

Integrate Barracuda Web Application Firewall

EventTracker v9.0 and Above

Abstract

This guide provides instructions to configure the Barracuda Web Application Firewall to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Barracuda Web Application Firewall.

Audience

Barracuda Web Application Firewall Admins, who wish to forward syslog events to 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.

© 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

Abstract	1
Scope	1
Audience	1
Overview	3
Prerequisites	3
Configuring Barracuda Firewall syslog	3
Adding Export Log Server	3
Adding Export Log Settings	5
Logs Format	8
EventTracker Knowledge Pack (KP)	9
Categories	9
Alerts	10
Importing Barracuda Firewall Knowledge pack into EventTracker	11
Category	11
Alerts	12
Verifying Barracuda Firewall knowledge pack in EventTracker	14
Categories	14
Alerts	15

Overview

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud.

Barracuda Web Application Firewall can be integrated with EventTracker using syslog. With the help of Barracuda Web Application Firewall KP items, we can monitor the network firewall logs, access logs, web firewall logs, system logs and audit logs on web applications. It also triggers the alert for authentication hijacking, buffer overflow attack, command injection attack, denial of service attack, and obfuscation attack.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **Barracuda Web Application Firewall** should be installed and proper access permissions to make configuration changes.

Configuring Barracuda Firewall syslog

Adding Export Log Server

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Export Logs** section, click **Add Export Log Server**. The **Add Export Log Server** window appears, specify values for the following:

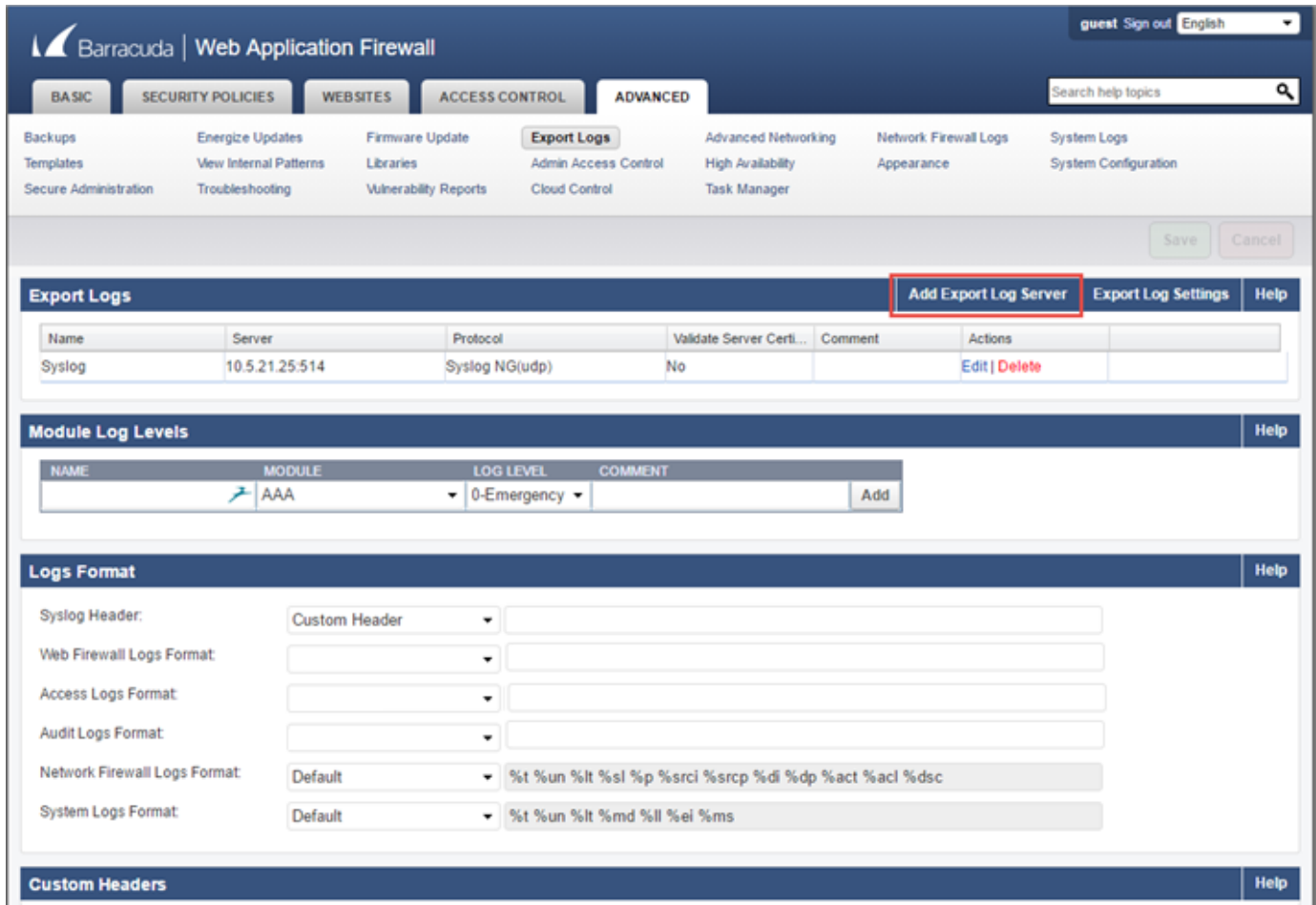


Figure 1

- **Name:** Enter a name.
- **Log Server Type:** Select **Syslog NG**.
- **IP Address:** Enter the EventTracker IP address.
- **Port:** Enter the Syslog server (514) port.
- **Connection Type:** Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the EventTracker.
- **Validate Server Certificate:** Select **No**.
- **Client Certificate:** Select **No**.
- **Log Timestamp:** Select **Yes**.

3. Click **Add**.

Web Application Firewall: Add Export Log Server - Google Chrome

waf.barracuda.com/cgi-mod/index.cgi?password=8f0a3518fe54aabf5408cecdac13c937&et=1473706864&aut

Add Export Log Server Help

Name:

Log Server Type: Syslog NG
Select the server type to which the logs needs to be exported.

IP Address: 1 . 1 . 1 . 1
The IP address of the log server.

Port: 514
The port associated with the IP address of the log server.

Connection Type: ☒ UDP ☐ TCP ☐ SSL
Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the Syslog server.

Validate Server Certificate: ☐ Yes ☒ No
Validates the syslog server certificate using the internal bundle of Certificate Authority's (CA's) certificates packaged with the system. If set to No, any certificate from the syslog server is accepted.

Client Certificate: ☐ Yes ☒ No
Set to Yes to validate the syslog server certificate using the internal bundle of Certificate Authority's (CA's) certificates packaged with the system. If set to No, any certificate from the syslog server is accepted.

Log Timestamp and Hostname: ☒ Yes ☐ No
Logs the date and time of the system events.

Comment:

Add

© 2016 Barracuda Networks, Inc. Serial #BAR-WF-489542 Firmware v8.1.0.009 (2016-05-24 03:24:30) More...

Figure 2

Adding Export Log Settings

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Export Logs** section, click **Export Log Settings**. The **Export Log Settings** window appears, specify values for the following:

The screenshot displays the Barracuda Web Application Firewall configuration interface. The top navigation bar includes tabs for BASIC, SECURITY POLICIES, WEBSITES, ACCESS CONTROL, and ADVANCED. The ADVANCED tab is selected, and the 'Export Logs' sub-tab is active. The 'Export Logs' section contains a table with one entry: 'Syslog' with server '10.5.21.25.514', protocol 'Syslog NG(udp)', and 'Validate Server Certi...' set to 'No'. The 'Export Log Settings' button is highlighted in red. Below this, the 'Module Log Levels' section shows a table with 'NAME' as 'AAA' and 'LOG LEVEL' as '0-Emergency'. The 'Logs Format' section contains several format settings: 'Syslog Header' (Custom Header), 'Web Firewall Logs Format' (.), 'Access Logs Format' (.), 'Audit Logs Format' (.), 'Network Firewall Logs Format' (Default), and 'System Logs Format' (Default). The 'Custom Headers' section is visible at the bottom.

Export Logs

Name	Server	Protocol	Validate Server Certi...	Comment	Actions
Syslog	10.5.21.25.514	Syslog NG(udp)	No		Edit Delete

Module Log Levels

NAME	MODULE	LOG LEVEL	COMMENT
	AAA	0-Emergency	

Logs Format

Syslog Header:	Custom Header	
Web Firewall Logs Format:	.	
Access Logs Format:		
Audit Logs Format:		
Network Firewall Logs Format:	Default	%t %un %lt %sl %p %srci %srp %di %dp %act %acl %dsc
System Logs Format:	Default	%t %un %lt %md %ll %ei %ms

Custom Headers

Figure 3

- 3 In the syslog settings section of the **Export Log Settings** dialog box, follow the below-mentioned screenshot process.
- 4 Click **Save**.

