

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

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

## 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:

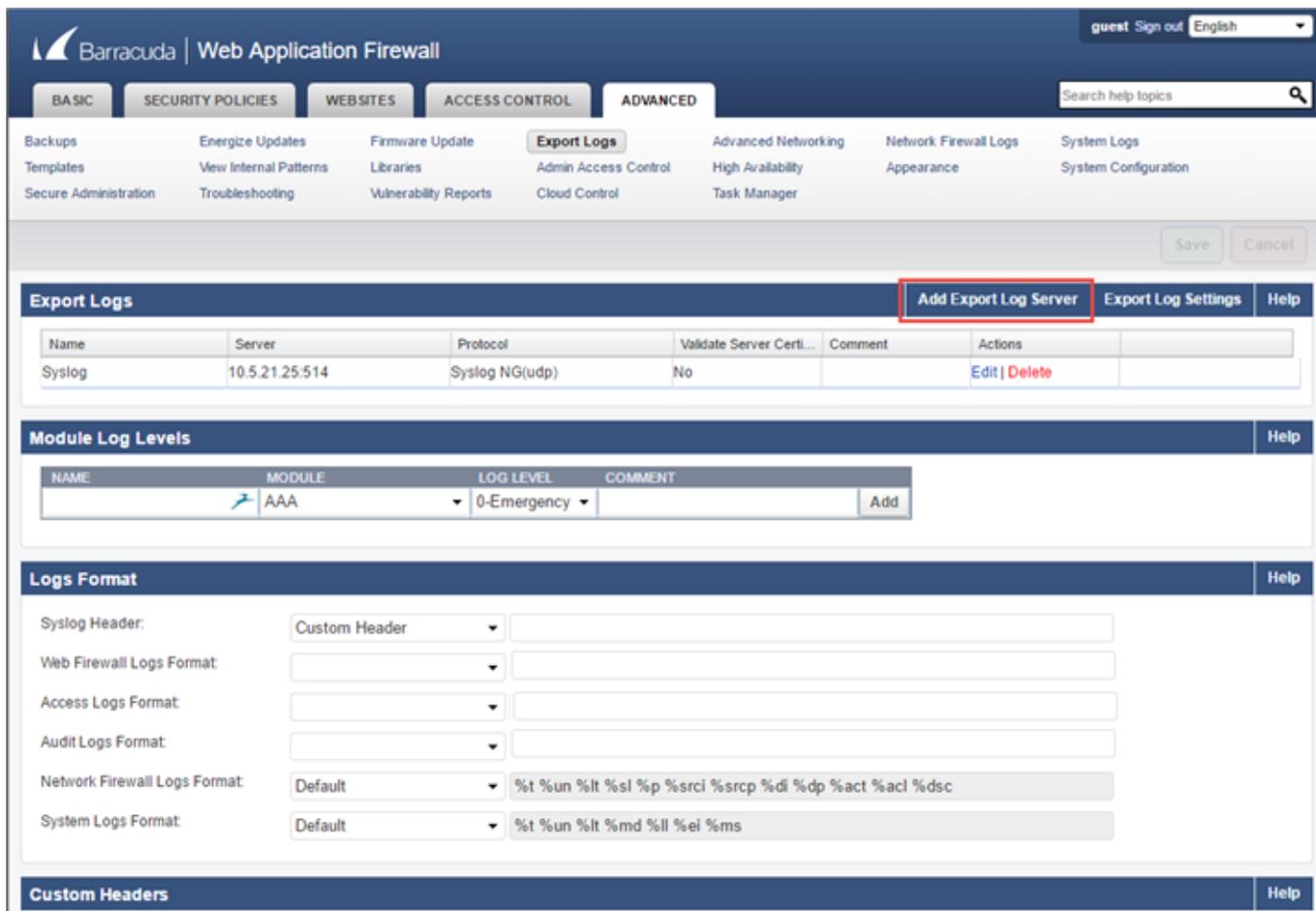


Figure 1

- **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:  Select the server type to which the logs needs to be exported.

IP Address:  The IP address of the log server.

