Netsurion™ | EventTracker

How to- Configure Barracuda Web Application Firewall to forward logs to EventTracker

EventTracker v9.0 and Above

Publication Date: June 14, 2019

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.

Table of Contents

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:

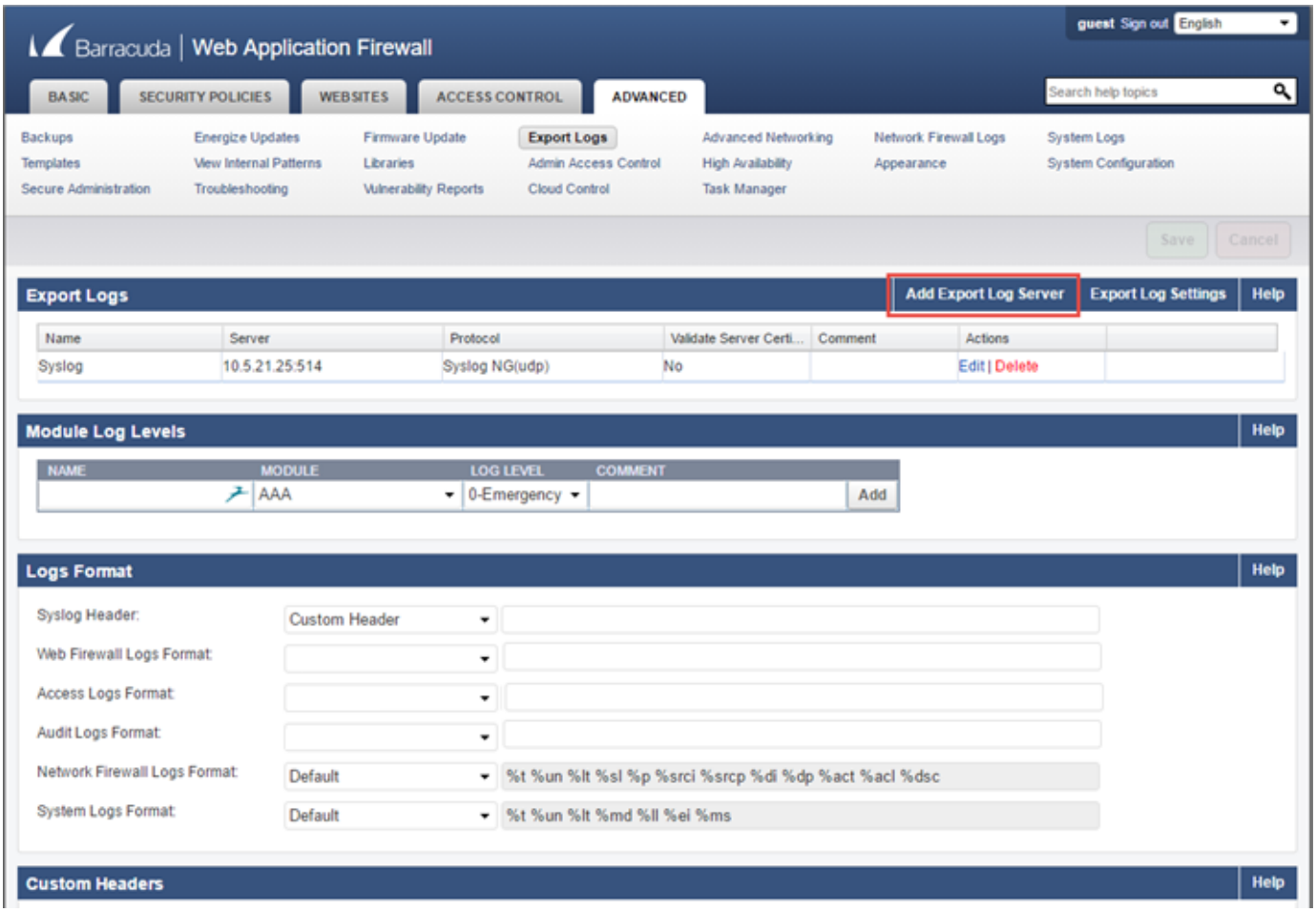

Figure 1

- **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**.

