

Integration Guide

Integrating Barracuda Web Security Gateway with EventTracker

EventTracker v9.2 and later

Publication Date:

March 26, 2021



Abstract

This guide provides instructions to retrieve the **Barracuda Web Security Gateway** events. Once **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor **Barracuda WSG**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Barracuda Web Security Gateway.**

Audience

Administrators who are assigned the task to monitor **Barracuda Web Security Gateway** events using EventTracker.



Table of Contents

Tal	ole	of Contents	3
1.	C	Iverview	4
2.	F	rerequisites	4
3.	I	ntegrating Barracuda Web Security Gateway events with EventTracker server	4
4.	E	ventTracker Knowledge Pack	4
	4.1	Categories	4
	4.2	Alerts	5
	4.3	Flex Reports	5
	4.4	Dashboards	10
5.	I	nporting Knowledge Pack into EventTracker	14
	5.1	Categories	15
	5.2	Alerts	16
	5.3	Flex Reports	17
	5.4	Knowledge Objects	18
	5.5	Dashboards	19
6.	١	erifying Knowledge Pack in EventTracker	21
	6.1	Categories	21
	6.2	Alerts	21
	6.3	Flex Reports	22
	6.4	Knowledge Objects	22
	6.5	Dashboards	22
	Ab	out Netsurion	24
	Cor	tact Us	24



1. Overview

The Barracuda Web Security Gateway lets organizations benefit from online applications and tools without exposure to web-borne malware and viruses, lost user productivity, and misused bandwidth.

Barracuda WSG logs can be integrated with EventTracker via syslog. Barracuda WSG can send events like user login failure, configuration changes, allowed traffic, blocked traffic, malware activities detected, and malware blocked, etc. It created detailed reports for user login failure, configuration changes, malware activities, web traffic allowed, and web traffic blocked. Its graphical representation shows the malicious URL's blocked by reason, malware detected by IP address, configuration changes by usernames, etc.

EventTracker triggers alerts in the event when a malware is detected, changes in configuration by any user, or an unsuccessful user login.

2. Prerequisites

- Barracuda Web Security Gateway version 610,710,810,910,1010.
- Barracuda Web Security Gateway firmware version 11.0.0.019.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

3. Integrating Barracuda Web Security Gateway events with EventTracker server

To enable syslog reporting on your Barracuda Web Security Gateway:

- Log into the web interface as Admin.
- Navigate to the **Advanced** >> **Syslog** page.
- For both the **Web Traffic Syslog** and **Web Interface Syslog**, enter the **IP address** (192.168.1.1) of the **EventTracker** with **port 514** to which you want to direct messages.

4. EventTracker Knowledge Pack

Once logs are received into EventTracker; alerts, reports can be configured into EventTracker.

The following knowledge packs are available in EventTracker to support Windows.

4.1 Categories

- 1. Barracuda WSG: Web Traffic This category provides events information related to allowed traffic, blocked traffic, and user known restricted traffic, etc.
- 2. Barracuda WSG: Configuration Changes This category provides events information related to configuration changes applied on Barracuda WSG.
- 3. Barracuda WSG: Login Failure This category provides events information related to user try to log into Barracuda WSG but fails.

4. Barracuda WSG: Logon Success – This category provides events information related to user try to log into Barracuda WSG and is successful.

4.2 Alerts

- 1. Barracuda WSG: Configuration changes This alert is generated when any configuration changes are done in the Barracuda web server gateway by different users or admins such as new user creation, group creation, backup scheduled, firmware updates etc.
- 2. Barracuda WSG: Potential threat has been detected This alert is generated when the web traffic content is infected by a malware or virus.
- 3. Barracuda WSG: Login Failure This alert is generated when failed logon attempts are done in the application.

4.3 Flex Reports

1. **Barracuda WSG - Clean policy allowed traffic:** This report provides all the allowed traffic content that pass through the Barracuda web security gateway.

