EventTracker
Secure. Comply. Succeed.

Remedial Actions

EventTracker v6.x

Publication Date: Jun 12, 2009

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.

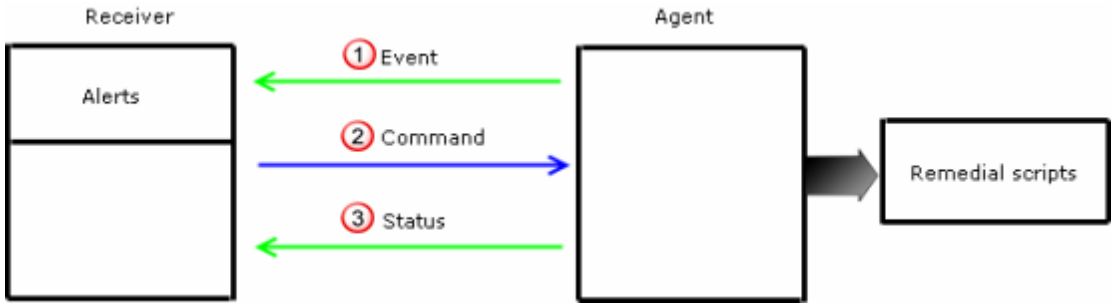

Figure 1

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. Open the Management Console.
2. Click the **Configure** menu and then select the **Configure Manager** option.

   EventTracker displays the Manager Configuration window.
3. Select the **Enable Remedial Action** check box.

