EventTracker
Secure. Comply. Succeed.

Remedial Actions

EventTracker v8

Publication Date: Sept 4, 2015

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

Abstract

The purpose of this document is to help users understand and execute remedial actions at Manager Console system and Remote Agent systems.

Table of Contents

Fault Monitoring/Alerting/Acting

Alerting is a reactive mechanism against critical events collected in EventTracker. The responsibility lies squarely with the user to configure required notifications like e-mail, beep, messages or custom actions.

If configured properly, notification mechanism spontaneously notifies the users about the events occurred in all monitored systems that include Windows, non-Windows, Agent based and Agent-less systems.

Notifications consist summary of the incident that helps users to investigate the root cause and explore efficient ways to take preventive and remedial measures.

Upon receiving a notification, the security personnel should act promptly to avert any disastrous consequences. What happens if the security person is not aware of the notification?

Is it not good to guard against mishaps than to suffer unnecessarily? Yes, it is always wise to be so. EventTracker provides the necessary facilities to automate remedial actions at the Manager Console and remote systems as well, where Agents are deployed.

Remedial Actions

Remedial Actions are automated corrective actions taken to mitigate issues that occur at the Manager and Agent systems.

Remedial Actions help users:

- Block unauthorized use of PC device access
- Protect enterprise network against threats posed by portable storage media
- Enumerate and kill processes that cause havoc
- Minimize maintenance effort
- Maximize uptime

How it works

Upon receiving Events that requires user's attention, EventTracker can be configured to

- Raise a beep sound from the PC speaker
- Send e-mail to one or more recipients
- Send network message to specific devices connected to the network
- Forward events as Traps to specific devices

These traditional notifications are good enough to analyze the impact and severity of events. But what is required is action.

- Execute remedial actions at Manager Console (Custom action in earlier versions) option helps to automate remedial action at the Manager Console.

At this juncture you may question,

- Is it possible to remedy the incidents that occur at remote Agent systems where real action is required?
- Could I execute actions on both Agent based and Agent-less systems?
- Could I execute actions on non-Windows systems?
- Could I execute scripts on remote systems? If so, should those scripts be present locally in all those systems?
- What are the custom actions could I perform on remote systems?
- Do I need any special privileges to perform actions on remote machines?

The answer is straight and simple. Through 'Agent side remedial action' feature, custom action such as blocking USB ports or running scripts is possible, provided

a. Remote system should be running Windows O/S (presently non-Windows O/S are not supported).
b. You cannot execute custom actions on Agent less systems.

c. If you execute scripts on multiple systems, the scripts should be present locally in each system in the EventTracker install directory, typically (...\Program Files\Prism Microsystems\EventTracker\Agent\Script).

d. Following are the custom actions you could perform on remote systems

- Run custom script
- Restart Service
- Restart System
- Shutdown system
- Stop Service
- Terminate process

e. Not really needed at this point, as you have already deployed the Agent with adequate privileges.

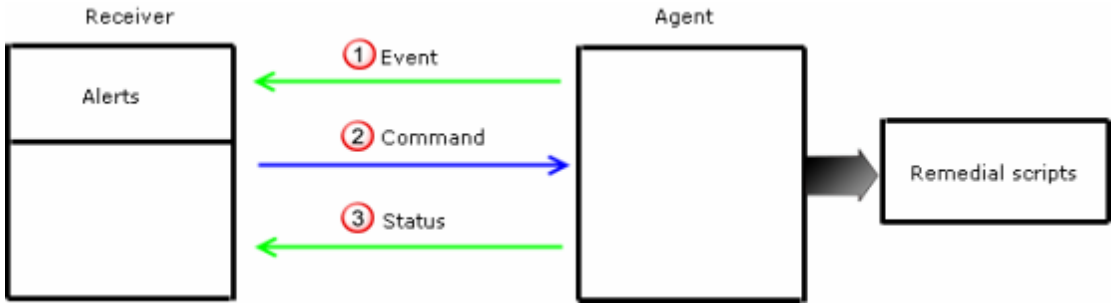

Figure 1

Remedial Actions Events and Traps

Remedial Actions Events and Traps
Manager Side: This event is generated and logged at the Manager side.
Event ID = 2035 Event Type = Information Desc = Matched Remedial action request. Initiating Remedial Action Type: <n> on system <system>
Agent side: The Agent forwards these traps to the Manager as acknowledgement.
Event ID = 3234 Usage = Remedial Events Event Type = Information Desc = Received Remedial action request for <Action Type> action.
Event ID = 3235 Usage = Remedial Events Event Type = Information Desc = Successfully initiated <Action Type> action.
Event ID = 3236 Usage = Remedial Events Event Type = Error Desc = Failed to initiate <Action Type> Remedial action.