Web Application Firewall: Export Log Settings - Google Chrome

waf.barracuda.com/cgi-mod/index.cgi?password=45d608342f28c78b40e54cae25bc9b63&et=1473710109&au

Save **Cancel**

Export Log Settings Help

Export Web Firewall Logs ☒ Enable ☐ Disable
Set to Enable to export web firewall logs to the configured log server.

Export Access Logs ☒ Enable ☐ Disable
Set to Enable to export access logs to the configured log server.

Export Audit Logs ☒ Enable ☐ Disable
Set to Enable to export audit logs to the configured log server.

Export System Logs ☒ Enable ☐ Disable
Set to Enable to export system logs to the configured log server.

Export Network Firewall Logs ☒ Enable ☐ Disable
Set to Enable to export network firewall logs to the configured log server.

Export Log Filters Help

Web Firewall Log Severity **6-Information** ▼
Select the severity level to export web firewall logs to the configured log server.

System Log Severity **6-Information** ▼
Select the severity level to export system logs to the configured log server.

Syslog Settings Help

Web Firewall Logs Facility **local0** ▼
Select the log facility to export web firewall logs to the configured syslog server. Web Firewall Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

Access Logs Facility **local0** ▼
Select the log facility to export access logs to the configured syslog server. Access Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

Audit Logs Facility **local0** ▼
Select the log facility to export audit logs to the configured syslog server. Audit Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

System Logs Facility **local0** ▼
Select the log facility to export system logs to the configured syslog server. System Logs Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

Network Firewall Logs Facility **local0** ▼
Select the log facility to export network firewall logs to the configured syslog server. Network Firewall Log Facility is used to identify the Barracuda Web Application Firewall and distinguish it from other hosts using the same syslog server.

© 2016 Barracuda Networks, Inc. Serial #BAR-WF-489542 Firmware v8.1.0.009 (2016-05-24 03:24:30) More...

Figure 4

Logs Format

The screenshot shows the Barracuda Web Application Firewall configuration interface. The 'Export Logs' tab is active, and the 'Logs Format' section is highlighted with a red border. This section contains several configuration fields:

- Syslog Header:** Set to 'Custom Header'.
- Web Firewall Logs Format:** Set to 'Custom Format'.
- Access Logs Format:** Set to 'Custom Format'.
- Audit Logs Format:** Set to 'Custom Format'.
- Network Firewall Logs Format:** Set to 'Default'.
- System Logs Format:** Set to 'Default'.

Below the 'Logs Format' section is a 'Custom Headers' section, which is currently empty.

Figure 5

1. From the **Web Firewall Logs Format** list box, select Custom Format.
2. In the **Web Firewall Logs Format** field, type the following custom event format:
t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au
3. From the **Access Logs Format** list box, select Custom Format.
4. In the **Access Logs Format** field, type the following custom event format:
t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu
5. From the **Audit Logs Format** list box, select Custom Format.
6. In the **Audit Logs Format** field, type the following custom event format:
t=%t|trt=%trt|an=%an|li=%li|lp=%lp18.
7. From the **Network Firewall Logs Format** list box, select Default.
8. From **System Logs Format** list box, select Default.
9. Click **Save Changes**.

Barracuda Web Application Firewall events are automatically discovered. Events forwarded to EventTracker by Barracuda Web Application Firewall are displayed on the Log Search tab of EventTracker.

EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Alerts and, categories can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v9.x to support Barracuda Web Application Firewall monitoring:

Categories

- **Barracuda: Application platform exploits** - This category based report provides information related to application platform exploit.
- **Barracuda: Authentication hijacking** - This category based report provides information related to authentication hijacking.
- **Barracuda: Buffer overflow attack** - This category based report provides information related to buffer overflow attack.
- **Barracuda: Command injection attack** - This category based report provides information related to the command injection attack.
- **Barracuda: Cookie poisoning attack** - This category based report provides information related to a cookie poisoning attack.
- **Barracuda: Cross-site scripting attack** - This category based report provides information related to cross-site scripting attack.
- **Barracuda: Denial-of-service attack** - This category based report provides information related to the denial-of-service attack.
- **Barracuda: Directory traversal attack** - This category based report provides information related to directory traversal attack.
- **Barracuda: Error message interception** - This category based report provides information related to error message interception.
- **Barracuda: Firewall received messages** - This category based report provides information related to firewall received messages.
- **Barracuda: Firewall scan messages** - This category based report provides information related to firewall scan messages.

