

How-To Guide

Configuring Carbon Black Protection to Forward Logs to EventTracker

EventTracker v9.2 and later

Publication Date:

April 5, 2021



Abstract

This guide helps you in configuring Carbon Black Protection with EventTracker to receive Carbon Black Protection events. In this guide, you will find the detailed procedures required for monitoring Carbon Black Protection.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 and later, Carbon Black Protection Application Control for Servers & Critical Systems .

Audience

Administrators who are assigned the task to monitor and manage Carbon Black Protection events using EventTracker.

Table of Contents

1.	Overview	4
2.	Prerequisites	4
3.	Integrating Carbon Black Protection events to EventTracker server	4
4.	Verifying Carbon Black Protection Integration in EventTracker	7
	About Netsurion	10
	Contact Us	10

1. Overview

Carbon Black Protection (Carbon Black Protection), formerly Bit9, is an application control product that allows departments to monitor and control application execution on systems. The best aspect of Carbon Black Protection is its ability to hash out and quickly locate executables on all work stations and servers.

EventTracker integrates to Carbon Black Protection by logging through REST API and provides reports, knowledge objects and dashboards for all generated events. This helps largely in searching for and weeding out known-bad files and suspected-bad files from the network.

2. Prerequisites

- Carbon Black Protection must be deployed.
- Contact support to get the Hostname associated with your Carbon Black Protection API backend.

3. Integrating Carbon Black Protection events to EventTracker server

EventTracker utilizes Carbon Black Protection API to fetch events from Carbon Black Protection console in CSV format. The Carbon Black Protection API is accessible through a special hostname assigned to your organization. Authentication is handled by an API token, which is generated from the administration section of the Carbon Black Protection console.

API configuration for Carbon Black Protection API is explained below:

1. Log into the console as an administrator.

	📄 tesla 🔹	Home -	Reports •	Assets •	Rules -	Tools 🕶		Alerts: 🗜	۲	0	admin v
ADMINISTRATION O	Home + Configuration	- Configuration - Unit	fied Management					Verbi	on 8.0.0.1934		
Login Accounts Users	System Co	nfiguration									0
User Roles System Configuration	General Events	Security Advanced	Options Mail Lice	using External Ana	lytica Connectora	Unified Manageme	ent		_	_	
General Events	Unified Manag	gement Configura	tion								0
Security Advanced Options	Unit	ied Management	Enabled		e.						
Mai	Servers										
Licensing External Analytics		tesla (local)			denali			avantime			
Connectors Connectors	c	1/1 ormected/Total Comput	**		1/1 Connected/Total Com	puters	3	1/1 Connected/Total Computers			
Management System Health	Con	100% rected Computers Up To	Dete	0	100%	p To Date	Car	100% mected Computers Up To Date			
		15ms Current Response Time 03/29/2017 1:15 PM	0		31ms Current Response T (03/29/2017 1:15	ime PM)		62ms Current Response Time (03/29/2017 1:15 PM)			
		8.0.0.1954 Proper/heale			8.0.0.1934 https://denail			8.0.5.1954 https://avartime			
	Please click	on Edit button to r	make changes to	this configuration	n.						
	Please click	6.0.8.1934 https://tes/a	make changes to	this configuration	8.0.0.1954 https://denail			8.0.01954 https://austrine			

2. Select Administration -> Login Accounts.

3. Find the user in the list then click the **Edit** button on the left-hand side of the row containing their username.

API		
API Token:	Show API token E3C68C1F-9132-4C64-A018-BD586F958315	Generate Clear

- 4. This will show the details for the selected user. At the bottom of the details page, click the checkbox next to **Show API Token** in the API section. This will reveal the API token associated with the given user. If no API token is revealed, click the **Generate** button. If a new API token was created, it must be saved with the **Save** button before it becomes active.
- 5. Note down the API Token generated.

