How to- Configure Trend Micro Deep Security to forward logs to EventTracker

EventTracker v9.0 and above

Publication Date: November 5, 2019

Abstract

This guide will facilitate a Trend Micro Deep Security user to send logs to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker v9.x or later and Trend Micro Deep Security v9.5 and above.

Audience

Administrators who want to monitor Trend Micro Deep Security 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.

Table of Contents

1.Introduction

Trend Micro Deep Security delivers a comprehensive security platform optimized for virtual and cloud environments. Its comprehensive security capabilities include anti-malware with web reputation, host-based firewall, intrusion detection and prevention (IDS/IPS), integrity monitoring, and log inspection.

Trend Micro Deep Security can be integrated with EventTracker using syslog forwarding. Trend Micro Deep Security KP helps to monitor the malware detection, malicious sites visited by users, authentication failures, policy management, group management, device management and firewall activities. EventTracker triggers the alert whenever any malware is detected, any action is taken on malware, failure to act on the malware and a malicious URL detection happens. EventTracker dashboard will help you to visualize the group management, policy management, device management, and user authentication failures.

2.Pre-requisites

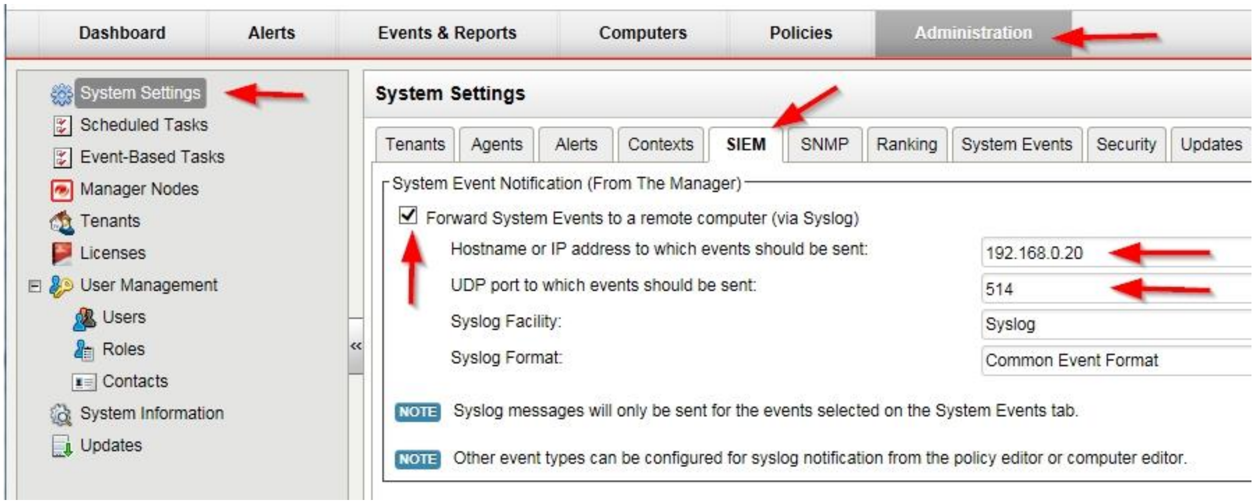
- EventTracker 9.x or later should be installed.
- Users should have administrator privileges to Trend Micro Deep Security Manager (DSM) console.

3.DSM syslog configuration

Deep Security has the option that either an Agent can forward events to the syslog server or the DSM can collect the events on the Agent collection interval and forward the events from the DSM server to the syslog server.

3.1 DSM server configuration

1. Log in to the DSM console.
2. Click **Administration -> System Settings -> SIEM** in the main menu.
3. Under **System Event Notification**:
   a. Select **Forward System Events to a remote computer** checkbox to allow the DSM manager to send logs to EventTracker.
   b. Specify the EventTracker machine **IP address**.
   c. Specify the **UDP Port** Eg:**514**
   d. Select **syslog facility** as **syslog**.
   e. Specify the **syslog format** as **Common Event Format** (CEF).
4. Click **Save**.



System Settings

System Event Notification (From The Manager)

☑ Forward System Events to a remote computer (via Syslog)

Hostname or IP address to which events should be sent: 192.168.0.20

UDP port to which events should be sent: 514

Syslog Facility: Syslog

Syslog Format: Common Event Format

NOTE Syslog messages will only be sent for the events selected on the System Events tab.

NOTE Other event types can be configured for syslog notification from the policy editor or computer editor.

