Netsurion | EventTracker®

How to – Configure Comodo Endpoint Protection to forward logs to EventTracker

EventTracker v9.2 and later

Publication Date: December 28, 2020

Abstract

This guide provides instructions to retrieve the **Comodo Endpoint Protection** events. Once **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor **Comodo Endpoint Protection**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Comodo Endpoint Protection.**

Audience

Administrators who are assigned the task to monitor **Comodo Endpoint Protection** events using EventTracker.

Table of Contents

1. Introduction

Comodo Endpoint Protection (EP) is a powerful event analysis tool that provides real-time monitoring and detection of malicious events on Windows endpoints. Endpoint Protection allows you to view the threats in a detailed timeline while instantly alerts about an attack.

Comodo Endpoint protection agent writes events automatically on Windows event viewer. EventTracker agent picks logs and sends to EventTracker. Comodo sends events like antivirus scan, HIPS, HIDS, containment, file rating, autorun, and configuration changes. Generates reports on potentially unwanted applications, antivirus scan detail, file rating, intrusion activities, configuration changes on Endpoint, alerts, threats detected, and unwanted files removed, etc. It contains username, client IP address, status, action, file path, file name, and hash. Graphically displays threat detected by file name, device name, device IP, file management Intrusion detected by filename, etc.

2. Prerequisites

- Comodo Endpoint Manager should be installed.
- Administrative access on Comodo EP Console.
- EventTracker agent should be installed on the system where comodo agent is installed.

Note: Comodo Endpoint Protection cloud platform send logs using syslog if EventTracker have the public IP address.

3. Configuring Comodo Endpoint Protection logging

Configuring Syslog Message Forwarding for windows:

1. Log in to Comodo Endpoint Agent console.
2. Click **Settings > General Settings > Logging**.

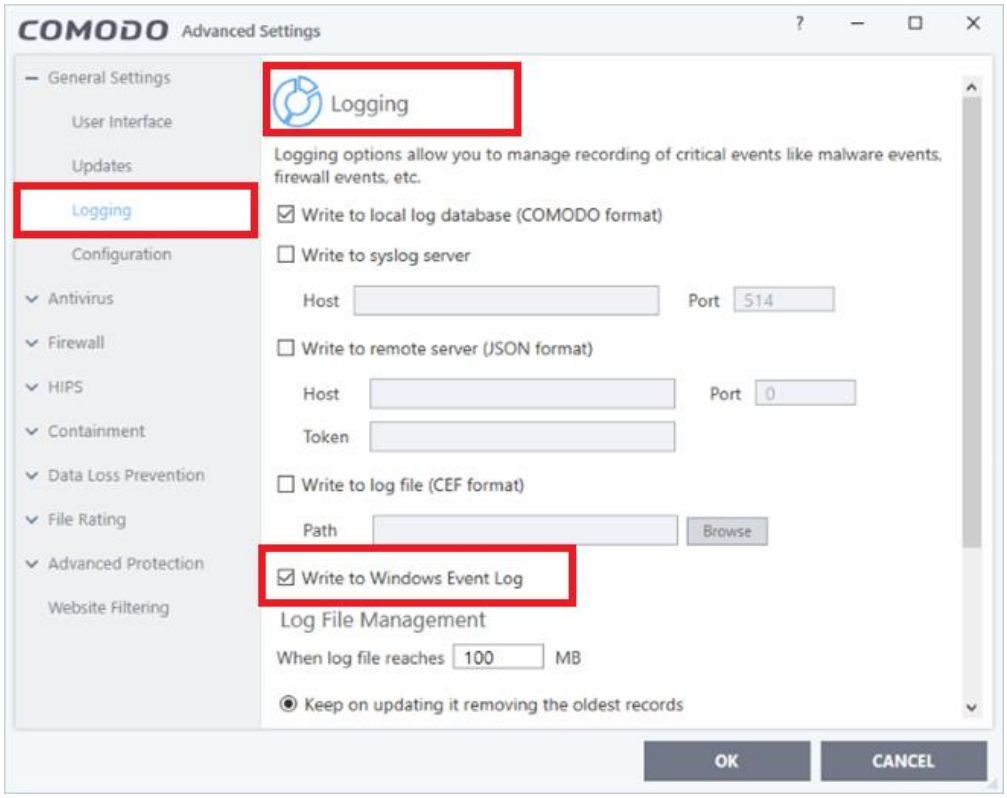

Figure 1

3. Enable **Write to Windows Event Log**. (Default = Enabled)
4. Click **OK.**

Configuring Syslog Message Forwarding for Linux and Mac:

Method 1

1. Log in to Comodo Endpoint Agent console.
2. Click **Settings** > **General Settings** > **Logging**. (as shown in Figure1).
   - Enable **Write to Syslog server**.
   - Enter **EventTracker manager IP** in Host.