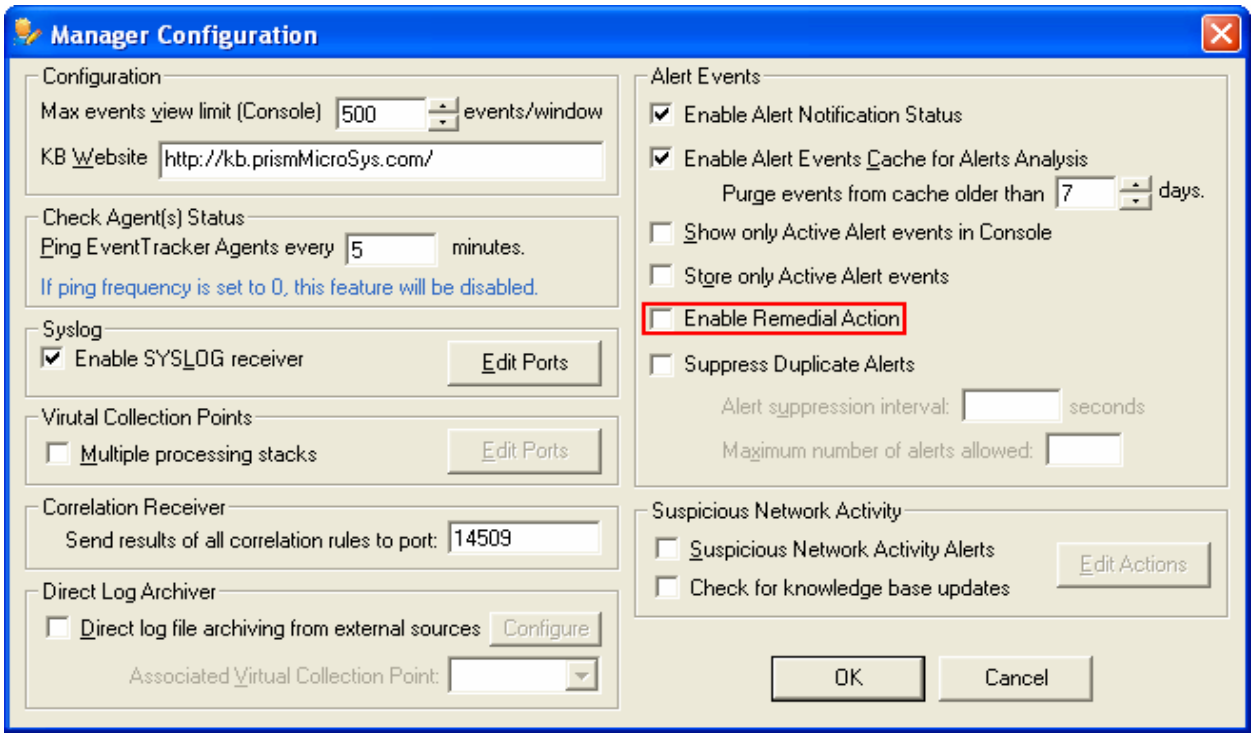

Figure 2

EventTracker displays the Caution dialog box.

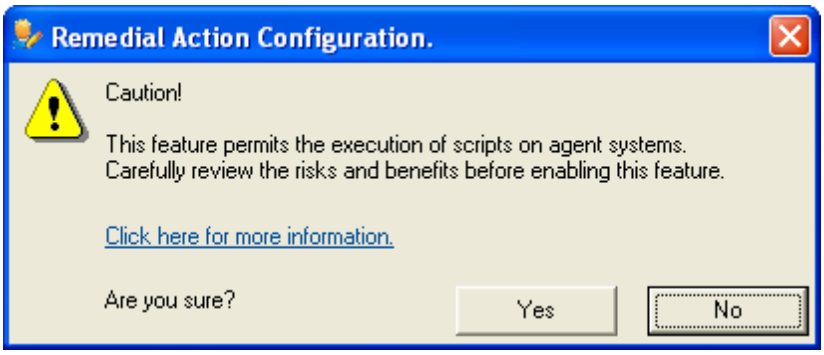

Figure 3

4. Click **Yes**.
5. Click **OK** on the Manager Configuration window.

   EventTracker displays confirmation dialog box to save changes.
6. Click **Yes**.

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 Management Console.
2. Click the **Configure** menu and then select the **Configure Agents** option.
3. Select a system where you want to execute remedial actions from the **Select Systems** drop-down list.
4. Click the **File** menu and then select the **Security** option.

   EventTracker displays the Security window.

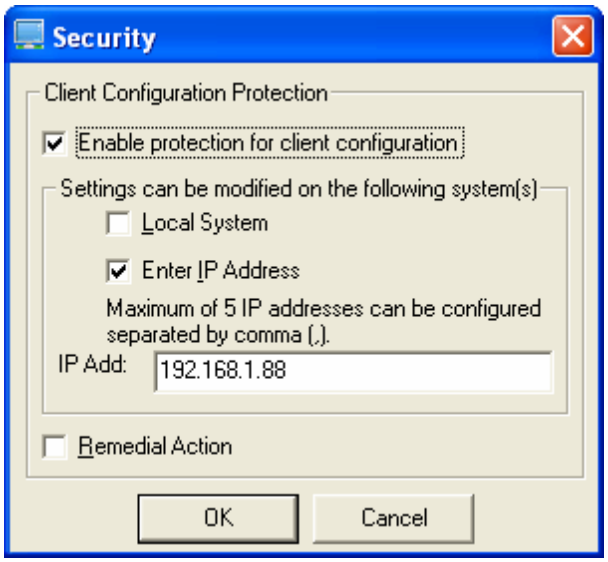

Figure 4

5. Select the **Remedial Action** check box.
6. Click **OK**.

   EventTracker displays the confirmation message box to save changes.

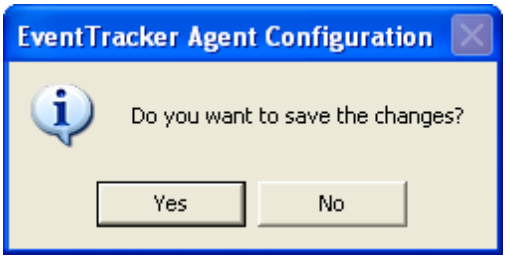

Figure 5

7. Click **Yes**.
8. Click **Save,** and then click **Close**.

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. Double-click **Alert Configuration** on the Control Panel.