- **Barracuda: Firewall sending messages** - This category based report provides information related to firewall sending messages.
- **Barracuda: Forceful browsing attack** - This category based report provides information related to forceful browsing attack.
- **Barracuda: Form tampering attack** - This category based report provides information related to form tampering attack.
- **Barracuda: Malicious file execution attack** - This category based report provides information related to the malicious file execution attack.
- **Barracuda: Obfuscation attack** - This category based report provides information related to obfuscation attack.
- **Barracuda: Protocol exploit attack** - This category based report provides information related to protocol exploit attack.
- **Barracuda: SQL injection attack** - This category based report provides information related to the SQL injection attack.
- **Barracuda: Traffic allowed** - This category based report provides information related to traffic allowed.
- **Barracuda: Traffic denied** - This category based report provides information related to traffic denied.

Alerts

- **Barracuda: Authentication hijacking** - This alert is generated when authentication hijacking occurs.
- **Barracuda: Buffer overflow attack** - This alert is generated when a buffer overflow attack occurs.
- **Barracuda: Command injection attack** - This alert is generated when command injection attack occurs.
- **Barracuda: Cookie poisoning attack** - This alert is generated when a cookie poisoning attack occurs.
- **Barracuda: Cross-site scripting attack** - This alert is generated when cross-site scripting attack.
- **Barracuda: Denial-of-service attack** - This alert is generated when a denial-of-service attack occurs.
- **Barracuda: Error message interception** - This alert is generated when error message interception occurs.

- **Barracuda: Malicious file execution attack**- This alert is generated when a malicious file execution attack occurs.
- **Barracuda: Obfuscation attack**- This alert is generated when the obfuscation attack occurs.

Importing Barracuda Firewall Knowledge pack into EventTracker

1. Launch the **EventTracker Control Panel**.
2. Double click **Export/Import Utility**, and then click the **Import** tab.

