

How-To Guide

# Configuring WatchGuard Firebox to Forward Logs to EventTracker

**Publication Date:**

March 23, 2022

## Table of Contents

Table of Contents	2
1. Overview	3
2. Prerequisites	3
3. Configuring syslog forwarding to EventTracker	3
About Netsurion	6
Contact Us	6

## 1. Overview

WatchGuard Firebox Series appliances combine the firewall/VPN with the powerful security services and a suite of flexible management tools.

WatchGuard Firebox forwards the logs to EventTracker via syslog. The EventTracker WatchGuard Firebox report provides information about the possible attacks, suspicious network traffic, device configuration changes, user login, and user authentication activities. Using these reports, one can track which user has logged in successfully and login failed with reason. With the help of these reports one can inspect the endpoints to analyze the type of attack that happens, suspicious network traffic like IP spoofing, intrusion prevention traffic detected.

Dashboards display a graphical representation of the user logon activities, device configuration changes, and attack detected. By using the geo-location dashboard one can track the IPs traffic by country/ ISO code.

Alerts are triggered when a user performs any of the following: configuration changes on the endpoints, user login failed, user authentication failed, etc.

## 2. Prerequisites

- EventTracker v9.x or later should be installed.
- Fireware OS v11.10.0 to v12.7.0 should be deployed and configured.
- Users must have the device Administrator access credentials for the WatchGuard Firebox and EventTracker.
- Port 514 must be opened on WatchGuard Firebox.
- An exception should be added to the Windows Firewall on the EventTracker manager system for syslog port 514.

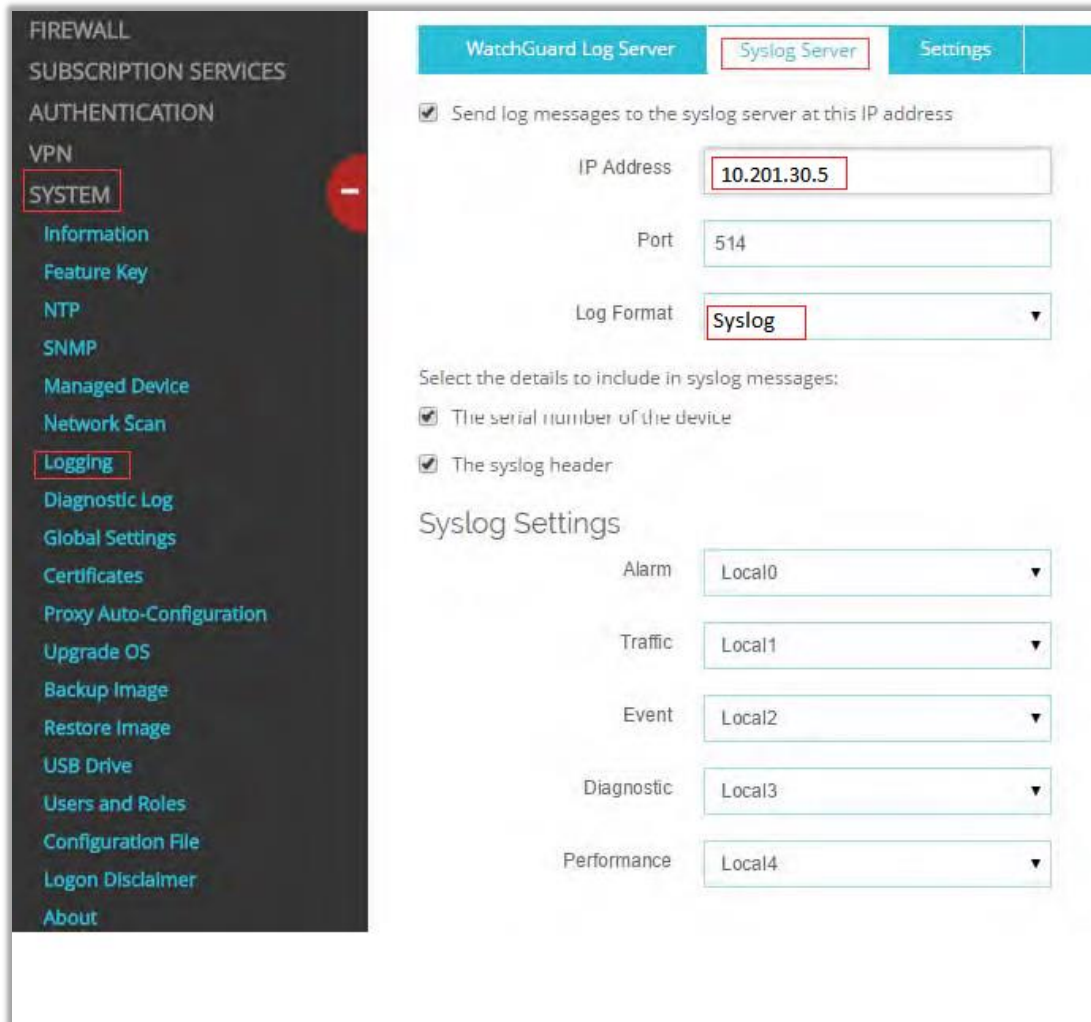
**NOTE:** Port 514 must not be used by other services of WatchGuard Firebox.

