

Integration Guide

Integrating Bitdefender GravityZone (Onpremises)

EventTracker v9.2x and above

Publication Date:

August 27, 2021

© Copyright Netsurion. All Rights Reserved.



Abstract

This guide provides instructions to configure a Bitdefender GravityZone to send its syslog to EventTracker.

Scope

The configuration details 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

Ta	able of	Contents3
1.	Ove	rview4
2.	Prei	equisites4
3.	Con	figuring Bitdefender GravityZone (On-prem)4
4.	Eve	ntTracker Knowledge Pack6
	4.1	Categories6
	4.2	Alerts6
	4.3	Reports
	4.4	Dashboards8
5.	Imp	orting Bitdefender GravityZone Knowledge Pack into EventTracker
	5.1	Categories11
	5.2	Alerts
	5.3	Reports
	5.4	Knowledge Object14
	5.5	Dashboard15
6.	Veri	fying Bitdefender GravityZone Knowledge Pack in EventTracker
	6.1	Categories16
	6.2	Alerts
	6.3	Knowledge Objects17
	6.4	Reports
	6.5	Dashboard18
	About	Netsurion



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-premise) 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.

Tasks	Mail Server Proxy Miscellaneous Backup Active Directory Domains Virtualization Certificates
Policies	image is needed: " Notify the administrator and do not download
Assignment Rules	
Reports	When an unavailable kit is needed: O Download the kit automatically
Duarantine	Notify the administrator and do not download
	Concurrent deployments:
User Activity	
configuration	instead of integration specific ones:
Update	NTP Server Settings
License	NTP Server Address: 0 pool.ntp.org
License	NTP Server Address: pool.ntp.org Finable Systog
License	NTP Server Address: pool.ntp.org Fnable Syslog
License	NTP Server Address: pool.ntp.org Fnable Syslog
License	NTP Server Address: pool.ntp.org Enable Systog Server Name / IP Protocol Port Activ
License	NTP Server Address: pool.ntp.org Enable Systog Server Name / IP Protocol Port Activ 10.252.67 TCP 514
License	NTP Server Address: pool.ntp.org Enable Systog Server Name / IP Protocol Port Activ 10.252.67 TCP 514

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

Bitdefender GravityZone		Welcome	, Luca 🗸 (0 🌲
Tasks	Mail Server Proxy Miscellaneous Backup Active Directory Domains Virtualization Certificates		Notifications	0
Assignment Rules	image is needed: " Notify the administrator and do not download		GravityZone Upd	late +
Reports	When an unavailable kit is needed: O Download the kit automatically Notify the administrator and do not download		GravityZone Upd	late +
Quarantine				

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



Notifications Settings			×
When available include:	Device Name Device FQDN		
Notification		Visibility	
Malware Outbreak	= = 1	Show in Control Center	
License Expires		✓ Log to syslog server	
License Usage Limit Has Been Re		Send per email	
License Limit Is About To Be Reac			
Update Available			
Internet Connection	=		
SMTP Connection		Configuration	
Save Cancel			

8. Click on Save.

4. EventTracker Knowledge Pack

After logs are received by EventTracker, Knowledge Packs can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker to support **Bitdefender GravityZone**.

4.1 Categories

- **Bitdefender GravityZone: Suspicious application activities** This category provides information related to the suspicious activities by blocked applications and their attributes.
- **Bitdefender GravityZone: Portscan blocked** This category provides information related to the portscan performed on their networks and it's been blocked.

4.2 Alerts

- **Bitdefender GravityZone: Application suspicious activities have been detected** This alert will generate whenever an application launches malicious activity.
- **Bitdefender Gravityzone: Portscan has been blocked** This alert will generate whenever port scan has been detected on their networks.

4.3 Reports

• **Bitdefender GravityZone : Suspicious application activities** – This report gives information about the blocked application and its attributes. It contains field information like destination IP, source IP, exploit type, exploits path, process id, process path, and status.



