

# Integrate Barracuda Essentials with EventTracker

EventTracker v9.0 and above

Publication Date: January 22, 2020

### Abstract

This guide will facilitate a Barracuda Essentials users to send logs to EventTracker.

#### Scope

The configurations detailed in this guide are consistent with **EventTracker 9.x or later and Barracuda Essentials.** 

### Audience

Administrators who want to monitor the Barracuda Essentials using EventTracker.

The information contained in this document represents the current view of Netsurion on the issues discussed as of the date of publication. Because Netsurion must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Netsurion, and Netsurion cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Netsurion MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Netsurion, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2020 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.



# Table of Contents

1.	Intr	oduction	3
	1.1	Pre-requisites	3
	1.2	Integrating Barracuda Essentials events to EventTracker via syslog	3
2.	Eve	ntTracker Knowledge Pack	4
	2.1	Saved Searches	4
	2.2	Alerts	4
	2.3	Report	4
	2.4	Dashboards	5
3.	Imp	oorting knowledge pack into EventTracker	8
	3.1	Categories	9
	3.2	Alerts	10
	3.3	Parsing Rule	11
	3.4	Flex Reports	12
	3.5	Knowledge Objects	13
	3.6	Dashboards	15
4.	Ver	ifying knowledge pack in EventTracker	16
	4.1	Categories	16
	4.2	Alerts	17
	4.3	Parsing Rules	17
	4.4	Flex Reports	18
	4.5	Knowledge Objects	18
	4.6	Dashboards	19

Netsurion... EventTracker\*

# 1. Introduction

Barracuda Essentials provides critical multi-layer security, archiving, and backup for Office 365, Microsoft Exchange, and G Suite.

The Barracuda Essentials service basically consists of:

- Barracuda Email Security
- > Barracuda Cloud Archiving Service
- Barracuda Cloud Backup

Barracuda Essentials event is integrated with EventTracker via syslog. It helps to monitor both inbound and outbound emails against the latest spams, viruses, worms, and phishing.

Reports provide a detailed information about the email traffic allowed and email traffic blocked.

Reports provide insight into the security statistics like suspicious email such as spam links and suspicious attachments. One can analyze suspicious emails using the dashboards, we can view the top sender and recipient. Dashboards show emails with spam links, suspicious attachments along with action taken like blocked, quarantined and deferred with reason. Alerts are generated if emails have spam links, malicious attachments, and those that are getting blocked.

#### 1.1 Pre-requisites

- The host machine should have installed the EventTracker agent.
- Administrator privilege for Barracuda Essentials web interface.
- Please use a new port that should support TCP+TLS certificate enabled in EventTracker for receiving Barracuda Essentials syslog messages.
- EventTracker manager IP address and TCP+TLS certificate enabled port should be publically reachable.

Note: Please enable EventTracker bad syslog receiving to receive Barracuda Essentials syslog messages.

# 1.2 Integrating Barracuda Essentials events to EventTracker via syslog

1. Log into Barracuda Essentials web console (In Barracuda Cloud Control, in the left panel, click Barracuda Email Security Service) and navigate to the **Account Management** tab.



<≡ ESS	Overview	Domains	Inbound Settings	Outbound Se	ettings	ATP Settings	Users	Reports	Account Management	Support	
Accou	Account Management (?)										
Syslog Ir	Syslog Integration										
IP Address / Hostname			Port	Actions							
TCP+TLS is required to connect successfully. Non-TLS is not supported				6514	Test	Delete					

#### Figure 1

- 2. Open any firewall ports needed for communicating with EventTracker.
- 3. Enter the IP Address/Hostname and Port for EventTracker Manager syslog VCP port.
  - IP Address/Hostname: Enter EventTracker Public IP address.
  - **Port**: Enter the TCP+TLS certificate enabled port number.
- 4. Click **Test** to ensure that the Barracuda Essentials can connect with EventTracker.

**Note**: If the test works, your message log data begins transferring to EventTracker.

# 2. EventTracker Knowledge Pack

Once Barracuda Essential's events are received in EventTracker, alerts, and reports is configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support the Barracuda Essentials monitoring.

#### 2.1 Saved Searches

**Barracuda Essentials: Not allowed traffic –** This saved search will give email blocked traffic, deferred traffic, and quarantined traffic logs.

Barracuda Essentials: Allowed traffic – This saved search will give allowed email traffic.

Barracuda Essentials: Rejected traffic – This saved search will give rejected email traffic.