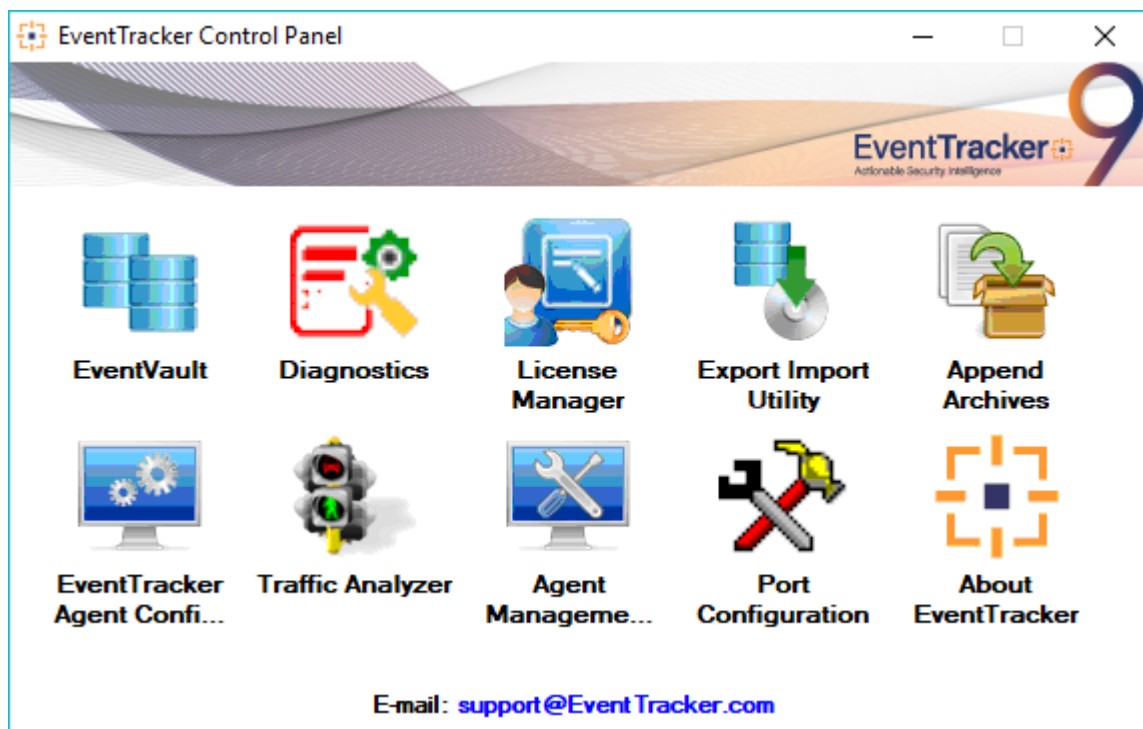


Figure 6

3. Import **Category and Alerts** as given below.

Category

1. Click **Category** option, and then click the browse  button

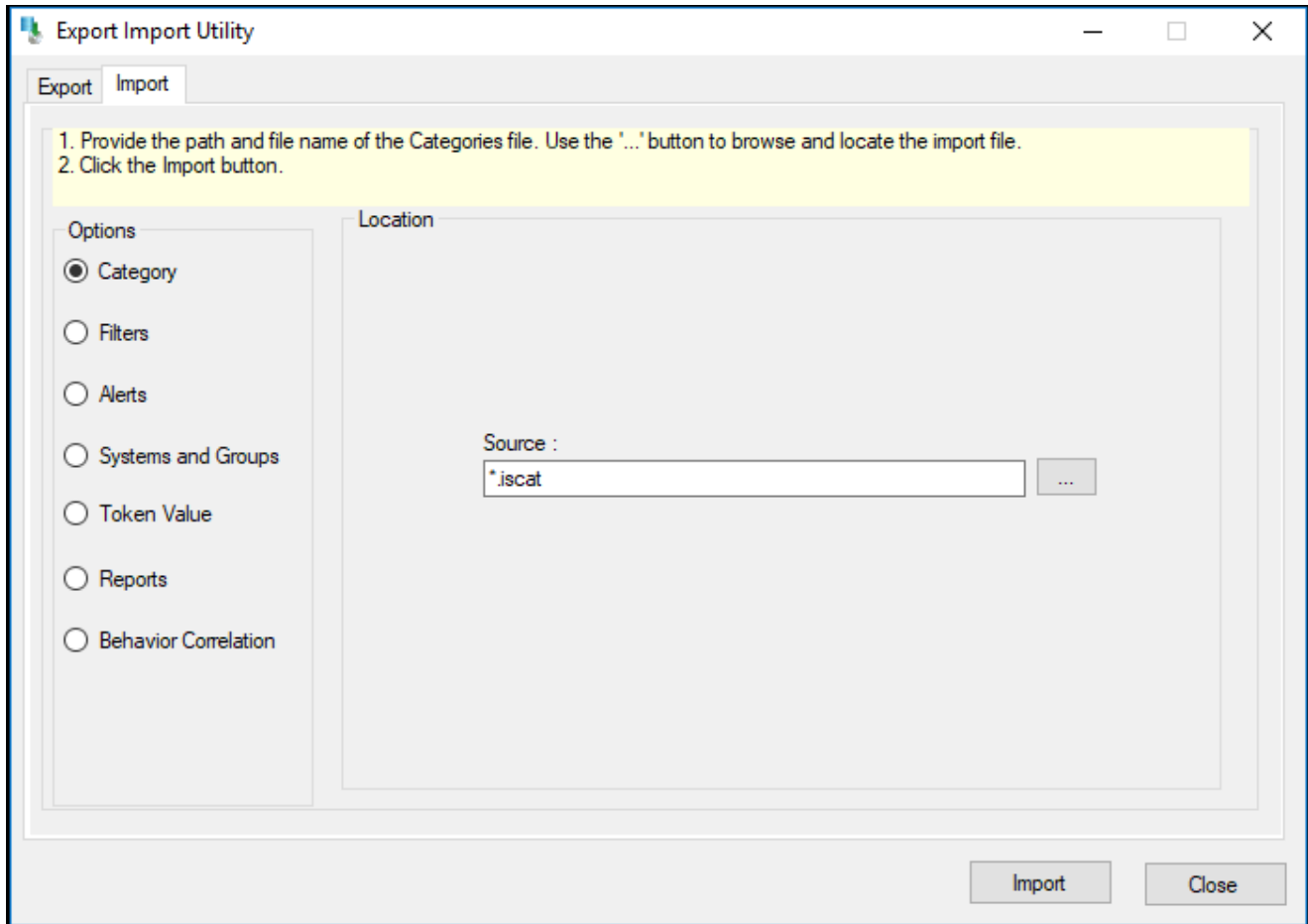


Figure 7

2. Locate **All Barracuda firewall group of Categories.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
4. EventTracker displays a success message.