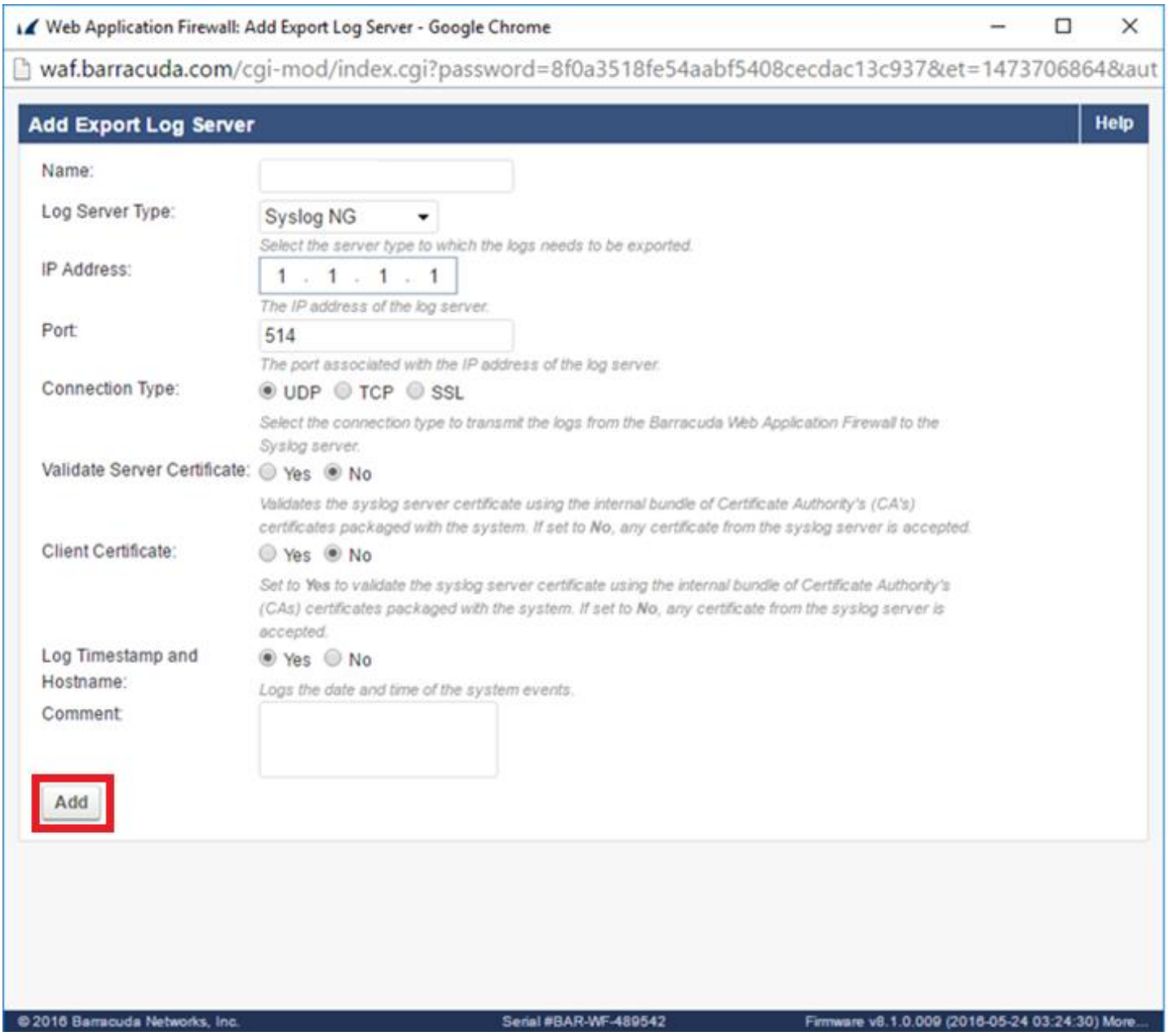

Figure 2

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:

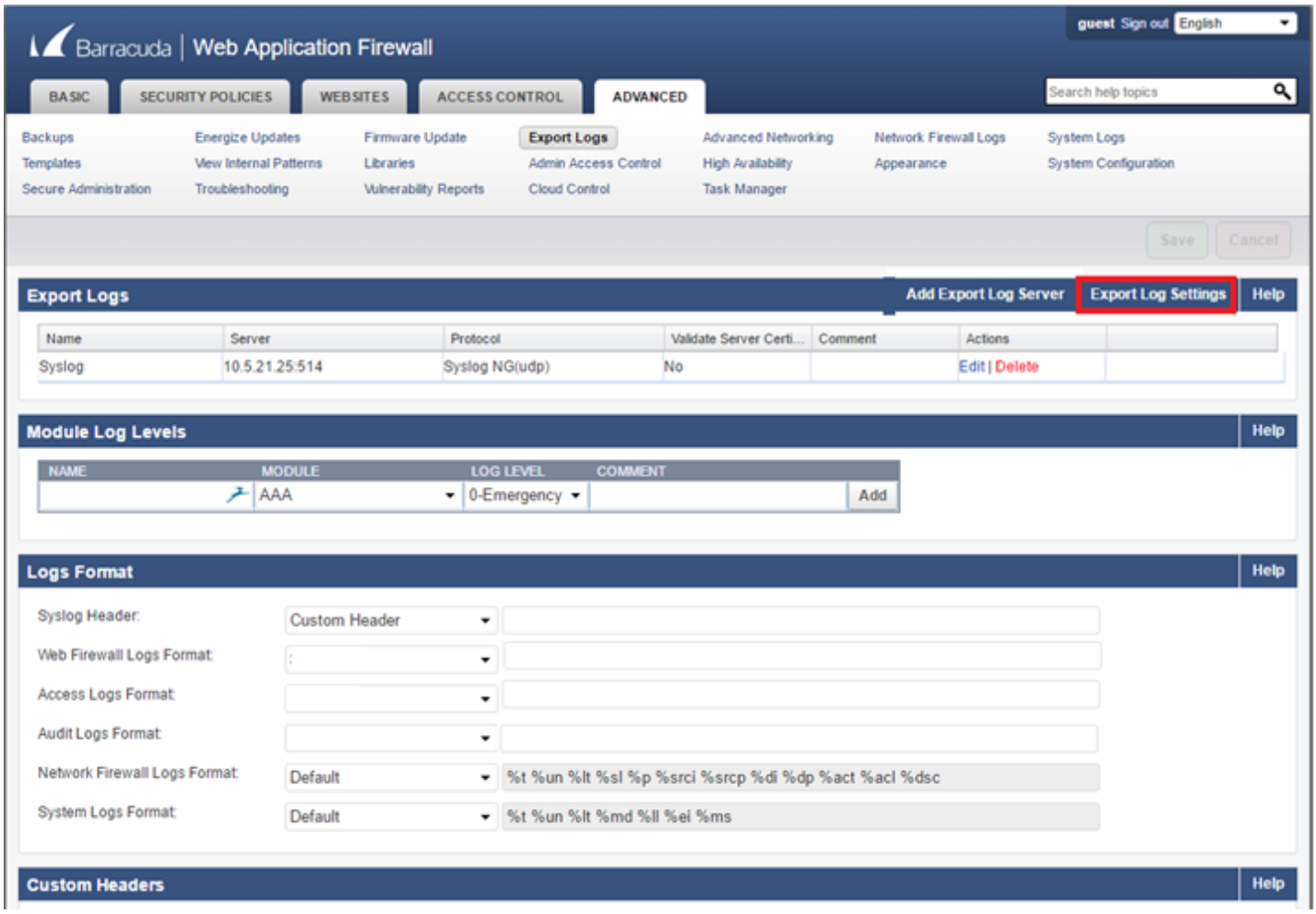

Figure 3

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

4 Click **Save**.

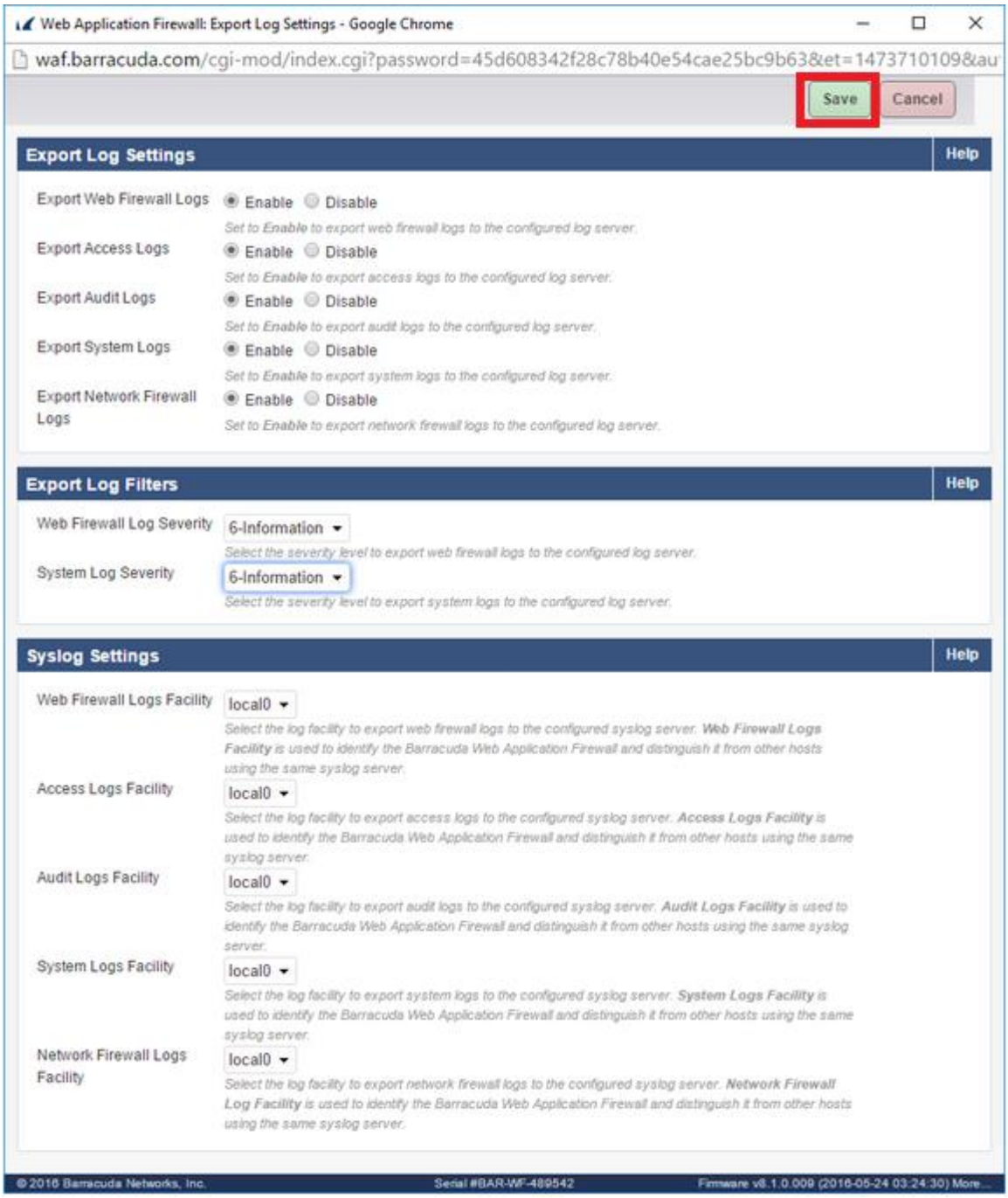
Web Application Firewall: Export Log Settings - Google Chrome
waf.barracuda.com/cgi-mod/index.cgi?password=45d608342f28c78b40e54cae25bc9b63&et=1473710109&au
Save
Cancel
Export Log Settings
Help
Export Web Firewall Logs
Enable
Disable
Set to Enable to export web firewall logs to the configured log server.
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

