

How to - Guide

# How to - Configure Sophos Web Appliance to forward logs to EventTracker

**EventTracker v9.3 and above**

**Author: Marketing**

July 6, 2021

## Abstract

This guide helps you in configuring **Sophos Web Appliance** with EventTracker to receive **Sophos Web Appliance** events.

## Scope

The configuration details in this guide are consistent with EventTracker version v9.3 or above and **Sophos Web Appliance**.

## Audience

Administrators, who are assigned the task to monitor and manage **Sophos Web Appliance** events using **EventTracker**.

## Table of Contents

Table of Contents	3
1. Overview	4
2. Prerequisites	4
3. Configuring Sophos Web Appliance to forward logs to EventTracker	4
About Netsurion	7
Contact Us	7

## 1. Overview

Sophos is a Web Security Application (web appliance), built to secure web gateway that makes web protection simple. It provides advanced protection from today's sophisticated web malware and gives user full control over their employees' online activity. User can easily create policies for individuals or groups while gaining important insights into user activity on their network.

EventTracker helps to monitor events from Sophos web appliance. Its dashboard, alerts and reports will help you track allowed and blocked traffic activities. It will trigger alert such as, ' Warned URL accessed by User or any 'URL with malicious category accessed'.

## 2. Prerequisites

Prior to configuring Sophos Web Appliance and the EventTracker, ensure that you meet the following prerequisites:

- EventTracker v9.3 or above should be installed.
- Admin role on Sophos Web Appliance to make configuration changes.
- Administrative access on the EventTracker.
- EventTracker IP and port need to add in firewall allowed list.

## 3. Configuring Sophos Web Appliance to forward logs to EventTracker

The steps provided below will help to configure the EventTracker to receive Sophos Web Appliance events via Syslog.

1. On the **Configuration > System > Alerts & Monitoring** page, select the **Syslog** tab.
2. Select the **Enable syslog transfer of web traffic** check box.
3. In the **Hostname/IP** text box, enter the address of the EventTracker Manager IP/EventTracker Agent Syslog relay to which the appliance will send logs.  
**Note:** If the Syslog server becomes unavailable to the appliance, it is possible that some log information may be dropped before the server becomes available again. The amount of information dropped depends on the duration that the server is unavailable.
4. In the **Port** text box, enter the port number that EventTracker Agent Syslog relay uses. Eg.,514(UDP port)
5. Select a **Protocol** option button to select whether the appliance will send Syslog data using UDP and TCP (encrypted/unencrypted).(Note: - If on-premises solution, select UDP protocol)
6. Click **Apply**.

- UDP

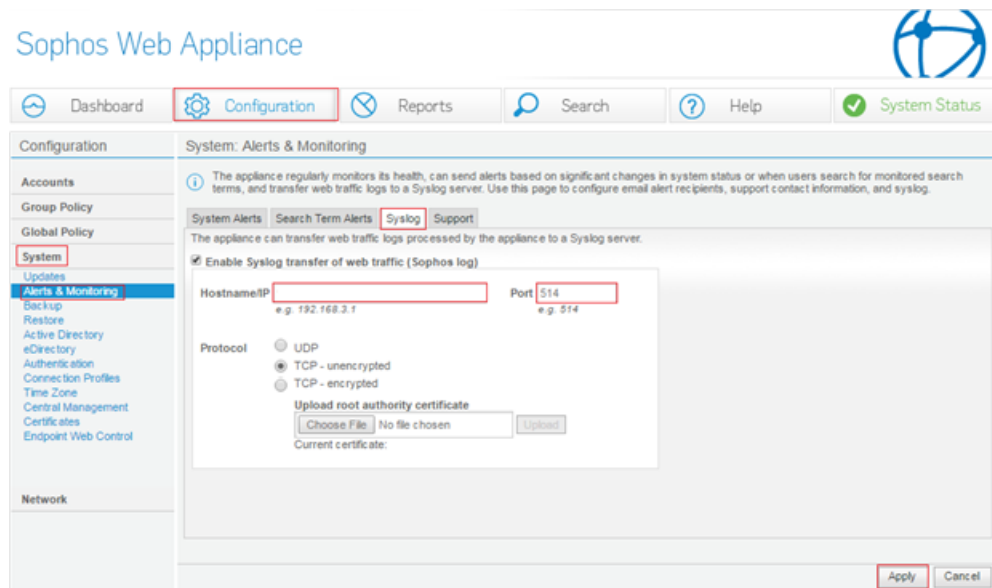
The screenshot shows the Sophos Web Appliance configuration interface. The left sidebar contains a navigation menu with categories: Configuration, Accounts, Group Policy, Global Policy, System, Updates, Alerts & Monitoring, Backup, Restore, Active Directory, eDirectory, Authentication, Connection Profiles, Time Zone, Central Management, Certificates, and Endpoint Web Control. The 'Configuration' section is expanded, and 'Alerts & Monitoring' is selected. The main content area is titled 'System: Alerts & Monitoring'. It includes a description of the appliance's monitoring capabilities and a section for configuring Syslog. The 'Enable Syslog transfer of web traffic (Sophos log)' checkbox is checked. The 'Hostname/IP' field is set to '192.168.3.1' and the 'Port' field is set to '514'. The 'Protocol' section has three radio buttons: 'UDP' (selected), 'TCP - unencrypted', and 'TCP - encrypted'. There is also a section for 'Upload root authority certificate' with a 'Choose File' button and an 'Upload' button. The 'Current certificate' field is empty. At the bottom right, there are 'Apply' and 'Cancel' buttons.

- TCP-encrypted

This screenshot is identical to the one above, showing the same Sophos Web Appliance configuration interface. The only difference is that the 'TCP - encrypted' radio button under the 'Protocol' section is now selected, while 'UDP' is no longer selected. All other settings, including the 'Enable Syslog transfer' checkbox, 'Hostname/IP' (192.168.3.1), 'Port' (514), and certificate upload options, remain the same.

Note: Attach the valid signing certificate.

- TCP-Unencrypted



The screenshot shows the Sophos Web Appliance configuration interface. The top navigation bar includes Dashboard, Configuration (highlighted), Reports, Search, Help, and System Status. The left sidebar lists various configuration categories: Configuration, Accounts, Group Policy, Global Policy, System (highlighted), Updates, Alerts & Monitoring (highlighted), Backup, Restore, Active Directory, eDirectory, Authentication, Connection Profiles, Time Zone, Central Management, Certificates, and Endpoint Web Control. The main content area is titled 'System: Alerts & Monitoring' and contains a sub-tabbed interface with System Alerts, Search Term Alerts, Syslog (highlighted), and Support. A descriptive text states: 'The appliance regularly monitors its health, can send alerts based on significant changes in system status or when users search for monitored search terms, and transfer web traffic logs to a Syslog server. Use this page to configure email alert recipients, support contact information, and syslog.' Below this, there is a checkbox labeled 'Enable Syslog transfer of web traffic (Sophos log)' which is checked. The configuration fields include: Hostname/IP (with a red box around the input field and a hint 'e.g. 192.168.3.1'), Port (with a red box around the input field and a hint 'e.g. 514'), Protocol (with radio buttons for UDP, TCP - unencrypted (selected), and TCP - encrypted), and an 'Upload root authority certificate' section with a 'Choose File' button (highlighted with a red box), an 'Upload' button, and a 'Current certificate:' label. At the bottom right, there are 'Apply' and 'Cancel' buttons, with 'Apply' highlighted by a red box.

## 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](https://www.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>