Port:  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:

© 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:

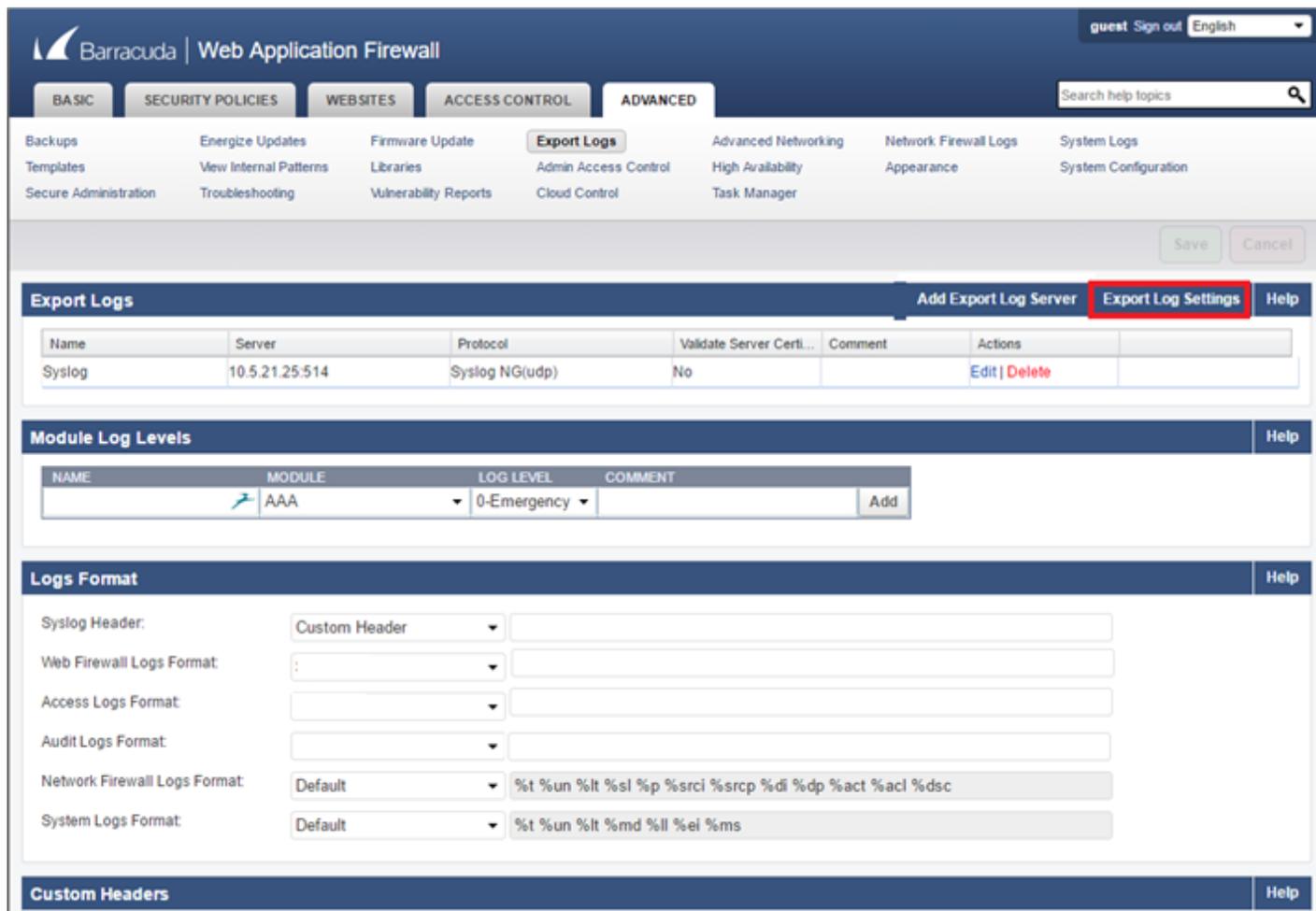


Figure 3

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

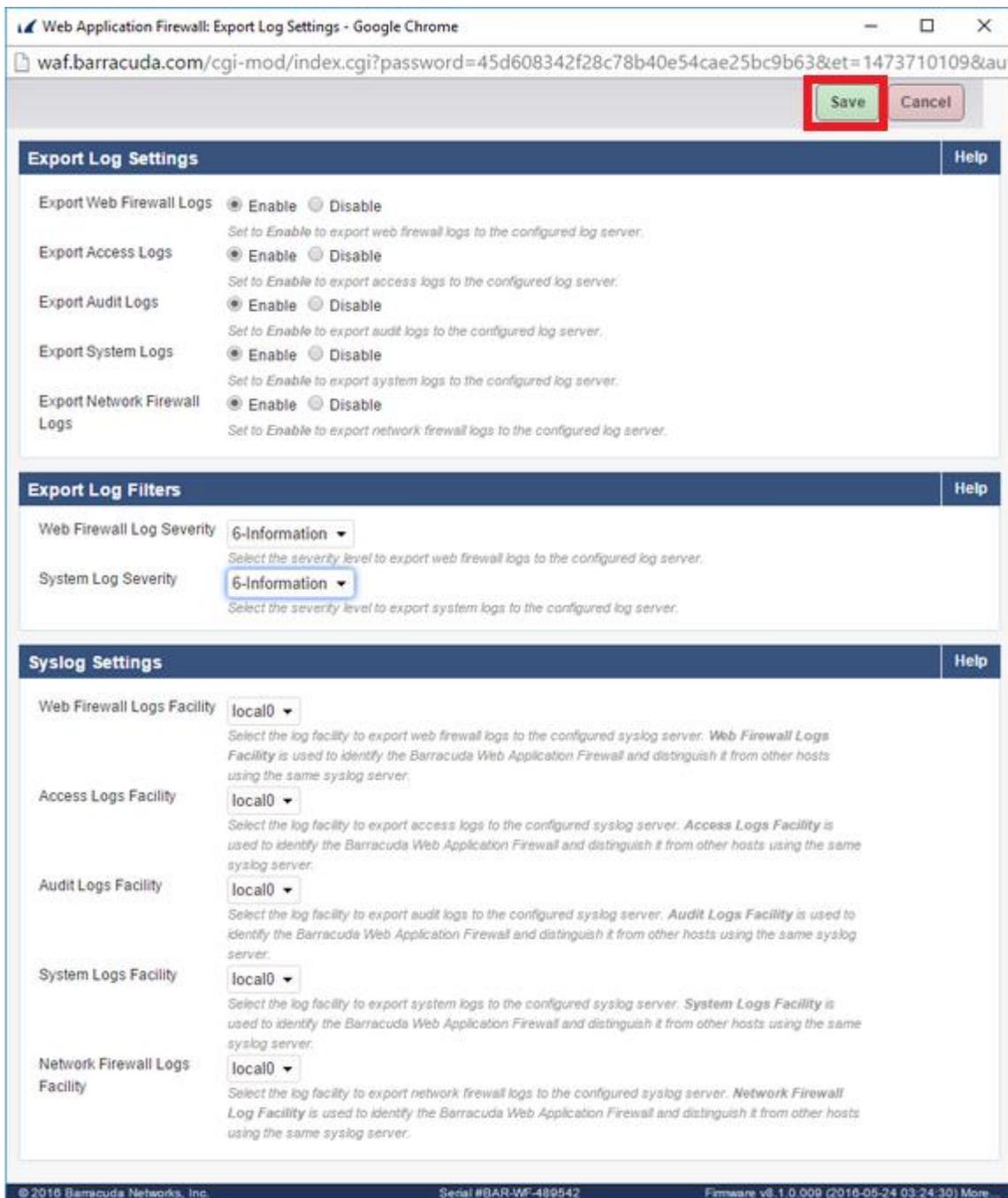


Figure 4

## Logs Format

The screenshot shows the Barracuda Web Application Firewall configuration interface. The 'Logs Format' section is highlighted with a red border. It contains the following configuration options:

- Syslog Header:** Custom Header
- Web Firewall Logs Format:** Custom Format
- Access Logs Format:** Custom Format
- Audit Logs Format:** Custom Format
- Network Firewall Logs Format:** Default
- System Logs Format:** Default

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.