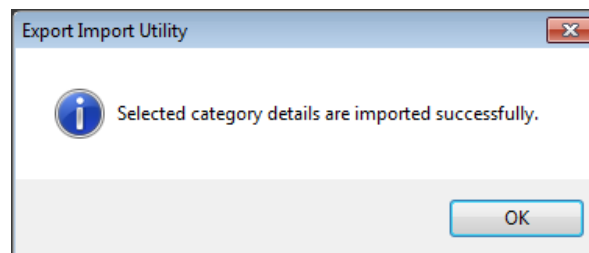



Figure 8

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

Alerts

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

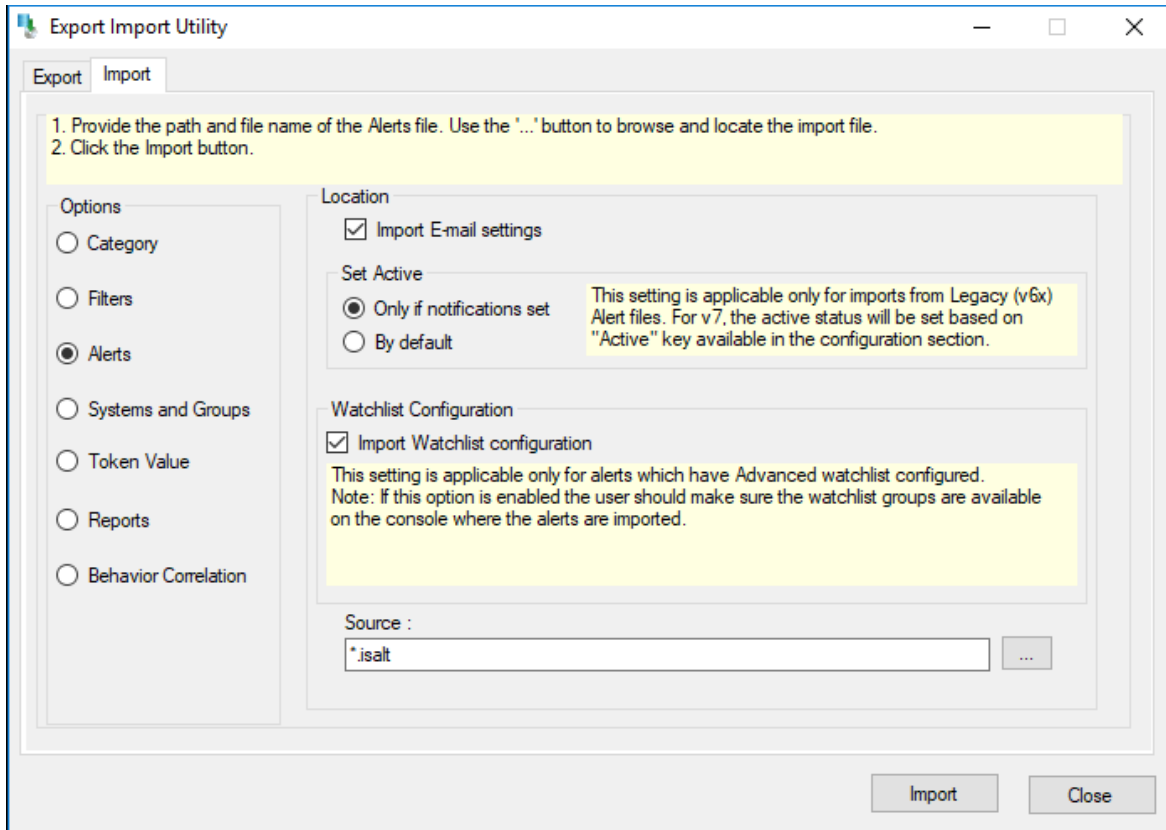


Figure 9

2. Locate **All Barracuda firewall group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
 - EventTracker displays a success message.

