

# How to – Configure WatchGuard XTM to forward logs to EventTracker

EventTracker v9.x or above

## Abstract

This guide provides instructions to configure WatchGuard XTM to send the event logs to EventTracker. Once events are configured to send to EventTracker alerts, dashboard and reports can be configured into EventTracker.

## Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and WatchGuard XTM Fireware v12.5

## Audience

WatchGuard XTM users, who wish to forward event logs to EventTracker and monitor events using 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
- Configure syslog forwarding to EventTracker ..... 3

## Overview

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

EventTracker continually collects firewall events and leverages machine learning to identify possible attacks, suspicious network traffic and user behavior analytics.

## Prerequisites

- EventTracker v9.x and later should be installed.
- Fireware OS v12.5 or later should be deployed and configured.
- User must have device Administrator access credentials for the WatchGuard XTM and EventTracker.
- Port 514 must be opened on WatchGuard XTM.
- Port 514 must not be used by other services of WatchGuard XTM.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.

## Configure syslog forwarding to EventTracker

To collect events from Fireware OS, you must configure your Firebox to send events to EventTracker. You can use Policy Manager or Fireware Web UI to make the changes. In this Integration Guide, we are using Web UI.

Follow the below steps 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 XTM configuration interface for the Syslog Server. 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 includes a checkbox for 'Send log messages to the syslog server at this IP address' which is checked. Below this are input fields for 'IP Address' (10.201.30.5), 'Port' (514), and a 'Log Format' dropdown menu 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 contains 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, select 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 Agent** machine.
6. In the **Port** text box, type 514.
7. From the **Log Format** drop-down list, select “**syslog**”.
8. Select both 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**.

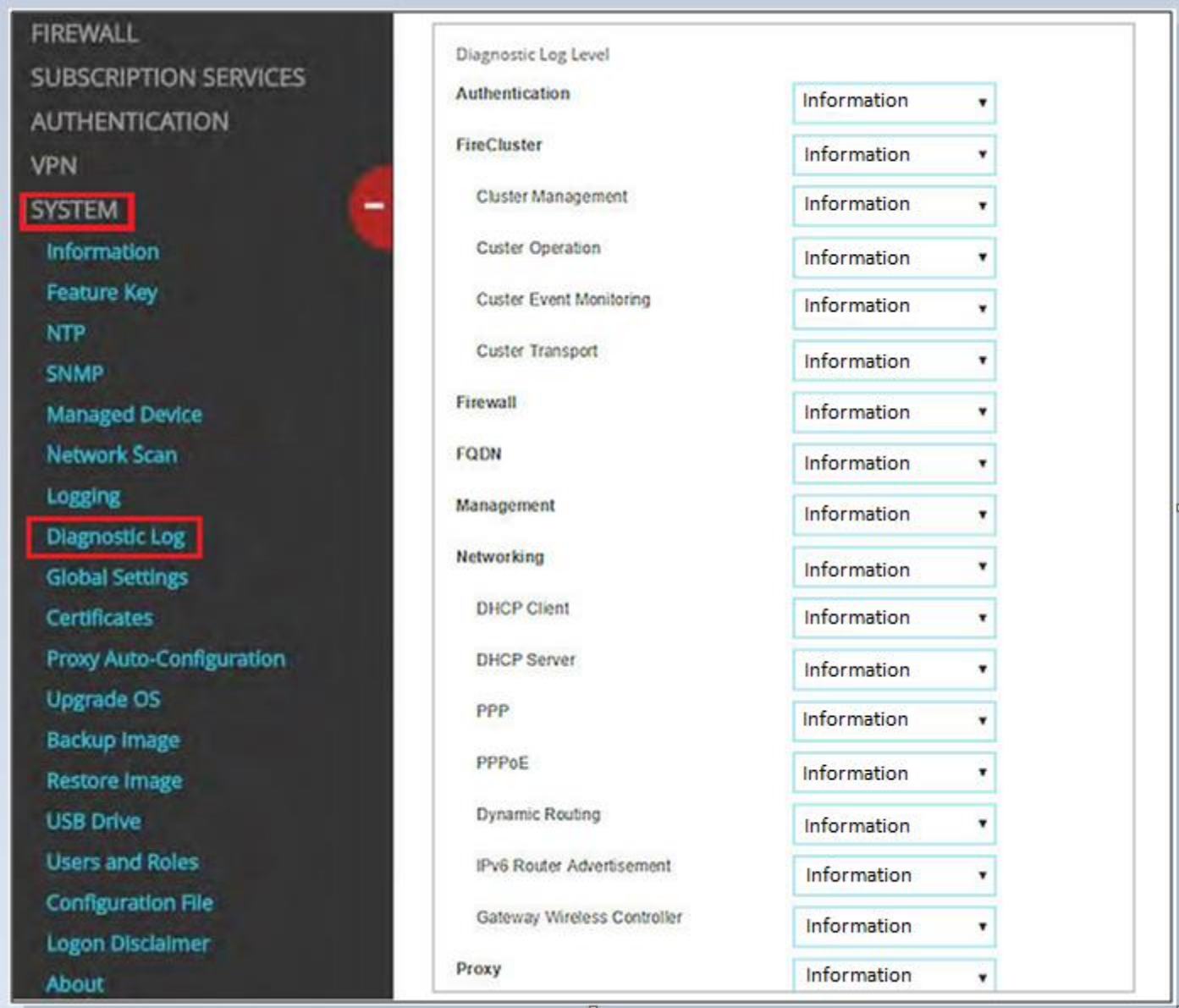


Figure 2

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