EventTracker
Secure. Comply. Succeed.

Monitor Alert Surge in EventTracker

Publication Date: May 27, 2015

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

About this Guide:

This document helps EventTracker Admin to configure Monitoring of sudden surge in alerts generated in EventTracker.

Scope:

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later and Windows Operating systems.

Audience:

EventTracker Administrators.

Table of Contents:

Introduction

Alerts are configured in EventTracker to get alerted when any configured specific incident occurs. Actions are configured to send email or launch remedial action scripts or just display in EventTracker alert dashboard. Sometime it is observed that because of misconfiguration of alert rules or alerts are not tuned user gets their email flooded with same alert emails and that causes problem and other critical alerts are missed or gets hidden. To overcome this problem EventTracker provides script pack to monitor no of alerts generated within configured time and if it is more than the configure threshold alert count, It send out an email to healthcheck@eventtracker.com.

Pre-requisite

- EventTracker v7.x should be installed.
- Windows PowerShell 3.0 and later must be installed.

Automating Monitoring of Alerts Surge

Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the MonitorAlertSurge pack.
- Save MonitorAlertSurge.zip (saved to D:\MonitorAlertSurge\ folder in the example below).
- Extract all files to D:\MonitorAlertSurge\.
- Files in the package are shown below.

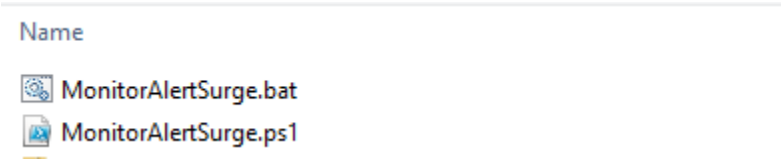

Figure 1

- Copy both the scripts files inside the install path '..\EventTracker\ScheduledActionScripts" folder.

Scheduling the scripts

Schedule MonitorAlertSurge Script

For scheduling MonitorAlertSurge Script, Go to **Task Scheduler** and create a new task with the same name.

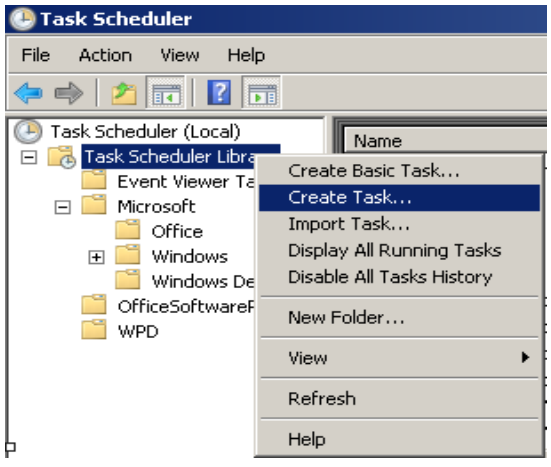

Figure: 2

Now, in the **General** tab, enter the name: Monitor Alert Surge and select the check box as highlighted below in the figure:

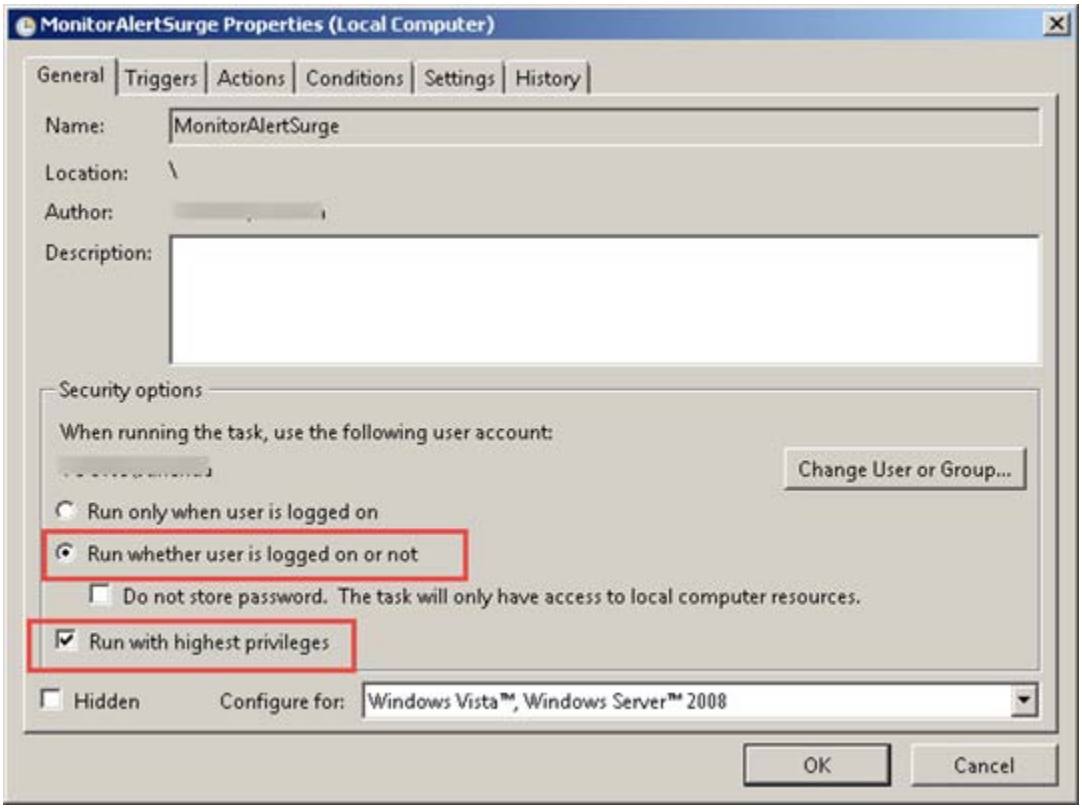

Figure: 3

In the **Trigger** tab, select **New** button and set the time as 12:01 AM and the duration as '1day", where the **Repeat Task every** field would be '15 minutes".

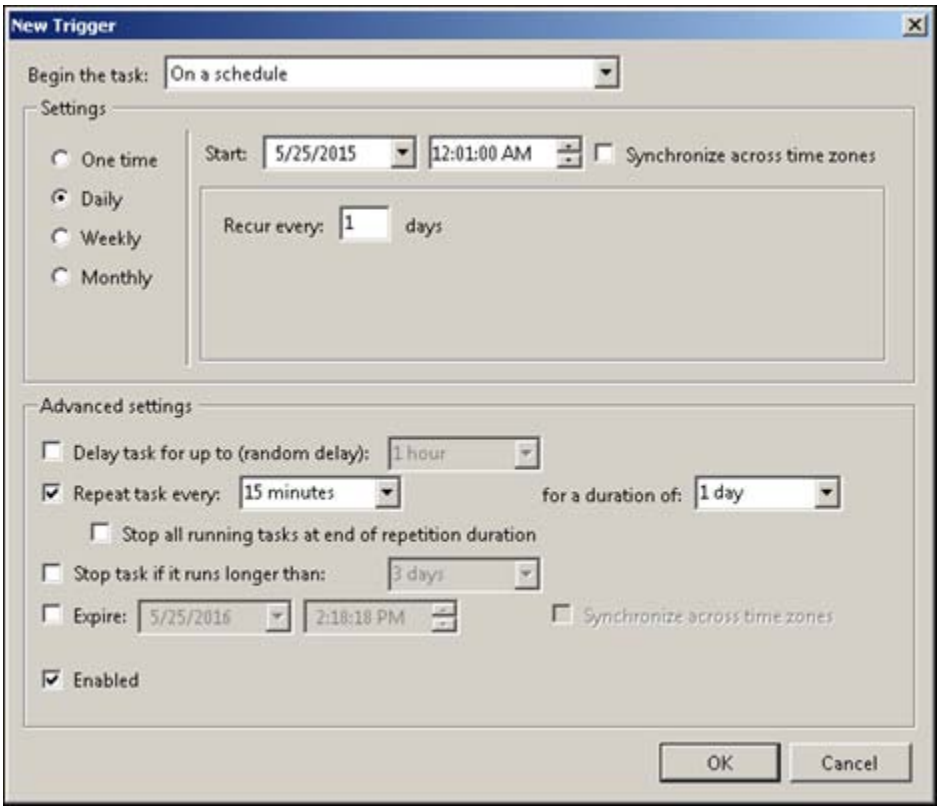

Figure: 4

After configuring the Trigger, click the **OK** button.