### 2.2 Alerts

**Barracuda Essentials: Suspicious emails blocked –** This alert will trigger whenever emails have spam links, threat attachments and blocked by Barracuda Essentials.

### 2.3 Report

**Barracuda Essentials: Email traffic blocked:** This report provides information related to email traffic blocked, deferred, and quarantined by Barracuda Essentials email security service.

#### Log Considered

# Netsurion... EventTracker\*

#### 645 <6> 2019-12-26T10:38:52Z ip-100-69-12-62.us-east-2.compute.internal ESS101777[1]:

{"message\_id":"1577356724-893443-25789-521440-1","src\_ip":"205.233.73.32","hdr\_from":"eicar@alephtec.com","account\_id":"ESS101777","domain\_id":"205534","ptr\_record":"batch.outbound.your-

site.com","attachments":[{"name":"SecretNumber.gif"},{"name":"eicarpasswdocr.zip"}],"recipients":[{"action":"blocke d","reason":"atd\_subscribed","reason\_extra":"eicarpasswdocr.zip","delivered":"not\_delivered","delivery\_detail":"","e mail":"info@connect-ag.in"}],"hdr\_to":"serous \u003cinfo@connect-

ag.in\u003e","recipient\_count":1,"dst\_domain":"connect-ag.in","size":4129,"subject":"EICAR anti-virus test file:","env\_from":"eicar@aleph-tec.com","timestamp":"2019-12-26T10:38:46+0000"}

#### Sample Report

1			Source IP			Email Delivery				
	LogTime	Action	Address	Sender Mail ID	Recipient Mail ID	Status	Domain Name	Reason	Reason Detailed	Attachment Names
	01/14/2020 12:04:56 PM	deferred	182.74.234.198	pavankumar258589@gmail.com	info@connect-	not_delivered	connect-	sender_rset		
					agcnet.in		agcnet.in			
	01/14/2020 12:04:57 PM	quarantined	100.69.30.7	noreply@barracuda.com	akash@connect-	rejected	connect-	dest_invalid_recipient		
					agcnet.in		agcnet.in			
	01/14/2020 12:04:57 PM	blocked	205.233.73.32	eicar@aleph-tec.com	info@connect-	not_delivered	connect-	atd_subscribed	eicarpasswdocr.zip	{"name":"SecretNumber.gif"},{"na
					agcnet.in		agcnet.in			me":"eicarpasswdocr.zip"}

#### Figure 2

**Barracuda Essentials – Email traffic allowed:** This report provides information related to inbound and outbound email traffic allowed by Barracuda Essentials email security service.

#### Log Considered

#### 772 <6> 2019-12-26T10:19:09Z ip-100-69-22-95.us-east-2.compute.internal ESS101777[1]:

{"message\_id":"1577355532-893278-20131-541688-1","src\_ip":"93.99.104.21","hdr\_from":"MAILER-DAEMON@localhost (Mail Delivery

System)","account\_id":"ESS101777","domain\_id":"205534","ptr\_record":"emkei.cz","attachments":null,"recipients":[{ "action":"allowed","reason":"recipient","reason\_extra":"default\_scan\_policy:exempt","delivered":"delivered","deliver y\_detail":"smtp.secureserver.net:25:250 2.0.0 kQEHil5TWH1uq – kQEHil5TWH1uqkQEIitWFp mail accepted for delivery","email":"info@connect-ag.in"}],"hdr\_to":"info@connect-ag.in","recipient\_count":1,"dst\_domain":"connectag.in","size":3566,"subject":"Undelivered Mail Returned to Sender","env\_from":"","timestamp":"2019-12-26T10:18:54+0000"}

#### Sample Report

	Source IP							
LogTime	Address	Sender Mail ID	Email Subject	Recipient Mail ID	Domain Name	Reason	Reason Detailed	Attachment Names
12/30/2019 03:57:07 PM	209.85.210.196	tirupathipavan11@gmail.com	Quarantine check	info@connect-ag.in	connect-ag.in	recipient	default_scan_policy:exempt	null
12/30/2019 03:57:07 PM	100.69.30.7	eicar@aleph-tec.com	EICAR anti-virus test file:	info@connect-ag.in	connect-ag.in	ui_delivered		null
12/30/2019 03:57:07 PM	93.99.104.21		Undelivered Mail Returned to Sender	info@connect-ag.in	connect-ag.in	recipient	default_scan_policy:exempt	null

Figure 3

### 2.4 Dashboards

**Barracuda Essentials – Top sender detail** – This dashboard shows the sender details by Barracuda Email security service.