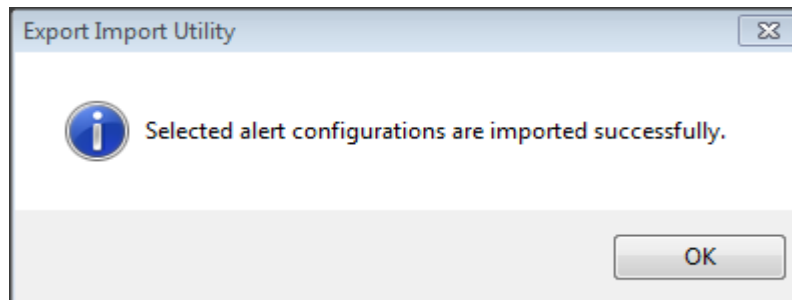


Figure 10

4. Click **OK**, and then click the **Close** button.

Verifying Barracuda Firewall knowledge pack in EventTracker

Categories

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

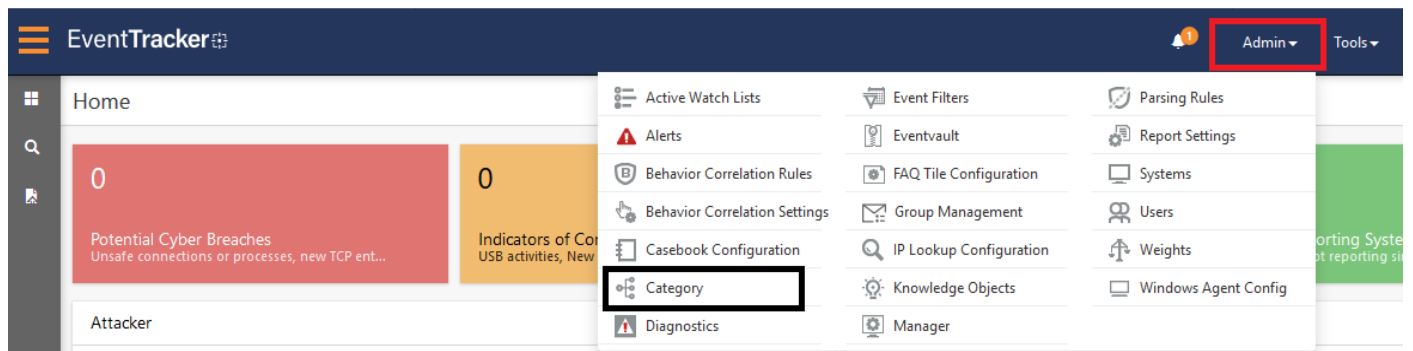


Figure 11

3. Click the **search**, and then **search** with **Barracuda**.

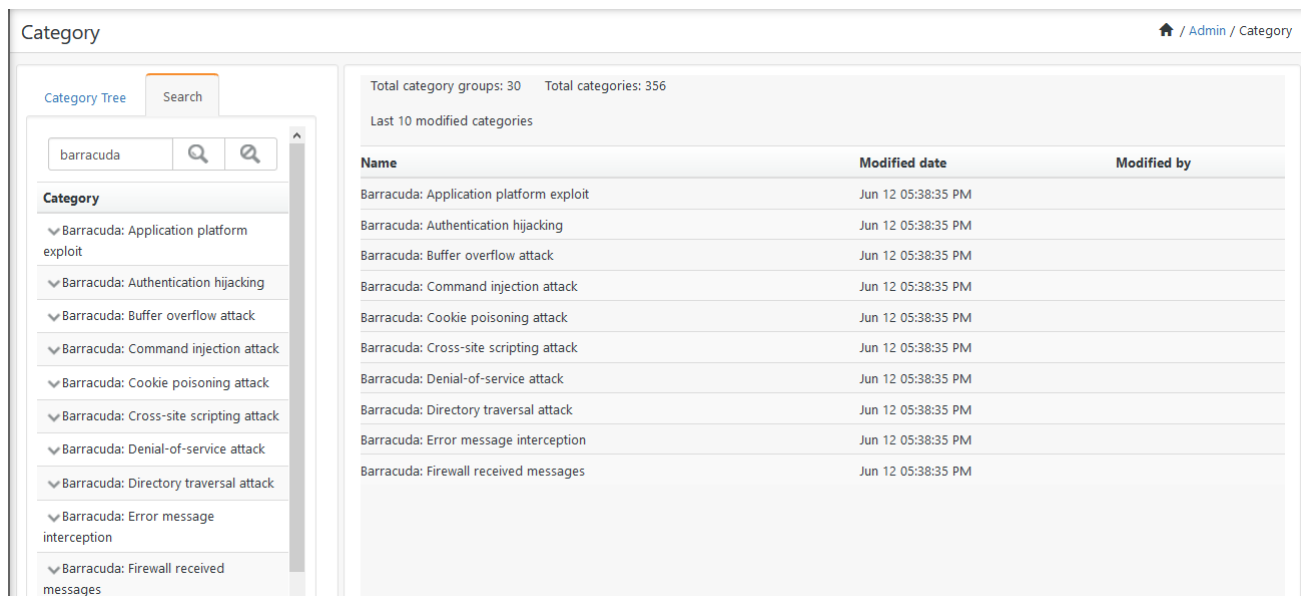


Figure 12

Alerts

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

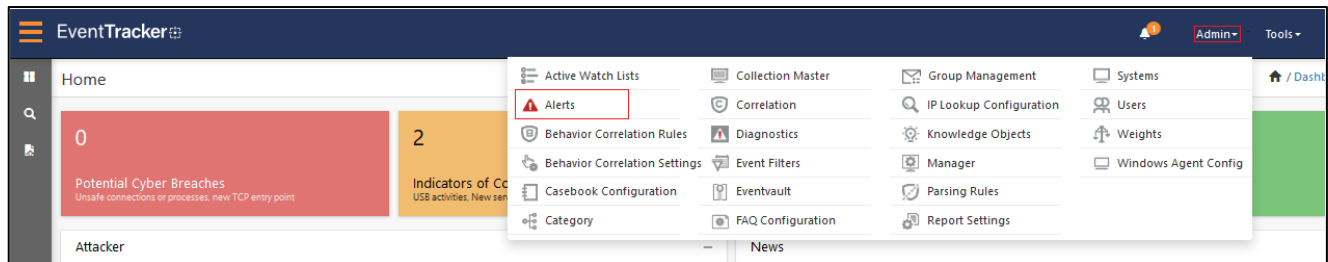