Following are the steps to integrate Carbon Black Protection to EventTracker:

- Contact the EventTracker support team for obtaining Carbon Black Protection Integrator pack.
- The Integrator package will be obtained in a Zip file format, extract the files to get the below file contents as shown in the image.

Name	Date modified	Туре	Size
📙 lcon	7/7/2017 11:02 AM	File folder	
CBForm.ps1	7/6/2017 6:35 PM	Windows PowerS	25 KB
CBScript.bat	7/6/2017 5:44 PM	Windows Batch File	1 KB
CBScript.ps1	7/6/2017 6:35 PM	Windows PowerS	16 KB

1. Double-click on the CARBON BLACKScript.bat to initialize configuration.

Carbon Black Integrator configuration window will pop-up.

CB Integrator		\times
API Token		
API HostName	api5.confer.net	
	OK Cancel	,

2. In the Carbon Black Integrator configuration window, enter the following details:



- API Token Enter the API key of the configured user.
- API HostName Enter the API backend hostname.
- 3. Click **OK** to proceed.
- 4. Enter an appropriate schedule period. It is prescribed to keep it Daily.

Please select a	a task schedu	ler trigger	period		
Hourly		_			
Daily					
Weekly					
Monthly					

- 5. Click **OK** to proceed.
- 6. Enter admin credentials for scheduling the task.



7. Click OK to proceed.

Successful configuration pop-up message is shown.



8. Click **OK** to exit Carbon Black Integrator configuration.



4. Verifying Carbon Black Protection Integration in EventTracker

- 1. Launch the EventTracker Manger.
- 2. Select Manager under Admin drop-down.

			🔎 Admin-
	Active Watch Lists	🖉 Eventvault	MITRE ATT&CK Rules
	Alerts	FAQ Tile Configuration	😥 Parsing Rules
	Casebook Configuration	Group Management	Report Settings
	● Category	🔍 IP Lookup Configuration	Systems
ial Insider Threats ated, promoted to admin. a	Collection Master	🔆 Knowledge Objects	🙊 Users
	© Correlation	M Machine Learning Jobs	r Weights
	A Diagnostics	🇞 Machine Learning Settings	
0	Event Filters	💇 Manager	

3. Go to the **Direct Log Archiver** tab and check if the configurations are replicated as shown below:

MANAGER	CO	NFIGURATIO	N					
CONFIGURATION	syslo	g / VIRTUAL COLLECTI	ON POINT	DIRECT LOG	ARCHIVER / N	ETFLOW RECEIVER	AGENT SETTIN	IGS
E-MAIL CONFIGURA	TION	STATUSTRACKER	COLLECTI	ON MASTER PO	RTS NEWS	S		
Direct log file a Purge files after	rchiving fr	rom external sources ays	Maximum file	es per cycle 0		Global virtual (collection point 14	505 🗸
LOG FILE FOLDER			CONFIGURATI	ON NAME	LOG FILE EXTENS	SION VCP PORT	FIELD SEPARATOR	LOG TYPE
	H L L L L L L L L L L L L L L L L L L L	mp\CB Output	СВ		CSV	GLUBAL		
							ADD	EDIT REMOVE



4. Select Carbon Black Protection integrator DLA configuration and click **Edit** to verify DLA configuration further.

Direct Archiver Configuratio	n	3
		^
Туре	Others	
Logfile Extension	csv 2	
Configuration Name	СВ	
Log File Folder	CI/Joerni/Jurnamitech/JoeliCapi(CI BROWSE	
Use global virtual colle	tion point port for configuration	
VCP Port No	~	
	Single Line O Multi Line	
Field Separator	Others 🗸	
Separator	•	
Starting Line Offset	0	
Extract field names from header		
		~