How Remedial Actions Help

Easily configure group-based protection.

You can organize computers into different groups and specify different rule sets to allow or disallow access to PC devices.

Enable Remedial Actions
Manager

It is mandatory to enable remedial action at Manager Console. Otherwise you cannot execute remedial action at the Agent systems.

1. Login to **EventTracker** web.
2. Click the **Admin** dropdown and then select the **Manager** option.

   EventTracker displays the Manager Configuration window.

3. Select the **Enable Remedial Action** check box.

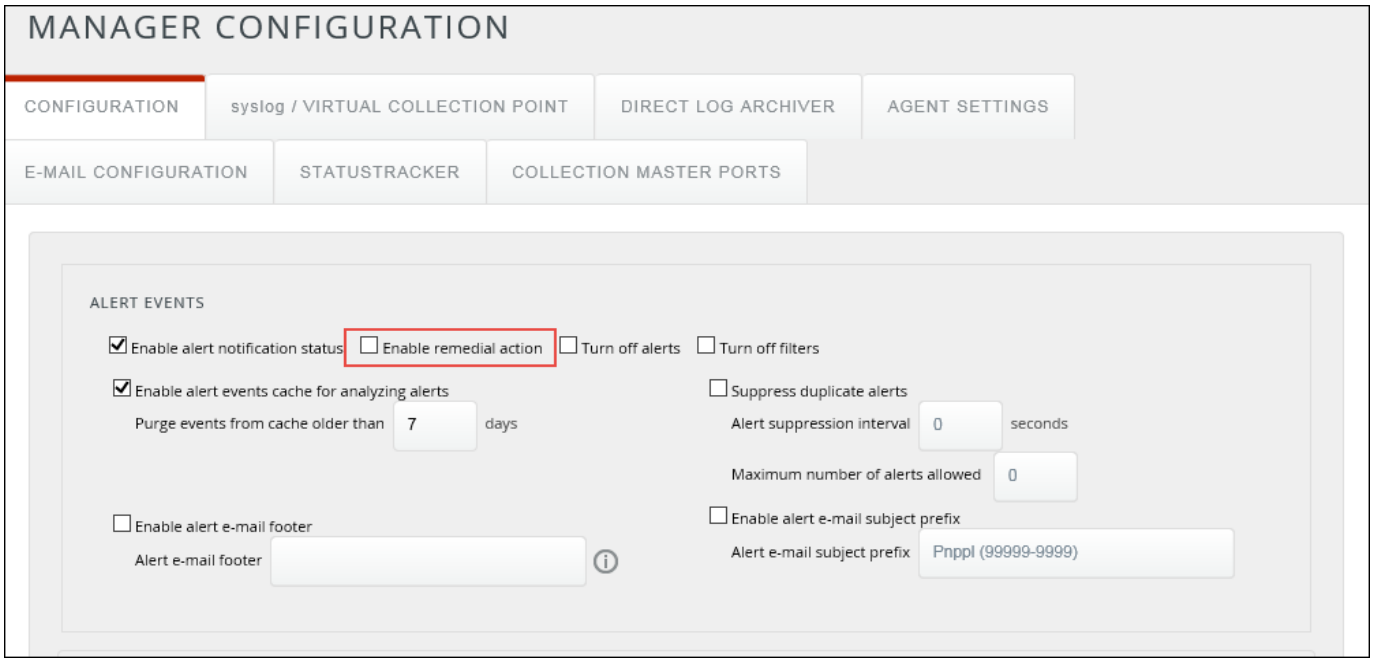

Figure 2

EventTracker displays the Caution dialog box.

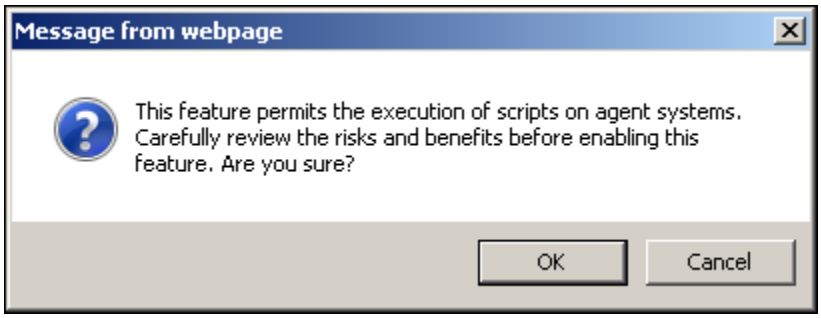

Figure 3

4. Click **OK.**
5. Now click the **Save** button on the Manager Configuration window.

Agent

After enabling remedial actions at the Manager Console, you have to individually enable Remedial Action on all the Agent systems. You can also include or exclude Agents from taking remedial actions.