LogTime		Source IP	Destination IP	Destination Url	Data size	Format Version	TQ flag	User Info
02/24/2017 0	4:23:48 PM	192.168.137.1	216.58.220.35	http://www.google.co.in/?gfe_rd=c r&ei=PHyqWLXwNunl8AeizZXoCg	* 1064	2	ъ	MIKE
02/24/2017 0	4:23:48 PM	192.168.137.1	172.217.26.163	http://fonts.gstatic.com/s/lato/v13/ H2DMvhDLycM56KNuAtbJYA.woff 2	23159	2	ъ	ANON
02/24/2017 0	4:23:48 PM	192.168.137.1	104.24.127.96	http://analytics.planwallpaper.com /piwik.php?action_name=High0De finition0and0high0resolution0wallp apers&idsite=7&rec=1&r=400261& h=11&m=2&s=35&url=httpA	520	2	0	Doe, John, CN=Users, DC=qo, DC=local

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE			
2/24/2017 12:33:20 PM	160	PNPL-6-KP / PNPL-6-K	N/A	N/A	SYSLOG local4			
Event Type: Warning Log Type: Application Description: Feb 24 12:33:20 PNPL-6-KP http_scan[11287]: 1487919778 1 192.168.1.140 172.217.26.174 - 192.168.1.140 https://clients1.google.com/ 5423 BYF Category Id: 4 ALLOWED CLEAN 2 0 0 0 (-) 0 - 0 - 0 clients1.google.com cat-lookup-failed [deepu.v] https://clients1.google.com - 1								
2/24/2017 12:33:00 PM	160	PNPL-6-KP / PNPL-6-K	N/A	N/A	SYSLOG local4			
Event Type: Warning Log Type: Application Category Id: 4	Description: Feb 24 12:33:00 PNPL-6-KP http_scan[11287]: 1487919758 1 192.168.1.140 172.217.26.163 - 192.168.1.140 https://ssl.gstatic.com/ 4796 BYF ALLO WED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 ssl.gstatic.com cat-lookup-failed [deepu.v] https://ssl.gstatic.com - 1							

2. Barracuda WSG-Clean policy denied traffic: This report provides all the denied traffic content that pass through the Barracuda web security gateway. The denial is based on the policies and rules written by the admins.

LogTime	Source IP	Destination IP	Destination URL	Content Type	Data size	Match flag	TQ flag	User Info
02/20/2017 11:02:31 AM	192.168.137.1	104.24.126.96	http://www.planwallpa per.com/static/assets/c ss/fcnt- awesome.min.css	text/css	6043	2	0	[ZOE]
02/20/2017 11:02:32 AM	192.168.137.1	173.223.235.8	http://www.msftncsi.c om/ncsi.txt	text/plain	277	2	0	[cn=Administrator,cn =Users,dc=Contoso, dc=Com]
02/20/2017 11:02:30 AM	192.168.137.1	96.43.137.99	http://rules.emergirgthr eats.net/fwrules/emerg ing-Elock-IPs.txt	text/plain	28206	2	0	[ANON]

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
— 2/27/2017 1:06:17 PM	<u>5555</u>	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description Feb 20 fwrules merging	on: 11:00:21 PNPL-6-KP http_scan[96 /emerging-Block-IPs.txt 28206 B\ gthreats.net/fwrules/emerging-B	588]: 1487568595 1 /F BLOCKED CLEAN lock-IPs.txt 0	192.168.137.1 96.43.137.99 t 2 0 0 0 0 (-) 0 - 0 - 0 rules.em	ext/plain 192.168.137.1 http://rules.emergingthreats.net/ ergingthreats.net cat-lookup-failed [ANON] http://rules.e
— 2/27/2017 1:06:17 PM	<u>5555</u>	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Feb 20 t 277 B ^v] http://	on: 10:49:21 PNPL-6-KP http_scan[96 YF BLOCKED CLEAN 2 0 0 0 0 (-) 0 /www.msftncsi.com/ncsi.txt 0	89]: 1487567934 1 - 0 - 0 www.msftnc	192.168.137.1 173.223.235.8 si.com cat-lookup-failed [cn=/	text/plain 192.168.137.1 http://www.msftncsi.com/ncsi.tx Administrator,cn=Users,dc=Contoso,dc=Com - LDAP USER

3. Barracuda WSG - Configuration changes: This report provides all the configuration changes that are done in the Barracuda web server gateway by different users and admins such as new user creation, group creation, backup scheduled, firmware updates etc.

