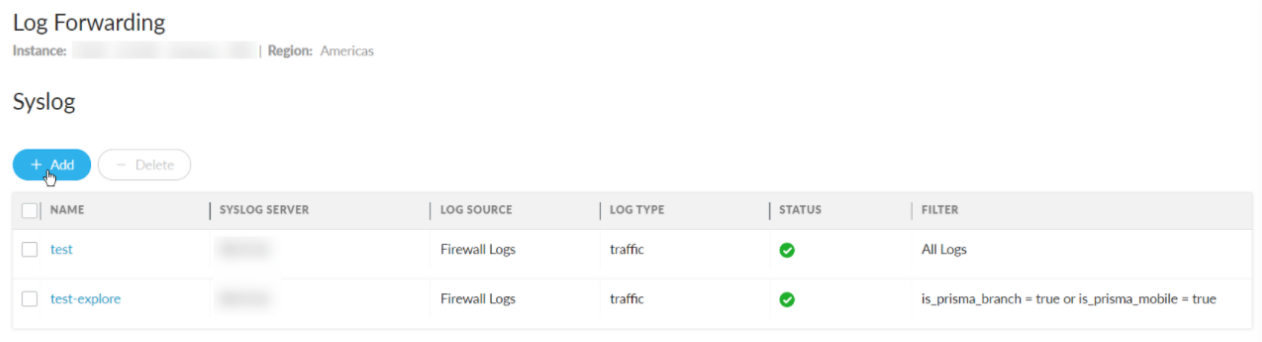
- **EventTracker v9.x or above** should be installed.
- A user with global administrator of Palo Alto Networks® Cortex Data Lake.
- Syslog port should be allowed in the firewall.
- Administrative access on EventTracker.

3. Configuring Palo Alto Networks® Cortex Data Lake to Forward Logs to EventTracker

Palo Alto Networks® Cortex Data Lake can be integrated with EventTracker by forwarding the syslogs to EventTracker manager.

3.1 Forwarding syslog data to EventTracker

1. Login to Palo Alto Cortex Data Lake <https://apps.paloaltonetworks.com/>.
2. Select the Cortex Data Lake instance that you want to configure for syslog forwarding. (If you have multiple Cortex Data Lake instances, click the Cortex Data Lake tile and select an instance from the list of those available.)
3. Select **Log Forwarding** -> **Add** to add a new Syslog forwarding profile.



Log Forwarding
Instance: [redacted] | Region: Americas

Syslog

+ Add - Delete

<input type="checkbox"/>	NAME	SYSLOG SERVER	LOG SOURCE	LOG TYPE	STATUS	FILTER
<input type="checkbox"/>	test	[redacted]	Firewall Logs	traffic	✓	All Logs
<input type="checkbox"/>	test-explore	[redacted]	Firewall Logs	traffic	✓	is_prisma_branch = true or is_prisma_mobile = true

4. Enter a descriptive **Name** for the profile as EventTracker Syslog.
5. Enter the **EventTracker Manager Syslog Server IP address**.
6. Enter the **Port** on which the syslog server is listening.
For UDP (recommended if on-premises) port 514.

• NAME: EventTracker Syslog
 • SYSLOG SERVER: EventTracker IP Address
 • PORT: 514
 • FACILITY: LOG_USER
 Server Authentication
 Public CAs
[List of trusted certificate authorities](#)
 + Upload - Delete
Upload a self-signed certificate and a private CA-signed certificate to authenticate your Syslog server. Please make sure that if you are using a certificate signed by a private CA, it contains CRL or OCSP information needed for certificate revocation checks. Delete the self-signed or private CA-signed certificate to go back to using a publicly signed certificate.
 Test Connection
 • Required Fields

7. Click **Next**.
8. Specify the **Format** in which you would like to forward your logs.
9. Specify the **Delimiter** that you would like to separate the fields in your log messages.
10. Select the logs need to forward.
 - I. Add a new log filter.

Syslog Forwarding Profile
 • FORMAT: CEF
 • DELIMITER: Space: " "
 STATUS NOTIFICATION: Enter email address to send status notification
 PROFILE TOKEN: Enter the token to be included in the syslog message
 • FILTERS

<input type="checkbox"/>	LOG SOURCE	LOG TYPE	FILTER
No data found			

 + Add - Delete
 ⚠ Saving the profile will make all changes permanent, including any additions, deletions, and modifications to the filters
 • Required Fields Back Cancel Save

- II. Select the log type.
 - Threat
 - Traffic
 - Authentication
 - Configuration

Network/Traffic

TIME RECEIVED	DEVICE SN	SUB TYPE	CONFIG VERSION	TIME GENERATED	SOURCE ADDRESS
08/25/2020 09:58:21 AM PDT	007099000010916	end		08/25/2020 09:58:21 AM PDT	65.113.40.3
08/25/2020 09:42:37 AM PDT	007099000010916	end		08/25/2020 09:42:37 AM PDT	65.113.40.3
08/25/2020 03:33:15 PM PDT	007099000010916	end		08/25/2020 03:33:15 PM PDT	65.113.40.3
08/25/2020 03:16:39 PM PDT	007099000010916	end		08/25/2020 03:16:39 PM PDT	65.113.40.3
08/25/2020 03:28:19 PM PDT	007099000010916	end		08/25/2020 03:28:19 PM PDT	65.113.40.3

Cancel Save

III. Click **Save**

11. Verify that the status of your syslog forwarding profile is Running.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's [EventTracker](#) cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's [BranchSDO](#) delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#). Netsurion is #19 among [MSSP Alert's 2020 Top 250 MSSPs](#).

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
<https://www.netsurion.com/eventtracker-support>