How-To Guide

Configure InQuest to forward logs to EventTracker

Publication Date:

June 17, 2022

Abstract

This guide provides instructions to retrieve events from different InQuest detection engines and forward the logs to the EventTracker via the syslog extension.

Scope

The configuration details in this guide are consistent with InQuest Manager versions 3.87.x or later and EventTracker version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring the InQuest events to forward logs to EventTracker.

Table of Contents

1 Overview

InQuest focuses its analysis on identifying, processing, and inspecting files downloaded over the web or received via email to detect malicious code in transit. In addition to threat detection, InQuest encounters sensitive data in motion like confidential documents and personally identifiable information.

Netsurion facilitates monitoring events retrieved from the InQuest. The dashboard, category, alerts, and reports in Netsurion’s threat protection platform, EventTracker, will benefit you in tracking possible attacks, suspicious activities, or any other threat noticed.

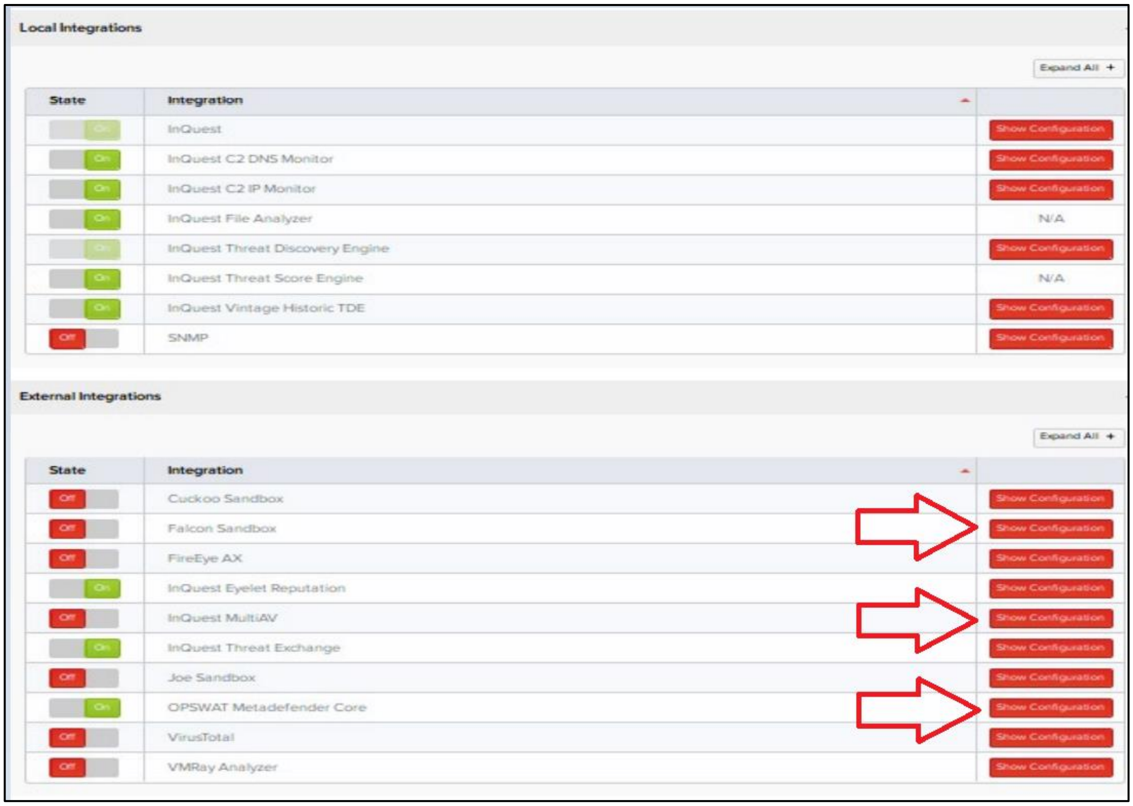
2 Prerequisites

- Admin access to the InQuest Manager console.
- InQuest Manager versions 3.87.x or later must be configured which supports CEF syslog messages.

3 Configure InQuest to send logs via syslog

Perform the following steps to forward logs via syslog to EventTracker.

1. Log in to the **InQuest Manager** console and go to the **Administration** > **Devices** interface.
2. In the **Local Integrations** section, click the **Show Configuration** button of each device to view the configuration details.
3. Click **Add property** to add the EventTracker Manager details.



Local Integrations

State	Integration	
On	InQuest	Show Configuration
On	InQuest C2 DNS Monitor	Show Configuration
On	InQuest C2 IP Monitor	Show Configuration
On	InQuest File Analyzer	N/A
On	InQuest Threat Discovery Engine	Show Configuration
On	InQuest Threat Score Engine	N/A
On	InQuest Vintage Historic TDE	Show Configuration
Off	SNMP	Show Configuration

External Integrations

State	Integration	
Off	Cuckoo Sandbox	Show Configuration
Off	Falcon Sandbox	Show Configuration
Off	FireEye AX	Show Configuration
On	InQuest Eyelet Reputation	Show Configuration
Off	InQuest MultiAV	Show Configuration
On	InQuest Threat Exchange	Show Configuration
Off	Joe Sandbox	Show Configuration
On	OPSWAT Metadefender Core	Show Configuration
Off	VirusTotal	Show Configuration
Off	VMRay Analyzer	Show Configuration

Note

Make sure the state of each InQuest device is set to **ON.**

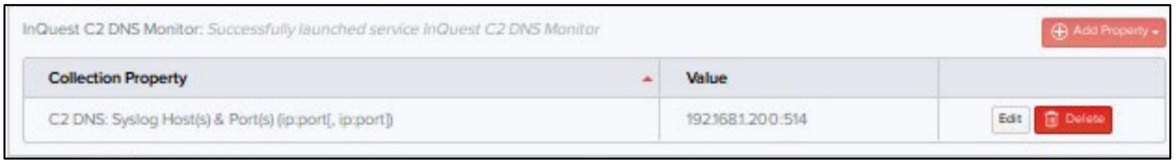
Note

Each InQuest device needs to be separately configured to forward logs to EventTracker.

4. Each InQuest device has a property named Syslog Host(s) and Port(s).

5. Specify the IP address and port number of the EventTracker Manager to which you want to send the InQuest logs.

6. The **Collection Property** of each InQuest device will display the integrated EventTracker Manager details**.**



InQuest C2 DNS Monitor: *Successfully launched service InQuest C2 DNS Monitor*

Collection Property	Value	
C2 DNS: Syslog Host(s) & Port(s) (ip:port[, ip:port])	192.168.1.200:514	Edit Delete

7. Repeat the same process if you want to integrate the InQuest device logs of the **External Integrations** section.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both. Netsurion Managed Threat Protection combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion Secure Edge Networking delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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.

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 MSPs 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