LogTime	IP address	Changed for	Object changed	Object Value	Changed by
02/22/2017 04:08:22 PM	192.168.137.1	global	LDAP_user_pass_new_repea t	W*****3	admin
02/22/2017 04:12:39 PM	192.168.137.1	zoe	user_password	*****	admin
02/22/2017 04:22:50 PM	192.168.137.74	global	backup_schedule_WF_Config _minute	00	mike
02/22/2017 04:12:39 PM	192.168.137.1	anne	user_tempwl_direct_override	No	admin



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE		
2/27/2017 1:54:46 PM	5555	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog		
Event Type: Information Description: Feb 22 16:22:50 PNPL-6-KP web: [192.168.137.74] global[] CHANGE backup_schedule_WF_Config_minute (00) [mike] Category Id: 0 Feb 22 16:22:50 PNPL-6-KP web: [192.168.137.74] global[] CHANGE backup_schedule_WF_Config_minute (00) [mike]							
2/27/2017 1:54:46 PM	5555	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog		
Event Type: Information Log Type: Application Category Id: 0	Description: Feb 22 16:08:22 PNPL-6-KP web: [192.168.137.1] global[] CHANGE LDAP_user_pass_new_repeat (W********3)[admin]						
2/27/2017 1:54:46 PM	5555	PNPL-6-KP / PNPL-6-K	N/A	N/A	Syslog		
Event Type: Information Log Type: Application	Description: Feb 22 16:12:39 PNPL-6-KP web: [192.168.137.1] user[anne] CHANGE user_tempwl_direct_override (No) [admin]						

4. Barracuda WSG - Malware activities: This report provides all the malware infected traffic details.

				Data	Virus stream			
LogTime	Source IP	Destination IP	Destination Url	size	details	Match flag	User Info	Referer Url
02/21/2017 12:44:22 PM	192.168.137.1	188.225.32.177	fo5.a1- downloader.org/g 2v9s1.php?id=yo urname@yourdo main.com.zip	538	Trojan	2	ANON	http://fo5.a1- downloader.or g/- Download.zip fo5.a1-
02/21/2017 12:44:22 PM	192.168.137.1	213.211.198.62	http://www.eicar .org/download/ei car_com.zip	538	Eicar	2	CN=Jane Doe, CN=Users , DC=qc, DC=local	http://www.ei car.org/85-0- Download.html www.eicar.or g
02/21/2017 12:44:22 PM	192.168.137.1	107.180.51.15	http://aadroid.net/ sys.olk	101236	Ransomware	2	MIKE	http://aadroid .net/- Download.zip aadroid.net/sy s.olk
02/21/2017 12:44:22 PM	10.1.1.8	127.0.0.1	http://www.eicar .org/download/ei car.com.txt	1223	Eicar-Test-Signature FOUND	2	DOE	http://www.ei car.org/index.h tml



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
2/23/2017 5:11:50 PM	<u>5555</u>	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Description: Feb 21 12:15:00 PNPL-6-KP http_scan[10713]: 1487656934 1 192.168.137.1 107.180.51.15 application/html 192.168.137.1 aadroid.net/sys.olk 236 BYF BLOCKED VIRUS stream=>Ransomware 2 0 0 0 0 (-) 0 - 0 - 0 aadroid.net/sys.olk cat-lookup-failed [MIKE] http://aadroid.net/-Download aadroid.net/sys.olk - 0					
2/23/2017 5:11:50 PM	5555	PNPL-6-KP / PNPL-6-K	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Description Feb 21 /g2v9s1 -failed	on: 12:05:20 PNPL-6-KP http_scan[10 I.php?id=yourname@yourdomaii (ANON] http://fo5.a1-downloader	0991]: 1487656793 n.com.zip 538 BYF E r.org/-Download.zip	l 192.168.137.1 188.225.32.1 BLOCKED VIRUS stream=>Troj fo5.a1-downloader.org - 0	77 application/html 192.168.137.1 fo5.a1-downloader.org an 2 0 0 0 0 (-) 0 - 0 - 0 fo5.a1-downloader.org/ cat-lookup	

5. **Barracuda WSG -Inline Traffic details:** This report provides all internet traffic requests. It performs content filtering and scan downloads for spyware and viruses , filter web based and non-web-based applications. This is determined by the traffic that traverses via the automatic configured proxy (PAC).