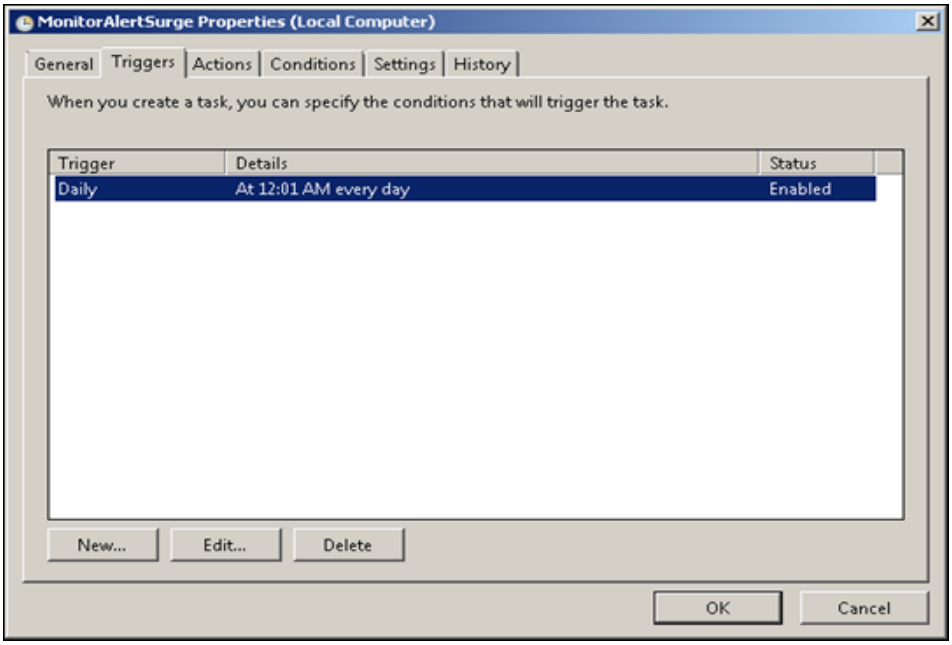

Figure: 5

In the **Action** tab, click **New** button and browse the script file **MonitorAlertSurge.bat** and for the alert count threshold, enter '50" in the **Add arguments** field.

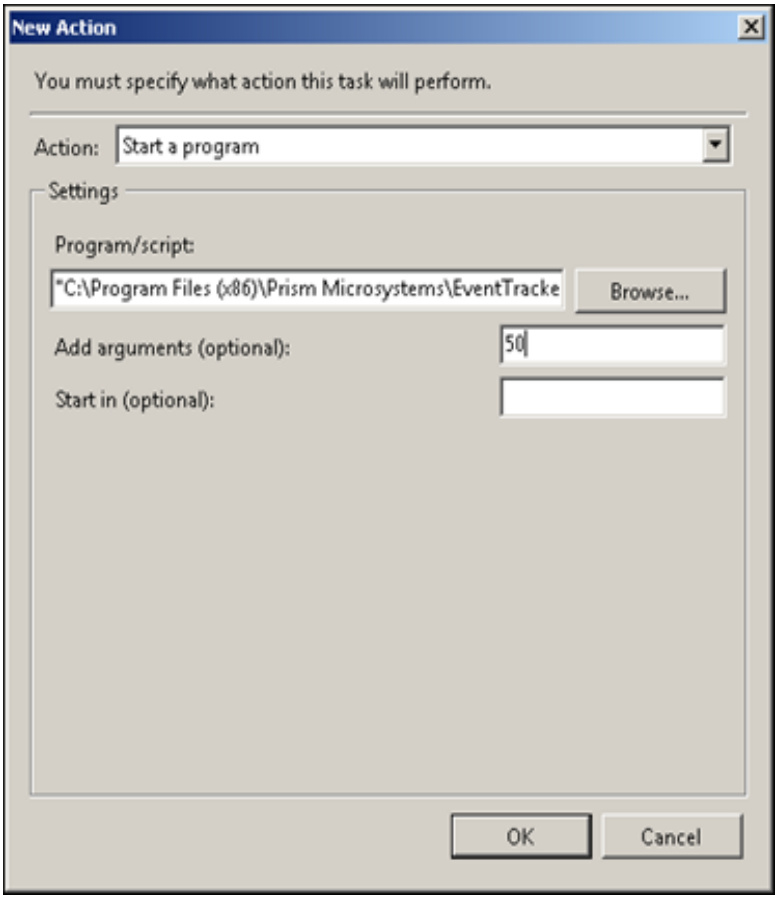

Figure: 6

NOTE: If the Alert count threshold exceeds the limit which is given as '50", the alerts generated will be disabled and an e-mail will be sent.

Click the **OK** button.

The below page is displayed.