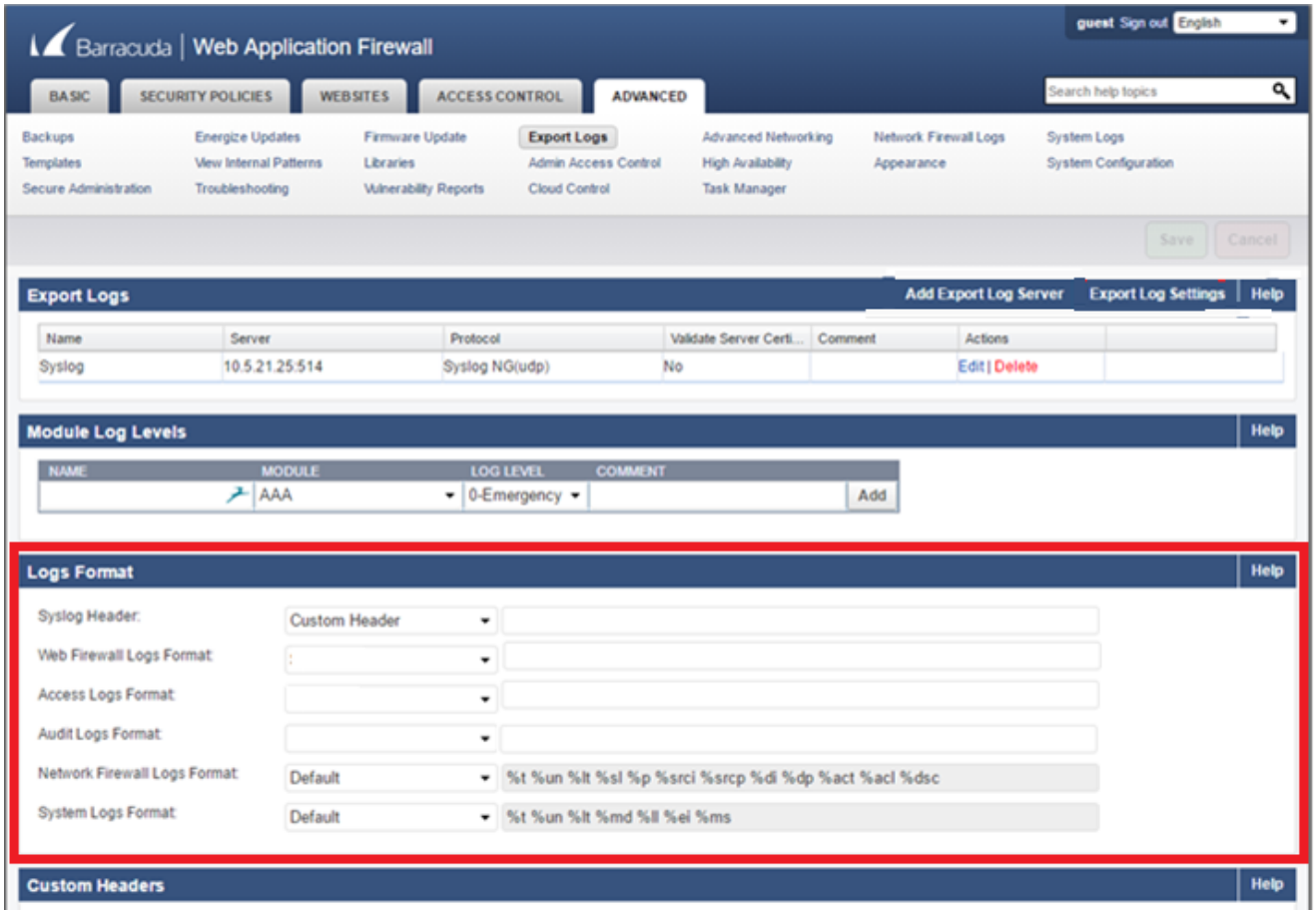

Figure 5

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.