## 3. Configuring syslog forwarding to EventTracker

To collect the events from the Fireware OS, you must configure your Firebox to send the events to EventTracker. You can use the Policy Manager or Fireware Web UI to make the changes.

Follow the steps below to configure syslog forwarding to EventTracker.

1. Login to Fireware Web UI.
2. Select **System** from left side pane.
3. Select **Logging** and then click the **Syslog Server** tab.



The screenshot displays the WatchGuard Log Server configuration interface. The left sidebar contains a navigation menu with the following items: FIREWALL, SUBSCRIPTION SERVICES, AUTHENTICATION, VPN, SYSTEM (highlighted), Information, Feature Key, NTP, SNMP, Managed Device, Network Scan, Logging (highlighted), Diagnostic Log, Global Settings, Certificates, Proxy Auto-Configuration, Upgrade OS, Backup Image, Restore Image, USB Drive, Users and Roles, Configuration File, Logon Disclaimer, and About. The main content area is titled 'WatchGuard Log Server' and 'Syslog Server'. It features a 'Settings' tab. The configuration includes a checked checkbox for 'Send log messages to the syslog server at this IP address'. Below this, the 'IP Address' is set to 10.201.30.5, the 'Port' is 514, and the 'Log Format' is set to Syslog. A section titled 'Select the details to include in syslog messages:' contains two checked checkboxes: 'The serial number of the device' and 'The syslog header'. The 'Syslog Settings' section includes five dropdown menus for different log levels: Alarm (Local0), Traffic (Local1), Event (Local2), Diagnostic (Local3), and Performance (Local4).

Figure 1

4. In the Syslog Server section, enable the **Send log messages to the syslog server at this IP address** check box.
5. In the **IP Address** text box, type the IP address of the EventTracker manager.
6. In the **Port** text box, type 514.
7. From the **Log Format** drop-down list, select **Syslog**.
8. Select both the check boxes **The serial number of the device** and **The syslog header**.
9. In the Syslog Settings section, ensure each log level is assigned a facility.
10. Click **Save**.
11. Go to **Diagnostic Log** under **System**.

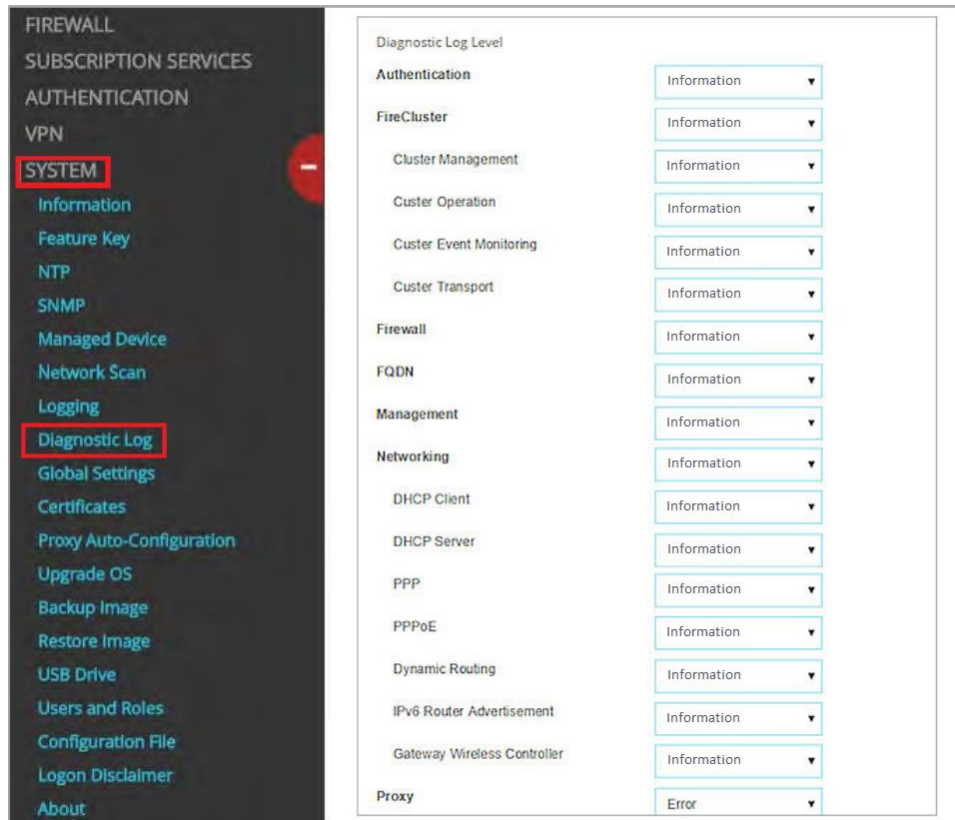


Figure 2

12. In the **Diagnostic Log Level**, select **Information** from the drop-down list for each log type.
13. Click **Save**.

## About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both.

Netsurion [Managed Threat Protection](#) combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion [Secure Edge Networking](#) delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all 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](#).

## 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>