EventTracker

Actionable Security Intelligence

# How to – Configure Cyberoam UTM to forward logs to EventTracker

EventTracker

Publication Date: September 17, 2018

# Abstract

This guide helps you in configuring **Cyberoam UTM** and EventTracker to receive Cyberoam UTM events. You will find the detailed procedures required for monitoring Cyberoam UTM Appliance.

# Audience

Administrators, who are assigned the task to monitor and manage events using EventTracker.

# Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and **Cyberoam UTM CR500i, Version 9.5.4 and later.**

# Table of Contents

# Overview

The Cyberoam Unified Threat Management hardware appliances offer comprehensive security to organizations, ranging from large enterprises to small and branch offices. Multiple security features integrated over a single, Layer 8 Identity-based platform make security simple, yet highly effective. Cyberoam's Extensible Security Architecture (ESA) and multi-core technology carry the ability to combat future threats for organization's security.

To monitor Cyberoam UTM Appliance in EventTracker, configure Cyberoam UTM Appliance to send all events as Syslog to the EventTracker system.

# Pre-requisite

- **EventTracker Agent v9.x and later** should be installed.
- **Cyberoam UTM** should be installed.

# Configure Cyberoam UTM to forward all logs to EventTracker

## Configure Syslog logging

1. Login to Cyberoam Web console using administrator credentials.
2. Select **Logs & Reports**, select **Configuration**. In **Syslog Servers** tab click "**Add**" button.


Figure 1

3. In the **Name*** field, type the name of the server.
4. In the **IP address*** field, type the IP address of the **EventTracker Agent**.
5. In the **Port*** field, type the remote port number.

   The port **514** is the standard syslog port.
6. Leave **Facility** setting unchanged. Daemon by default.
7. Select **Informational** from **Severity Level** drop-down.
8. Select **CyberoamStandardFormat** from Format drop-down.
9. Select the **OK** button.

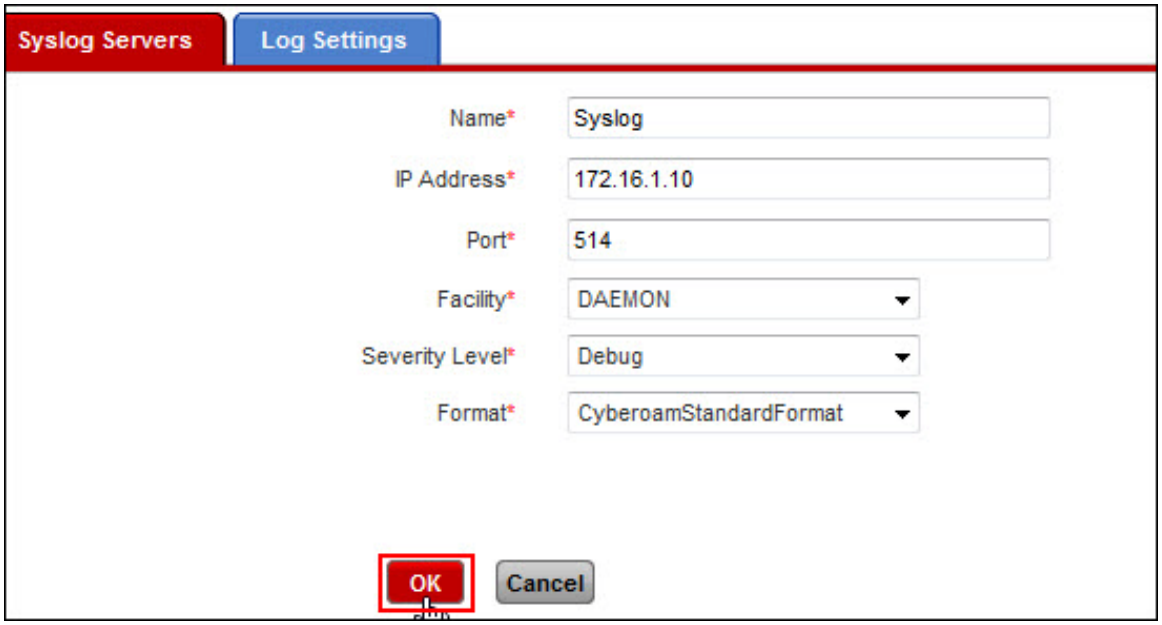


Figure 1