1. Open the **EventTracker Control Panel**.
2. Double-click the **EventTracker Agent Configuration** option.

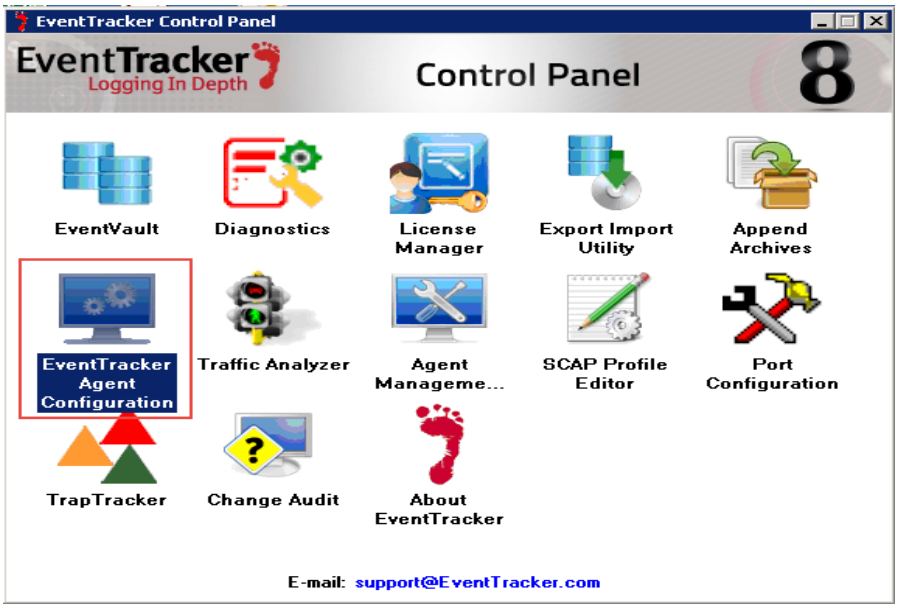

Figure 4

The **EventTracker Agent Configuration** Window displays.