LogTime	Source IP	Destination IP	Destination Url	Action	Reason	PAC	Support Email Id	Referer Url
02/23/2017 03:16:39 PM	192.168.137.1	172.217.26.195	https://www.gsta tic.com/	ALLOWED	CLEAN	CUSTOM- 353783667,CU STOM- 76676773536,C USTOM- 6760786767,	gstaticsupp@gstat. com	https://www. gstatic.com/
02/23/2017 03:16:39 PM	192.168.137.1	172.217.26.174	https://sb- ssl.google.com/	BLOCKED	VIRUS	CUSTOM- 5471171786,CU STOM- 6786786745,CU STOM- 7932342767,	sbibcol@sbs.com	https://sb- ssi.google.co m/
02/23/2017 03:16:39 PM	192.168.137.1	104.122.61.202	https://site- cdn.onenote.net/	BLOCKED	CLEAN	CUSTOM- 83834537676,C USTOM- 27537756435,C USTOM- 75377245376,	sitecdnon@cdn.co m	https://site- cdn.onenote. net/

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE	
2/23/2017 3:32:19 PM	<u>5555</u>	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog	
Event Type: Information Description: Log Type: Application Nov 21 20:13:35 2016 barracuda http_scan[10649]: 1487659023 1 192.168.137.1 104.122.61.202 - 192.168.137.1 https://site- Category Id: 0 Category Id: 0 49 BYF BLOCKED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 site-cdn.onenote.net computing-technology, CUSTOM-83834537676,CUSTOM-27 75377245376, [sitecdnon@cdn.com] https://site-cdn.onenote.net/ - 0						/site-cdn.onenote.net/ 400 DM-27537756435,CUSTOM-
2/23/2017 3:32:19 PM	<u>5555</u>	PNPL-6-KP / PNPL-6-K	N/A	N/A	Syslog	
Event Type: Information Log Type: Application Category Id: 0	Descripti Nov 21 BYF BL 767, [s	on: 20:13:35 2016 barracuda http_s .OCKED VIRUS 2 0 0 0 0 (-) 0 - 0 - 1 bibcol@sbs.com] https://sb-ssl.g	can[10840]: 148765 0 sb-ssl.google.com oogle.com/ 0	9118 1 192.168. computing-tech	.137.1 172.217.26.174 - 192.168.137.1 https:/ inology, CUSTOM-5471171786,CUSTOM-6786	//sb-ssl.google.com/ 1272 i786745,CUSTOM-7932342

6. **Barracuda WSG - Login and Logoff activity:** This report provides all the login and logoff activities that are done in the Barracuda application.

LogTime	Source IP	Action	User	
02/23/2017 06:12:12 AM	192.168.137.74	LOGIN	zoe	
02/23/2017 07:42:00 AM	192.168.137.1	LOGOFF	zoe	
02/23/2017 08:35:19 AM	192.168.137.1	LOGIN	jack	
02/23/2017 12:26:04 PM	192.168.137.1	LOGOFF	jack	
02/23/2017 04:58:12 PM	192.168.137.74	LOGIN	glenn	
02/23/2017 07:14:53 PM	192.168.137.74	LOGOFF	glenn	

Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
— 2/23/2017 6:12:21 PM	5555	PNPL-6-KP / PNPL-6-K	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Description: Feb 20 09:42:55 PNPL-6-KP web: [192.168.137.1] LOGIN (admin)				
— 2/23/2017 6:12:21 PM	5555	PNPL-6-KP / PNPL-6-K	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Feb 20	on: 10:12:09 PNPL-6-KP web: [192.16	8.137.1] LOGOFF (a	dmin)	

7. Barracuda WSG -Login Failure: This report provides all the failed logon attempts that are done in the Barracuda application.