5. Verify configured settings and click **Configure** to proceed.

Computer Name Computer IP System Type Unknown System Description Comment Line Token Entire Row as Description Log File Format Message Fields Select Event Date and Time Fields No of Fields CB Protection GET IP GET IP GET IP System Description Custom Log File Format ADD eventTime REMOVE Select Column Mapping No of Fields	Log Source	2	
Computer IP 0.0.0.0 System Type Unknown System Description Comment Line Token Entire Row as Description Log File Format Message Fields Select Event Date and Time Fields Select Event Date and Time Fields Select Column Mapping No of Fields 1	Computer Name	CB Protection	
System Type Unknown System Description Comment Line Token Comment Line Token Comment Line Token Custom Log File Format Custom	Computer IP	0.0.0.0 GET IP	
System Description Comment Line Token Comment Line Token Centire Row as Description Log File Format Custom Log File Format Custom Log File Format ADD eventTime REMOVE Select Event Date and Time Fields Select Date Time Format Fields Select Column Mapping No of Fields 1 Format Value AUTO Computer Custom Log Computer	System Type	Unknown	
Comment Line Token Centire Row as Description Log File Format Message Fields Select Event Date and Time Fields No of Fields 1 Format Value AUTO Computer Commutation Custom Log File Format ADD Custom Log File Format ADD Custom Log File Format Custom Log File Custom Lo	System Description		
Centire Row as Description Log File Format Custom Log File Format Custom Log File Format Custom Log File Format ADD eventTime REMOVE Select Event Date and Time Fields Select Date Time Format Fields Select Column Mapping No of Fields 1 Format Value AUTO Computer	Comment Line Token		
Log File Format Custom Log File Format ADD eventTime REMOVE Select Event Date and Time Fields Select Date Time Format Fields Select Column Mapping No of Fields 1 Format Value AUTO Computer Computer	O Entire Row as Description	Formatted Description	
Message Fields ADD event Time REMOVE Select Event Date and Time Fields Select Column Mapping No of Fields 1 Format Value AUTO O computer V	Log File Format	Custom Log File Format 🗸 🗸	
Select Event Date and Time Fields Select Date Time Format Fields Select Column Mapping No of Fields 1 ✓ Format Value AUTO ① Computer ✓	Message Fields	eventTime ADD REMOVE	
No of Fields 1 Y Format Value AUTO Y i Computer Y	Select Event Date and Time Fields	Select Date Time Format Fields Select Column Mapping	
Date Field event Time	No of Fields 1	Format Value AUTO 💙 🚺 Computer	~

- 6. Verify configured settings and click Cancel if settings are correct.
- 7. Go to Start and open Task Scheduler to verify Carbon BlackProtection Logging scheduled task.

🕑 Task Scheduler				
File Action View Help				
🗢 🄿 🖄 📰 🚺				
Task Scheduler (Local) Task Scheduler Library	Name	Status	Triggers	Next Run Ti ^
> Microsoft	🕒 ActiveSync Reporting	Disabled	At 5:08 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	10/22/2017
MvSOL	🕒 Adobe Flash Player Updater	Disabled	At 5:55 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	10/22/2017
Symantec Endpoint Pi	🕒 AWS Logging	Disabled	At 6:23 PM every day	10/22/2017
	🕒 CBDefense Logging	Disabled	At 2:10 PM every day	10/22/2017
	🕒 CbProtection Logging	Ready	At 10:33 AM every day	10/23/2017
	🕒 CCleanerSkipUAC	Disabled		
	Citrix VPN GeoLocation	Disabled	At 5:49 PM every day	10/22/2017
	EventTracker-Attackers	Disabled	At 11:55 AM every day	10/22/2017
	EventTracker-DShieldOrgBlockedIPList	Disabled	At 11:55 AM every day	10/22/2017
	C	Distance	As 11.55 ANA	±0/10/17 ¥

- Adjust task trigger schedule for the task as per your requirement.
- If task is altered, save it with admin credentials.



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 <u>EventTracker</u> 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 <u>BranchSDO</u> 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 <u>netsurion.com</u> or follow us on <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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