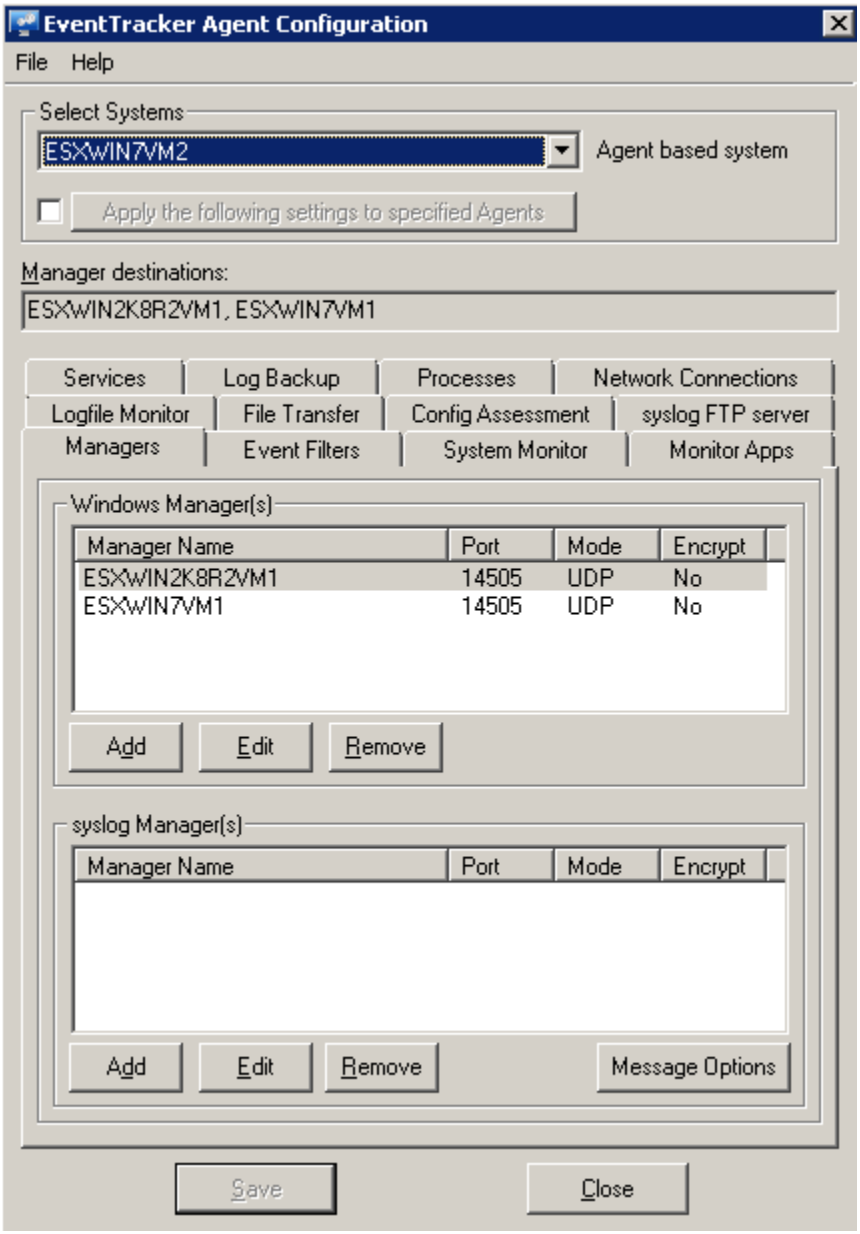

Figure 5

3. Select a system where you want to execute remedial actions from the **Select Systems** drop-down list.

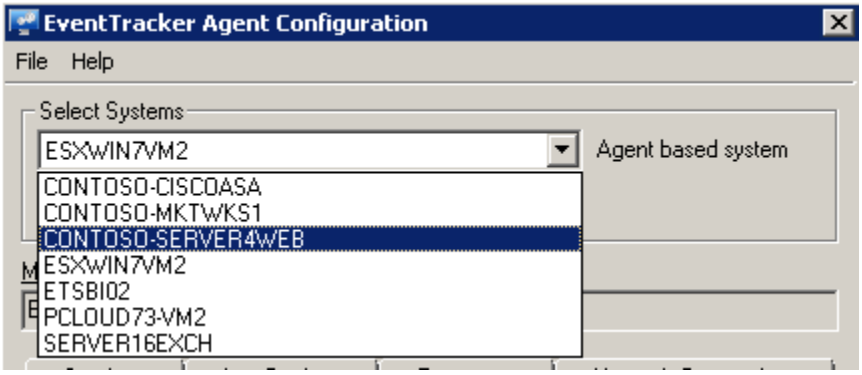

Figure 6

4. Click the **File** menu and then select the **Security** option.

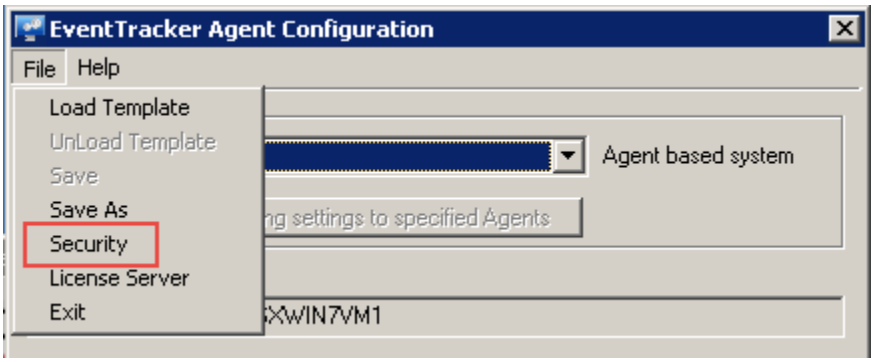

Figure 7

EventTracker displays the Security window.

