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

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 workstations 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

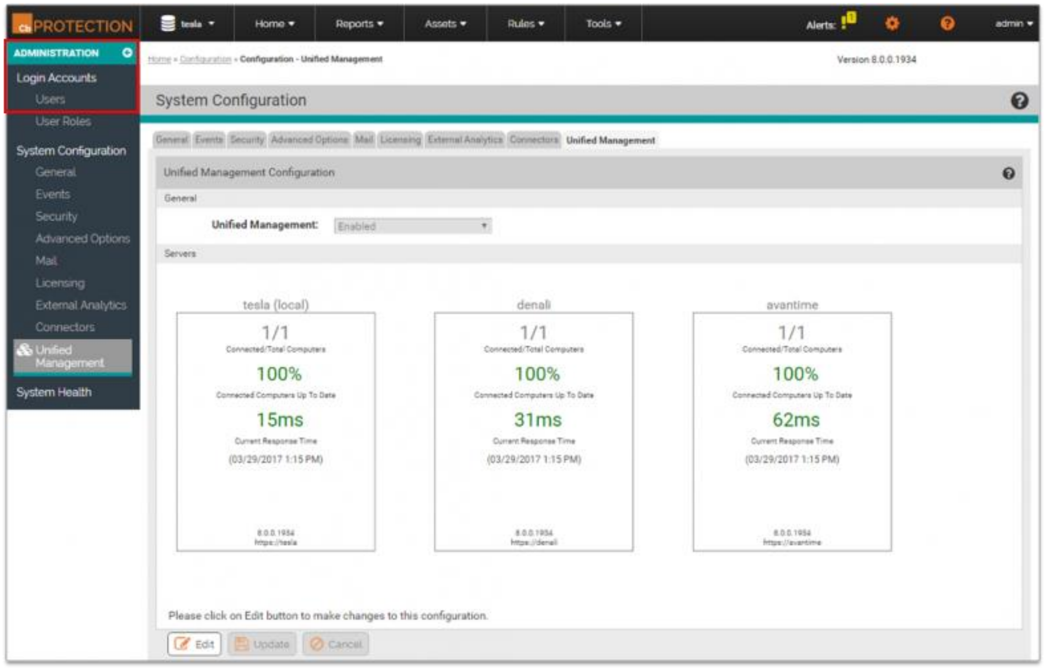
- Carbon Black Protection must be deployed.
- Contact support to get the Hostname associated with your Carbon Black Protection API backend.

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:

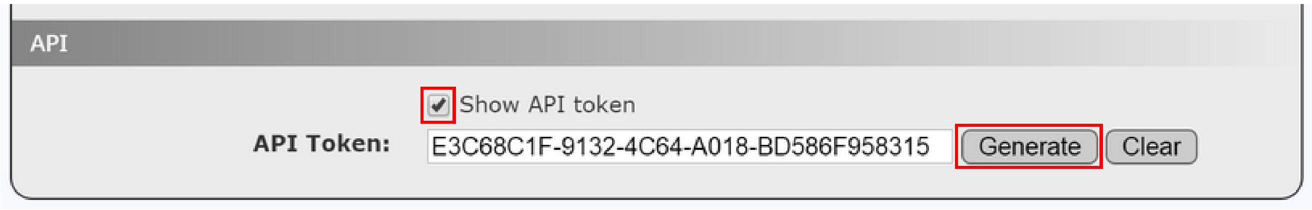
1. Log into the console as an administrator.



Unified Management: Enabled

Please click on Edit button to make changes to this configuration.

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

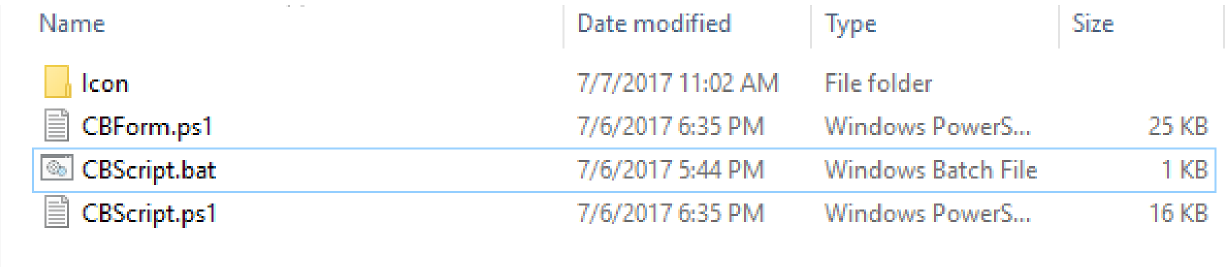
☑ Show API token

API Token: E3C68C1F-9132-4C64-A018-BD586F958315

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:

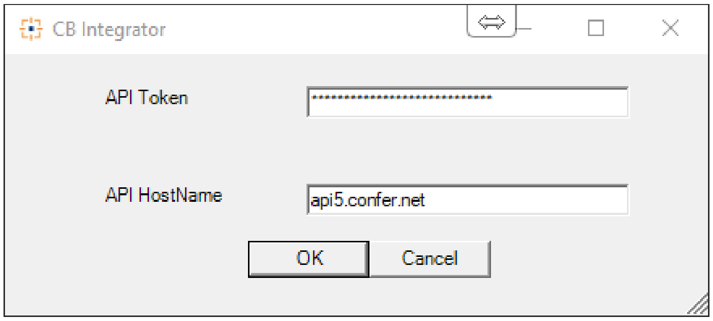
- Contact the EventTracker support team for obtaining Carbon Black Protection Integrator pack.
- The Integrator package will be obtained in a Zip file format, extract the files to get the below file contents as shown in the image.



Name	Date modified	Type	Size
Icon	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

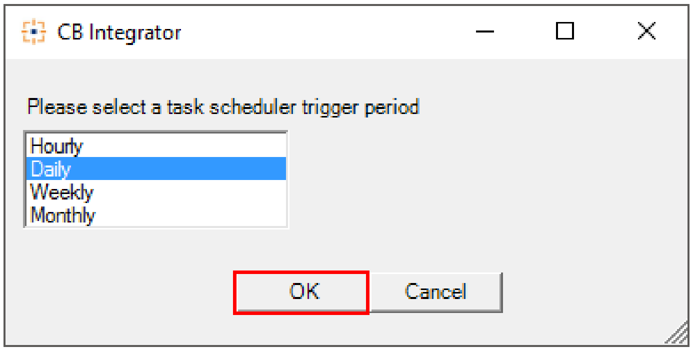
API Token: ******************************

API HostName: api5.confer.net

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.

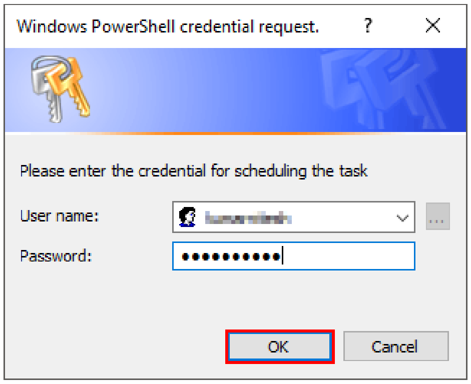
3. Click **OK** to proceed.
4. Enter an appropriate schedule period. It is prescribed to keep it Daily.



Please select a task scheduler trigger period

Hourly
Daily
Weekly
Monthly

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



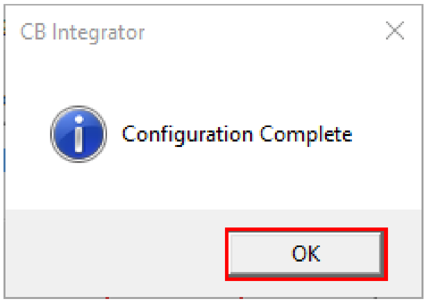
Please enter the credential for scheduling the task

User name: [redacted]

Password: ••••••••••

7. Click OK to proceed.

Successful configuration pop-up message is shown.