   (OR)

   Click the **Configure** menu and then select the **Configure Alerts** option.

   EventTracker displays the Alert Groups console.

2. Select an Alert.

3. Click the option against the selected Alert under **Agent side remedial action**.

   EventTracker displays the Actions dialog box.

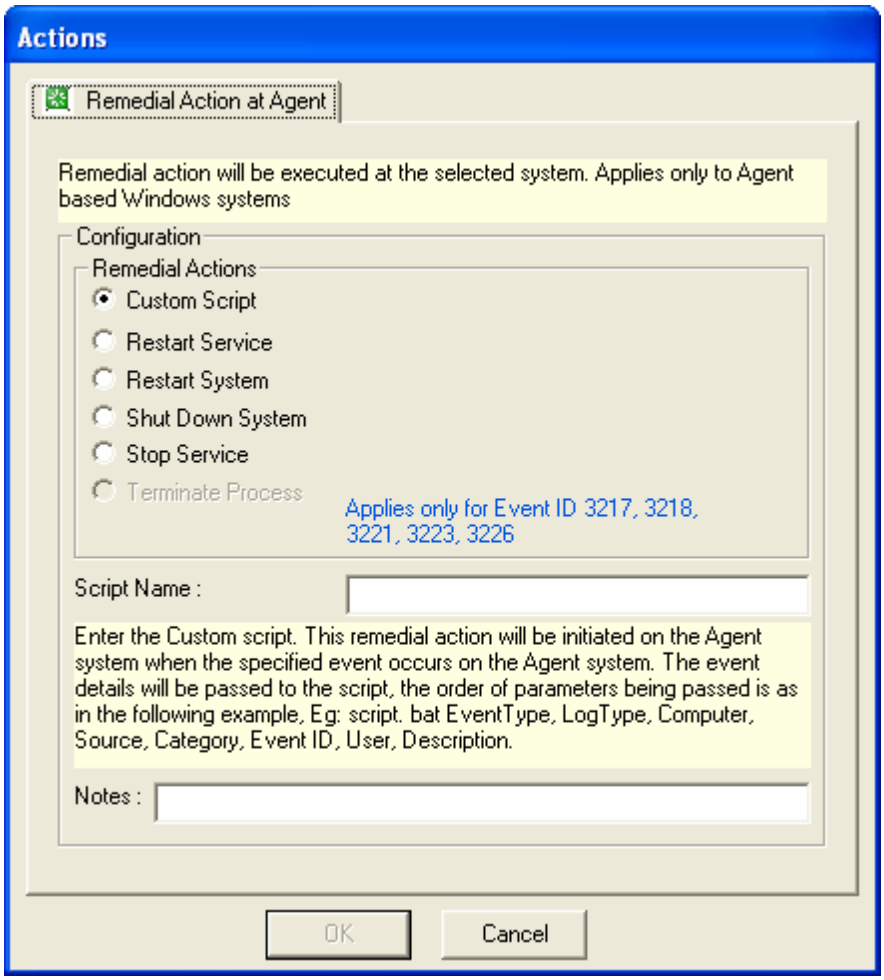

Figure 6

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.