L	ogTime	Computer	Destination IP	HostName	Host FQDN	Exploit Type	Exploit Path	Parent Process ID	Parent Process Path	Status
08	8/23/2021 01:29:02 PM	BITD_GZ	10.10.10.91	BG0014556	bg0014556.bdgz.ca.gov	AVC APP	C:\\Windows\\System32\\Windows PowerShell\v1.0\\powershell.exe	C:\\Windows\\System32\\Runtime Broker.exe	C:\\Windows\\System32\\Runtime Broker.exe	avc_blocked
08	8/23/2021 01:29:02 PM	BITD_GZ	10.20.210.29	BG0014556	bg0014556.bfgza.ca.gov	AVC APP	C:\\Windows\\System32\\Windows PowerShell\\v1.0\\powershell.exe	C:\\Windows\\System32\\vine.exe	C:\\Windows\\System32\\vine.exe	avc_blocked

Sample logs:

Aug 09 12:37:41 bdgz11 Aug 9 19:37:41 BDGZ11 gravityzone: [avc]
{"module":"avc","product_installed":"BEST","user":{"id":"S-1-5-21-12144403391637723038-72534554317088","name":"HelpJH@HF"},"computer_name":"BG0014556","computer_fqdn":"bg001455
6.bdgza.ca.gov","computer_ip":"10.10.20.219","computer_id":"5db0853292c3a0555d15
41e2","exploit_type":"AVC
APP","exploit_path":"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.
exe","parent_process_id":9220,"parent_process_path":"C:\\Windows\\System32\\Runt
imeBroker.exe","status":"avc_blocked","last_blocked":"2021-0809T19:37:36.000Z","count":1}

 Bitdefender GravityZone – Portscan blocked – This report gives information about the networks that have been scanned. It contains fields information like source IP, destination IP, hostname, protocol, and status.

LogTime	Computer	Source IP	Destination IP	HostName	Host FQDN	Protocol ID	Status
08/23/2021 11:40:06 AM	BITD_GZ	10.10.1.19	192.168.12.139	BG0014673	bg0014673.bdgza.ca.g ov	6	portscan_blocked
08/23/2021 11:40:08 AM	BITD_GZ	10.10.1.18	192.168.12.139	BG0014673	bg0014673.bdgza.ca.g ov	6	portscan_blocked

Sample logs:

```
Aug 06 15:54:15 bdgz11 Aug 6 22:54:15 BDGZ11 gravityzone: [fw]
{"module":"fw","product_installed":"BEST","computer_name":"bg0014673","computer_
fqdn":"bg0014673.bdgza.ca.gov","computer_ip":"192.18.12.19","computer_id":"5e0e4
e86d48cf85bc5117a83","status":"portscan_blocked","protocol_id":"6","source_ip":"
10.23.10.19","last_blocked":"2021-08-06T22:54:09.000Z","count":1}
```



4.4 Dashboards

• Bitdefender GravityZone - Suspicious activities by exploit path



- BitDefender GravityZone Suspicious activities by pa...
- BitDefender GravityZone Suspicious activities by parent process path

• Bitdefender GravityZone - Module names





• Bitdefender GravityZone - Suspicious activities detected by hostname

• Bitdefender GravityZone - Porscan detected by destination IP



BitDefender GravityZone - Portscan detected by sour...

• Bitdefender GravityZone - Portscan detected by source IP

5. Importing Bitdefender GravityZone Knowledge Pack into

EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Knowledge Objects
- Flex Reports
- Dashboard
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.

