

How to – Configure FortiAuthenticator to forward logs to EventTracker

EventTracker v8.x and above

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.

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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

1. Overview.....	3
2. Integrating FortiAuthenticator	3

1. Overview

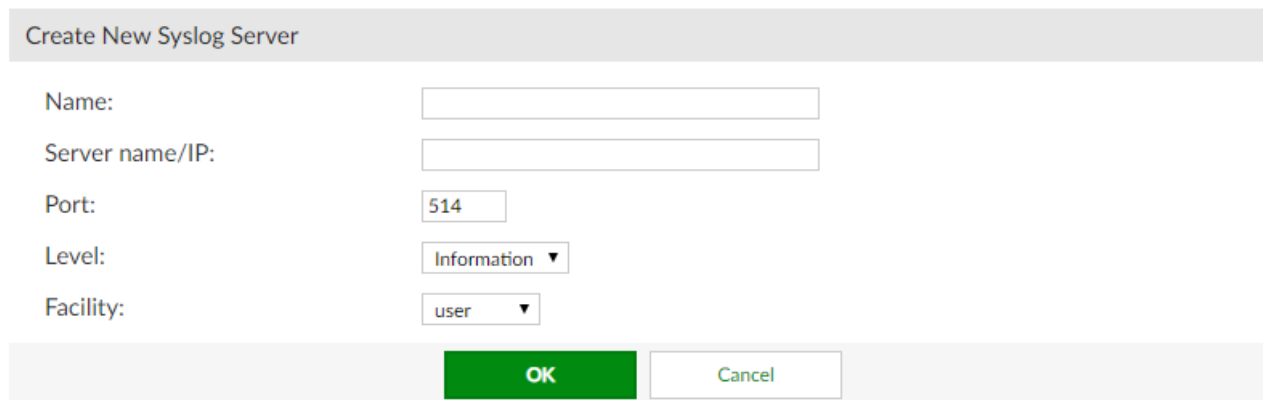
The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

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.



Create New Syslog Server

Name:

Server name/IP:

Port:

Level:

Facility:

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.

Edit Log Setting

Log Backup

Enable remote backup

Frequency: Daily Weekly Monthly

Time: 00:00 Now | ⌵

FTP directory:

FTP server: [Please Select] ▾

Log Auto-Deletion

Enable log auto-deletion

Auto-delete logs older than: 1 month(s) ▾

FortiManager/FortiAnalyzer

Send logs to FortiManager/FortiAnalyzer

IP Address:

Remote Syslog

Send logs to remote Syslog servers

Remote syslog servers:

Available syslog servers: Filter

Send logs to EventTracker

Chosen syslog servers: Send logs to EventTracker

Choose all Remove all

OK

Figure 2

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