Netsurion®
Powering Secure and Agile Networks

How-To Guide

Configuring SentinelOne Integrator to Forward logs to EventTracker Manager

Publication Date:

September 1, 2021

Abstract

This guide provides instructions to configure or retrieve SentinelOne events using EventTracker application. This will collect the logs from SentinelOne cloud like user activity,threat details, etc. After EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor SentinelOne.

Scope

The configuration details in this guide are consistent with EventTracker version v9.x or above and SentinelOne.

Audience

Administrators who are assigned the task to monitor SentinelOne using EventTracker.

Table of Contents

1. Overview

SentinelOne is a next-generation endpoint security product used to protect against all threat vectors. Keeps known and unknown malware and other bad programs out of endpoints

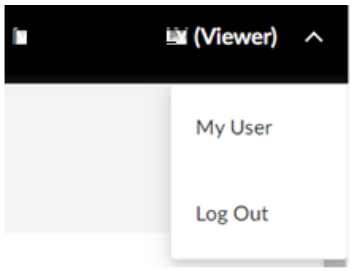
EventTracker collects the events from SentinelOne API and filters it out to get some critical event types for creating reports, dashboards, and alerts. These are considered as knowledge Packs and helps you to analyze and manage the SentinelOne easily.

2. Prerequisites

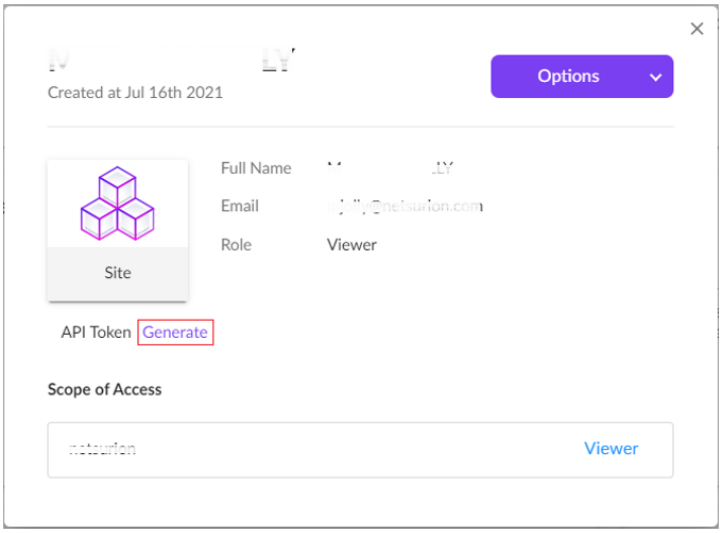
- EventTracker agent should be installed in a host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privilege on host system/ server to run PowerShell.
- User must have viewer role on the SentinelOne console.

3. Generate API Token for SentinelOne

1. Login into **Sentinelone** Console with viewer role User.
2. Click on drop down and select **My User**.



3. Click on the **Generate** button for getting API Token.

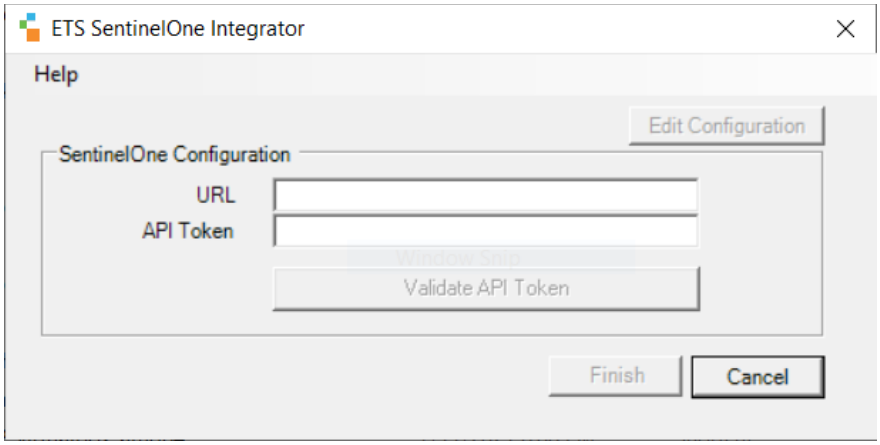


Note: Note the API Token for using it in next steps.

4. Configuring SentinelOne to Forward Logs to EventTracker

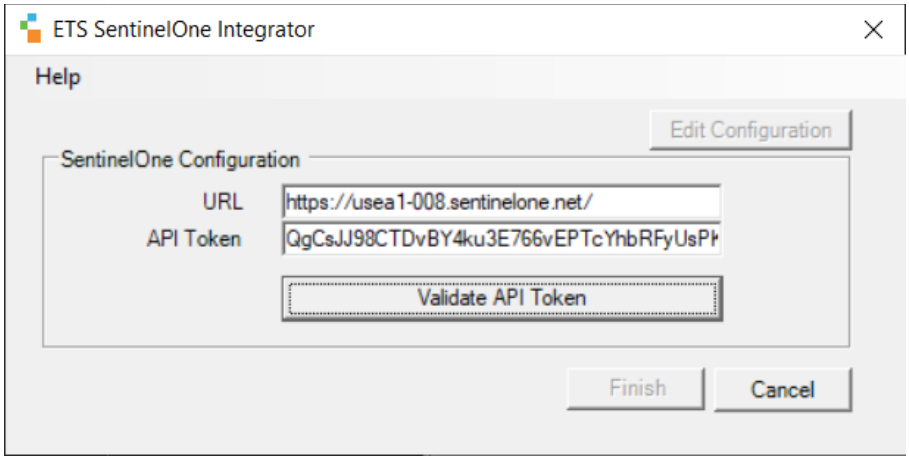
The steps provided below will help to configure the EventTracker to receive events from SentinelOne API.

1. Get the **SentinelOneIntegrator.exe** executable file from the link.
2. After the executable application is received, run the application with administrator privilege.
3. After running the integrator, fill-in the given fields.

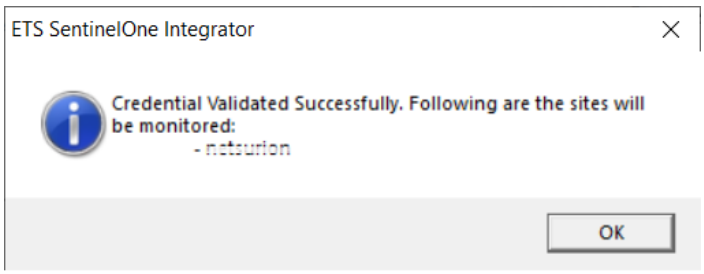


- **URL**: **SentinelOne console URL**
- **API Token: SentinelOne Viewer Role user token**

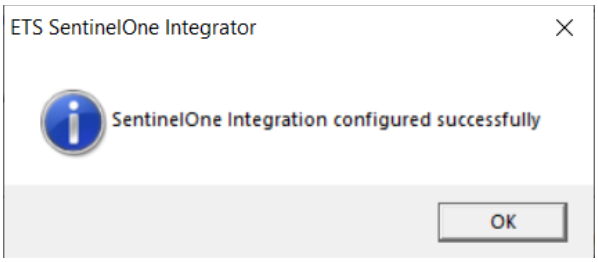
4. Once the required details have been filled, **Validate API Token** button will enable.



5. Click on the **Validate API Token** button to validate the given details.



6. Upon successful validation, a message pops-up, **click OK**.
7. Click **Finish** in the form bottom to complete the configuration.
8. Upon successful configuration it will display the message box as shown below.



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 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