How-To Guide

Configuring Bitdefender GravityZone (On-premises) to Forward Logs to EventTracker

EventTracker v9.2x and above

Publication Date:

August 27, 2021

Abstract

This guide provides instructions to configure Bitdefender GravityZone to forward Bitdefender GravityZone logs via syslog.

Scope

The configurations detailed in this guide are consistent with EventTracker version v9. 2x or above and Bitdefender GravityZone (on-prem) v6.5 to 7.0.

Audience

Administrators who are assigned the task to monitor Bitdefender GravityZone events using EventTracker.

Table of Contents

Table of Contents 3

1. Overview 4

2. Prerequisites..4

3. Configuring Bitdefender GravityZone (On-prem) 4

About Netsurion 6

1. Overview

Bitdefender GravityZone is the new Bitdefender enterprise security solution for medium to large Organizations. GravityZone leverages Bitdefender's acclaimed anti-malware technologies, and provides a centralized security management platform for physical, virtualized, and mobile endpoints.

Bitdefender GravityZone logs configuration can be achieved via syslog. It will send logs like user activities, website activities, application activities, license activities, data backup activities, firewall activities, and malware activities. With these events, EventTracker generates detailed reports for user logon activities, firewall activities, application activities, malware details, etc. Its graphical representation shows top malware file names, malicious websites by device name, user login failed, malware detected by IP, malware detected by device name, top policy names, action taken on malware, etc. It will generate alerts whenever the user login fails, malware has been detected, an application has been blocked, etc.

2. Prerequisites

- **Admin** access to **Bitdefender GravityZone** (on-prem) console.

3. Configuring Bitdefender GravityZone (On-prem)

Note: Bitdefender GravityZone supports the syslog option from v6.50 to 7.0.

Following are the steps to configure Bitdefender Gravityzone (On-premises) to send logs to EventTracker.

1. Log in to GravityZone Control center.
2. Click on **Configuration** > **Miscellaneous.**
3. Put the flag on **Enable Syslog** and write the IP of EventTracker.
4. Enter EventTracker port and select protocol TCP.

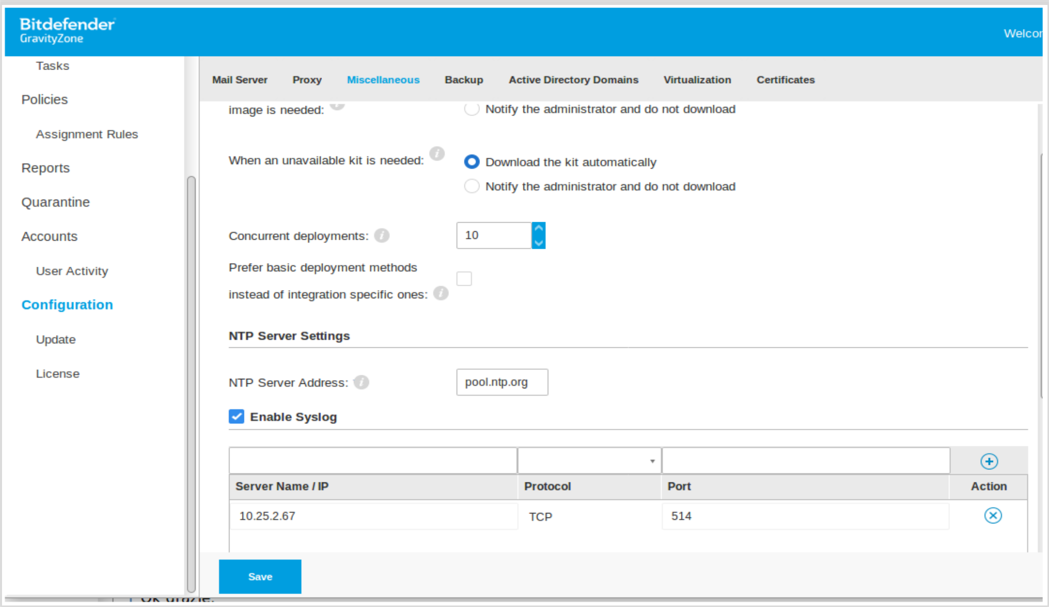


image is needed: ○ Notify the administrator and do not download

When an unavailable kit is needed: ● Download the kit automatically ○ Notify the administrator and do not download

