EventTracker

Actionable Security Intelligence

How to – Configure Untangle to forward logs to EventTracker

EventTracker

Publication Date: September 17, 2018

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.

Table of Contents

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.

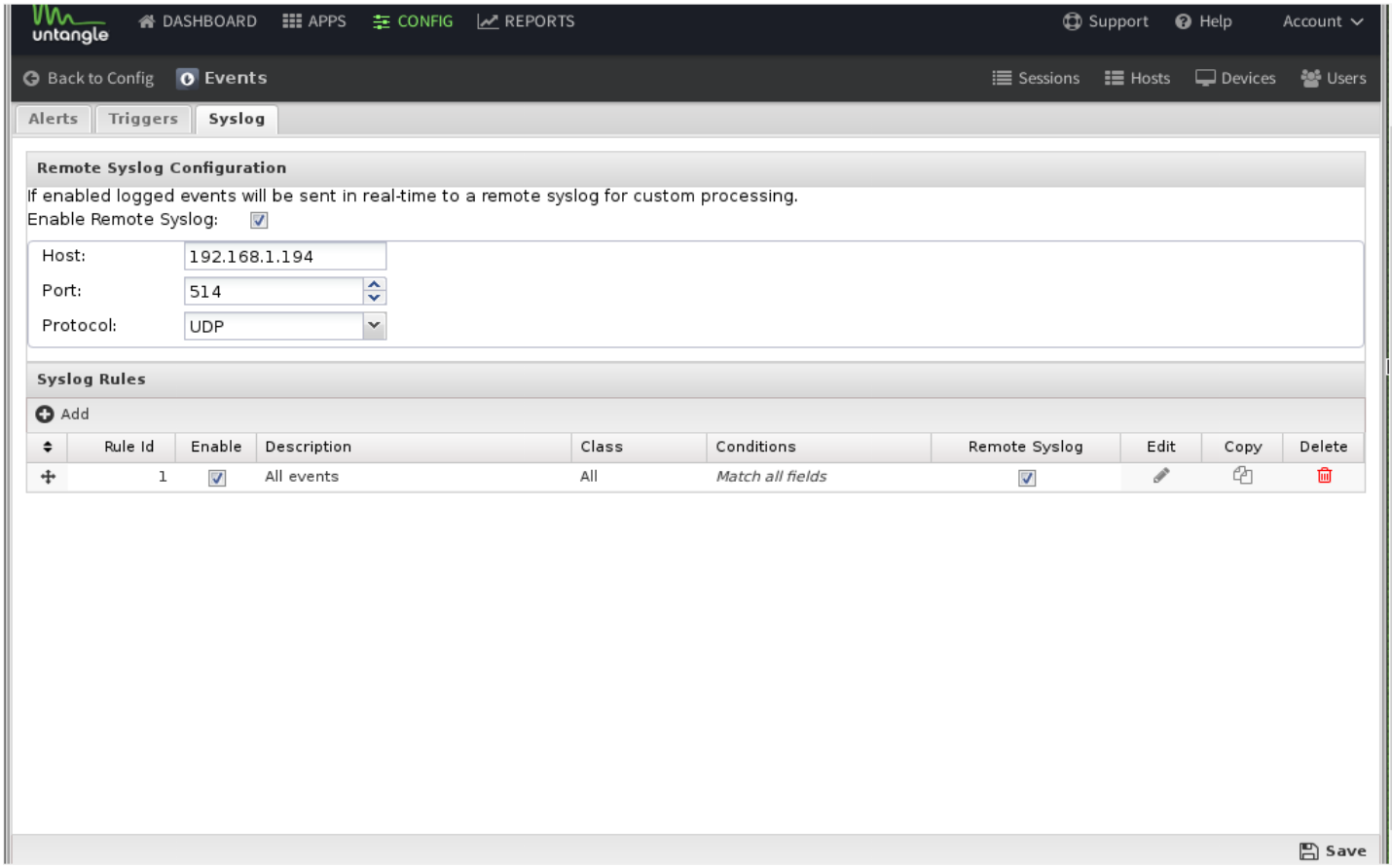

Figure 1