

How-To Guide

Configuring Threat Stack to Forward Logs to EventTracker

EventTracker v9.3 and above

Publication Date:

May 10, 2021

Abstract

This guide helps you in configuring **Threat Stack** with EventTracker to receive **Threat Stack** events.

Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and **Threat Stack**.

Audience

Administrators, who are assigned the task to monitor **Threat Stack** events using **EventTracker**.

Table of Contents

1. Overview.....	4
2. Prerequisites	4
3. Configuring Threat Stack to forward logs to EventTracker	4
3.1 Configuring EventTracker Threat Stack Integrator	4
About Netsurion.....	6
Contact Us.....	6

1. Overview

Threat Stack Cloud Security Platform provides continuous security monitoring in cloud environments where network-based controls cannot be deployed. It is a platform-independent solution intended for companies of all sizes operating on-premises or in public, private, or hybrid cloud environments.

EventTracker helps to monitor events from Threat Stack. EventTracker flex reports, alerts, and dashboards will help you to analyse the activity logs such as, user action on modification or alerts triggered by Threat Stack.

2. Prerequisites

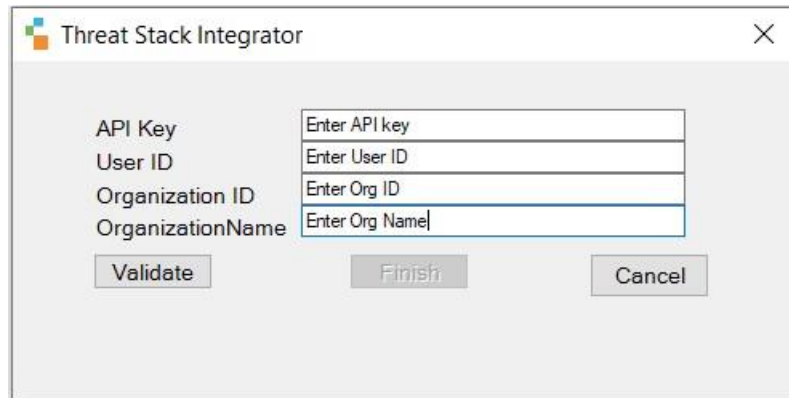
- EventTracker agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run PowerShell.
- Python 3 should be installed on the host system/ server.
- Python need to add as path environment variable.
- Below python modules need to install.
 - mohawk
 - requests
 - xml.etree.cElementTree
 - winregistry
 - ctypes
 - configparser
 - itertools
- Admin access to Threat Stack platform.

3. Configuring Threat Stack to forward logs to EventTracker

The steps provided below will help to configure the EventTracker to receive Threat Stack events using REST API based on Hawk Authentication.

3.1 Configuring EventTracker Threat Stack Integrator

1. Get the **Threat Stack Integrator** executable file:
<https://downloads.eventtracker.com/kp-integrator/ThreatStackIntegrator.exe>
2. Once the executable application is received, click on the file.
3. In the dialog box, enter your Api key, user ID, organization ID, and your organization name; and click on the **Validate** button to verify the credentials.



The screenshot shows a dialog box titled "Threat Stack Integrator" with a close button (X) in the top right corner. The dialog contains four input fields with labels to their left: "API Key", "User ID", "Organization ID", and "OrganizationName". Each input field has a placeholder text: "Enter API key", "Enter User ID", "Enter Org ID", and "Enter Org Name" respectively. Below the input fields are three buttons: "Validate", "Finish", and "Cancel".

4. On successful verification, a pop window will appear with a message: **Credential Validated Successfully.**
5. Click on the **Finish** button to complete the integration process.

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 multilocation 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>