Netsurion™ | EventTracker

How to – Configure FortiAuthenticator to forward logs to EventTracker

EventTracker v8.x and above

Publication Date: October 9, 2019

Abstract

This document guides the users to integrate FortiAuthenticator with EventTracker to monitor the activities on the FortiAuthenticator such as Channel events, File uploads, User events etc.

Scope

The configurations detailed in this guide are consistent with EventTracker version 8.x and later, and FortiAuthenticator v6.0.0.

Audience

FortiAuthenticator users, who wish to forward logs to EventTracker Manager and monitor events using Event Tracker.

Table of Contents

1.Overview

The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

EventTracker, when integrated with FortiAuthenticator, enables users to view critical information's related to user logon activities performed in FortiAuthenticator or other Fortinet devices. These information's are represented in the form of report, alert and graphical/ pictorial representation(dashboard).

2.Integrating FortiAuthenticator

FortiAuthenticator logs we can get by using syslog.

1. To add a syslog server
   a. Go to **Logging > Log Config > Syslog Servers**.
   b. From the syslog servers list, select Create New.
   c. Enter the following information.
      - **Name**: Enter a name for the syslog server on FortiAuthenticator.
      - **Server Name/IP**: Enter **EventTracker IP** address.
      - **Port**: Enter the syslog server port number **514**.
      - **Level**: Select a log level as **information** from the dropdown menu.
      - **Facility**: Select a facility from the dropdown menu.

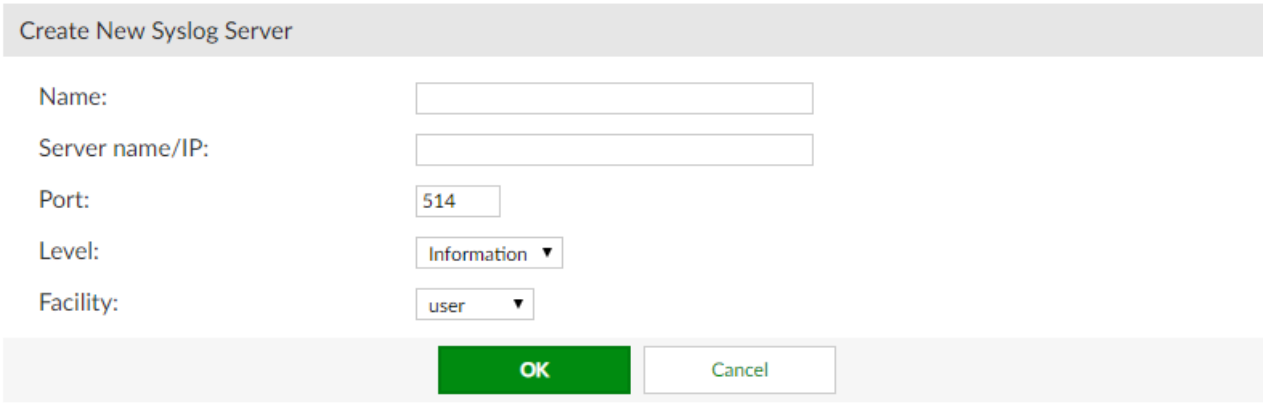

Figure 1

   - **Select OK to add the syslog server.**

2. To configure logging to a remote syslog server
   a. Go to Logging > Log Config > Log Settings.
   b. Under **Remote Syslog**, select **Send logs to remote Syslog servers**.

c. Move the syslog servers to which the logs will be sent from the **Available syslog servers'** box to the **Chosen syslog servers'** box.

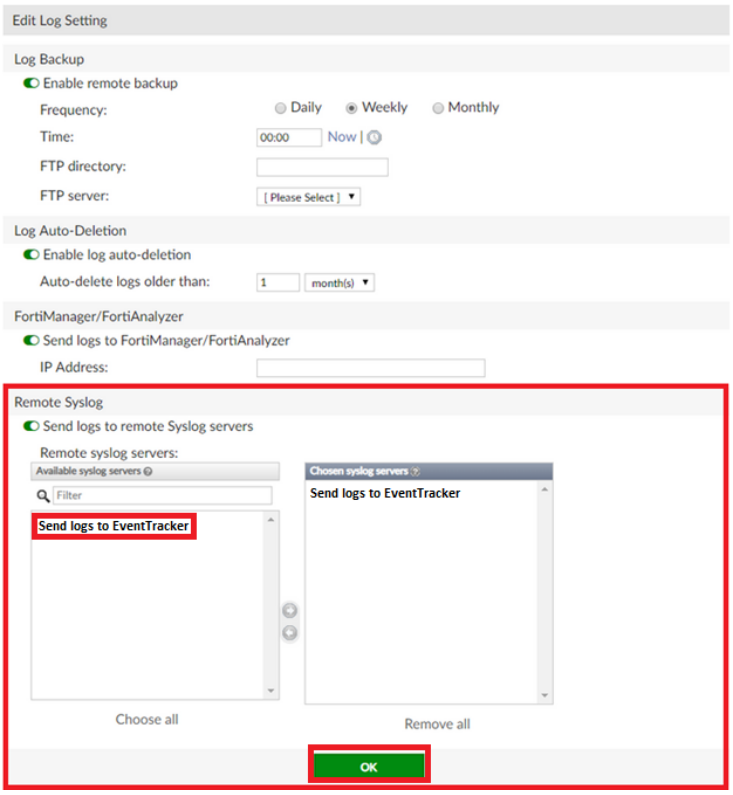

Figure 2

3. Select **OK** to save your settings.