EventTracker
Secure. Comply. Succeed.

EventTracker: Text Messaging Using- Textbelt API

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

Publication Date: July 10, 2012

About The Document

EventTracker triggers an alert on more than one occurrence of the same event. In addition, EventTracker will run any batch file or custom script. Using these functionalities, a text message is generated and forwarded to mobile phone. This document explains how to use **Textbelt API** to generate a text message when an alert is triggered.

DISCLAIMER

THIS CODE AND INFORMATION ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE.

Table of Contents

Prerequisites

- The **Curl** utility - Required to generate message on Textbelt API.
- **Batch file**- Required to parse value of alert description and send message.
- **Enable firewall settings** -Create an exception for http://textbelt.com , port 80 on firewall.

Textbelt.com Limitations

- IP addresses are limited to 75 texts per day. Phone numbers are limited to 3 texts every 3 minutes.
- Some carriers may deliver text messages from "txt@textbelt.com.
- Textbelt.com support only U.S. providers: Alltel, Ameritech, AT&T Wireless, Boost, CellularOne, Cingular, Sprint PCS, Telus Mobility, T-Mobile, Metro PCS, Nextel, O2, Orange, Qwest, Rogers Wireless, US Cellular, Verizon, Virgin Mobile
- Only 160 characters are allowed in a message. Above 160 characters, the message will be truncated.

Summary

This tool consists of batch files. Once an alert is triggered on EventTracker server, configured console remedial action runs the script. The script parses the alert details and results are passed to Textbelt API with support of the **Curl** utility.

Configuration Steps

Step 1- Download Curl on EventTracker host machine

Download Curl from http://curl.haxx.se/download.html link. Extract the files and place them on root folder (Example: - c:\curl).

Step 2- Create a batch file containing following script

```
@echo on
rem %1 = Event Type
rem %2 = Log Type
rem %3 = Source system
rem %4 = Event Source
rem %5 = Category
rem %6 = Event ID
rem %7 = User
rem %8 = Description

set dt=%date% %time%
set srcsys=%3%
set evtid=%6%
set dscr=%8%
set appname=none
rem echo %dscr%

for /f "tokens=2  delims=\<>"  %%i  in (%dscr%) do set appname=%%i
echo %appname%

cd c:\curl
curl.exe http://textbelt.com/text -d number=4438xxxxxx -d message="Software Uninstalled-
%appname% from -%srcsys% at %dt%" > log.txt
```

Note: The newly created batch file can be placed on the same folder as **Curl** folder.

Example of event description:-

```
Event Time: 2012-06-06 18:46:51.
Type: Info.
Computer: PNPL-7-SUP
Source: EventTracker
EvtID: 3209
User: N/A\SYSTEM
```

Descr: Detected software <Kiwi SyslogGen> has been uninstalled from this system.

Name: Kiwi SyslogGen

Output Message Example: -

Software Uninstalled- Mozilla Firefox 11.0 (x86 en-US) from -PNPL-7-SUP at Wed 05/30/2012 20:42:00.21

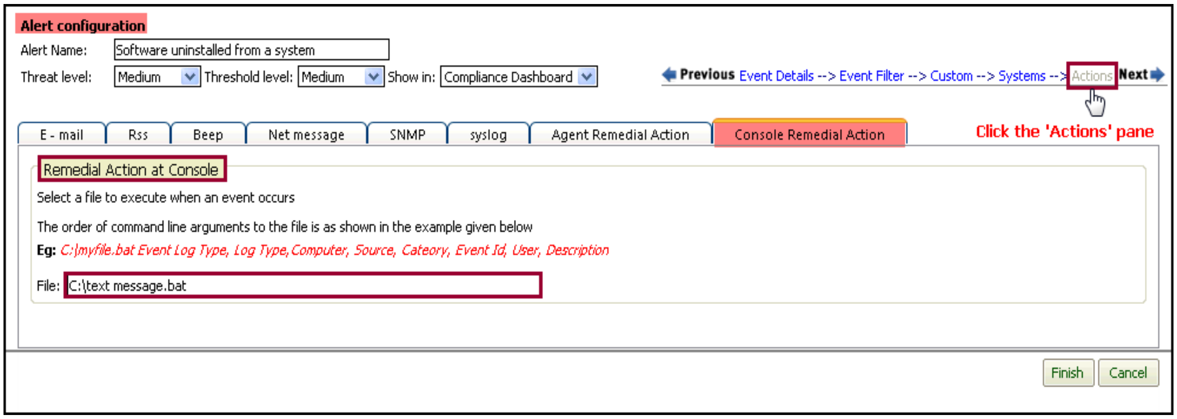
Note: -

The message will contain application name and system name, which has been parsed from EventTracker event. The date & time are also included when the message is sent.