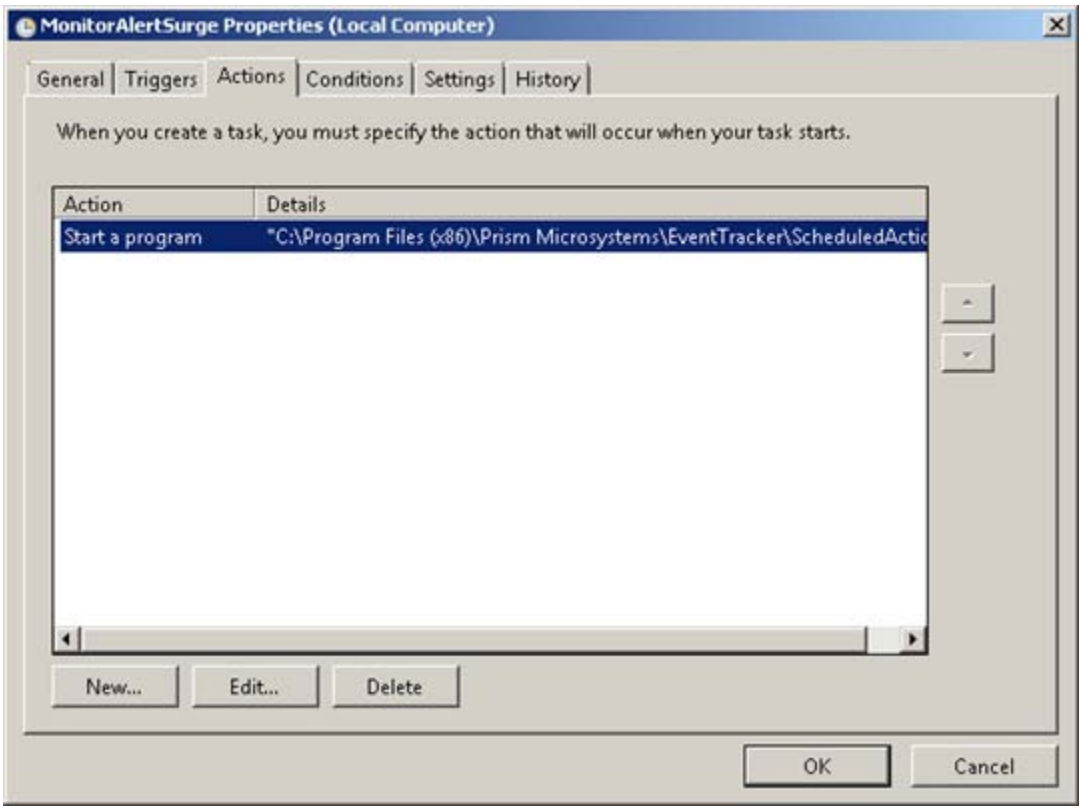

Figure: 7

After clicking **OK**, enter user name and password which is used for EventTracker configuration.

Once Task scheduler runs and if Number of alerts generated in last 15 mins is more than the alert count threshold provided while configuring schedule task, then it will disable the alert and restart EventTracker Receiver service and send an email to healthcheck@eventtracker.com containing message as below.

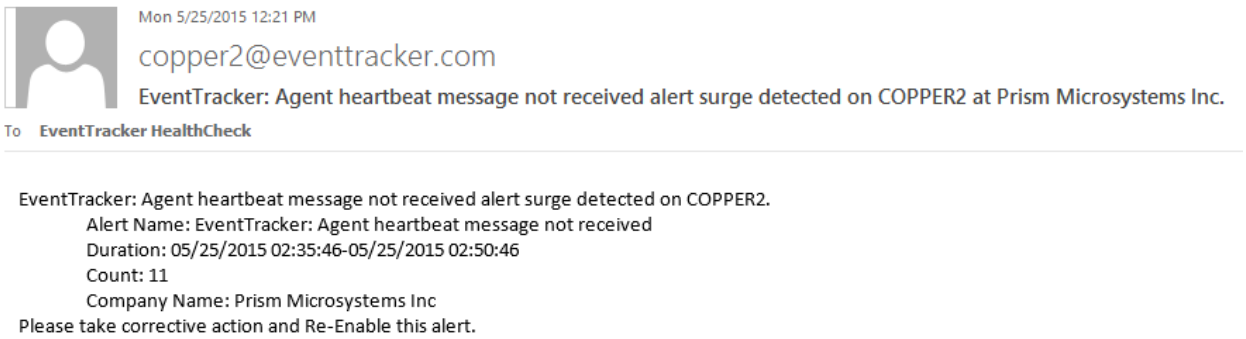

Figure: 8

Re-enabling the disabled alert

Once you have received email for AlertSurgeDetection you should tune and enable the alert by correcting the rule if it is wrong or if you feel this is the expected behavior then increase the Alert count threshold value in Task scheduler.