Method 2

1. Log in to Comodo Cloud Platform from the admin account.
2. Click **Application** > **Endpoint Protection.**

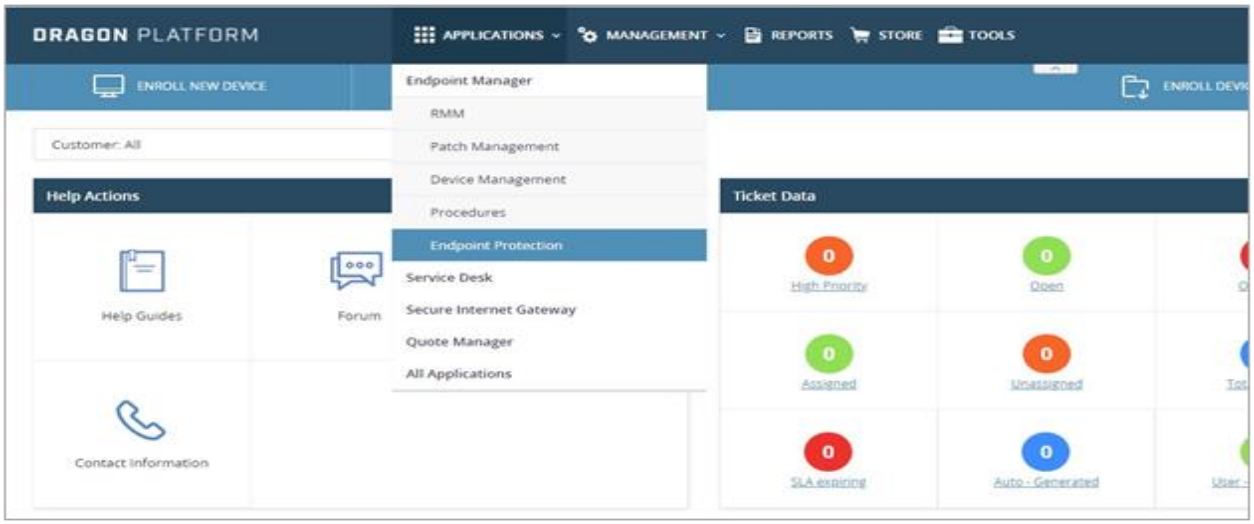

Figure 2

3. From the sidebar, click **Configuration Template** > **Profiles.**

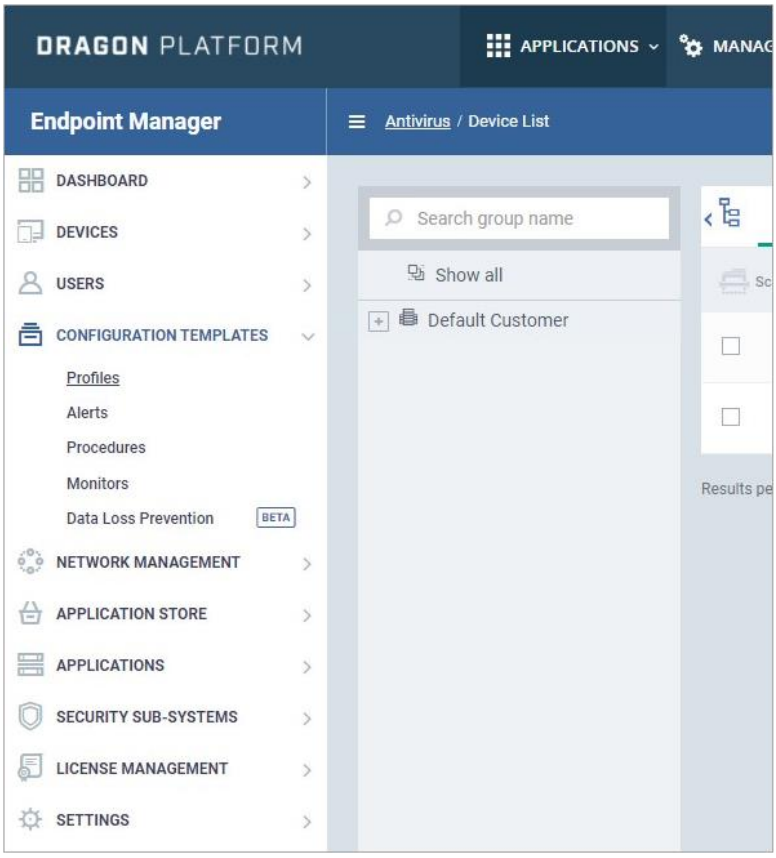

Figure 3

