Netsurion | EventTracker®

Integration Guide for NetMotion Mobility

EventTracker v9.x and later

Publication Date: April 16, 2020

Abstract

This guide provides instructions to retrieve the **NetMotion Mobility** events by syslog configuration. Once **EventTracker** is configured to collect and parse these logs, dashboard and reports can be configured to monitor **NetMotion Mobility**.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x or above and **NetMotion Mobility.**

Audience

Administrators who are assigned the task to monitor **NetMotion Mobility** events using EventTracker.

Table of Contents

1. Overview

NetMotion Mobility is a mobile VPN software, designed specifically for wireless environments. NetMotion Mobility provides IT managers with the security and centralized control to effectively manage a mobile deployment.

EventTracker, when integrated with NetMotion Mobility, collects log from NetMotion Mobility and creates a detailed reports, alerts, dashboards and saved searches. This KP (knowledge Pack) provides detailed information about the User logon failure, in real time. It is helpful to investigate and take responsive actions against Brute-Force Attack.
EventTracker provides a thorough information about policies such as pending policies that must be applied and the policies that have been applied. It also provides information related to Proxy events which contain many important information such as source user, source IP address and session ID. Sessions can be monitored to identify details of user logon and logoff success required for Auditing.
Alerts are provided for critical events such as user logon failure to identify logon attempt. Using the EventTracker's Dashboards we can view and monitor events like user logon events (success, failed), user policy details, user/group management, etc.

2. Prerequisites

- EventTracker manager v9.x is required.
- Enable external logging on your **NetMotion Mobility** appliance.
- Allow Port 514 in the firewall.

3. Integrating NetMotion Mobility with EventTracker

NetMotion Mobility can be integrated with EventTracker using syslog forwarding.

3.1 Configuring a Syslog Server

The NetMotion Mobility server can send NetMotion Mobility events to EventTracker. NetMotion Mobility support for syslog is only implemented on the NetMotion Mobility server; the NetMotion Mobility client cannot log messages to a syslog server.

To log NetMotion Mobility events to EventTracker:

1. Go to **Mobility console > Configure > Server Settings**.
   In the left-hand pane, select the level at which you want to configure logging:
   - To apply the setting to all Mobility servers in a server pool, select **Global Server Settings**.

- To apply the setting to a single server, select the name of the Mobility server you want to configure.

Settings applied at the server level take precedence over global settings.

Configure the following settings:

- Select **Syslog - On/Off,** and then select the Turn syslog event logging on check box. This enables a Mobility server to log Mobility events to a syslog server. Any information, warning, or error events that are recorded in the Mobility event log are also sent to syslog. However, the Mobility server does not log debug events to syslog. To record debug events, use the Mobility event log.
- Select **Syslog - Server Host**. In the Host box, enter the **host name** or **IP address** of the **EventTracker**.

2. By default, the syslog protocol uses UDP **port 514**. To configure the Mobility server to use a different port, select Syslog - Server Port in the list of settings. In the Port box, enter the syslog server port.

3. In a syslog message, the facility identifies the type of software component that generated the message. Some facilities are reserved for the operating system, or for types of applications (for example, email). Applications that are not assigned a facility can use a “local use” facility, which is not reserved.