LogTime	Source IP	User
02/17/2017 11:16:39 AM	192.168.137.1	admin
02/20/2017 10:49:41 AM	192.168.137.74	aaron
02/21/2017 12:12:34 PM	192.168.137.1	admin
02/22/2017 11:16:02 AM	192.168.137.74	admin
02/21/2017 12:54:45 PM	192.168.137.1	neeson



Logs Considered:

	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/27/2017 2:54:04 PM	5555	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Feb 21	on: 12:54:45 PNPL-6-KP web: [192.16	8.137.1] FAILED_LO	GIN (neeson)	
— 2/27/2017 2:54:04 PM	<u>5555</u>	PNPL-6-KP / <u>PNPL-6-K</u>	N/A	N/A	Syslog
Event Type: Information Log Type: Application Category Id: 0	Descriptio Feb 21	on: 12:12:34 PNPL-6-KP web: [192.16	8.137.1] FAILED_LO	GIN (admin)	

4.4 Dashboards

• Barracuda WSG – User login success



• Barracuda WSG – User login failed



Netsurion®

• Barracuda WSG – Configuration changes by username



• Barracuda WSG – Threat type by source IP





• Barracuda WSG – Top URLs allowed

Barracuda WSG - Top URLs allowed	⊠ – ×
	<
https://www.facebook.com/ https://teams.events.data.microsoft.com/	
https://presence.teams.microsoft.com/ https://outlook.office365.com/	
https://inspect.tcplusmobius.com/ https://ib.adnxs.com/	
Mar 15 11:21 AM - Mar 22 11:22 AM	

• Barracuda WSG – Web traffic trend



Netsurion®



• Barracuda WSG – Allowed traffic by destination IP

• Barracuda WSG – Top Suspicious URLs





• Barracuda WSG – Web traffic by log category



5. Importing Knowledge Pack into EventTracker

NOTE: Import knowledge pack items in the following sequence :

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





Export-Import Utility window opens.

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

3. Click the **Import** tab.

5.1 Categories

- 1. In Export-Import Utility window, select the Category option, and click Browse
- 2. Navigate to the knowledge pack folder and select the file with the extension ".iscat", like "Categories_Barracuda WSG.iscat" and click Import.

🐁 Export Import Uti	lity				_		\times
Export Import							
1. Provide the path 2. Click the Import	and file name of the Ca button.	tegories file. Use the '	.' button to browse a	nd locate the import file.			
Options Category Filters Alerts Systems and C Token Value Reports Behavior Corre	Groups	Source : *iscat]		
					mport	Clos	e

EventTracker displays a success message.





5.2 Alerts

- 1. In **Export-Import Utility** window, select the **Alert** option and click **Browse**.
- 2. Navigate to the knowledge pack folder and select the file with the extension ".isalt", e.g., "Alerts_ Barracuda WSG.isalt" and click Import.

Export Import Utility		- 0	×
Export Import			
1. Provide the path and file na 2. Click the Import button.	me of the Alerts file. Use the '' but	ton to browse and locate the import file.	
Options	Location		
	Import E-mail settings		
	Set Active		
 Filters 	Only if notifications set	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on	
Alerts	O By default	"Active" key available in the configuration section.	
O Systems and Groups	Watchlist Configuration		
O Talvas Valua	Import Watchlist configurat	ion	
	This setting is applicable only f	for alerts which have Advanced watchlist configured.	
O Reports	on the console where the alert	ts are imported.	
O Behavior Correlation			
	Source :	_	
	*.isalt		
		Import	llose

EventTracker displays a success message.





5.3 Flex Reports

 In Export-Import Utility window, select the Import tab. Click the Reports option, and choose "New (*.etcrx)".

2. Click the Import button	ne of Schedule reportine, ose the button to browse and locate the importante.	
Options	Location	
Category		
Filters		
O Alerts	Legacy (*.issch) New (*.etcrx)	
Systems and Groups	Source :	
◯ Token Value	Jadol I	
Reports		
Robavier Completion		
O Benavior Conelation		

2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension ".etcrx", e.g., "Reports_Barracuda WSG.etcrx".