Figure 13

3. In the **Search** box, type '**Barracuda**', and then click the **search**.
Alert Management page will display all the imported alerts.

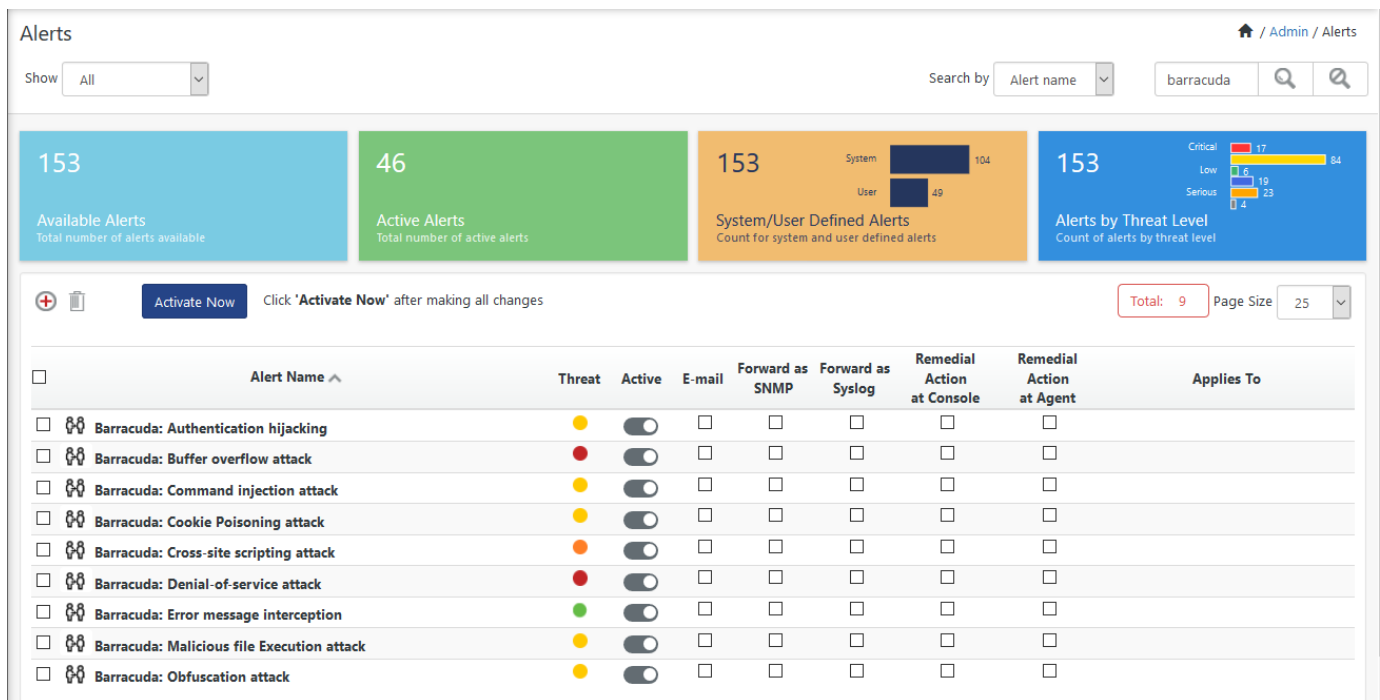


Figure 14

4. To activate the imported alerts, select the respective checkbox in the **Active** column.
EventTracker displays a message box.

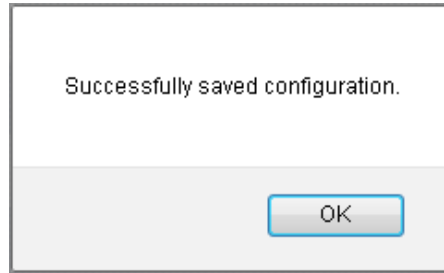


Figure 15

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

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