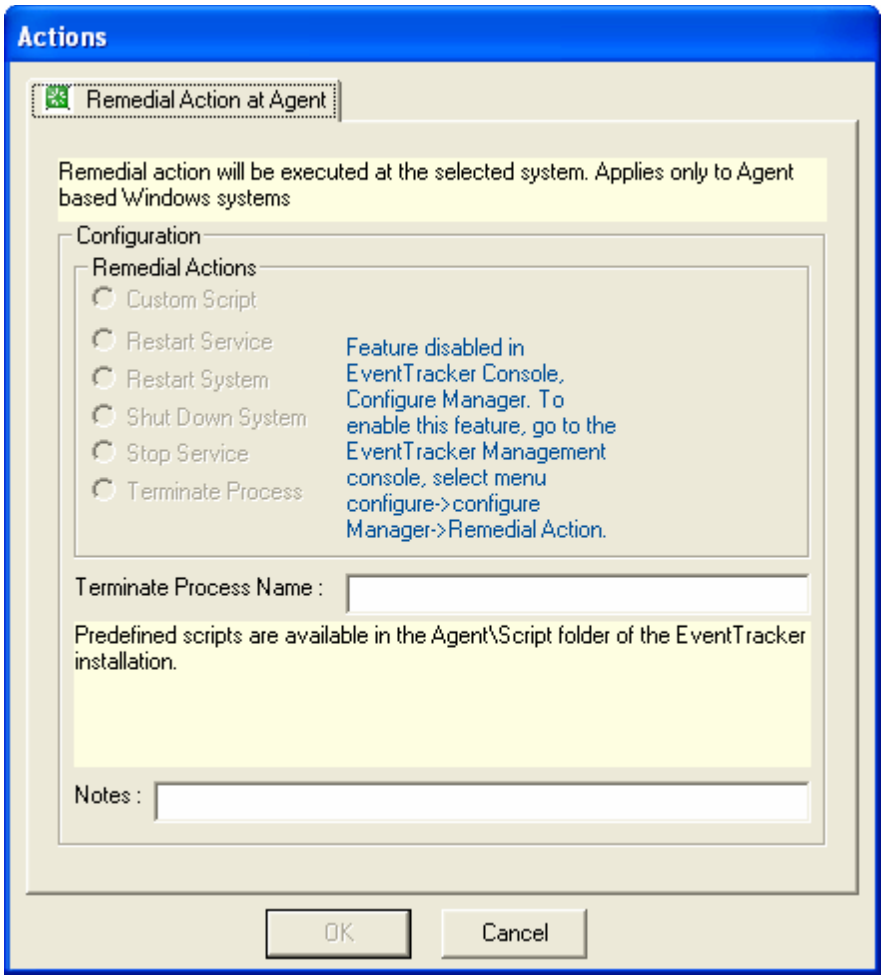

Figure 7

4. Select an appropriate option and then click **OK**.
5. Click **Save** on the toolbar.
6. Restart the Management Console.

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

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

User-defined Alerts

1. Double-click **Alert Configuration** on the Control Panel.

   EventTracker displays the Alert Groups console.

2. Click **New** on the toolbar.

   EventTracker displays Alert Group Configuration window.

3. Enter / select appropriately in the **Alert Name**, **Event Details**, and **Event Filters** tabs.
4. Click the **Systems** tab.