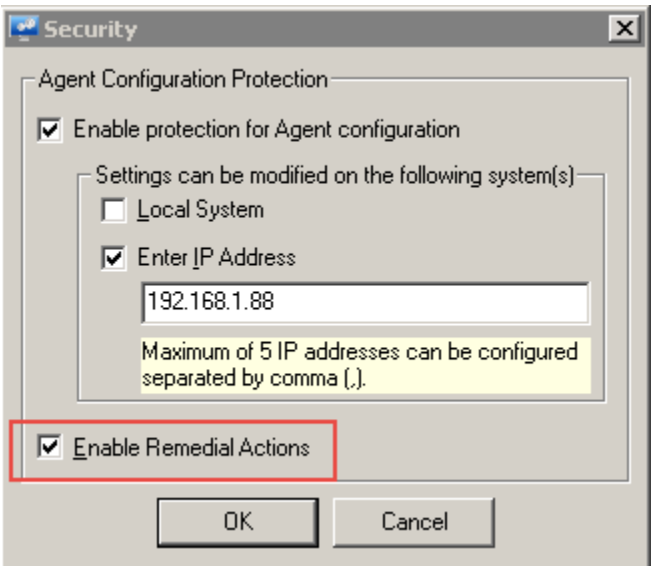

Figure 8

5. Select the **Remedial Action** check box.
6. Click **OK**.
7. Click **Save,** and then click **Close** in the **EventTracker Agent Configuration** window.

Configure Remedial Actions

Though EventTracker is shipped with predefined Alerts that are applicable to all monitored systems irrespective of O/S and mode of monitoring (Agent based or Agent less), to get Alert notification messages you need to explicitly configure Alert Actions. While configuring Alert Actions it is left to your discretion to include and exclude systems. Same rule holds good for User-defined Alerts. Note that remedial actions can be executed only on systems where EventTracker Agent has been deployed.

Excluding systems for Alert Actions doesn't mean that you are excluding them from monitoring. EventTracker logs all events that occur in monitored systems into MS Access database, you can plow through the data by performing Log Search.

So, utilize this feature judiciously to draw maximum benefits.

Execute Remedial Actions at Agent

Predefined Alerts

1. In **EventTracker** web, click the **Admin** dropdown and then select the **Alerts** option.
   EventTracker displays the **Alert Management** page..
2. Select an Alert.
3. Click the checkbox against the selected Alert under **Remedial action at Agent**.

   (OR)

1. Double-click an Alert.
   The Alert Configuration page displays.
2. Click the **Action** option at the right-hand side corner and select the **Agent Remedial action** tab.

   EventTracker displays the Agent dialog box.

