Netsurion™ | EventTracker

How to- Configure FortiMail to forward logs to EventTracker

EventTracker v9.0 and Above

Publication Date: June 4, 2019

Abstract

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

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 9.x and later, and FortiMail v6.0 and later.

Audience

IT admins, FortiMail administrators and EventTracker users who wish to forward logs to EventTracker manager and monitor events using EventTracker Enterprise.

The information contained in this document represents the current view of Netsurion 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.

Table of Contents

Overview

Fortinet FortiMail is an email security gateway product that monitors email messages on behalf of an organization to identify messages that contain malicious content, including spam, malware, and phishing attempts.

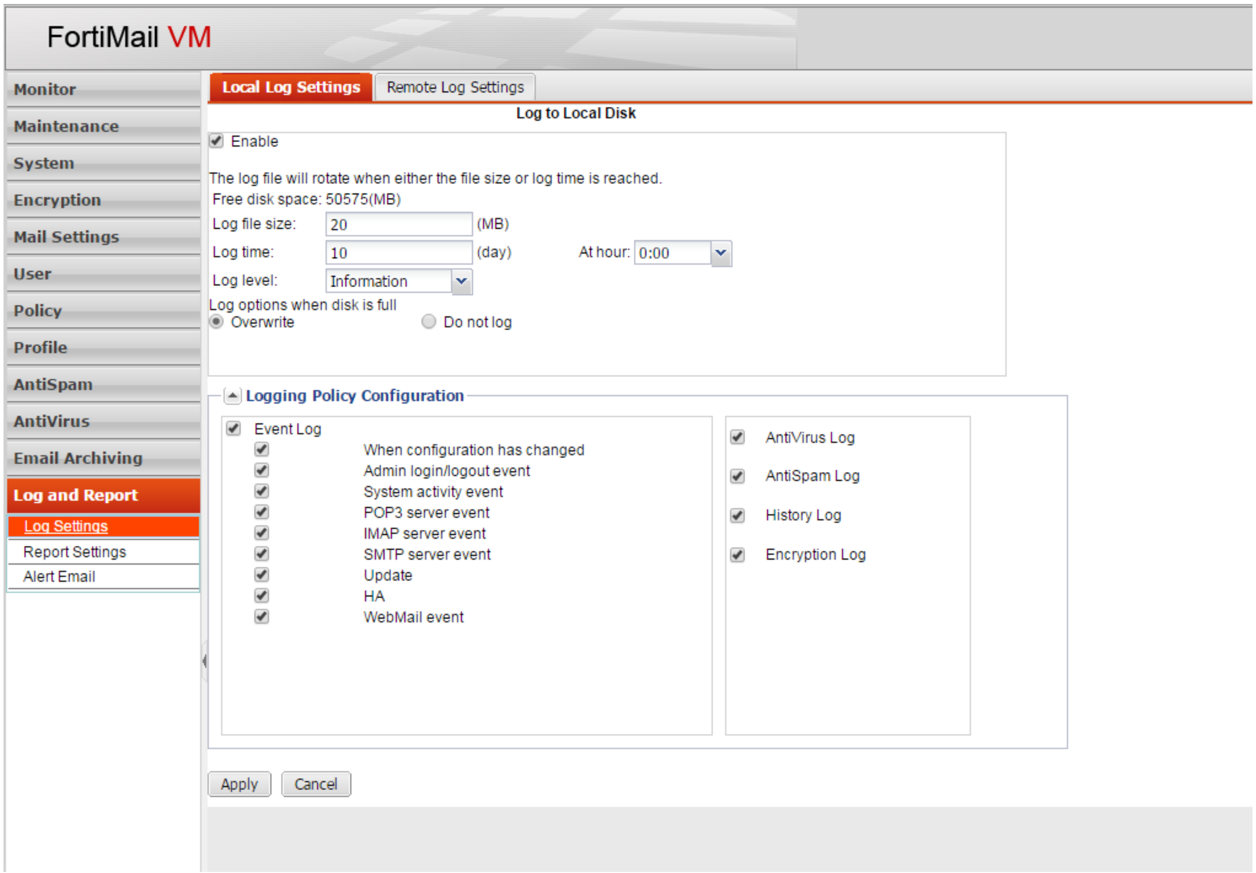
FortiMail can be integrated with EventTracker using syslog. With the help of FortiMail KP items, we can monitor the spam, and virus happening on mail servers and also trigger the alert whenever any virus and spam is detected. EventTracker dashboard will help you to visualize the malicious activities happening in the mail servers. It can even create the report which helps to collect malicious activities happening on mail servers on time bases which help you to review the malicious activities. EventTracker CIM will help you to correlate the malicious activities with another log source like a virus, spam events, etc.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **FortiMail v6.0** or the latest version should be installed.

Configuring FortiMail Syslog

1. Go to Log and Report → Log Settings → Remote Log Settings.
2. Toggle is enabled for your preferred profile.
3. Go to Log and Report → Log Settings → Remote Log Settings.
4. The **Remote Log Settings** tab is displayed.
5. Select **New** to create a new entry or double-click an existing entry to modify it.
6. Select **Enable** to allow logging to a remote host.
7. Enter a profile name and the **IP address** of the EventTracker.
8. Enter the **514** in the port section.
9. Select the **severity** level that a log message must equal or exceed in order to be recorded and stored from the Level dropdown menu.
10. Select the facility identifier that the FortiMail unit uses to identify itself from the **Facility** dropdown menu.
11. Expand the **Logging Policy Configuration** and enable the types of logs you want to monitor. (recommended: Select all)
12. Select **Create**.



Log to Local Disk

☑ Enable

The log file will rotate when either the file size or log time is reached.

Free disk space: 50575(MB)

Log file size: 20 (MB)

Log time: 10 (day) At hour: 0:00

Log level: Information

Log options when disk is full

● Overwrite ○ Do not log

Logging Policy Configuration

☑ Event Log

- ☑ When configuration has changed
- ☑ Admin login/logout event
- ☑ System activity event
- ☑ POP3 server event
- ☑ IMAP server event
- ☑ SMTP server event
- ☑ Update
- ☑ HA
- ☑ WebMail event

☑ AntiVirus Log

☑ AntiSpam Log

☑ History Log

☑ Encryption Log

Figure 1