Netsurion®

🕄 Reports Import						
Note : If report(s) contains template, first im Select file *.etcrx	port template and proceed with	report import proces	S .			Select file
Available reports Title	Free	quency Show all	•	Q Q		
	Sites	Groups	Systems	Frequency	Runtime	Туре

3. Wait while reports populate. Select all the relevant reports and click Import T.

Note: Set run time option is not applicat	le for Defined Reports and Hourly Reports			1
Set run time for report(s) from	AM • at interval of _ minutes	Set (i)		l
Replace	to Replace	Assign systems		l
		Note: Make sure that Site(s), Group(s) and System(s) selections are valid.	\otimes	l

EventTracker displays a success message.

Export Import Utility	×
Selected reports configurations are impo	orted successfully
	ОК

5.4 Knowledge Objects

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

		🔎 Admin -	Tools 👻 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Das
Alerts	Sector Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
mi Sr sc Casebook Configuration	🔍 IP Lookup Configuration	🕀 Weights	since the last 24 hours
ංලී Category	`⊙. Knowledge Objects	Windows Agent Config	
Diagnostics	O Manager		



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



 A pop-up box appears, click Browse 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 WSG.etko" and click Upload.

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

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



5.5 Dashboards

- 1. Login to the **EventTracker web interface**.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.
- 3. In My Dashboard, Click the Import button.





- Click Browse 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 WSG.etwd" is saved and click Upload.
- 5. Wait while EventTracker populates all the available dashboards. Enable Select All and click "Import".

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





6. Verifying Knowledge Pack in EventTracker

6.1 Categories

- 1. Login to the **EventTracker web interface**.
- 2. Click Admin dropdown and click Categories.
- 3. In **Category Tree** to view imported categories, click the **Search** tab and enter **Barracuda WSG** in the search.

Category					
Category Tree Search					
Barracuda WSG	Q Q				
Category					
✓ Barracuda WSG: Configuration Changes					
🗸 Barracuda WSG: Login Failure					
🗸 Barracuda WSG: Logon Success					
👽 Barracuda WSG: Web Traffic					

6.2 Alerts

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

Alerts Show All v							~	★ / Admi barracuda wsg	n / Aler		
	291 Available Alerts Tota Austra of a last available	103 Active Alerts Total number of active alerts				291 System/User Defined Count for system and user def	System User 91 Alerts ned alerts	200	291 Alerts by Threat I Count of alerts by threat	Concer 17 10 Low 10 even 6 or 6 0 7	
	Activate Now Click 'Activate Now' after making all e	hanges								Total: 3 Page Size 2	5 🗸
	Alert Name A	Three	at	Active	Email	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To	
	ြ နိုန် Barracuda WSG: Configuration changes	•								Barracuda web security gateway 11	
	📋 βδ Barracuda WSG: Login failure	•								Barracuda web security gateway 11	
	βδ Barracuda WSG: Potential threat has been detected	•								Barracuda web security gateway 11	

6.3 Flex Reports

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



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

Report Configuration					
Scheduled OQueued ODefined					
Report Groups			Ð		
🔁 Barracuda WSG	Ē	Ø			

6.4 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 WSG** group folder to view the imported Knowledge objects.



6.5 Dashboards

1. In the EventTracker web interface, Click **Home** and select **My Dashboard**.



	Home
Dashb	My Dashboard
R	Threats
	Incidents

2. In the Barracuda WSG dashboard you see the following screen.

Customize dashlets			×
Barracuda wsg			Q
Barracuda WSG - Allowed tra	Barracuda WSG - Configurati	Barracuda WSG - Threat typ e	Barracuda WSG - Top Suspici
Barracuda WSG - Top URLs al	Barracuda WSG - User login	Barracuda WSG - User login	Barracuda WSG - Web traffic
Barracuda WSG - Web traffic			
			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, endpoint 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 <u>Twitter</u> or <u>LinkedIn</u>. Netsurion is #19 among <u>MSSP Alert's 2020 Top 250 MSSPs</u>.

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