Step 3- Enable remedial action in EventTracker Enterprise

1. Login to **EventTracker Enterprise**.
2. Click the **Admin** hyperlink, and then click **Alerts**.
3. Click an alert which needs to be configured to send the text message.

   EventTracker takes you to **Alert configuration** page.



Alert configuration

Alert Name: Software uninstalled from a system

Threat level: Medium Threshold level: Medium Show in: Compliance Dashboard

Remedial Action at Console

Select a file to execute when an event occurs

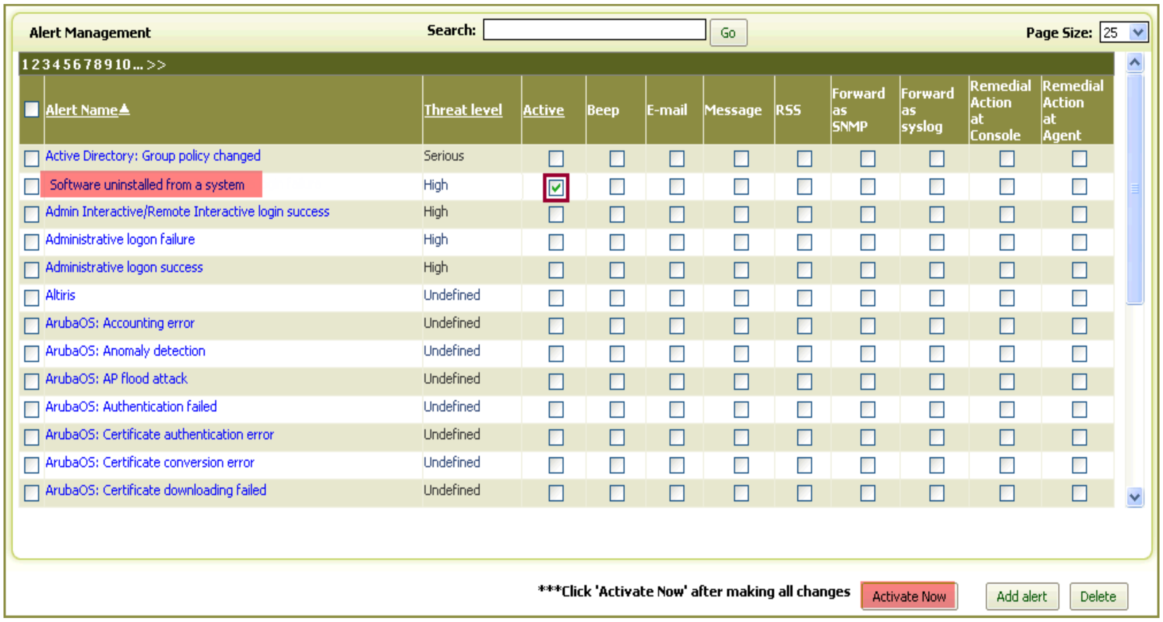
The order of command line arguments to the file is as shown in the example given below

Eg: *C:\myfile.bat Event Log Type, Log Type,Computer, Source, Cateory, Event Id, User, Description*

File: C:\text message.bat

Figure 1

4. Configure Event Details and other tabs appropriately.
5. Click **Next** or click the **Actions** hyperlink, and then click the **Console Remedial Action** tab.
6. In the **File** field, type the batch file path.
7. Click the **Finish** button to save the alert configuration.
8. On the **Alert Management** page, search for the configured alert.



