Netsurion®
Powering Secure and Agile Networks

How to - Guide

How to – Configure Carbon Black Cloud Endpoint Standard to forward logs to EventTracker

EventTracker v9.3 and above

Author: Marketing

April 28, 2021

Abstract

This guide helps you in configuring Carbon Black Cloud Endpoint Standard (formerly called CB Defense) with EventTracker to receive Carbon Black Endpoint Standard events via REST API.

Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and Carbon Black Cloud Endpoint Standard (formerly called CB Defense).

Audience

Administrators who are assigned the task to monitor Carbon Black Cloud Endpoint Standard (formerly called CB Defense) events using EventTracker.

Table of Contents

1. Overview

Carbon Black Cloud Endpoint Standard (formerly called CB Defense) is a Next-Generation Antivirus (NGAV) and Endpoint Detection and Response (EDR) solution that protects against the full spectrum of modern cyber-attacks. Next-Generation Anti-Virus (NGAV) uses machine learning and behavioral models to analyze endpoint activity and uncover malicious behavior to stop all types of attacks before they reach critical systems.

EventTracker integrates Carbon Black Cloud Endpoint Standard logging through REST API and provides reports, knowledge objects and dashboards for all generated events including attacks, network connections, registry access, file auditing etc.

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.
- Admin access to Carbon Black Cloud console.

3. Configuring CB Endpoint Standard to forward logs to EventTracker

The steps provided below helps to configure the EventTracker to receive specific events related to email traffic and links clicked by using CB Endpoint Standard enriched_events REST API.

3.1 Creating RBAC permissions required for API

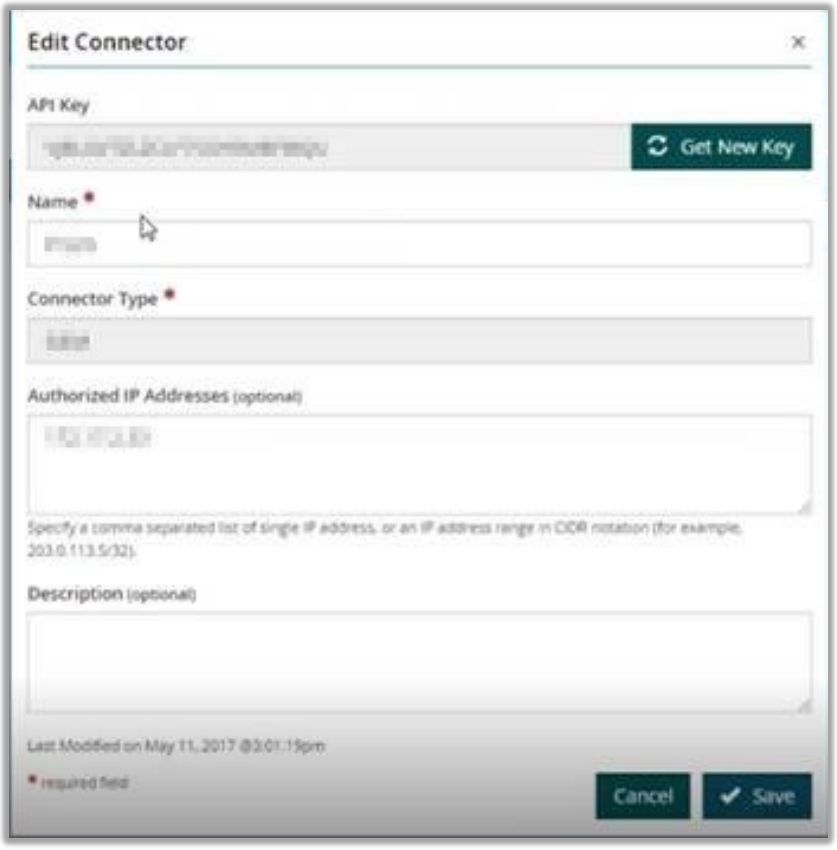
Before you create your API Key, you need to create a **Custom** Access Level.

