Netsurion | EventTracker®

# How to - Configure Trend Micro Apex One (On-Prem) to forward logs to EventTracker

## EventTracker v9.2 and later

Publication Date: December 29, 2020

# Abstract

This guide provides instructions to retrieve the **Trend Micro Apex One** via syslog forwarding. Once the logs start coming-in into EventTracker, reports, dashboards, alerts and saved searches can be configured.

**Note** - Trend Micro OfficeScan and Trend Micro Control Manager are now named Trend Micro Apex One and Trend Micro Apex Central respectively.

# Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Trend Micro Apex One/Central 2019.**

# Audience

Administrators who are assigned the task to monitor **Trend Micro Apex One** events using EventTracker.

# Table of Contents

# 1. Overview

Trend Micro Apex One is an integrated solution that protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks.

Trend Micro Apex Central is a centralized management console that manages Trend Micro products and services which allows administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points.

Apex One consists of the Security Agent program that resides at the endpoint and a server program that manages all agents.

Reports are the best way to view the historical data (depending on the timeline defined). Some of the reports provided by EventTracker for Apex One are: summary of activities such as, managed user logon and logoff activity, spyware detection, virus detection, suspicious file detection, endpoint application control violation information, etc.

Dashboards are the graphical representations of activities occurring in Apex One. These dashboards can be a pie chart, or a bar diagram, or even a map. This allows user to see the key highlights of Apex One events. ex. Dashboards display Indicator of Compromises (IOC) , such as file-hash or filename or login activities of managed user with their source IP address.

Alerts such as, potential threat quarantined, are included in the knowledge packs. These alerts can be configured to forward emails to users/admin of Apex One as soon as any suspicious events are detected.

# 2. Prerequisites

- EventTracker v9.2 and above should be installed.
- Administrative/root access to Trend Micro Apex management UI.
- Port 514 should be allowed in firewall.

# 3. Integrating Trend Micro Apex with EventTracker

## 3.1 Enable Syslog Forwarding

1. Log in to Apex Central console using an Administrator account.
2. Go to **Administration > Settings > Syslog Settings**. The **Syslog Settings** screen appears.
3. Select the **Enable syslog forwarding** check box.
4. Configure the following settings for the server that receives the forwarded syslog:

- **Server address**: FQDN or IP address of the EventTracker machine.
- **Port**: Syslog server port number. For UDP, the IANA standard port number is 514.
- **Protocol**: Select UDP as the method of communication with the syslog server.

5. Select the log **Format**:
   - **CEF**: Uses the standard Common Event Format (CEF) for log messages.
6. In **Log Type,**
   a. Select "**Security Logs**" from the drop-down menu and select all log types.
   b. Select "**Product information**" from the drop-down menu and select "**Managed Product Logon/Logoff Events**".
7. Click **Test Connection** to test the server connection. The syslog server connection status appears at the top of the screen.
8. Click **Save**.

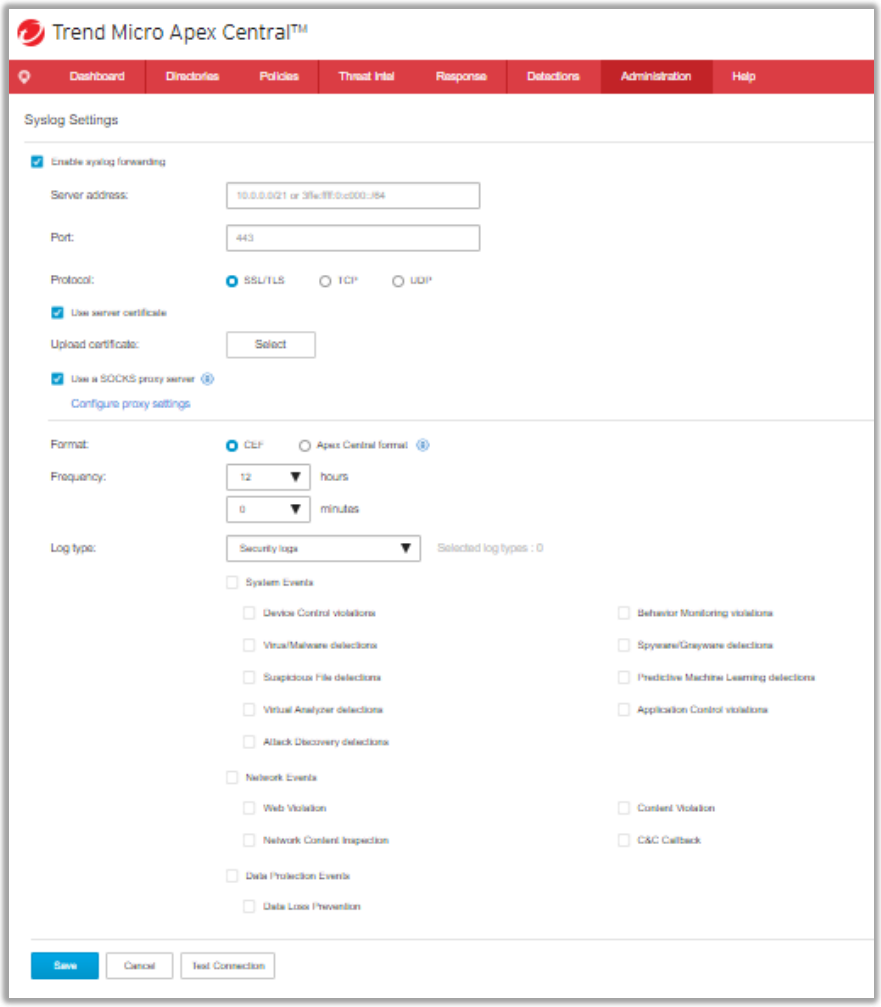


Figure 1