How to- Configure FortiManager to forward logs to EventTracker

EventTracker v9.x and later

Publication Date: October 7, 2019

Abstract

This guide provides instructions to configure/ retrieve **FortiManager** events via syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **FortiManager**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **FortiManager 6.2.0 and later**.

Audience

Administrators who are assigned the task to monitor **FortiManager** events 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.Overview

FortiManager appliance allows you to centrally manage many Fortinet devices from a few to thousands, including FortiGate, FortiWiFi, FortiCarrier, FortiMail, and FortiAnalyzer appliances and virtual appliances, as well as FortiClient endpoint security agents.

EventTracker, when integrated with FortiManager, enables users to view critical information related to activities performed in FortiManager or other Fortinet devices. This information is represented in the form of report, alert and graphical/ pictorial representation(dashboard).

In this integration guide, logging is performed by forwarding FortiManager logs to the EventTracker syslog server.

The logs which FortiManager forwards includes,

1. System manager (SYSTEM) events.
2. FortiGuard service (FGD) events.
3. FortiManager web service (FMGWS) events.
4. Managed device operations (DEVOPS) events.
5. High Availability (HA) events.
   Etc.

2.Prerequisites

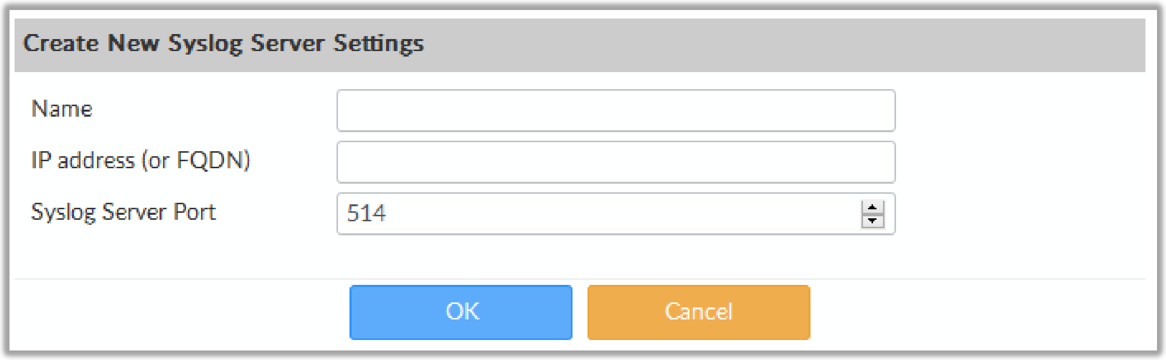
- EventTracker agent should be installed in the host system/ server.
- PowerShell 5.0 should be installed on the host system/ server.
- User should have administrative privileges on the host system/ server to run PowerShell.

3.Integrating FortiManager with EventTracker

3.1 Forwarding FortiManager Logs to EventTracker

EventTracker receives the logs from FortiManager, once the syslog is configured in FortiManager:

1. Go to **System Settings** → **Advanced** → **Syslog Server**.
2. Select **Create New** to open the **New Syslog Server** window. (The Create New Syslog Server Settings pane opens.)



Create New Syslog Server Settings

Name	
IP address (or FQDN)	
Syslog Server Port	514

Figure 1

3. Fill in the Name, for example, “EventTracker”.
4. Fill in the IP address or FQDN of the EventTracker receiver.
5. Enter the Port number. The default is 514.