EventTracker Con	trol Panel		EV	entTracker ()
EventVault	Diagnostics	License	Export Import	Append
		Manager	Utility	Archives
0 ⁰ 0		X	\mathbf{X}	
EventTracker Agent Confi	Traffic Analyzer	Agent Manageme	Port Configuration	TrapTracker
?	- 문급 -			
Change Audit	About EventTracker			
	E-mail: s	support@Event Tra	icker.com	

🐁 Export Import Utility	
Export Import	
1. Provide the path and file n 2. Click the Import button.	name of the Categories file. Use the '' button to
Options	Location
Category	

3. Click the **Import** tab.

5.1 Categories

- 1. After you have opened **Export Import Utility** via **EventTracker Control Panel**, click the **Category** option, and then click Browse .
- 2. Navigate to the Knowledge Pack folder and select the file with extension ".iscat", e.g., "Categories_Bitdefender GravityZone .iscat" and then click on the Import button.

2. Click the Import button.	ame of the Categories nie. Use the button to browse and locate the import nie.	
Options Category Filters	Location	
○ Alerts		
 Systems and Groups Token Value 	Source : *Jscat	
Reports Behavior Correlation		

EventTracker displays a success message:

Export Import Utility	×
Selected category details are imported successfully	
ОК	

5.2 Alerts

1. Click the **Alert** option, and then click the **Browse** button.

Click the Import button. Options Category	Location	
🗇 Filters	Import E-mail settings	
Alerts	Set Active Only if notifications set	This setting is applicable only for imports from Legacy
Systems and Groups	 By default 	based on "Active" key available in the configuration section.
RSS Feeds		
Reports	Source : *.isalt	
Behavior Rules		
SCAP		
🗇 Token Value		



- 2. Locate Alerts_Bitdefender GravityZone.isalt file, and then click the Open button.
- 3. To import alerts, click the **Import** button.
- 4. EventTracker displays a success message.



5. Click the OK button, and then click the Close button.

5.3 Reports

1. In EventTracker Control Panel, select **Export/ Import utility** and select the **Import tab**. Then, click **Reports** option, and choose **New (*.etcrx)**:

2. Click the Import button Note : If report(s) contains templa	te, first import template and proceed with exportimport utility.	
Options	Location	
 Filters 		
○ Alerts	Legacy (*.issch) New (*.etcnx)	
O Systems and Groups	Source :	
O Token Value		
Reports		

 Once you have selected New (*.etcrx), a new pop-up window appears. Click on the Select File button and navigate to the file path with a file having the extension ".etcrx", e.g., Reports_ Bitdefender GravityZone.etcrx.

단글 Reports In	nport							
Note : If repo	rt(s) contains tem	plate, first import te	mplate and procee	ed with report import proces	s.			
Select file	*.etcrx							Select file
Available repo	orts							
Title				Frequency Show all	•	Q Q		
		Title	Sites	Groups	Systems	Frequency	Runtime	Туре



3. Wait while reports are being populated in below tables. Now, select all the relevant reports and then click **Import b**utton.

Note: Set run time option is not applical	ole for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM ▼ at interval of minutes	Set
Replace	to Replace	Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

4. EventTracker displays a success message:

Export Import Utility	\times
Selected reports configurations are imported successfully	,
ОК	

5.4 Knowledge Object

1. Click **Knowledge objects** under the **Admin** option in the EventTracker page.

		🔎 Admin -	Tools 👻 📀
Active Watch Lists	Event Filters	😥 Parsing Rules	🔒 / Das
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	🙁 Users	
Casebook Configuration	Q IP Lookup Configuration	🕀 Weights	since the last 24 hours
Category	·☆ Knowledge Objects	Windows Agent Config	
▲ Diagnostics	Manager		

2. Click on the **import object** icon:



A pop-up box appears, click Browse in that and navigate to knowledge packs folder (type %et_install_path%\Knowledge Packs in navigation bar) with the extension ".etko", e.g., KO_BitdefenderGravityZone.etko and then click Upload.

🖀 Browse.	. Upload
	🚝 Browse.

4. List of available knowledge object will appear. Select the relevant files and click on **Import** button.



5.5 Dashboard

- 1. Login to **EventTracker**.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.



3. In My Dashboard, click on Import Button.



4. Select the browse button and navigate to Knowledge Pack folder (type %et_install_path%\Knowledge Packs in navigation bar) where .etwd, e.g., Dashboards_Bitdefender GravityZone .etwd is saved and click on Upload button.