Concurrent deployments: 10

Prefer basic deployment methods instead of integration specific ones: □

NTP Server Settings

NTP Server Address: pool.ntp.org

☑ Enable Syslog

Server Name / IP	Protocol	Port	Action
10.25.2.67	TCP	514	⊗

5. Click on the configuration button (the rowel) in the top-right corner.

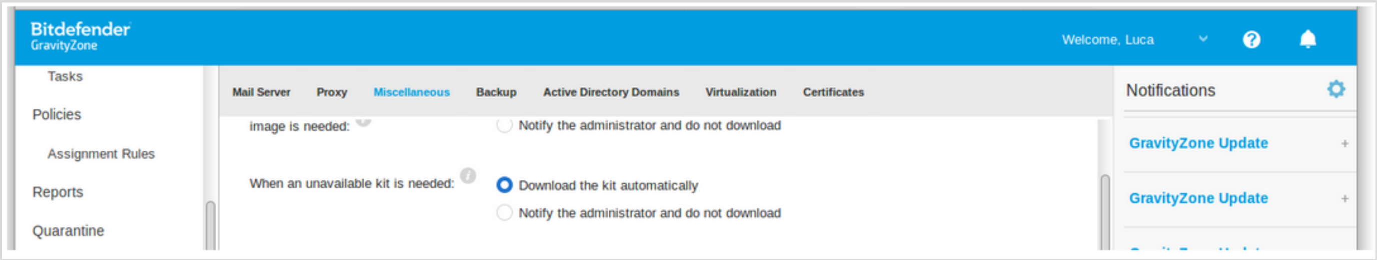
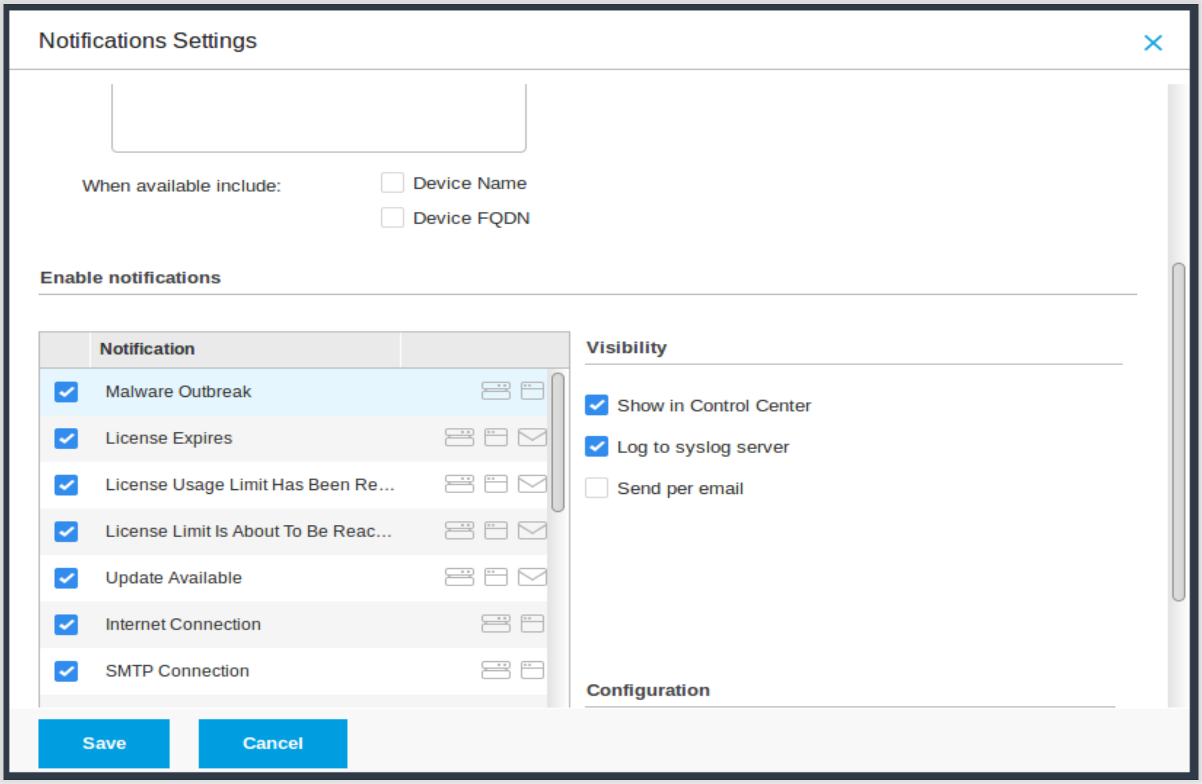


image is needed: ○ Notify the administrator and do not download

When an unavailable kit is needed: ● Download the kit automatically
○ Notify the administrator and do not download

6. Select log format as JSON.
7. Define the events you want to send to EventTracker.



When available include: □ Device Name
□ Device FQDN

Enable notifications

	Notification
☑	Malware Outbreak
☑	License Expires
☑	License Usage Limit Has Been Re...
☑	License Limit Is About To Be Reac...
☑	Update Available
☑	Internet Connection
☑	SMTP Connection

Visibility

☑ Show in Control Center
☑ Log to syslog server
□ Send per email

Configuration

8. Click on Save.

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, end protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service.

Netsurion's Branch SDO 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