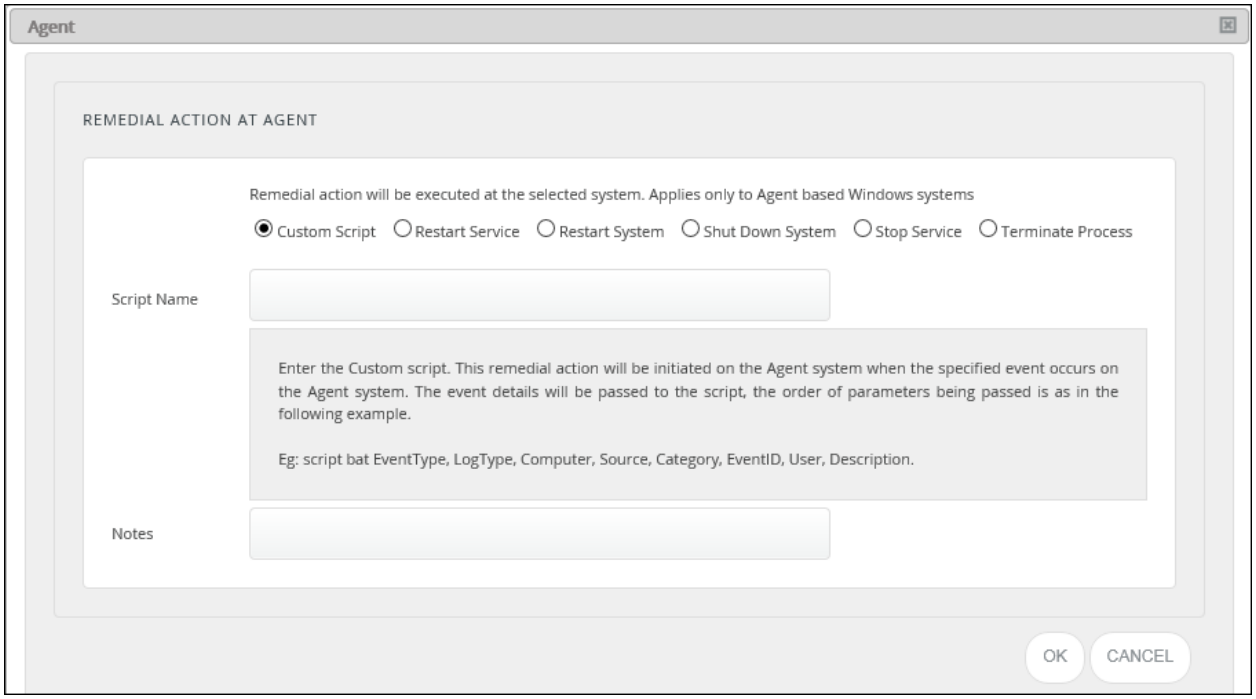

Figure 9

Field	Description
Custom Script	Type the name of the script in **Script Name** field. Script files are stored in the default EventTracker Agent installation path typically ...\Program Files\Prism Microsystems\EventTracker\Agent Type appropriate description in the **Notes** field for future reference.
Restart Service	Type the name of the service that you want to restart in **Service Name** field. Type appropriate description in the **Notes** field for future reference.
Restart System	EventTracker disables the **Script Name** field. Type appropriate description in the **Notes** field for future reference.
Shut Down	EventTracker disables the **Script Name** field.
System	Type appropriate description in the **Notes** field for future reference.
Stop Service	Type the name of the service that you want to stop in **Service Name** field. Type appropriate description in the **Notes** field for future reference.
Terminate Process	EventTracker enables this option only when you set an alert for Events 3217, 3218, 3221, 3223, and 3226.

As said earlier you ought to enable Remedial Action in the Manager Configuration window. Had you not enabled, EventTracker will display Actions window with appropriate message to enable Remedial Action.

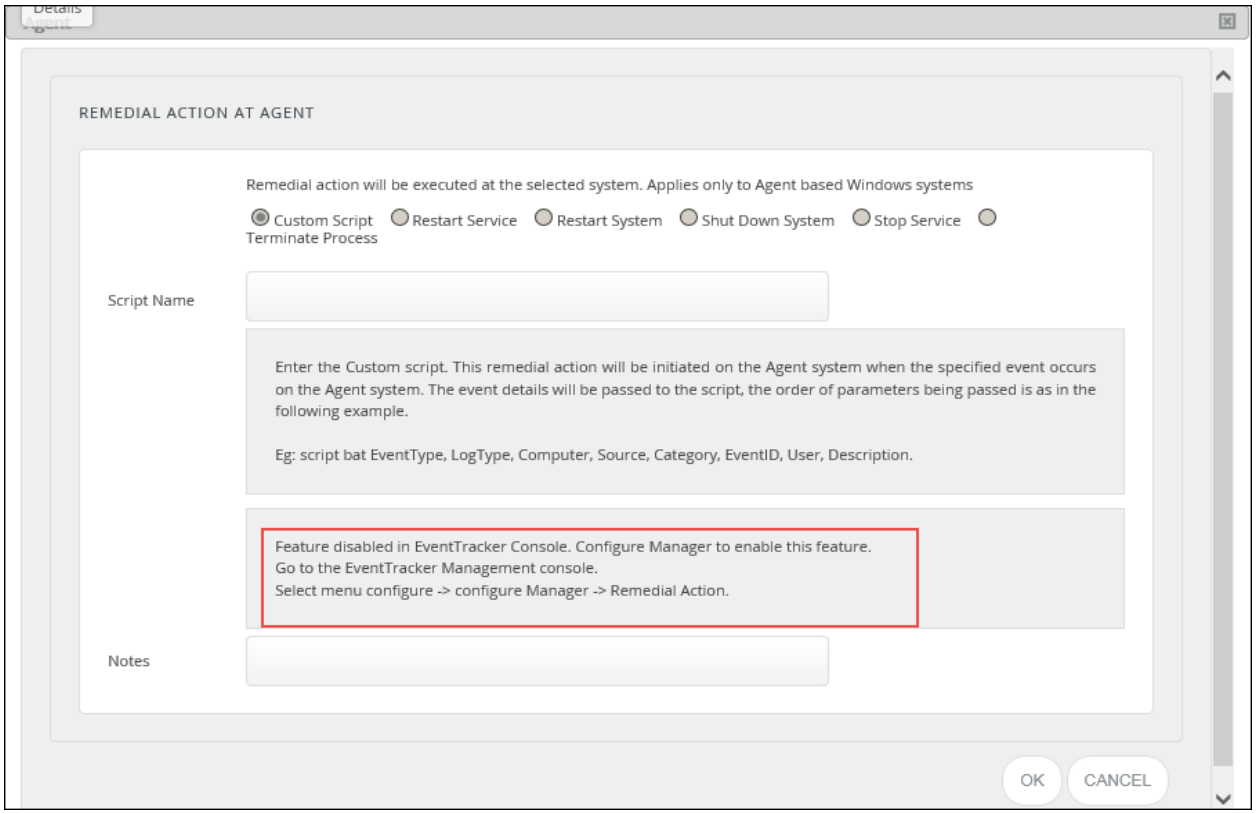

Figure 10

4. Select an appropriate option and then click **OK**.
5. Now, click the **Activate Now** button, in the Alert Management page.