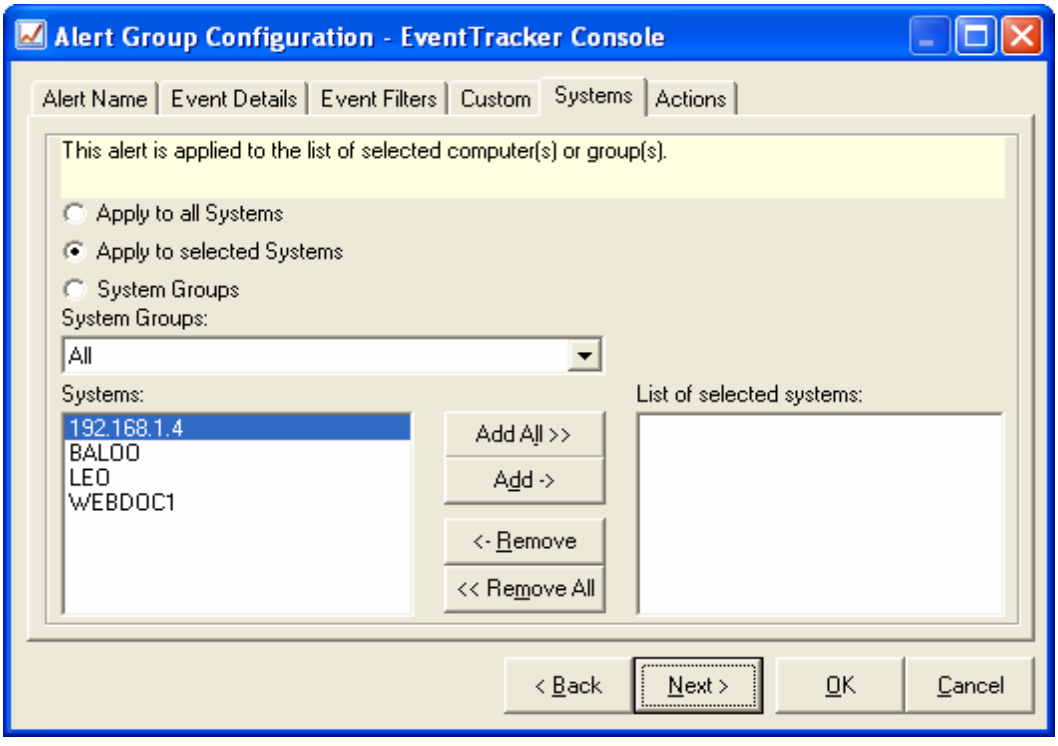

Figure 8

Field	Description
Apply to all Systems	Select this option to apply the Alert to all computers irrespective of System Groups. If you select this option, EventTracker will disable **System Groups** drop-down box, **Systems** list box, and **List of selected systems** list box.
Apply to selected Systems	Select this option to apply the Alert to the selected systems. By default, EventTracker selects the **All** option in the **System Groups** drop-down box and displays all systems where EventTracker Agent has been deployed in the **Systems** list box. Select a group from the System Groups drop-down box to view monitored systems in that group.
System Groups	Select this option, if you want to apply the Alert to all monitored systems in a group. When you select this option, EventTracker disables the **System Groups** drop-down box. EventTracker displays all discovered enterprise system groups in the **Group(s)** list box. Select the groups and click the arrow buttons to add the selected groups to the **List of selected groups** list box.
System Groups	EventTracker enables this drop-down box only when you select the **Apply to selected systems** option. Select a group of systems for which you want to apply the Alert from the drop-down box. Select the systems and click the arrow buttons to add the selected systems to the **List of selected systems** list box.

5. Select and add the systems to the List of selected systems.
6. Click **Next >**.

   EventTracker displays the Actions tab.