4. Select the Linux or Mac Profile used in the organization.

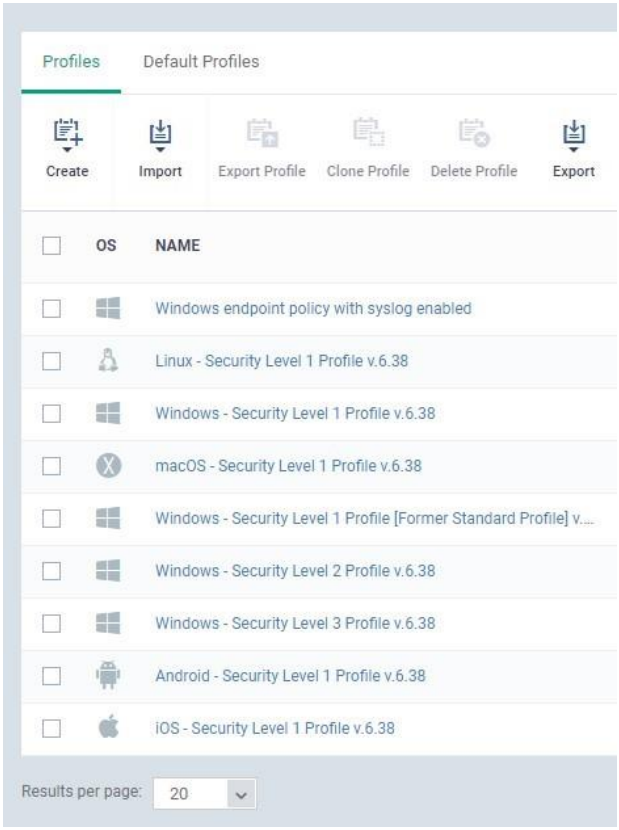

Figure 4

5. Go to **Logging Settings.** Click **Edit.**

Figure 5

6. Enable **Write to Syslog.**
7. Enter the **EventTracker Manager Public IP** in host.
8. Click **Save.**

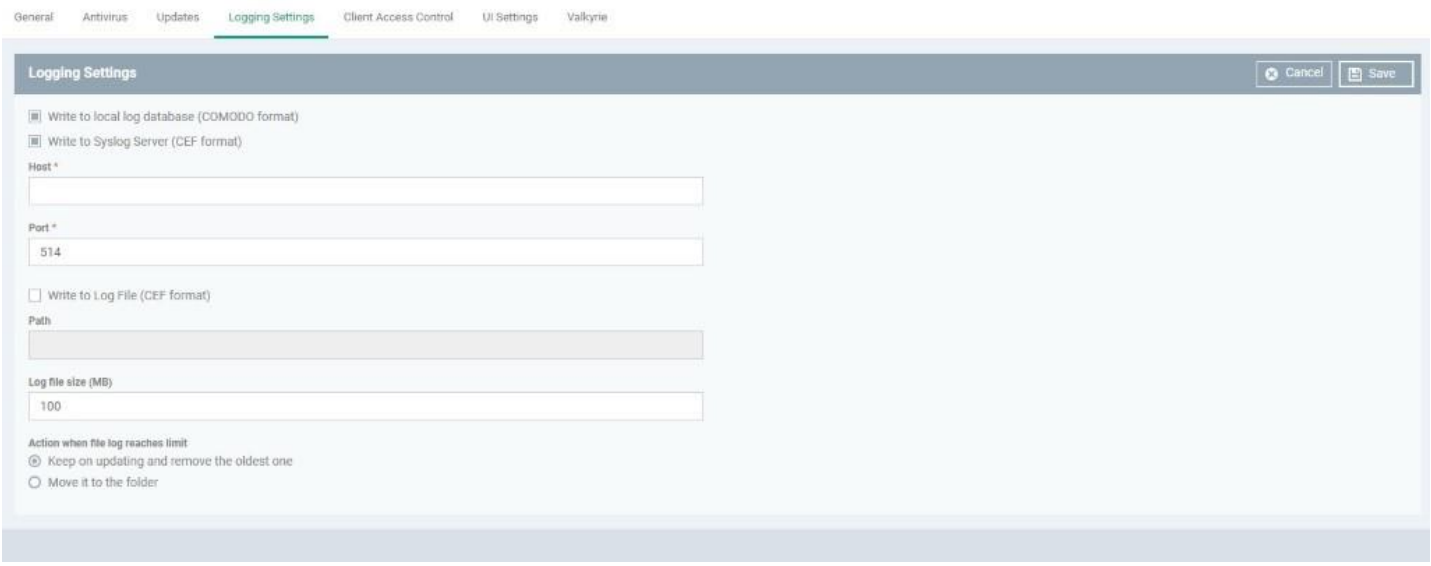

Figure 6