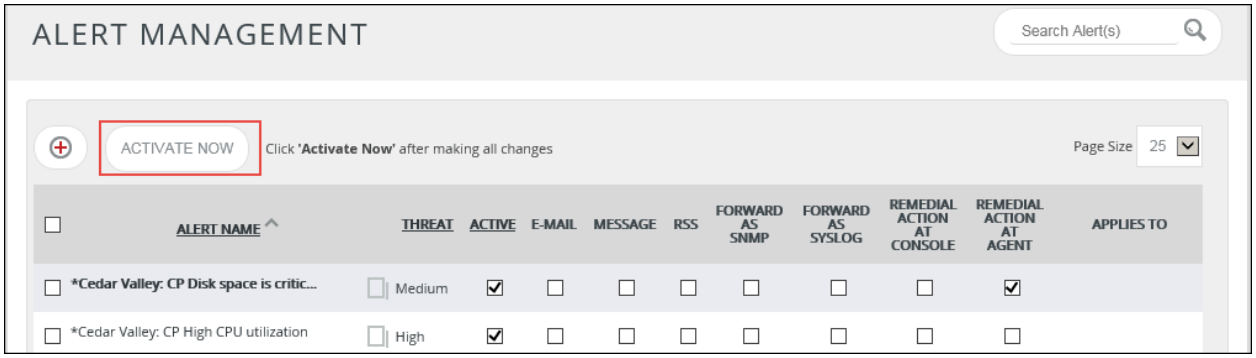

Figure 11

Remedial actions will be initiated only on systems where Remedial Action is enabled.

You can also exclude systems where remedial actions have been enabled.

Execute Console Remedial Actions

This option enables you to configure custom action to be executed on receipt of an event at the Manager system.

For example: If you want to execute Console remedial Action to the **Bad Ip reputation-process lookup** alert:

1. Click the **Admin** dropdown and then select the **Alerts** option.

EventTracker displays the Alert Management page.

