

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

EventTracker

## 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.**

*The information contained in this document represents the current view of EventTracker. on the issues discussed as of the date of publication. Because EventTracker must respond to changing market conditions, it should not be interpreted to be a commitment on the part of EventTracker, and EventTracker cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.*

*EventTracker 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 EventTracker, 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.*

*© 2018 EventTracker Security LLC. 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
Audience.....	1
Scope .....	1
Overview.....	3
Pre-requisite .....	3
Configure Cyberoam UTM to forward all logs to EventTracker .....	3
Configure Syslog logging.....	3

## 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.

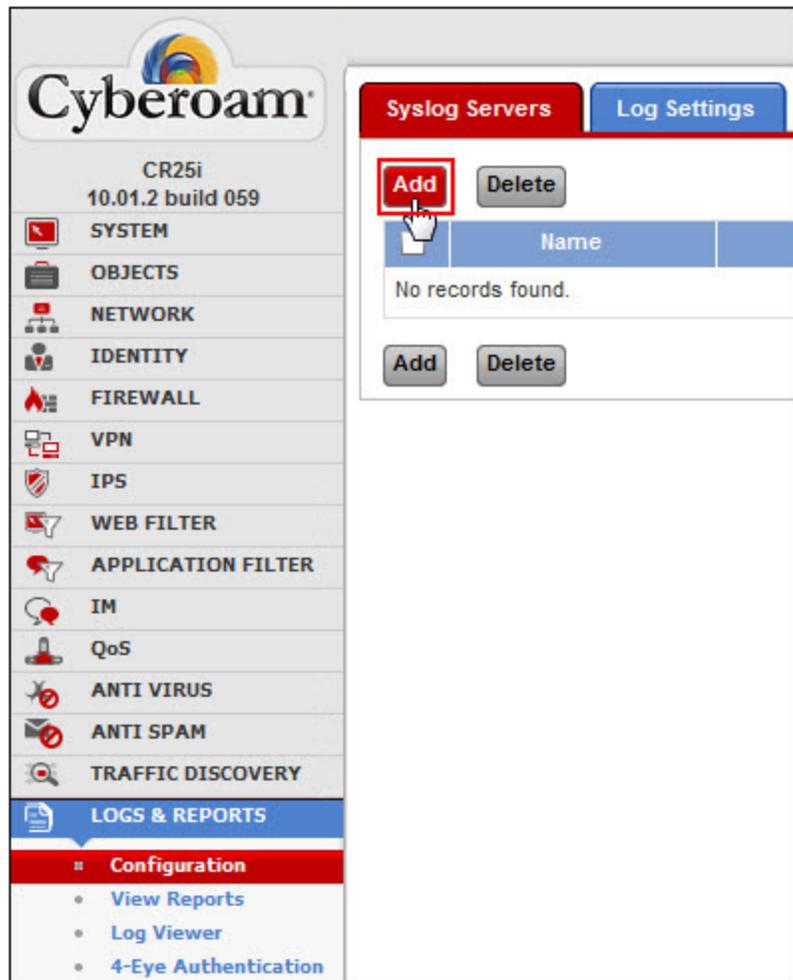


Figure 1

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.

The screenshot shows a configuration window for Syslog Servers. It features two tabs: 'Syslog Servers' (highlighted in red) and 'Log Settings' (highlighted in blue). The configuration fields are as follows:

Field	Value
Name*	Syslog
IP Address*	172.16.1.10
Port*	514
Facility*	DAEMON
Severity Level*	Debug
Format*	CyberoamStandardFormat

At the bottom of the window, there are two buttons: 'OK' (highlighted with a red box) and 'Cancel'.

Figure 1