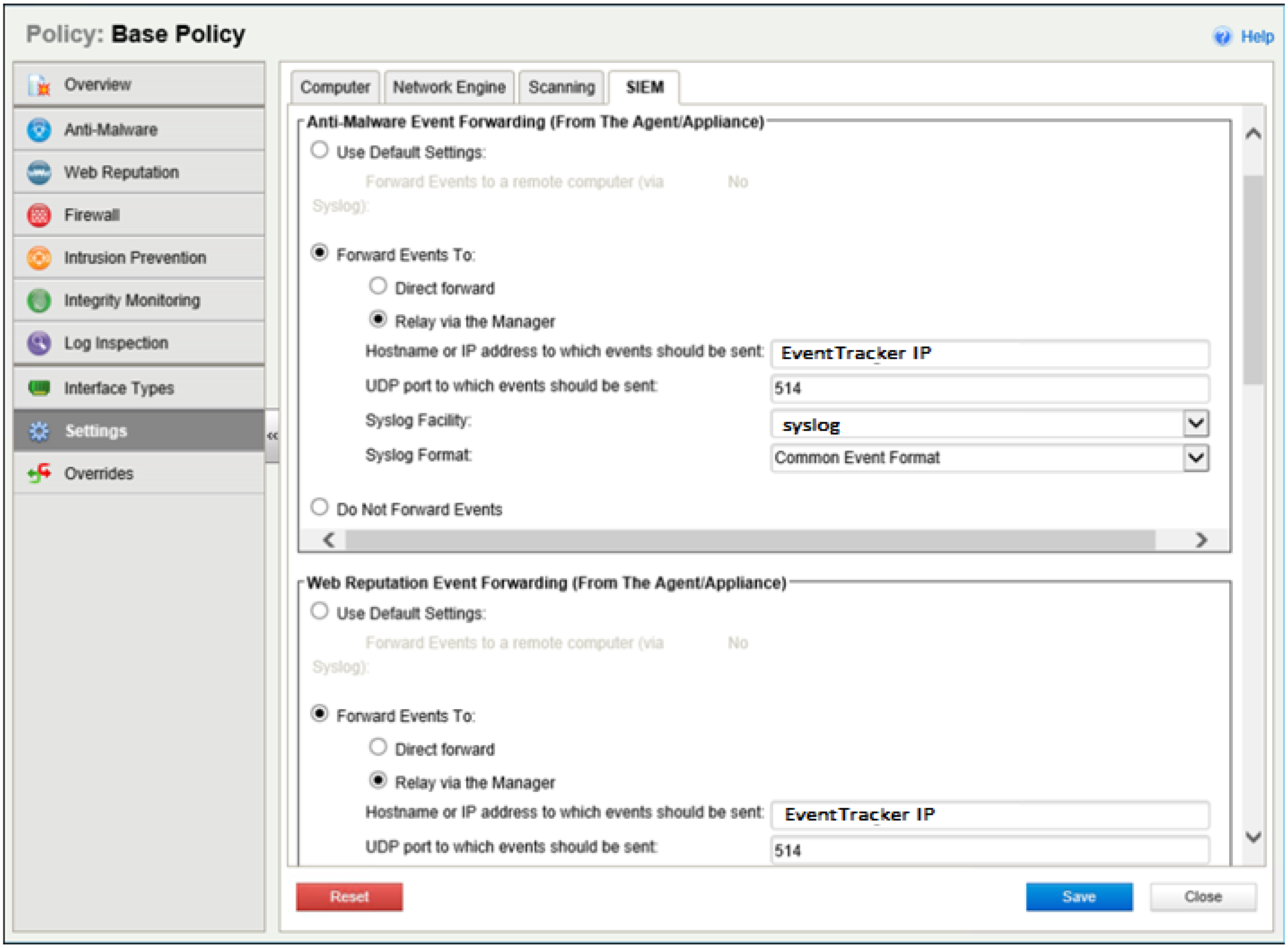
Figure 1

3.2 Configure the Policy

Forward security events directly in real-time from agent computers to an EventTracker.

Now you must add the syslog source to your policy configuration. Set the integration details at the top (root/base) policy as follows:

1. Click on **Policies**.
2. Go to **Settings > SIEM**.
3. For **Anti-Malware Event Forwarding**, select **Forward Events To:** and **Relay via the Manager**.
    a. Specify the EventTracker machine IP address.
    b. Specify the UDP port Eg:514
    c. Select syslog facility as syslog.
    d. Specify the syslog format as Common Event Format (CEF).
4. For **Web Reputation Event Forwarding**, select **Forward Events To** and **Relay via the Manager**.
    a. Specify the EventTracker machine IP address.
    b. Specify the UDP port Eg:514
    c. Select syslog facility as syslog.
    d. Specify the syslog format as Common Event Format (CEF).
5. Click **Save**.



Policy: **Base Policy**

Anti-Malware Event Forwarding (From The Agent/Appliance)

○ Use Default Settings:

Forward Events to a remote computer (via Syslog): No

● Forward Events To:

○ Direct forward

● Relay via the Manager

Hostname or IP address to which events should be sent: EventTracker IP

UDP port to which events should be sent: 514

Syslog Facility: syslog

Syslog Format: Common Event Format

○ Do Not Forward Events

Web Reputation Event Forwarding (From The Agent/Appliance)

○ Use Default Settings:

Forward Events to a remote computer (via Syslog): No

● Forward Events To:

○ Direct forward

● Relay via the Manager

Hostname or IP address to which events should be sent: EventTracker IP

UDP port to which events should be sent: 514

Figure 2