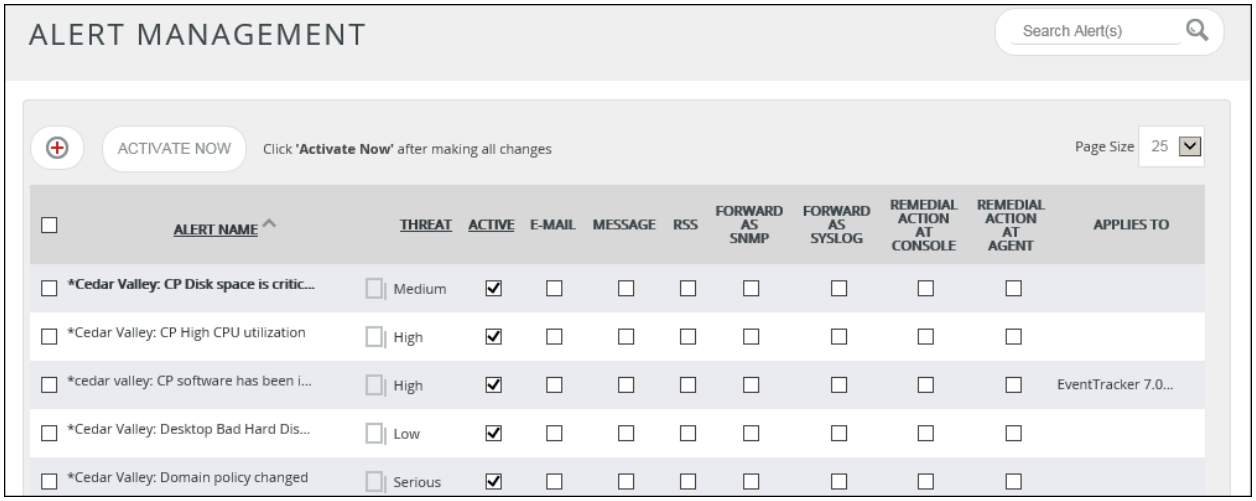

Figure 12

2. Search the Alert in the search box at the right hand side corner.

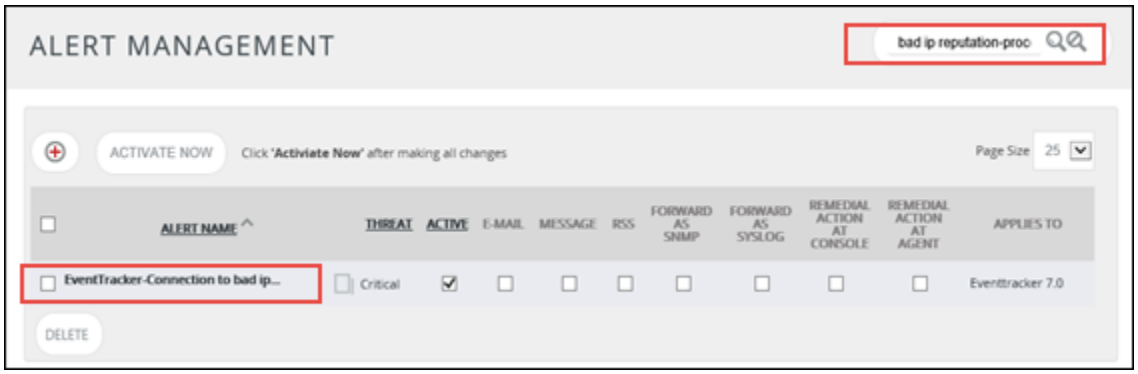

Figure 13

3. Select the Alert (**Bad Ip reputation-process lookup**); select the checkbox against the selected Alert under **Remedial action at Console**.

   (OR)
   Double-click the alert and click the **Action** option in the Alert configuration page. Now select the **Console Remedial Action** tab.

EventTracker displays the Remedial Action at Console window.

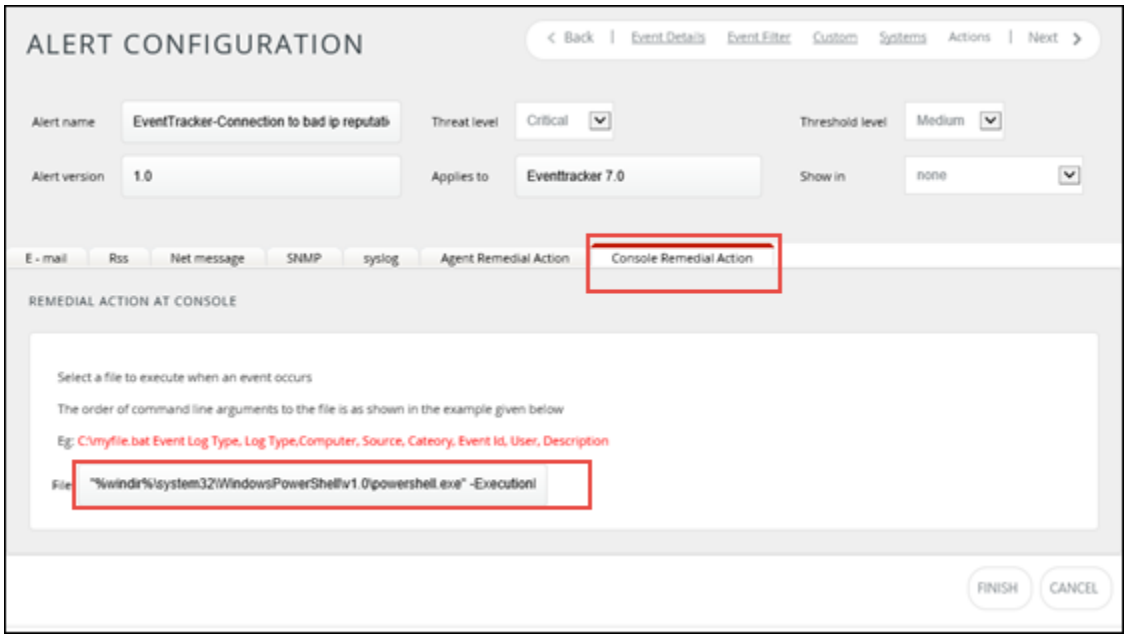

Figure 14

4. Enter the file name with the mentioned path and verify the appropriate script path to execute when an event occurs.

NOTE: In case if you have stored script in different path, replace it with the path where you have stored the script.

5. Check the appropriate script path to execute when an event occurs.

6. Click **Finish**.

7. Now click the **Activate Now** button after confirming all the changes made and activate the alert: **Bad IP reputation-process lookup**

Figure 15