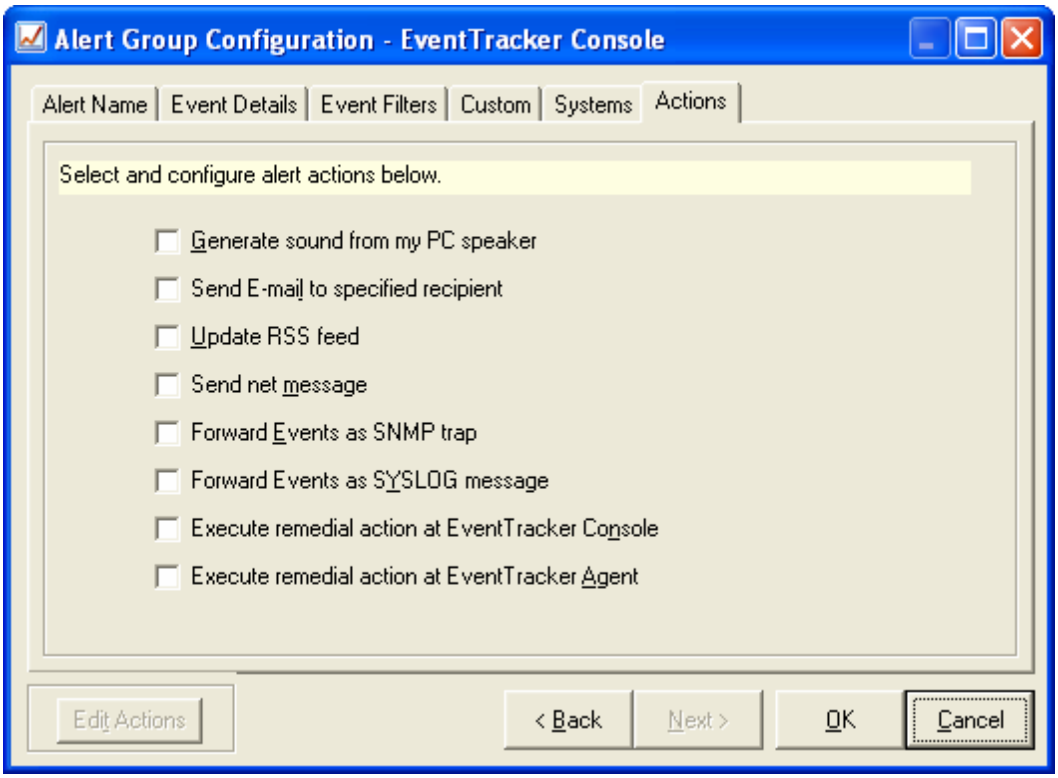

Figure 9

7. Select the **Execute remedial action at EventTracker Agent** check box.

   EventTracker displays the Remedial Action at Agent window.

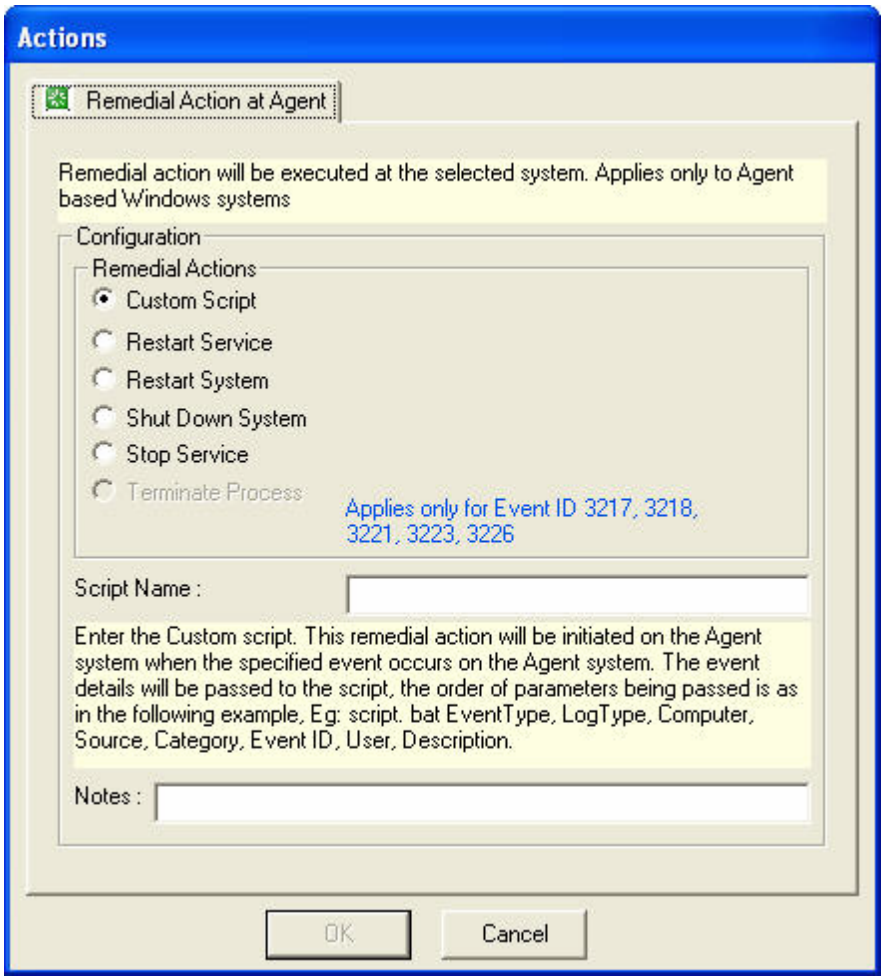

Figure 10

8. Select an appropriate option and then click **OK**.
9. Click **OK** on the Alert Group Configuration window.

   EventTracker displays the Alert Groups console with newly added Alert.
10. Click **Save** on the toolbar.

