

# Monitoring Log Volume Surge

*EventTracker Enterprise*

Publication Date: Aug 4, 2015

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://www.eventtracker.com)

## About this Guide:

This guide will help the end user to use the utility in monitoring log volume surge on specific system or machine.

## Scope:

The configurations detailed in this guide are consistent with **EventTracker Enterprise**.

## Audience:

IT/Security administrators who want to monitor if there is a surge of log volume, which might require attention.

*The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.*

*This document is for informational purposes only. Prism Microsystems 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 Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.*

*Prism Microsystems 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 Prism Microsystems, 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.*

*© 2015 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

About this Guide:.....	1
Scope:.....	1
Pre-requisite:.....	3
Introduction.....	4
Steps to schedule the Utility .....	5

## Introduction:

There might be instances where due to mis-configuration of a device/application or in cases of some error condition, there would be flooding of logs. This results in higher load on EventTracker Manager, which might further lead to low disk space or malfunctioning of manager system.

The “ **MonitorLogVolume** ” utility will help in monitoring if there is a surge in log volume observed on the EventTracker Manager server.

## Pre-requisite

- EventTracker should be installed.
- .NET 4.5 should be installed.

## Steps to Schedule the Utility

- Download and apply the updates as per your EventTracker version.
  - For v7.5, apply the update **ET75U15-2001**.
  - For v7.6, apply the update **ET76U15-2000**.
  - For v8.0, apply the update **ET80U15-2002**.

### Configure the "MonitorLogVolumeSurge.exe.config" as per requirement:

Under the <appSettings> section,

```
<appSettings>
  <!-- Count of EC2 file limit after which we assume cache build up is occurring-->
  <add key="EC2ThresholdCount" value="100"/>
  <!-- Increment count of EC2 file. The ec2 files should increase by this value or more everytime the
  check is done-->
  <add key="IncrementThreshold" value="5"/>
  <!--Email address to inform when log volume is observed. Multiple email ids separated by comma-->
  <add key="SendEmailAddress" value="healthcheck@eventtracker.com,myemail@company.com"/>
</appSettings>
```

### NOTE:

- In the threshold count, enter the count value beyond which you assume the cache build up might occur. The count value must be within double quotes ( Ex: "100")
- In the Increment Threshold, put the increment value by which the EC2 should increase everytime the check is done. ( The Increment Count should also be within double quotes ( Ex: "5" ).
- In the SendEmailAddress, you can add on email address for sending the details of log volume surge to the concerned user. (Make sure that the SMTP is configured in the **EventTracker** web. You can also provide multiple email ids, separated by comma).

For scheduling **MonitorLogVolume** Utility,

- Go to **Task Scheduler>Create a Task**.

- Now, in the **General** tab, enter the name: "MonitorLogVolume" and select the check box as highlighted below in the figure:

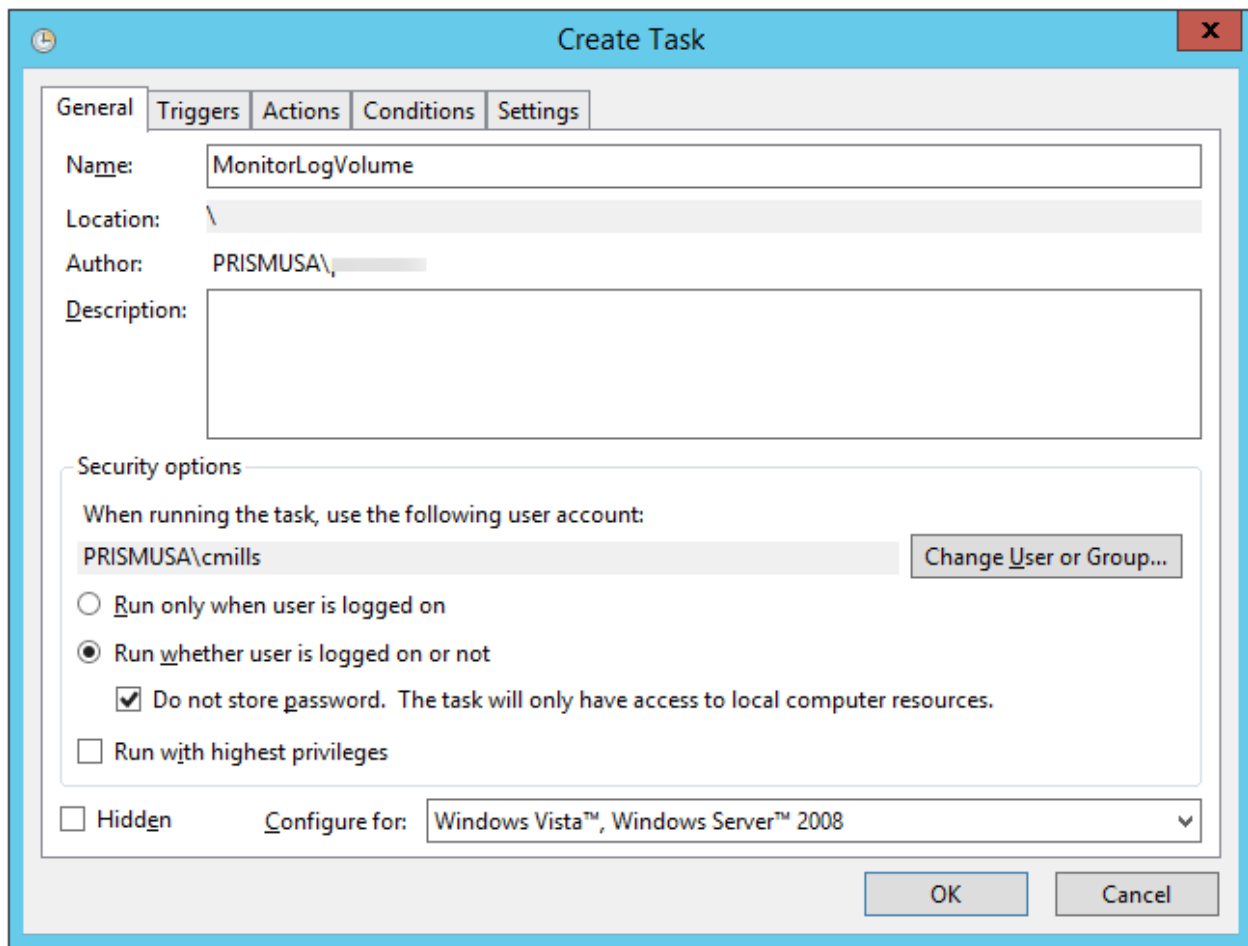


Figure 1

- In the **Trigger** tab, click the **New** button to create a New trigger.
- Select the date and the time.
- Select the option "Daily" and click the checkbox " **Repeat task every** " as "10 Minutes" and **for duration of** as "indefinitely" as highlighted below:

**NOTE:** It is suggested to run this task under the service account used for "EventTracker Remoting" service.

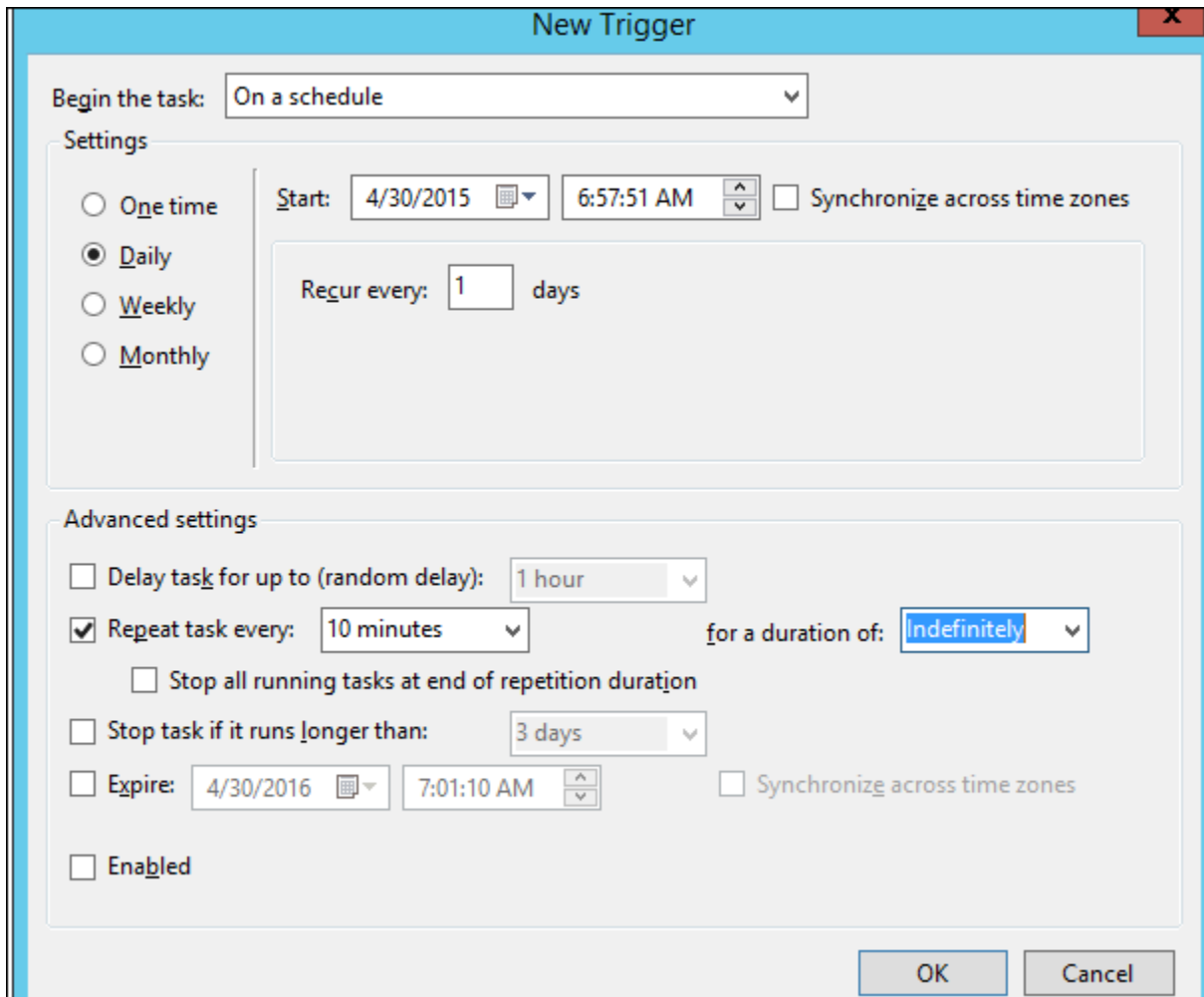


Figure 2

- In the **Action** tab, click the **New** button.
- Click the **Browse** button to select the path as shown below:



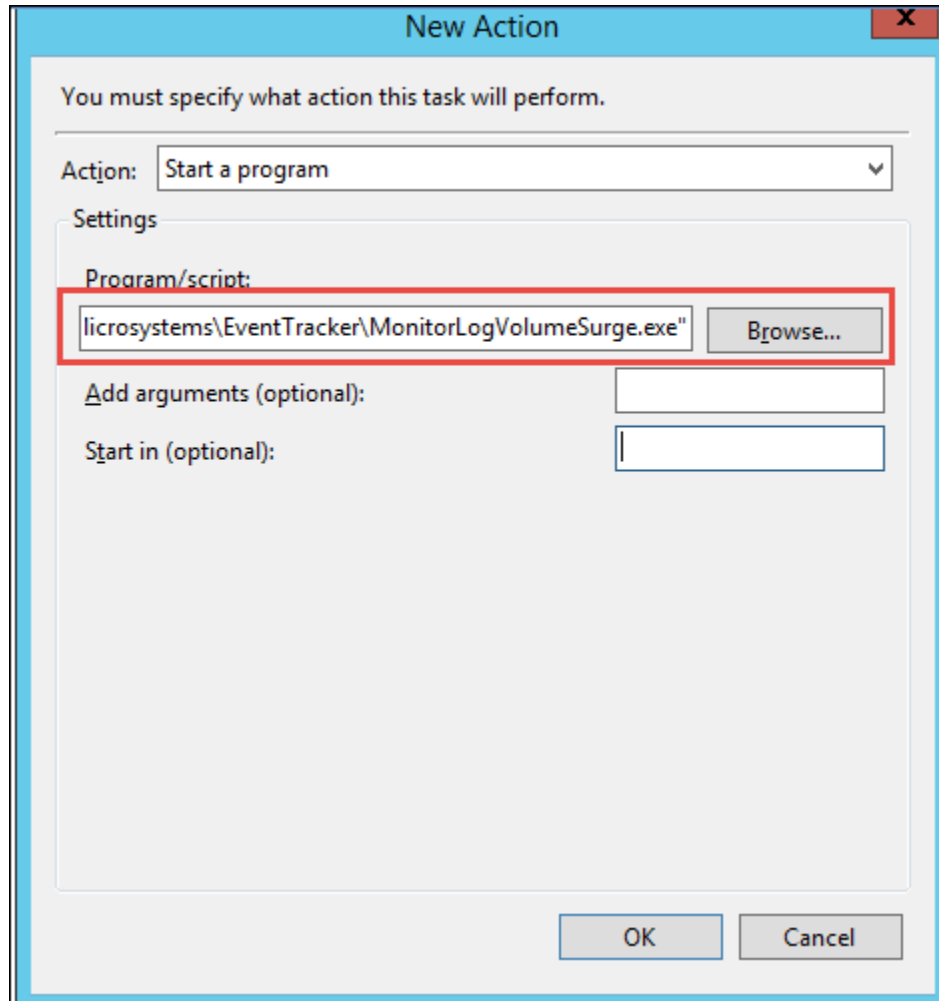


Figure 3

- Review the configuration settings and click **OK**.

The "MonitorLogVolume" utility gets configured and gets listed in the **Task Scheduler** to run on the scheduled time.

### Intimation of Log Volume Surge

The application will send an email to the email address(s) provided in the configuration explained above. Also an event with Event Id "9800" and Event Source "EventTracker" is logged to the eventlog.