Alert Management Search: Page Size: 25

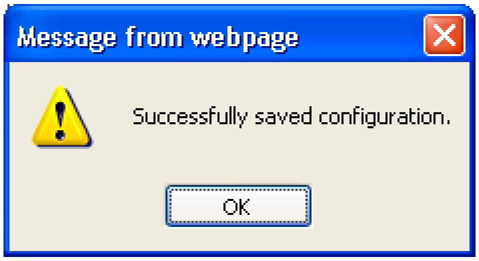
12345678910...>>

□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
□	Active Directory: Group policy changed	Serious	□	□	□	□	□	□	□	□	□
□	Software uninstalled from a system	High	☑	□	□	□	□	□	□	□	□
□	Admin Interactive/Remote Interactive login success	High	□	□	□	□	□	□	□	□	□
□	Administrative logon failure	High	□	□	□	□	□	□	□	□	□
□	Administrative logon success	High	□	□	□	□	□	□	□	□	□
□	Altiris	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Accounting error	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Anomaly detection	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: AP flood attack	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Authentication failed	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Certificate authentication error	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Certificate conversion error	Undefined	□	□	□	□	□	□	□	□	□
□	ArubaOS: Certificate downloading failed	Undefined	□	□	□	□	□	□	□	□	□

***Click 'Activate Now' after making all changes

Figure 2

9. Check the **Active** option.



Message from webpage

Successfully saved configuration.

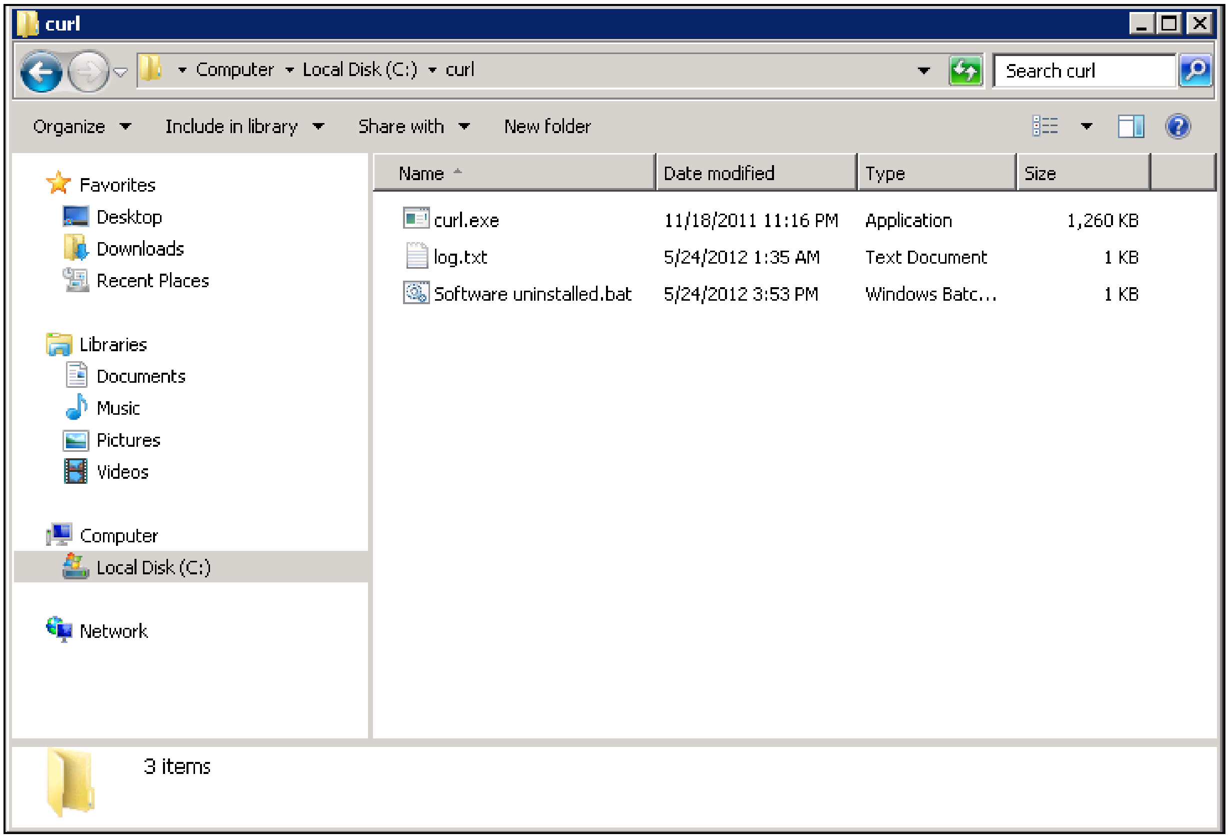
Figure 3

10. Click the **OK** button.
11. On the **Alert Management** page, click the **Activate Now** button to activate the configured alert.

Scenario: - Monitoring Software uninstalled on client machines.

- Created a batch file ‘software uninstalled.bat” and placed it on c:\curl folder.

  Remedial action will execute the batch file.



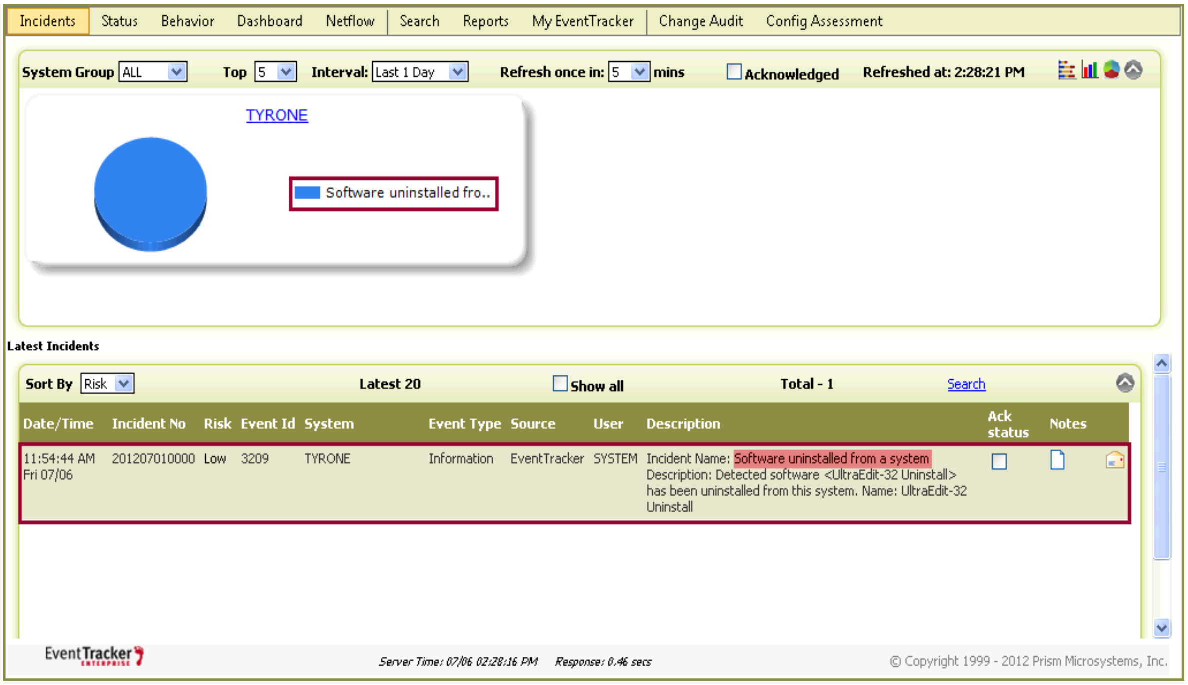
Name	Date modified	Type	Size
curl.exe	11/18/2011 11:16 PM	Application	1,260 KB
log.txt	5/24/2012 1:35 AM	Text Document	1 KB
Software uninstalled.bat	5/24/2012 3:53 PM	Windows Batc...	1 KB

Figure 4

- On **Alert Management** page, **Software uninstalled from a system** alert template is configured to generate the text message.

  Note: Software uninstalled event will be captured by EventTracker with **Event ID 3209**.

- Alert is tested successfully by uninstalling an application on one of the client machine.
- **Incident** dashboard will display the alert details as shown in the figure 5.



System Group ALL Top 5 Interval: Last 1 Day Refresh once in: 5 mins □ Acknowledged Refreshed at: 2:28:21 PM

Latest Incidents

Sort By Risk Latest 20 □ Show all Total - 1 Search

Date/Time	Incident No	Risk	Event Id	System	Event Type	Source	User	Description	Ack status	Notes
11:54:44 AM Fri 07/06	201207010000	Low	3209	TYRONE	Information	EventTracker	SYSTEM	Incident Name: Software uninstalled from a system Description: Detected software <UltraEdit-32 Uninstall> has been uninstalled from this system. Name: UltraEdit-32 Uninstall	□	

Server Time: 07/06 02:28:16 PM Response: 0.46 secs © Copyright 1999 - 2012 Prism Microsystems, Inc.

Figure 5