Figure 4

Barracuda Essentials – Top recipient detail- This dashboard shows the recipient details.



Figure 5





Barracuda Essentials – Geolocation by sender IP address – This dashboard will show sender geolocation.





Barracuda Essentials – Emails blocked by reason – This dashboard will show emails blocked by reasons.

Figure 7



## 3. Importing knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export-Import Utility.



Figure 8

Netsurion... EventTracker\*

🥾 Expo	Export Import Utility										
Export	Import										
Provide the path and file name of the Categories file. Use the '' bu     2. Click the Import button.											
Opti	ions Category		Location								



3. Click the Import tab.

#### 3.1 Categories

- 1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click the Category option, and then click the browse \_\_\_\_\_ button.
- 2. Navigate to the knowledge pack folder and select the file with the extension ".iscat", like "Categories\_Barracuda Essentials. iscat" and then click on the "Import" button:

🐁 Export Import Utility				_		$\times$
Export Import  1. Provide the path and file na 2. Click the Import button.	me of the Categories file.	Use the '' button t	to browse and locate the	e import file.		
Options  Category  Filters  Alerts  Systems and Groups  Token Value  Reports Behavior Correlation	Location Source *iscat	e : 1				
				Import	Close	•

Figure 10



EventTracker displays a success message:





### 3.2 Alerts

- 1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click Alert option, and then click the browse \_\_\_\_\_ button.
- Navigate to the knowledge pack folder and select the file with the extension ".isalt", e.g. "Alerts\_ Barracuda Essentials.isalt" and then click on the "Import" button:

<ol> <li>Provide the path and file na 2. Click the Import button.</li> </ol>	me of the Alerts file. Use the '' butt	ton to browse and locate the import file.
Options O Category	Location Import E-mail settings	
<ul> <li>Filters</li> <li>Alerts</li> </ul>	Set Active Only if notifications set By default	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.
<ul> <li>Systems and Groups</li> <li>Token Value</li> <li>Reports</li> </ul>	Watchlist Configuration Import Watchlist configuration This setting is applicable only f Note: If this option is enabled t on the console where the alert	ion for alerts which have Advanced watchlist configured. the user should make sure the watchlist groups are available is are imported.
Behavior Correlation	Source : *isalt	

Figure 12



EventTracker displays a success message:





### 3.3 Parsing Rule

- 1. Once you have opened "Export-Import Utility" via "EventTracker Control Panel", click the Token Value option, and then click the browse \_\_\_\_\_ button.
- Navigate to the knowledge pack folder and select the file with the extension ".iscat", like "Parsing Rule\_Barracuda Essentials. istoken" and then click on the "Import" button:

•	Export Import Utility	_		×
E	ixport Import			
	1. Provide the path and file na 2. Click the Import button	ame of token value file. Use the '' button to browse and locate the import file.		
	Options	Location		
	Category			
	O Filters			
	O Alerts			
	<ul> <li>Systems and Groups</li> </ul>	Source : :\Parsing Rule_Kaspersky Security Center.istoken		
	Token Value			
	O Reports			
	O Machine learning			
		Import	Close	в

Figure 14





Figure 15

### 3.4 Flex Reports

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

🐁 Export Import Utility	- 0	×
Export Import		
1. Provide the path and file nam 2. Click the Import button Note : If report(s) contains templ	e of Schedule Report file. Use the '' button to browse and locate the import file. ate, first import template and proceed with exportimport utility.	
Options	Location	
Category		
◯ Filters		
⊖ Alerts	<ul> <li>Legacy (*.issch)</li> <li>New (*.etcrx)</li> </ul>	
O Systems and Groups	Source : *issch	
◯ Token Value		
Reports		
Behavior Correlation		
	Import Close	

#### Figure 16

Once you have selected "New (\*.etcrx)", a new pop-up window will appear. Click the "Select File" button and navigate to the knowledge pack folder and select file with the extension ".etcrx", e.g. "Reports\_Barracuda Essentials.etcrx".

Reports Import											
Note : If report(s) contains template,	Note : If report(s) contains template, first import template and proceed with report import process.										
Select file *.etcrx	elect file *.etcnx Select file										
Available reports	Available reports										
Title	Frequency     Show all     Image: Constraint of the state of										
	Title Sites	Groups	Systems	Frequency	Runtime	Туре					

#### Figure 17

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

Note: Set run time option is not applicat	le for Defined Reports and Hourly Reports	
Set run time for report(s) from	AM • at interval of minu	es Set
Replace	to Re	lace Assign systems
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.