5. Wait while EventTracker populates all the available dashboards. Now, choose **Select All** and click on **Import** button.

Note: If dashlet	configured using pe	rsisted report, first ir	mport the report and	l proceed with impor	ing dashlet.	
					🗁 Browse	Upload
Available wide	ets					
Select All						

6. Verifying Bitdefender GravityZone Knowledge Pack in

EventTracker

6.1 Categories

- 1. Login to **EventTracker**.
- 2. Click Admin dropdown, and then click Categories.
- 3. In **Category Tree** to view imported categories, scroll down and expand **Bitdefender GravityZone** group folder to view the imported categories.

ategory	
Category Tree Search	
bitdefender	Q Q
Category	
→ Bitdefender GravityZone: Application activities	5
✓ Bitdefender GravityZone: Portscan blocked	

6.2 Alerts

- 1. Login to **EventTracker**.
- 2. Click the Admin menu, and then click Alerts.

Netstrion

≡	Event Tracker ⊕					🔎 🗚 Admin-	Tools -
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dasht
a		_	Alerts	Correlation	🔍 IP Lookup Configuration	Q Users	
	0	2	Behavior Correlation Rules	Diagnostics	· Knowledge Objects	r Weights	
<u>~</u>			🇞 Behavior Correlation Settings	s ⊽ Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Unsafe connections or processes, new TCP entry point	Indicators of Cc USB activities, New sen	Casebook Configuration	Seventvault	🧭 Parsing Rules		
				FAQ Configuration	Report Settings		
	Attacker			- News			

Figure 31

3. In the **Search** box, type **Bitdefender GravityZone**, and then click the **Go** button. Alert Management page will display all the imported alerts.

Alerts									🏦 / Admin / Alerts
Show All ~							Search by Alert name	~	bitdefender Q, Q
									Critical and At
531	311				531	System	232	531	Low 116 83 Sectors 80
Available Alerts Total number of alerts available	Active Alerts Total number of active alerts				System/User Define Count for system and u	d Alerts iser defined alerts		Alerts by Threa Count of alerts by	it Level ythreat level
Activate Now Click 'Activate Now' after making	all changes								Total: 2 Page Size 25 V
Alert Name A		Threat	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
Bitdefender GravityZone: Application suspicious activities has been detec		•							Bitdefender GravityZone Elite v6.50 and

4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays a message box.

Successfully saved configuration.
ОК

5. Click **OK**, and then click the **Activate Now** button.

Note: Specify appropriate systems in the alert configuration for better performance.

6.3 Knowledge Objects

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
- 2. In the **Knowledge Object** tree, expand the **Bitdefender GravityZone** group folder to view the imported Knowledge objects.



Knowledge Objects	
bitdefe	Q Q
Groups	🕀 🏈 🗓
BitDefender GravityZone	
BitDefender GravityZone	Ø 🗓

6.4 Reports

1. In the **EventTracker** web interface, click the **Reports** menu, and then select the **Report Configuration**.



- 2. In **Reports Configuration** pane, select the **Defined** option.
- 3. Click on the **Bitdefender GravityZone** group folder to view the imported reports.

Report Configuration			
O Scheduled O Queued O Defined			
Report Groups		•	
BitDefender GravityZ	<u> </u>	0	^

6.5 Dashboard

1. In the EventTracker web interface, click on Home Button and select **My Dashboard**.

	Home
Dashb	My Dashboard
R	Threats
	Incidents

2. Select **Customize daslets** (a) and type **Ubiquiti** in the search bar.





Customize dashlets			×
bitdefe			Q
BitDefender GravityZone - Mod	BitDefender GravityZone - Pors	BitDefender GravityZone - Ports	BitDefender GravityZone - Suspi
BitDefender GravityZone - Suspi	BitDefender GravityZone - Suspi		
			Add Delete Close



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, end 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 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