

## Integrate Barracuda Web Application

EventTracker v9.x and above

Publication Date: October 28, 2019

## Abstract

This guide provides instructions to retrieve Barracuda Web Application event logs and integrate it with EventTracker. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Barracuda Web Application.

### Audience

The configurations detailed in this guide are consistent with EventTracker version v9.x or above and Barracuda Web Application.

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.

© 2019 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.	0	verview	. 3
2.	In	Itegrating Barracuda WAF with EventTracker	. 3
3.	E\ 3.1	ventTracker Knowledge Pack Flex Reports	. 3 . 3
	3.2	Saved Searches	. 3
4.	In 4.1	nporting Barracuda Web Application knowledge pack into EventTracker Knowledge Object	. 4 . 5
	4.2	Token template	. 6
	4.3	Flex Reports	. 7
	4.4	Category	. 8
5.	V 5.1	erifying Barracuda Web Application knowledge pack in EventTracker Knowledge Object	. 8 . 8
	5.2	Token template	. 9
	5.3	Flex Reports	10
	5.4	Category	10



## 1. Overview

Barracuda offers a Web Application Firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

## 2. Integrating Barracuda WAF with EventTracker

- 1. Log into the Barracuda Web Application Firewall web interface.
- 2. Go to ADVANCED > Export Logs.
- 3. In the syslog section, click Add syslog server and specify the following:
  - Name Enter a name for the syslog server.
  - IP Address Enter the IP address of the EventTracker manager.
  - Port Enter the port number on which the syslog VCP configuration (e.g. 514).
  - **Connection Type** Set the connection type to transmit the logs from the Barracuda Web Application Firewall to the syslog server.
- 4. Verify that the logs in EventTracker manager are received or not.

## 3. EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker. The following Knowledge Packs are available in EventTracker to support Barracuda Web Application.

## 3.1 Flex Reports

• Barracuda Web Application – Traffic Activity : This report gives you information about the access log along with the username, source IP address, destination IP and session ID.

## 3.2 Saved Searches

• **Barracuda Web Application – Traffic Activity :** This saved search gives you information about the access log along with the username, source IP address, destination IP and session ID.



# 4. Importing Barracuda Web Application knowledge pack into EventTracker

**NOTE**: Import knowledge pack items in the following sequence:

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



Figure 1

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

Figure 2

3. Click the **Import** tab.



## 4.1 Knowledge Object

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

Ξ	Event <b>Tracker</b> ⊕				Admin-	Tools <del>-</del>
	Home	Active Watch Lists	Collection Master	Group Management	Systems	🕈 / Dashb
a		Alerts	Correlation	Q IP Lookup Configuration	🙊 Users	
	0 1	Behavior Correlation Rules	1 Diagnostics	💮 Knowledge Objects	The Weights	
*		👌 Behavior Correlation Setting:	s 😾 Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Indicators of Unsafe connections or processes, new TCP entry point USB activities, New	tors of Cc 🔲 Casebook Configuration	Sentvault	D Parsing Rules		
		or Category	FAQ Configuration	Report Settings		
	Attacker		- News			
		F	igure 3			

- 2. Click on the **Import** button.
- 3. Click on Browse.

Import		×
Select file 🝃 Brow	vse Upload	
		Close

- 4. Locate the file named **KO\_JIRA.etko**.
- 5. Now select all the checkbox and then clickon  $\mathbb{F}$  '**Import**' option.
- 6. Knowledge objects are now imported successfully.

File imported successfully.	
	01
	OK

Figure 5

## 4.2 Token template

1. Click on the **Parsing rule** under the **Admin** option in the EventTracker manager page.

		🔎 🛛 Admin 🗸
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules
Alerts	Group Management	Report Settings
Casebook Configuration	Q IP Lookup Configuration	Systems
● Category	Ò	Q Users
Diagnostics	B Machine Learning Jobs	De Weights
Event Filters	🖓 Machine Learning Settings	Windows Agent Config
Eventvault	🔯 Manager	

Figure 6

2. Select **Template** and click on **import (**icon in the top right corner.

Event <b>Tracker</b> ⊕				<b>Å</b>	Admin <del>-</del>	Tools <del>+</del>	🚯 Adarsh Pandey ·
Parsing Rules						A	/ Admin / Parsing Rule
Parsing Rule Templat	2						
Groups		<b>(+)</b>					CİT
Default			<b>•</b>				
ABC	Į.	1			Active		í

- 3. Select the file of type \*.ettd(EventTracker template dashlets.)
- 4. Select all the Barracuda Web Application template name.
- 5. And click on the **import**  $\mathbf{T}$  icon.
- 6. Template(s) imported successfully.



localhost:8080 says		
		ок
	Figure 8	

## 4.3 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)":

C Legacy (*.issch) Source : *.issch	(In the export import utility.	
		Import

- 2. Once you have selected "**New (\*.etcrx)**", a new pop-up window appears. Click the "**Select File**" button and navigate to the file path with a file having the extension ".etcrx".
- 3. Select all the relevant files and then click **Import T** button.
- 4. EventTracker displays a success message:





Figure 10

## 4.4 Category

- 1. Click the **Category** option, and then click the \_\_\_\_ browse button.
- 2. Locate the Category\_Barracuda Web Application.iscat file, and then click the open button.
- 3. To import category, click the Import button.
- 4. EventTracker displays a success message.