1. Login into your Carbon Black Cloud console using admin account.
2. Navigate to **Settings > API Access > Access Levels tab**.
    - For the category **Search > Events > "org.search.events"**, allow permission to CREATE to start a job, and READ to get results. **Category: Search > Permission: org.search.events**.

3.2 Collecting API ID and KEY

In your Carbon Black Cloud console,

1. Navigate to **Settings > API Access > API Keys tab**.
2. Define a new connector and note down its **API ID** and **API SECRET.**
3. Use an appropriate name for the connector.
4. Use the Access Level Type of **Custom**, then select the **Access Level** you created in previous step.
5. Leave the **Authorized IP address** blank.



3.3 Collecting API hostname

This is the URL of your Carbon Black Cloud console (This is the Dashboard URL).

E.g., defense-eap01.conferdeploy.net

3.4 Collecting Org Key

You can find your '**org_key**' in the Carbon Black Cloud Console.

1. Login to your Carbon Black Cloud console, Navigate to **Settings > API Access**.
   Note: It is an 8-digit alpha-numeric value, e.g., ABCD1234.

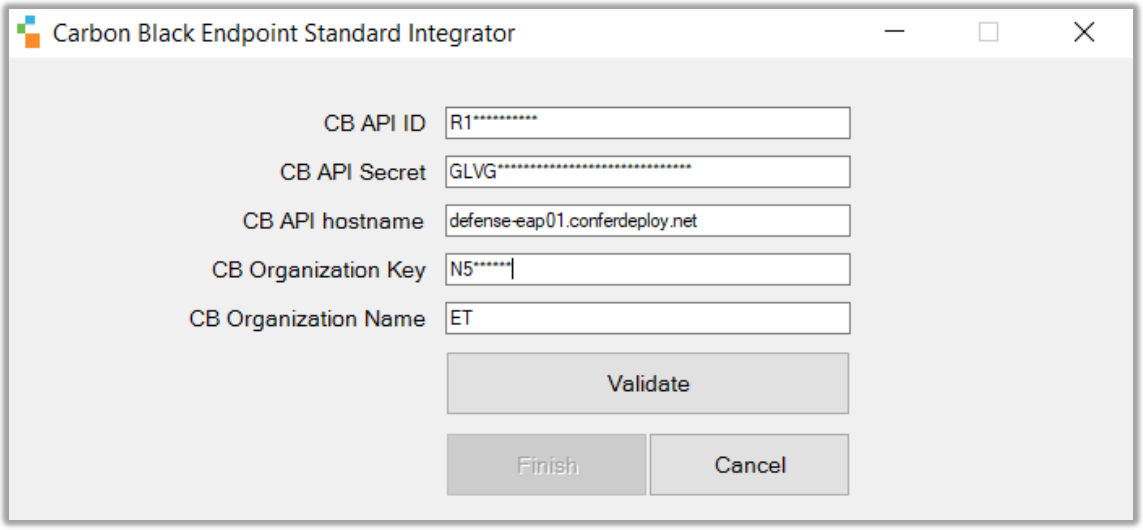
3.5 Configuring EventTracker Application to receive logs from Carbon Black Endpoint Standard

1. Get the Carbon Black Cloud Endpoint Standard Integrator executable file:

   https://downloads.eventtracker.com/kp-integrator/CBDefenseIntegrator.exe

2. Once the executable application is received, right click on the file, and select **Run as Administrator**.
3. In the dialog box, enter the required value as given below: (as collected from previous steps)
   a. **CB API ID**.
   b. **CB API SECRET**.
   c. **CB API Hostname**.
   d. **CB Organization Key**.

e. **CB Organization Name**. (Name of your company or organization).



4. Once you have filled all the required details, click on **Validate** button to check if credentials are working or not.
5. If successful, click on **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 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
713-929-0200

https://www.netsurion.com/company/contact-us