

How to – Configure Untangle to forward logs to EventTracker

EventTracker

Abstract

This guide provides instructions to configure Untangle to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Untangle.

Scope

The configurations detailed in this guide are consistent with EventTracker version v9.X or above and Untangle.

Audience

Administrators who are assigned the task to monitor Untangle events using EventTracker.

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
Scope	1
Audience	1
Overview.....	3
Prerequisites.....	3
Configure Untangle to forward logs to EventTracker	3

Overview

Untangle, a network software and appliance company, provides the most complete multi-function firewall and Internet management application suite available today.

EventTracker helps to monitor events from Untangle. It's knowledge object and flex reports will help you to analyze critical activities and to monitor login events.

Prerequisites

- **EventTracker Agent 9.x** should be installed.
- Untangle should be configured for forwarding logs.
- Please add exception for port **514** in firewall if exists in between Untangle and EventTracker Manager.

Configure Untangle to forward logs to EventTracker

To configure the Untangle to forward logs to a syslog server,

1. Log on to the Untangle Management Console as an Administrator.
2. From Web GUI choose **CONFIG**.
3. Go to **Events > Syslog** to display the configuration page.
4. Under the **Remote Syslog Configuration**.
5. Check the '**Enable Remote Syslog**' box to enable the remote logging.
6. For **Host**, type the IP address of **EventTracker Agent**.
7. For **Port**, type **514** for default syslog server port.
8. For **Protocol**, dropdown and select **UDP**.
9. Under the **Syslog Rules**.
10. Check the '**Enable**' and '**Remote Syslog**' box to set the rules.
11. Click the **Save** option to save the configurations.

The screenshot shows the Untangle configuration interface. At the top, there is a navigation bar with 'DASHBOARD', 'APPS', 'CONFIG', and 'REPORTS'. The 'CONFIG' tab is active. Below the navigation bar, there are tabs for 'Alerts', 'Triggers', and 'Syslog'. The 'Syslog' tab is selected. The main content area is titled 'Remote Syslog Configuration' and contains the following information:

if enabled logged events will be sent in real-time to a remote syslog for custom processing.
Enable Remote Syslog:

Host: 192.168.1.194
Port: 514
Protocol: UDP

Below this is the 'Syslog Rules' section, which includes an 'Add' button and a table with the following data:

Rule Id	Enable	Description	Class	Conditions	Remote Syslog	Edit	Copy	Delete
1	<input checked="" type="checkbox"/>	All events	All	Match all fields	<input checked="" type="checkbox"/>			

At the bottom right of the configuration area, there is a 'Save' button.

Figure 1