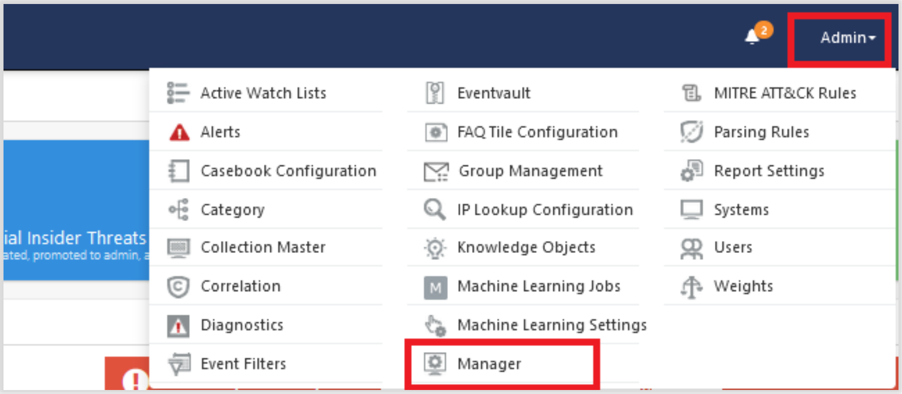
Configuration Complete

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

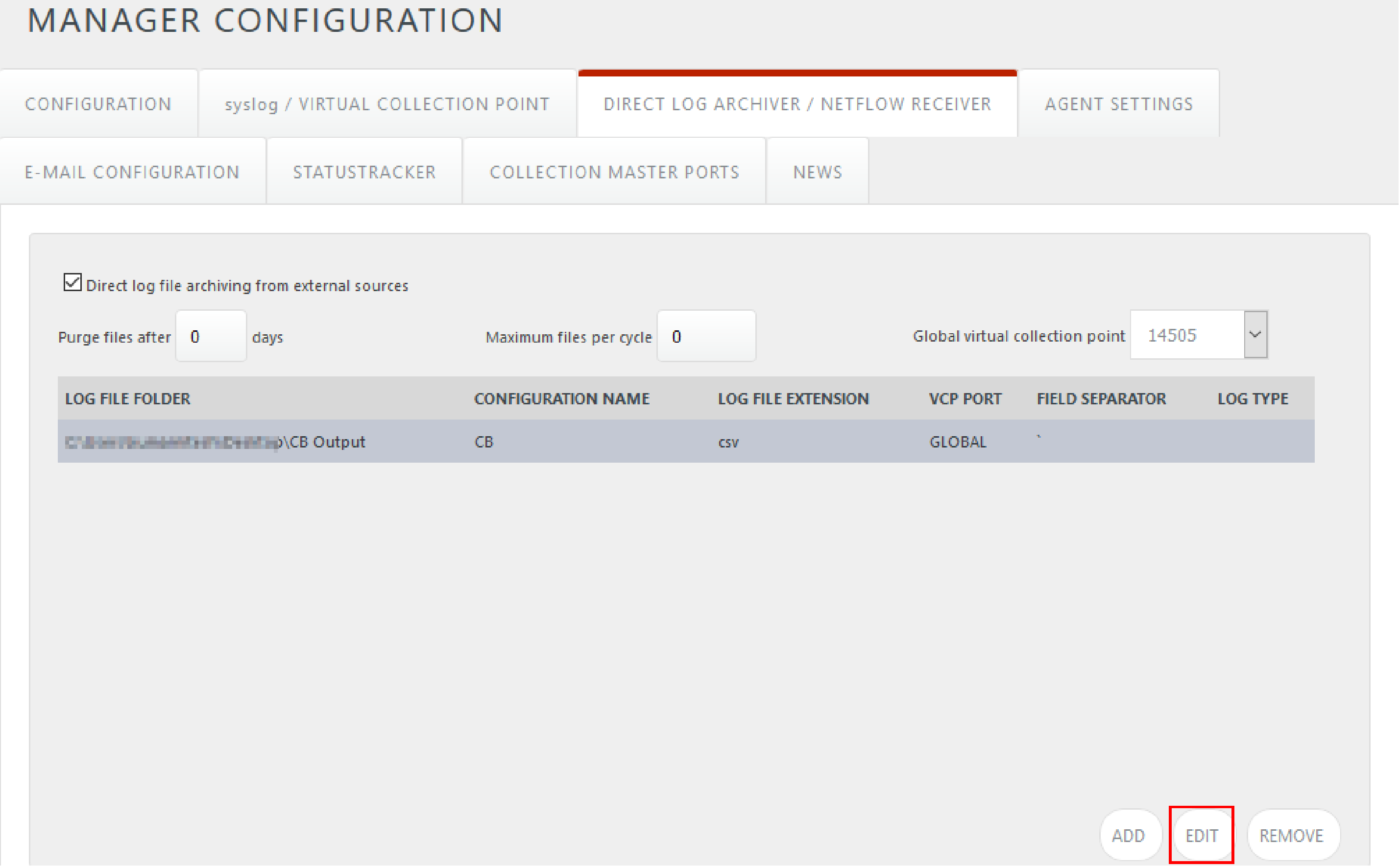
4. Verifying Carbon Black Protection Integration in EventTracker