Figure 18

EventTracker displays a success message:

Export Impo	rt Utility	×
Selected re	ports configurations are imported suc	cessfully
		ОК



### 3.5 Knowledge Objects

1. Click Knowledge objects under the Admin option in the EventTracker web interface.



		🔎 Admin 🗸	Tools 🗸 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	🏫 / Da
Alerts	Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
Casebook Configuration	Q IP Lookup Configuration	r Weights	Systems since the last 24 hour
● Category	·@· Knowledge Objects	Windows Agent Config	_
▲ Diagnostics	Danager 🖉		



2. Next, click the "import object" icon:

Admin / Knowledge Objects
Objects 🕂 丁 🏦 🌣
Import Objects



 A pop-up box will appear, click "Browse" in that and navigate to the knowledge packs folder (type "C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) with the extension ".etko", e.g. "KO\_Barracuda Essentials.etko" and then click the "Upload" button.

Import	
KO_ <product name="">.etko</product>	Browse Upload

Figure 22

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click on the "**Import**" button:



Figure 23



### 3.6 Dashboards

- 1. Login to the EventTracker web interface.
- 2. Navigate to **Dashboard**  $\rightarrow$  **My Dashboard**.
- 3. In "My Dashboard", click Import Button:

EventTracker				
	Home			
۹	My Dashboard			
2	Threats			
	Incidents			
	Behavior Correlation			
	Change Audit			
	Compliance			

Figure 24

👚 / Dashboard / My Dashboard	
+ 🖉 @ 🌣 1 Ţ @ ()	
Import configuration	n



- Select the browse button and navigate to the knowledge pack folder (type "C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs" in the navigation bar) where ".etwd", e.g. "Dashboard\_Barracuda Essentials.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.

Import	
Note: If dashlet configured using persisted report, first import the report and proceed with importing dashlet.	Upload
Available widgets	

#### Figure 26

Import	Close

Figure 27

# 4. Verifying knowledge pack in EventTracker

#### 4.1 Categories

- 1. Login to the EventTracker web interface.
- 2. Click Admin dropdown, and then click Categories.
- In Category Tree to view imported categories, please click on "Search" and search with the "Barracuda Essentials". You will see the below results:



Cat	tegory
(	Category Tree Search
	barracuda essentials Q Q
(	Category
	✓ Barracuda Essentials: Allowed traffic
	V Barracuda Essentials: Not allowed traffic
	✓ Barracuda Essentials: Rejected traffic
	Figure 28

### 4.2 Alerts

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
- 2. In the search box enter **"Barracuda Essentials"** and then click the **Search** button. EventTracker displays an alert related to Barracuda Essentials:

Alerts Show All							Search by Alert name	~	↑ / Admin / Alerts     barracuda essentials   Q   Q
217 Available Alerts Total number of alerts available	93 Active Alerts Total number of active alerts				217 System/User Defin Count for system and	System User 91 ed Alerts user defined alerts	128	217 Alerts by Three Count of alerts b	Crical 10 130 Low 15 12 130 Serios 5 20 at Level threat level
Il Activate Now Click 'Activate Now' after making a	all changes								Total: 2 Page Size 25 V
Alert Name A		Threat	Active	E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
ββ Barracuda Essentials: Email suspicious activities blocked		•							Barracuda Essentials Email Security Servi
βδ Barracuda Essentials: Malicious IP detected		•							Barracuda Essentials Email Security Servi



### 4.3 Parsing Rules

- 1. In the EventTracker web interface, click the Admin dropdown, and then click Parsing Rule.
- 2. In the **Parsing Rule** tab, click on the **"Barracuda Essentials"** group folder to view the imported Token Values.



Parsing Rules			
Parsing Rule Template			
Groups		e	
Barracuda Essentials	Ē	1	^

Figure 30

### 4.4 Flex 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 "Barracuda Essentials" group folder to view the imported reports.



Figure 32

### 4.5 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 **"Barracuda Essentials"** group folder to view the imported Knowledge objects.



#### Knowledge Objects

barracuda essentials	Q Q
Groups	🕀 🏈 🗓
Barracuda Essentials	
Barracuda Essentials	Ø 🗓
Figure 33	3

#### 4.6 Dashboards

1. In the EventTracker web interface, Click on Home Button and select "My Dashboard".





2. In "Barracuda Essentials" dashboard you should be now able to see something like this:



