Netsurion®
Powering Secure and Agile Networks

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

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 04:23:48 PM	192.168.137.1	216.58.220.35	http://www.google.co.in/?gfe_rd=cr&ei=PHyqWLXwNunI8AeizZXoCg	1064	2	0	MIKE
02/24/2017 04:23:48 PM	192.168.137.1	172.217.26.163	http://fonts.gstatic.com/s/lato/v13/H2DMvhDLycM56KNuAtbJYA.woff2	23159	2	0	ANON
02/24/2017 04:23:48 PM	192.168.137.1	104.24.127.96	http://analytics.planwallpaper.com/piwik.php?action_name=High0Definition0and0high0resolution0wallpapers&idsite=7&rec=1&r=400261&h=11&m=2&s=35&url=httpA	320	2	0	Doe, John, CN=Users, DC=qc, DC=local

Logs Considered:

LOG TIME	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 **Category Id:** 4	**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 ALLOWED CLEAN 2 0 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 ALLOWED 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.planwallpaper.com/static/assets/css/font-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.com/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.emergingthreats.net/fwrules/emerging-Block-IPs.txt	text/plain	28206	2	0	[ANON]

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/27/2017 1:06:17 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 11:00:21 PNPL-6-KP http_scan[9688]: 1487568595 1 192.168.137.1 96.43.137.99 text/plain 192.168.137.1 http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt 28206 BYF BLOCKED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 rules.emergingthreats.net cat-lookup-failed [ANON] http://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt - - 0				
2/27/2017 1:06:17 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 10:49:21 PNPL-6-KP http_scan[9689]: 1487567934 1 192.168.137.1 173.223.235.8 text/plain 192.168.137.1 http://www.msftncsi.com/ncsi.txt 277 BYF BLOCKED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 www.msftncsi.com cat-lookup-failed [cn=Administrator,cn=Users,dc=Contoso,dc=Com - LDAP USER] http://www.msftncsi.com/ncsi.txt - - 0				

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_repeat	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

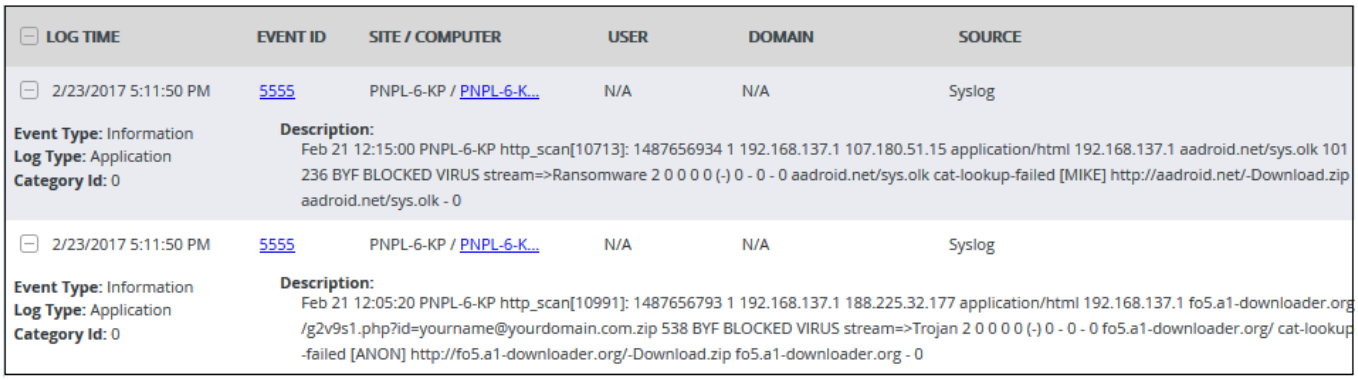
Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
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 **Category Id:** 0	**Description:** 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 / PNPL-6-K...	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.

LogTime	Source IP	Destination IP	Destination Url	Data size	Virus stream 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/g2v9s1.php?id=yourname@yourdomain.com.zip	538	Trojan	2	ANON	http://fo5.a1-downloader.org/-Download.zip fo5.a1-
02/21/2017 12:44:22 PM	192.168.137.1	213.211.198.62	http://www.eicar.org/download/eicar_com.zip	538	Eicar	2	CN=Jane Doe, CN=Users, DC=qc, DC=local	http://www.eicar.org/85-0-Download.html www.eicar.org
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/sys.olk
02/21/2017 12:44:22 PM	10.1.1.8	127.0.0.1	http://www.eicar.org/download/eicar.com.txt	1223	Eicar-Test-Signature FOUND	2	DOE	http://www.eicar.org/index.html

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
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 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 101 236 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.zip aadroid.net/sys.olk - 0

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/23/2017 5:11:50 PM	5555	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Syslog

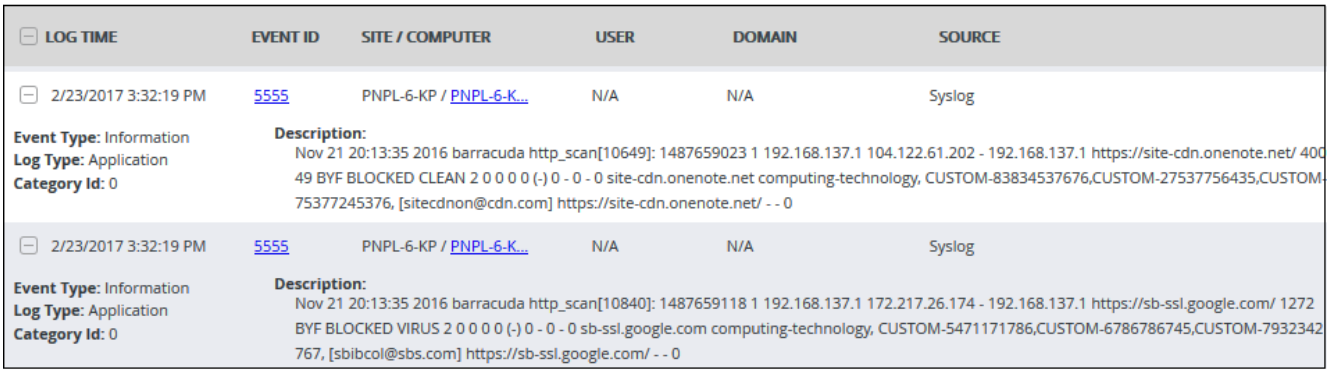
Event Type: Information
Log Type: Application
Category Id: 0

Description:
Feb 21 12:05:20 PNPL-6-KP http_scan[10991]: 1487656793 1 192.168.137.1 188.225.32.177 application/html 192.168.137.1 fo5.a1-downloader.org /g2v9s1.php?id=yourname@yourdomain.com.zip 538 BYF BLOCKED VIRUS stream=>Trojan 2 0 0 0 0 (-) 0 - 0 - 0 fo5.a1-downloader.org/ cat-lookup -failed [ANON] http://fo5.a1-downloader.org/-Download.zip fo5.a1-downloader.org - 0

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.gstatic.com/	ALLOWED	CLEAN	CUSTOM-353783667,CUSTOM-76676773536,CUSTOM-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,CUSTOM-6786786745,CUSTOM-7932342767,	sbibcol@sbs.com	https://sb-ssl.google.com/
02/23/2017 03:16:39 PM	192.168.137.1	104.122.61.202	https://site-cdn.onenote.net/	BLOCKED	CLEAN	CUSTOM-83834537676,CUSTOM-27537756435,CUSTOM-75377245376,	sitecdnon@cdn.com	https://site-cdn.onenote.net/

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/23/2017 3:32:19 PM	5555	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
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-cdn.onenote.net/ 400 49 BYF BLOCKED CLEAN 2 0 0 0 0 (-) 0 - 0 - 0 site-cdn.onenote.net computing-technology, CUSTOM-83834537676,CUSTOM-27537756435,CUSTOM-75377245376, [sitecdnon@cdn.com] https://site-cdn.onenote.net/ - - 0

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/23/2017 3:32:19 PM	5555	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Syslog

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Nov 21 20:13:35 2016 barracuda http_scan[10840]: 1487659118 1 192.168.137.1 172.217.26.174 - 192.168.137.1 https://sb-ssl.google.com/ 1272 BYF BLOCKED VIRUS 2 0 0 0 0 (-) 0 - 0 - 0 sb-ssl.google.com computing-technology, CUSTOM-5471171786,CUSTOM-6786786745,CUSTOM-7932342767, [sbibcol@sbs.com] https://sb-ssl.google.com/ - - 0

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:

LOG TIME	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	**Description:** Feb 20 10:12:09 PNPL-6-KP web: [192.168.137.1] LOGOFF (admin)				

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

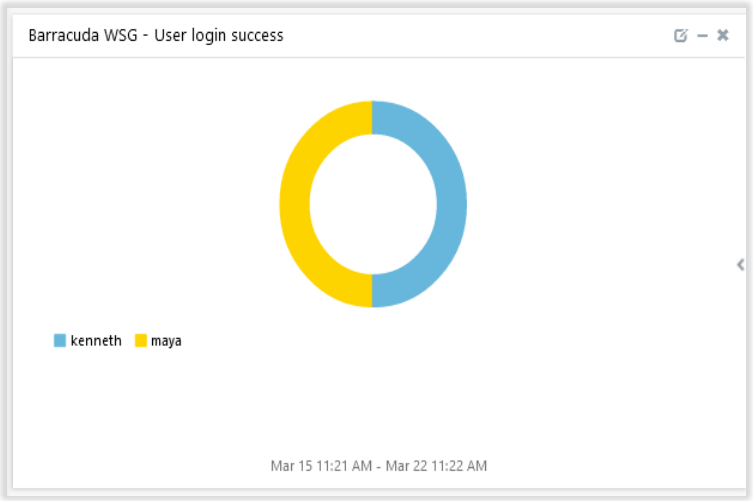
LogTime	Source IP	User
02/17/2017 11:16:39 AM	192.168.137.1	admin
02/20/2017 10:49:41 AM	192.168.137.74	aaron
02/21/2017 12:12:34 PM	192.168.137.1	admin
02/22/2017 11:16:02 AM	192.168.137.74	admin
02/21/2017 12:54:45 PM	192.168.137.1	neeson

Logs Considered:

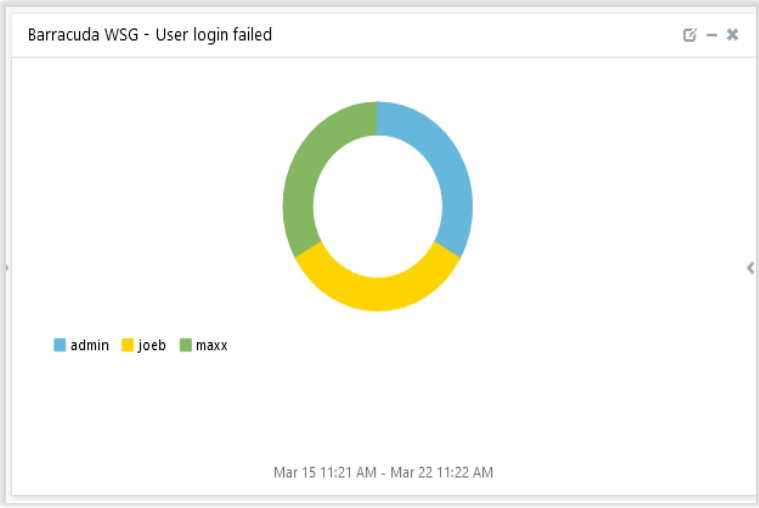
LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
2/27/2017 2:54:04 PM	5555	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Syslog
Event Type: Information **Log Type:** Application **Category Id:** 0	**Description:** Feb 21 12:54:45 PNPL-6-KP web: [192.168.137.1] FAILED_LOGIN (neeson)				
2/27/2017 2:54:04 PM	5555	PNPL-6-KP / PNPL-6-K...	N/A	N/A	Syslog
Event Type: Information **Log Type:** Application **Category Id:** 0	**Description:** Feb 21 12:12:34 PNPL-6-KP web: [192.168.137.1] FAILED_LOGIN (admin)				

4.4 Dashboards

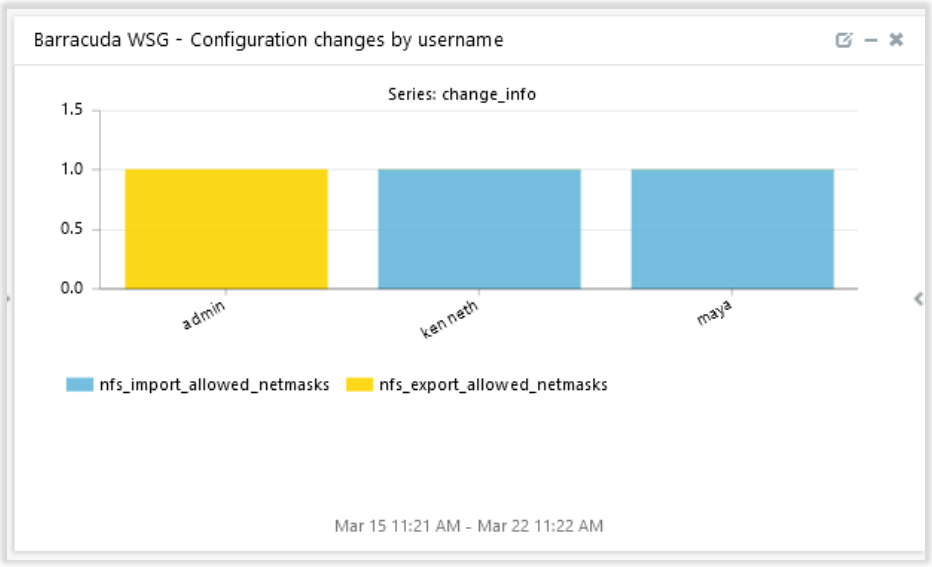
- **Barracuda WSG – User login success**



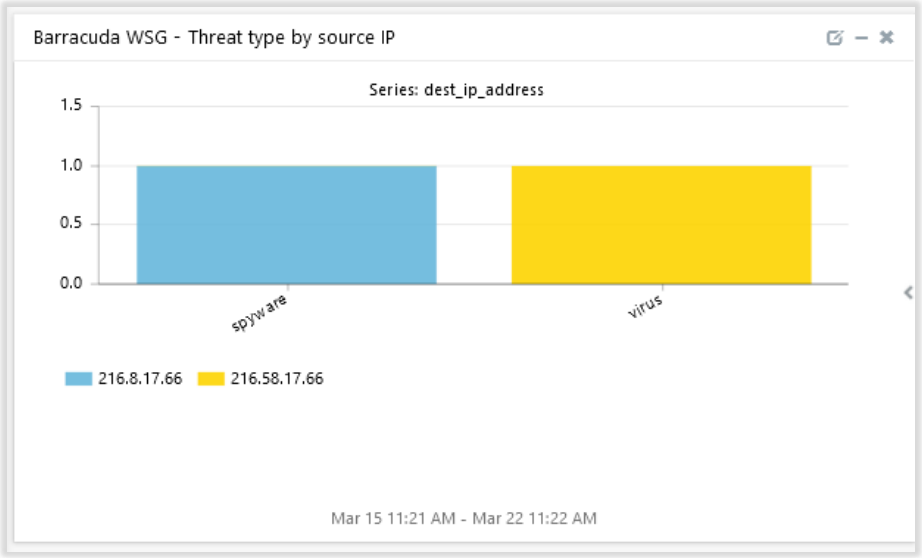
- **Barracuda WSG – User login failed**



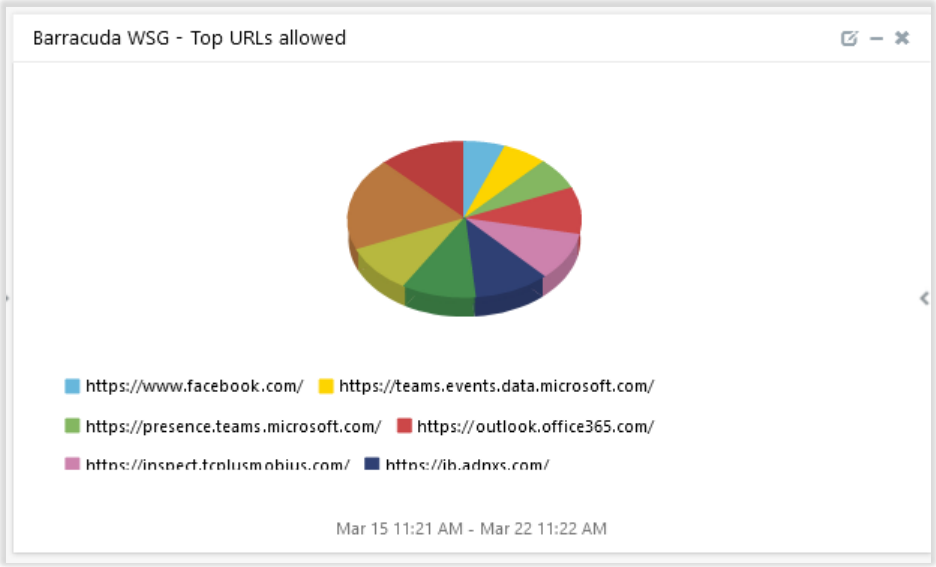
- **Barracuda WSG – Configuration changes by username**



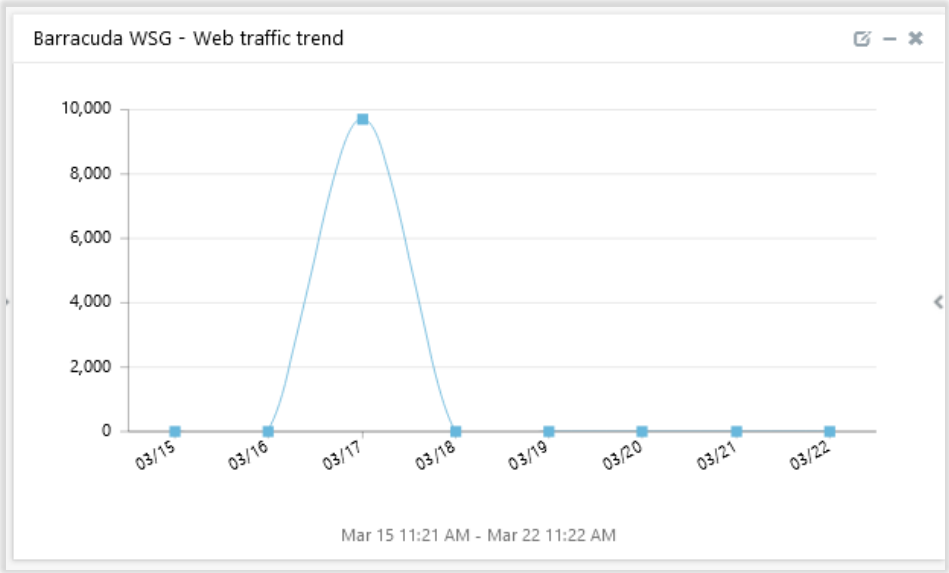
- **Barracuda WSG – Threat type by source IP**



- **Barracuda WSG – Top URLs allowed**

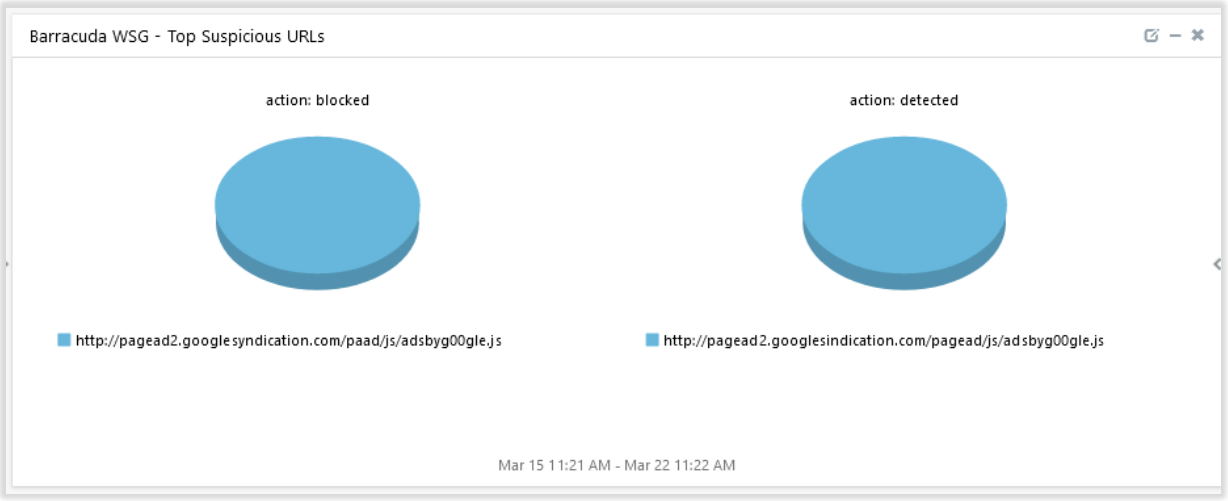


- **Barracuda WSG – Web traffic trend**

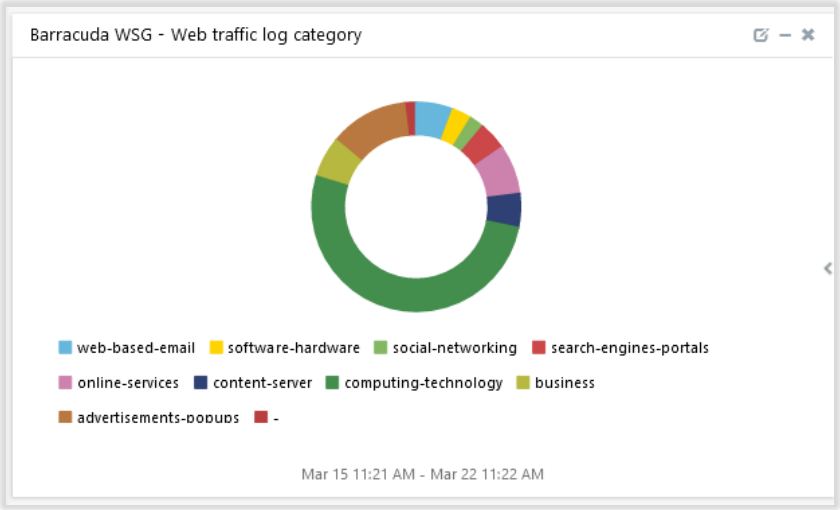


- **Barracuda WSG – Allowed traffic by destination IP**

- **Barracuda WSG – Top Suspicious URLs**



- **Barracuda WSG – Web traffic by log category**

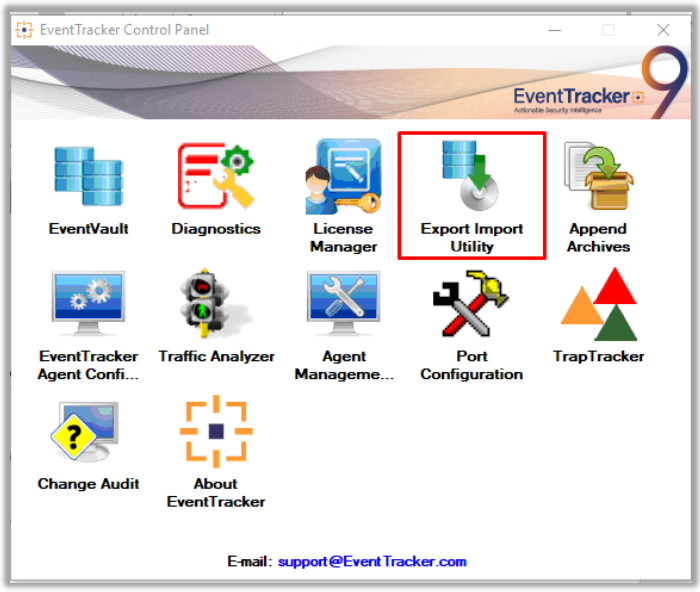


5. Importing Knowledge Pack into EventTracker

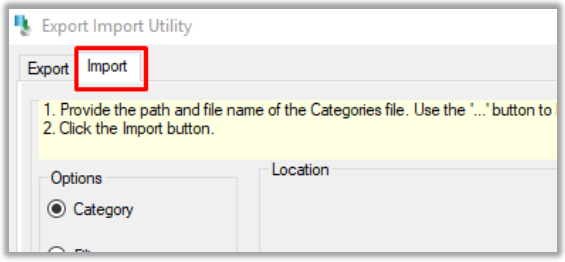
NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Flex Reports
- Knowledge Objects
- Dashboards

1. Launch the **EventTracker Control Panel**.
2. Double click **Export-Import Utility**.



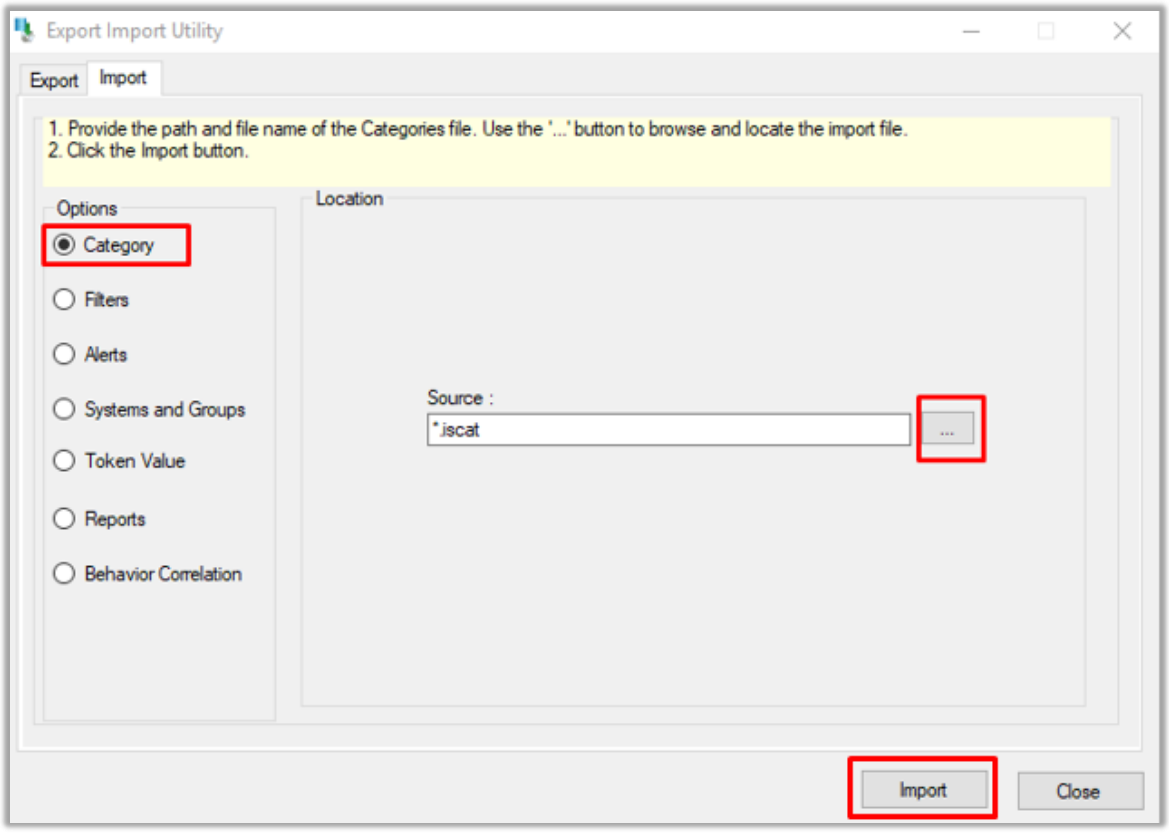
Export-Import Utility window opens.



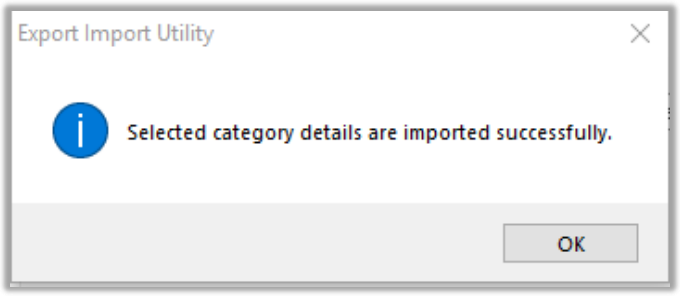
3. Click the **Import** tab.

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**.

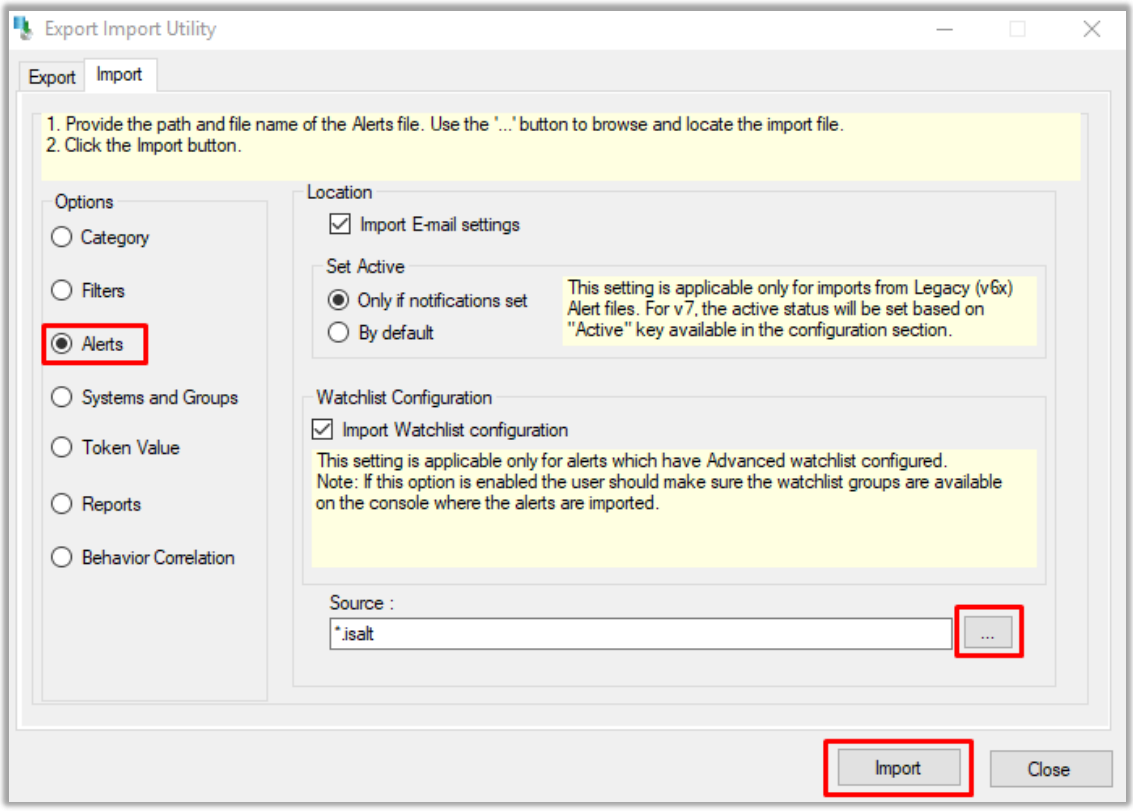


EventTracker displays a success message.

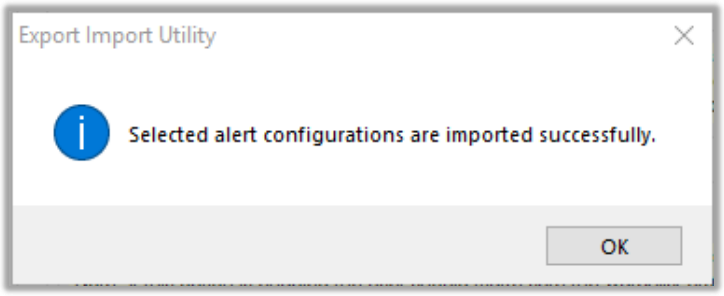


5.2 Alerts

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**.

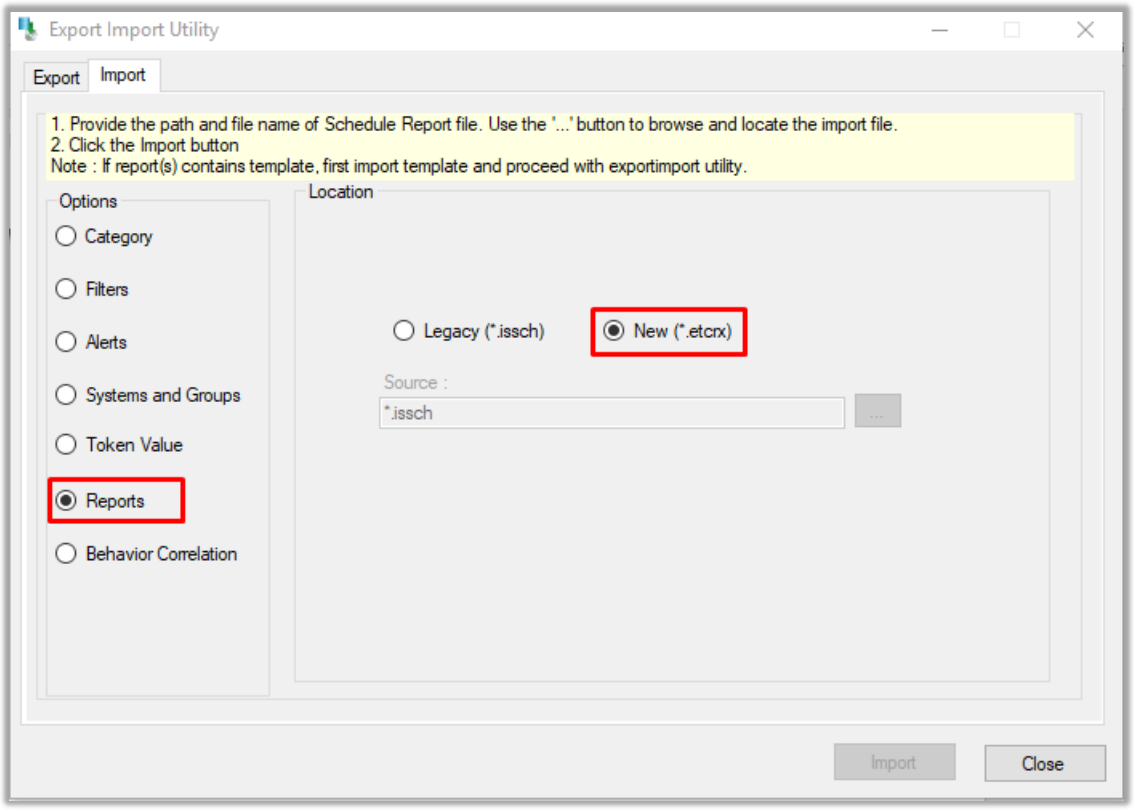


EventTracker displays a success message.

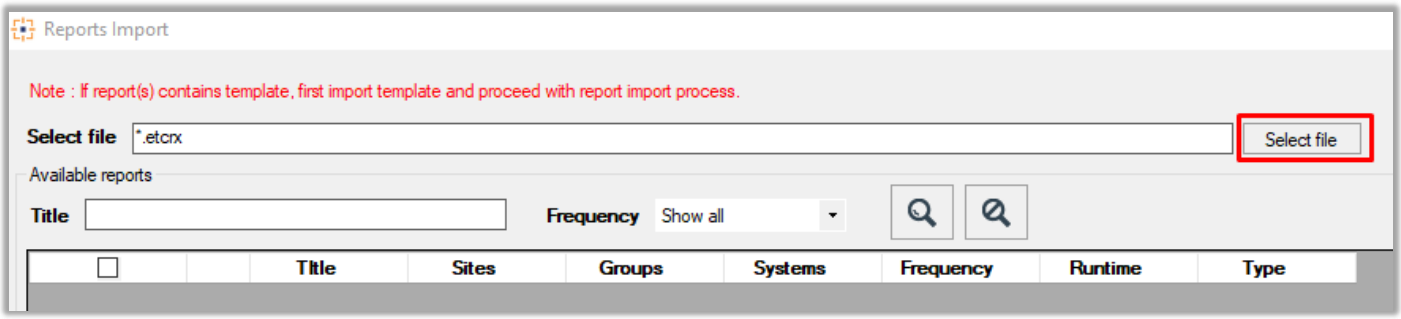


5.3 Flex Reports

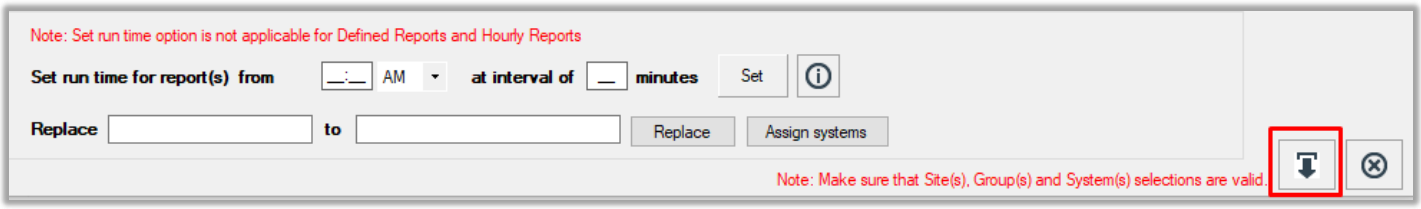
1. In **Export-Import Utility** window, select the **Import tab**. Click the **Reports** option, and choose "**New (*.etcrx)**".



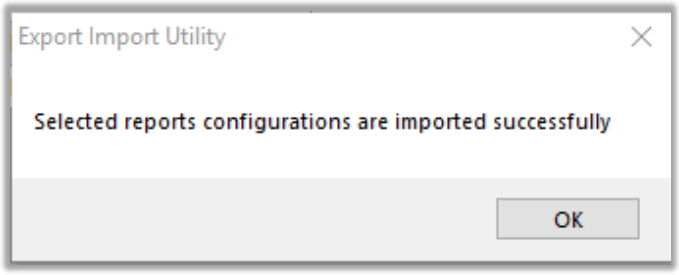
2. A new pop-up window appears. Click the **Select File** button and navigate to the knowledge pack folder and select file with the extension **".etcrx", e.g., "Reports_Barracuda WSG.etcrx".**



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

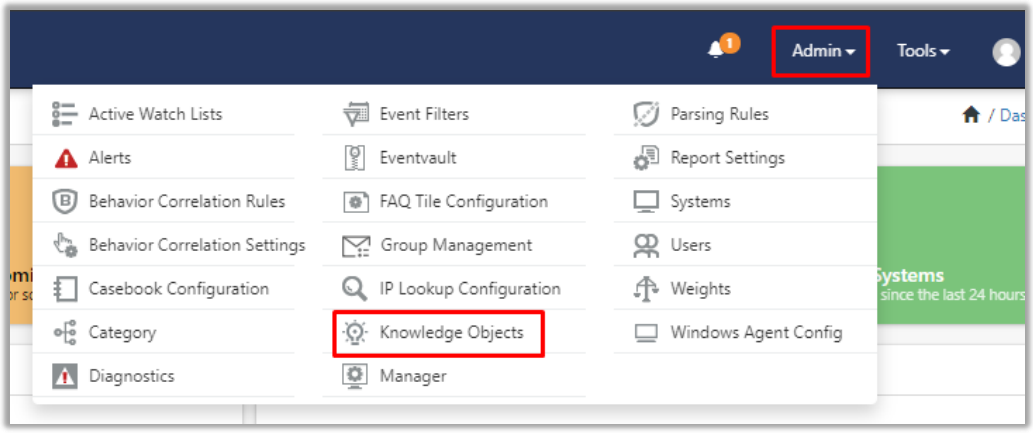


EventTracker displays a success message.

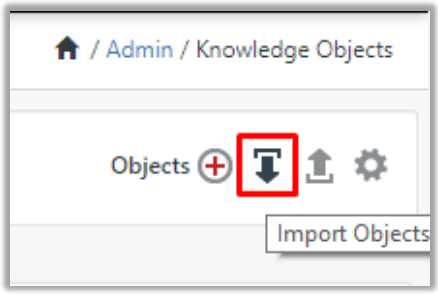


5.4 Knowledge Objects

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



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

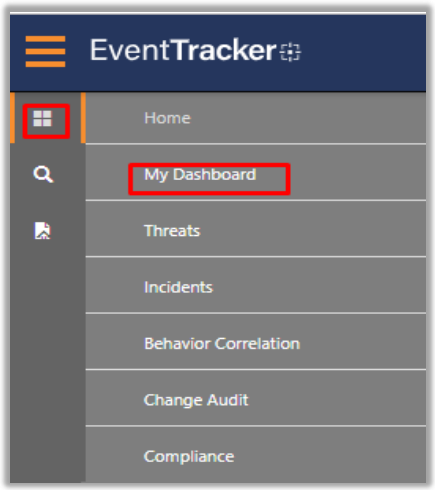


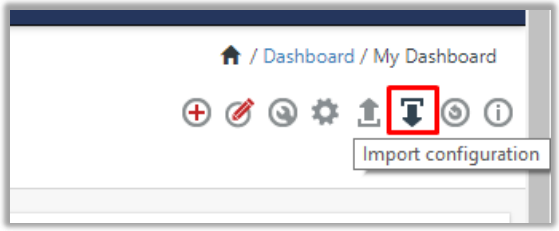
3. A pop-up box appears, click **Browse** and navigate to the knowledge packs folder (type "**C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs**" in the navigation bar) with the extension **".etko", e.g., "KO_Barracuda WSG.etko"** and click **Upload**.

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

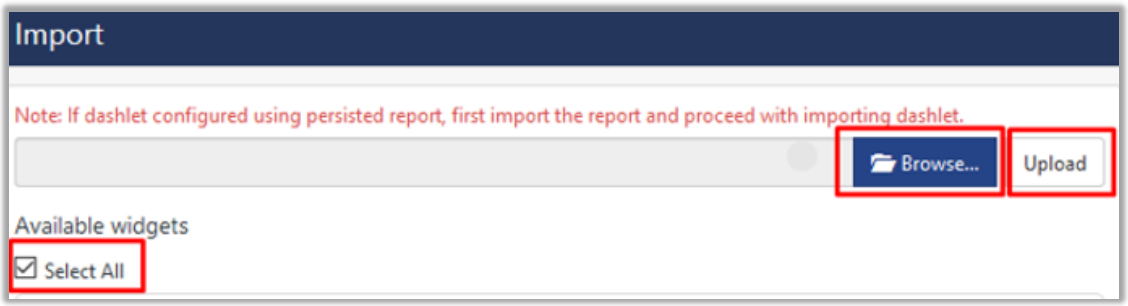
1. Login to the **EventTracker web interface**.
2. Navigate to **Dashboard** → **My Dashboard**.
3. In **My Dashboard**, Click the **Import** button.





4. 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**.

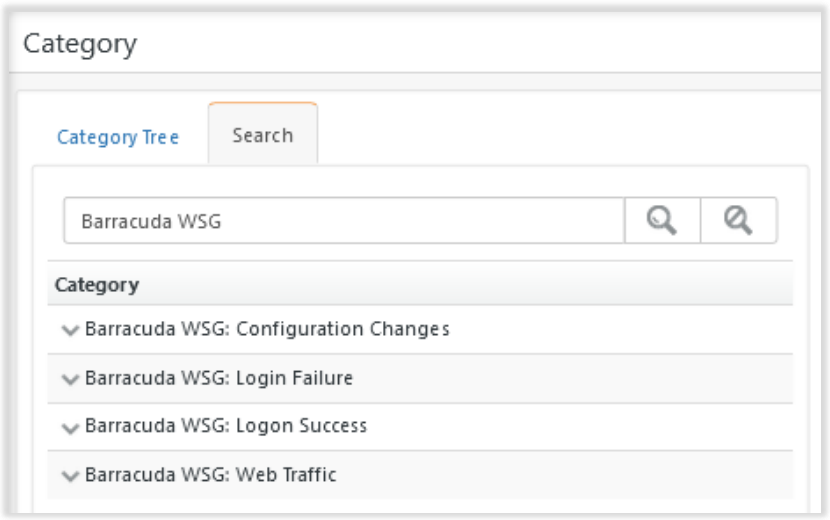
5. Wait while EventTracker populates all the available dashboards. Enable **Select All** and click **"Import"**.



6. Verifying Knowledge Pack in EventTracker

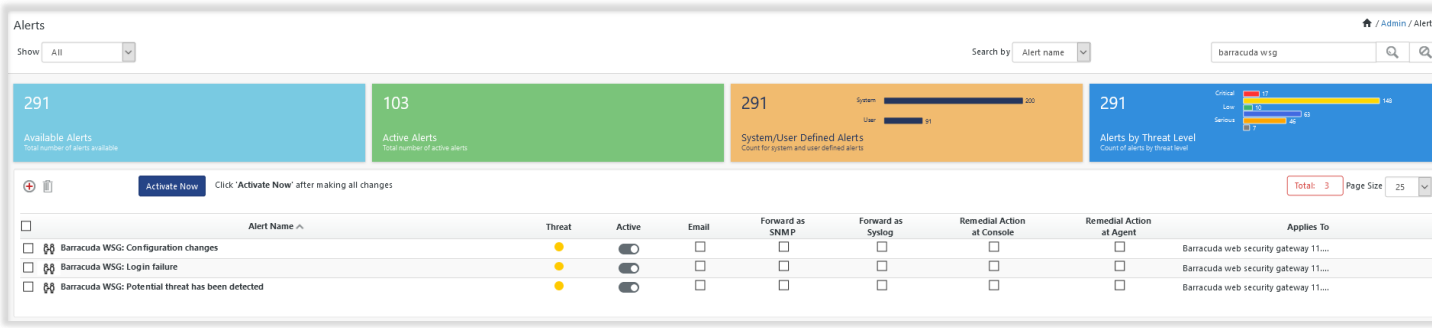
6.1 Categories

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**.**



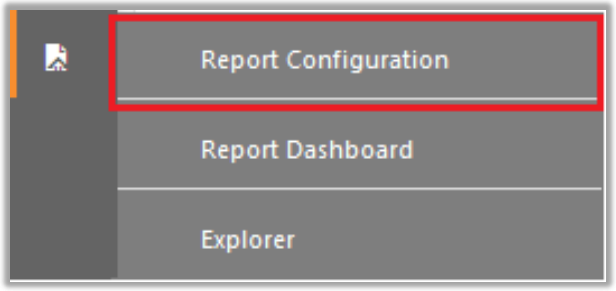
6.2 Alerts

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**.**

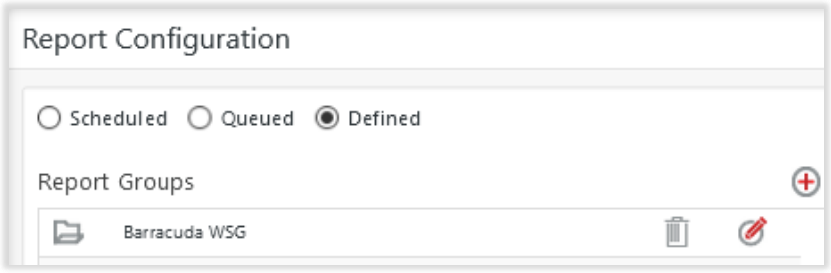


6.3 Flex Reports

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

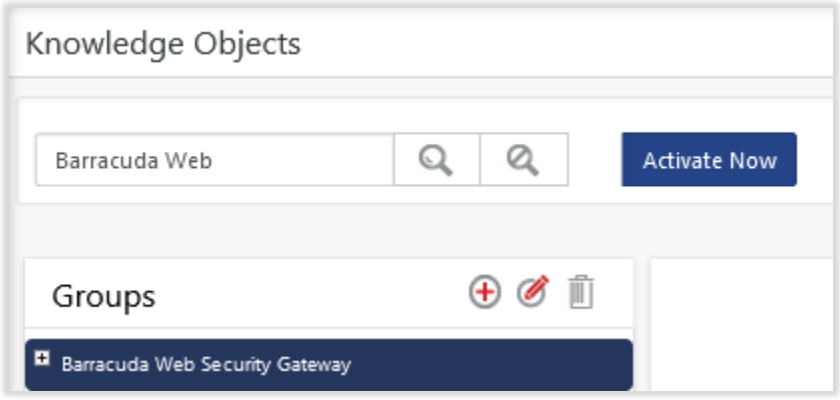


2. In the **Reports Configuration** pane, select the **Defined** option.
3. Click on the **Barracuda WSG** group folder to view the imported reports.



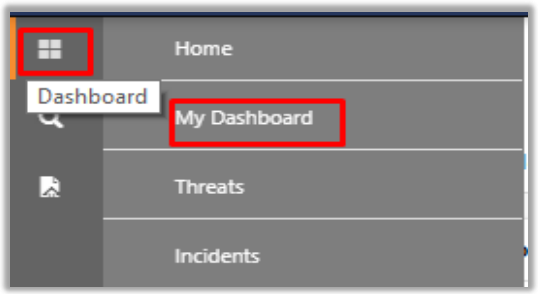
6.4 Knowledge Objects

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.

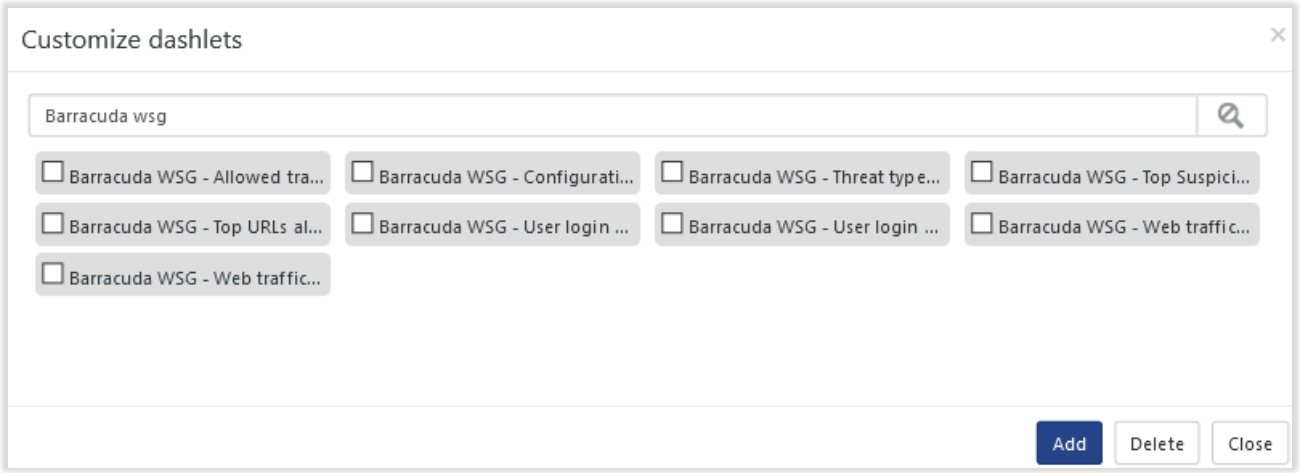


6.5 Dashboards

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



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



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, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO 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