1. Launch the EventTracker Manger.

2. Select Manager under Admin drop-down.



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



☑ Direct log file archiving from external sources

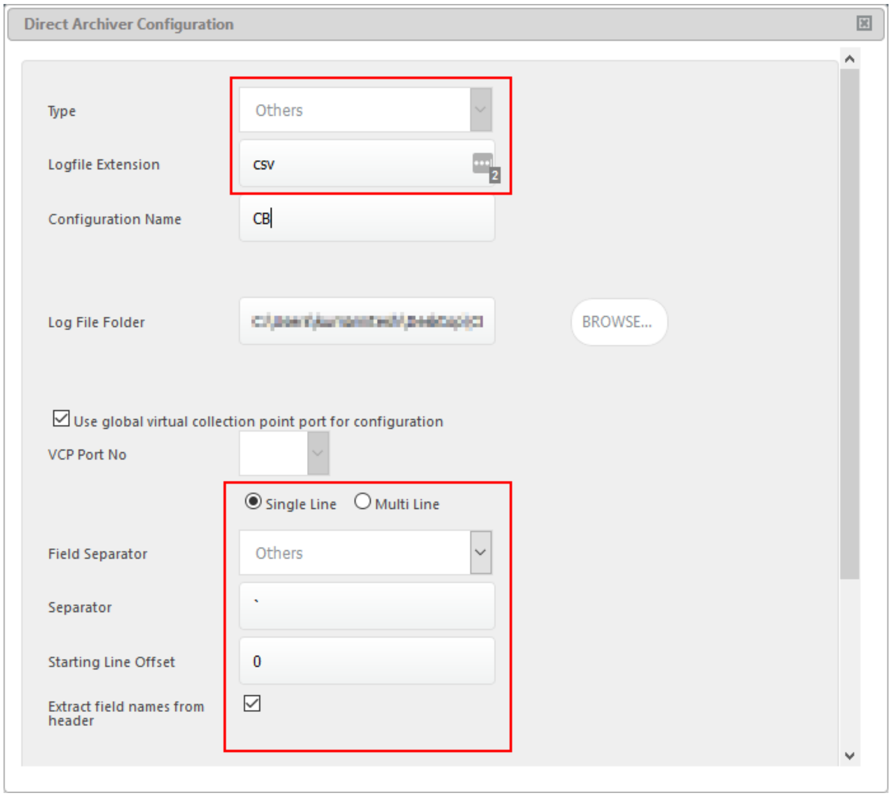
Purge files after 0 days

Maximum files per cycle 0

Global virtual collection point 14505

LOG FILE FOLDER	CONFIGURATION NAME	LOG FILE EXTENSION	VCP PORT	FIELD SEPARATOR	LOG TYPE
[redacted]\CB Output	CB	csv	GLOBAL	`	

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



Direct Archiver Configuration

Type: Others

Logfile Extension: csv

Configuration Name: CB

Log File Folder: [redacted]

☑ Use global virtual collection point port for configuration

VCP Port No:

● Single Line ○ Multi Line

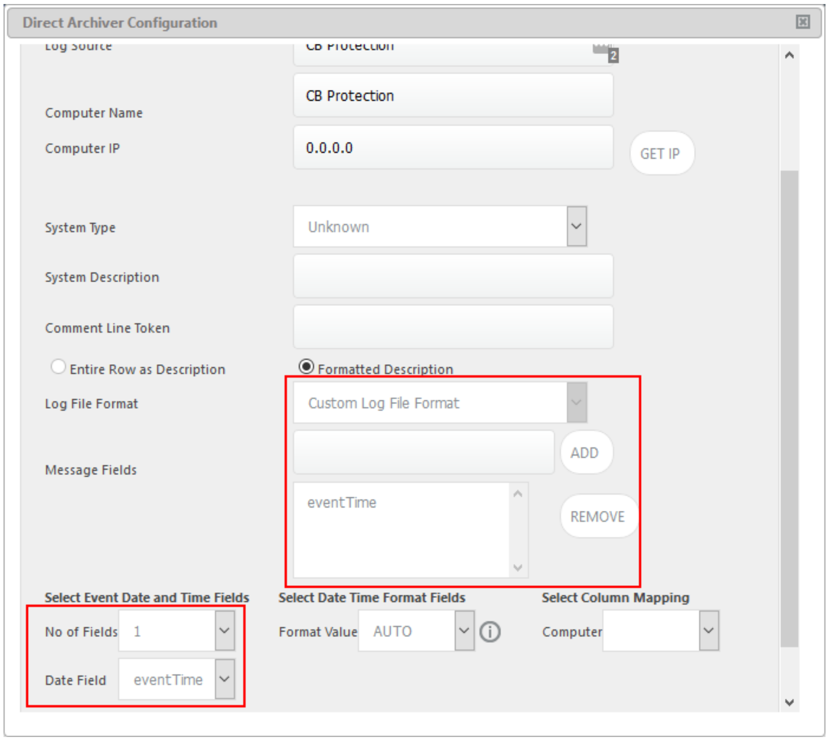
Field Separator: Others

Separator: `

Starting Line Offset: 0

Extract field names from header: ☑

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



Direct Archiver Configuration

Log Source: CB Protection

Computer Name: CB Protection

Computer IP: 0.0.0.0

System Type: Unknown

System Description:

Comment Line Token:

○ Entire Row as Description ● Formatted Description

Log File Format: Custom Log File Format

Message Fields: eventTime

Select Event Date and Time Fields

No of Fields: 1

Date Field: eventTime

Select Date Time Format Fields

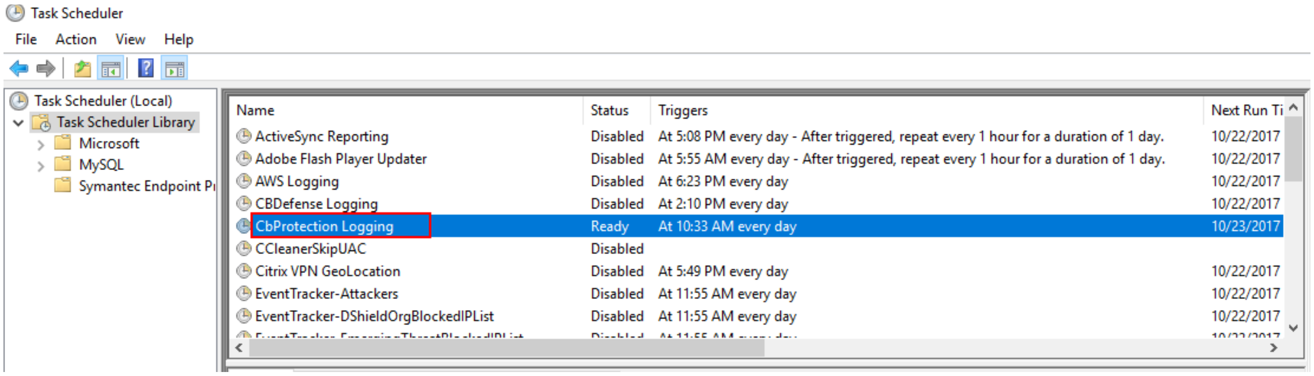
Format Value: AUTO

Select Column Mapping

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.



Name	Status	Triggers	Next Run Ti
ActiveSync Reporting	Disabled	At 5:08 PM every day - After triggered, repeat every 1 hour for a duration of 1 day.	10/22/2017
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
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
EventTracker-EmergingThreatBlockedIPList	Disabled	At 11:55 AM every day	10/22/2017

- 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 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