Netsurion | EventTracker®

How to - Configure SpamTitan Gateway to forward logs to EventTracker

EventTracker v9.2 and above

Publication Date: July 14, 2020

Abstract

This guide provides instructions to configure SpamTitan Gateway to send its logs to EventTracker.

Scope

The configuration details in this guide are consistent with EventTracker version v9.2 or above and **SpamTitan Gateway**

Audience

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

Table of Contents

1. Overview

SpamTitan Gateway is a powerful Anti-Spam appliance that equips network administrators with extensive tools to control mail flow and protect against unwanted email and malware.

EventTracker helps to monitor events from SpamTitan Gateway. EventTracker's reports provide detailed information of all events, alerts are helpful to determine and stop the attack and suspicious activities in real-time, and dashboards will help you to analyze all the security-related events in a single console. Also, we can create and save log search rules/queries under the saved search feature for real-time and historical log search.

2. Prerequisites

- Admin privileges for **SpamTitan Gateway** to configure logging.
- **EventTracker** should be installed in the system.
- Syslog Port 514 should be open.

3. Integration of SpamTitan Gateway with EventTracker

SpamTitan Gateway logs we can get by using syslog.

3.1 Configuring SpamTitan Gateway to send the logs to EventTracker

Syslog is the de facto standard for forwarding log messages in an IP network. All system log messages are written to local log files on SpamTitan Gateway using syslog and logs can be viewed in the Logs tab.

Besides, the log output can also be sent to a remote syslog server. This is useful for administrators who want to use EventTracker to view and analyze log files.

Go to **Settings > Remote syslog** to specify a remote syslog server for mail, interface, and messages log files. The remote servers defined must run a logging daemon compatible with the syslog protocol.

To specify a remote server:

1. Click **Enable** to turn the remote syslog status to ON.
2. Enter the **EventTracker's address** in the **syslog Server: field**.

Note:

To specify a port, put a colon after the remote syslog address, and add the port number. For example, **192.168.3.120:5826**

3. Click **Save**.

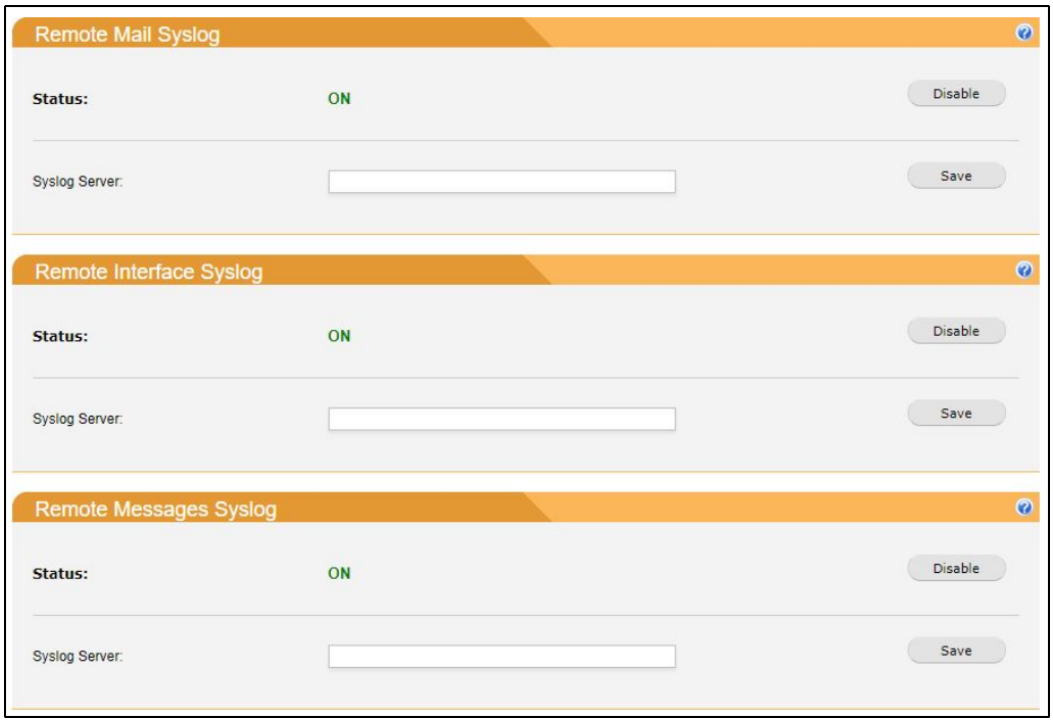

Figure 1