Export Im	port Utility	×
1	Selected category details are imported successfully.	
	ОК	

Figure 11

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

## 5. Verifying Barracuda Web Application knowledge pack in EventTracker

## 5.1 Knowledge Object

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

Ξ	Event <b>Tracker</b> ⊕						Tools <del>-</del>
	Home		Active Watch Lists	Collection Master	Group Management	Systems	🔒 / Dashb
0			Alerts	Correlation	Q IP Lookup Configuration	Q Users	
	0	1	Behavior Correlation Rules	1 Diagnostics	💮 Knowledge Objects	1 Weights	
~			🗞 Behavior Correlation Settings	Event Filters	Manager	Windows Agent Config	
	Potential Cyber Breaches Indicators of Unsafe connections or processes, new TCP entry point USB activities. New	Indicators of Co USB activities, New sen	Casebook Configuration	Eventvault	🧭 Parsing Rules		
			● Category	FAQ Configuration	Report Settings		
	Attacker			- News			
			Figure 1	2			

2. In the Knowledge Object tree, expand the **Barracuda Web Application** group folder to view the imported Knowledge objects.

Groups	🕀 🖉 🗓	Object name Barracuda WAF Access Log				
Barracuda NG Firewall		Applies to Barracuda WAF				
Barracuda WAF		Rules				
Barracuda WAF Access Log	Ø 🗓	Title				
Cisco ASA Firewall		🗄 🛛 Barracuda WAF - Access Log CEF				
Dall Farra 10 Suitzh		Message Signature: CEF.*?src=.*?dst=.*?in=.*?out=				
		Message Exception:				
EventTracker		Expressions				
E Fairwarning		Expression type				
FortiAnalyzer		Regular Expression				



## 5.2 Token template

1. Click on Parsing rules under Admin.

		🔎 Admin <del>v</del>	Tools <del>-</del>
Active Watch Lists	FAQ Tile Configuration	🧭 Parsing Rules	<b>†</b> / Ac
Alerts	Group Management Contai	ins set of rules which tell what kind of	data you w
Casebook Configuration	Q IP Lookup Configuration	Systems	0
● Category	·☆· Knowledge Objects	💭 Users	
Diagnostics	Machine Learning Jobs	r Weights	
Event Filters	🗞 Machine Learning Settings	Windows Agent Config	
Ventvault	Manager		

- 2. Select template under parsing rules and select the Barracuda Web Application group.
- 3. All the templates are present under **Barracuda Web Application**.



Parsing Rule	Template						
Groups			÷		Group : Barracuda WAF		Search
Default				-			0.0000000000000000000000000000000000000
Barracuda WAF		Ē	Ø		Template Name	Template Des	scription
Cybereason			1		Barracuda WAF - Access Logs	Barracuda WAF - Access Logs	
EventTracker		前	Ø				

Figure 15

## 5.3 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 Web Application group folder to view the imported reports.

Scheduled Queued I Defined					
Report Groups		÷ #		eports configuration: Barracuda WAF	
{: Security		-	<b>•</b> į	Î <i>2</i> ,	
Compliance		_	0		Title
Coperations					Barracuda WAF - Access Logs
Flex Flex		_			
Amazon AWS	Ē	1			
🔁 Barracuda WAF	Ē	1			
ConnectWise Manage	Ē	Ø			

Figure 17

## 5.4 Category

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

≡	Event <b>Tracker</b> ⊕				🔎 🛛 Admin 🗸	Tools <del>+</del>
	Home		Active Watch Lists	Event Filters	🧭 Parsing Rules	
a		_	Alerts	Contract Eventvault	Report Settings	_
	0	0	Behavior Correlation Rules	FAQ Tile Configuration	Systems	
~			behavior Correlation Settings	Group Management	Q Users	
	Potential Cyber Breaches Unsafe connections or processes, new TCP ent	Indicators of Co USB activities, New	Casebook Configuration	Q IP Lookup Configuration	Heights	orting Syste
			● Category	· C Knowledge Objects	Windows Agent Config	
	Attacker		Diagnostics	D Manager		



3. Click the search, and then search with Barracuda Web Application.

Category Tree	Search	
All Categories		
🖂 🔳 👘	or events	
🗐 *All info	prmation events	
*All wa	ning events	
- 🔳 *Securi	ty: All security events	
🛨 🔁 Amazo	n 53	
🗐 🔁 Barracu	da WAF	
E Bar	racuda WAF - Access Logs	
🛨 🔁 Change	Audit	
d	Figure 19	