Execute Remedial Actions at Console

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

1. Double-click **Alert Configuration** on the Control Panel.

   (OR)

   Click the **Configure** menu and then select the **Configure Alerts** option.

   EventTracker displays the Alert Groups console.

2. Select an Alert, select the option against the selected Alert under **Console side remedial action**.
   EventTracker displays the Remedial Action at Console window.

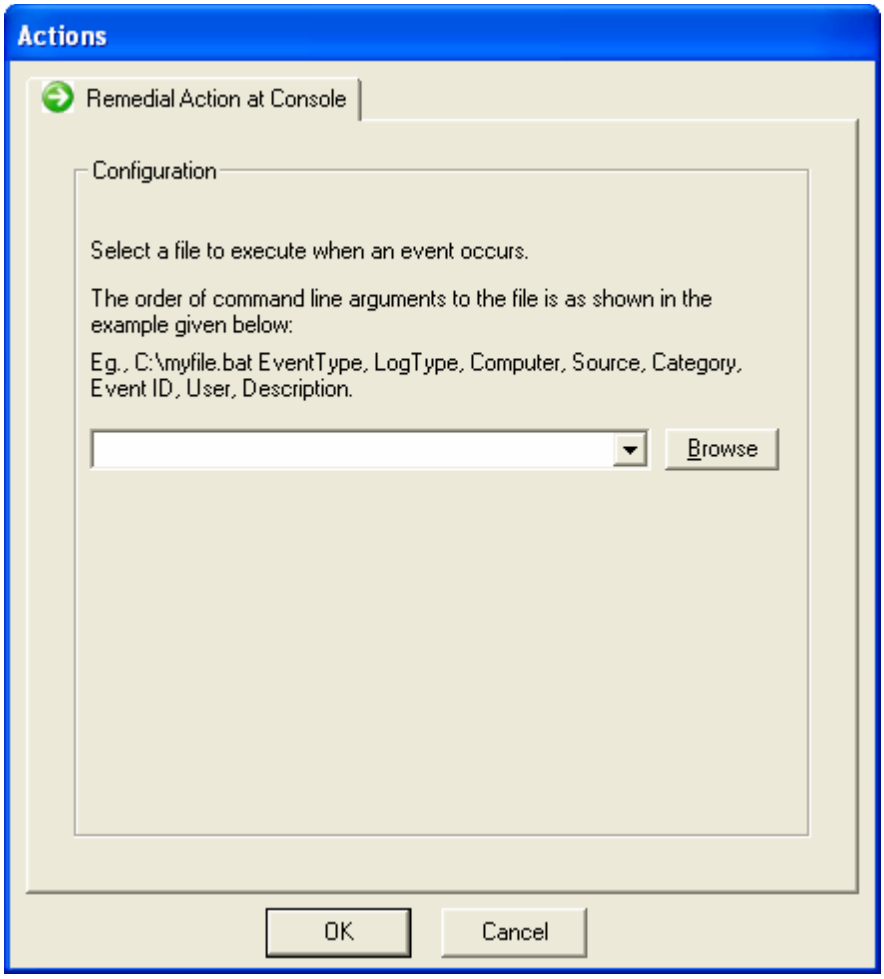

Figure 11

You can also access the Remedial Action at Console dialog box by selecting the corresponding check box under Remedial Action at Console on the Alerts Group dialog box.

3. Click **Browse**, navigate and select the appropriate file to execute when an event occurs.
4. Click **OK**.

   EventTracker displays the Remedial Action at Console window.

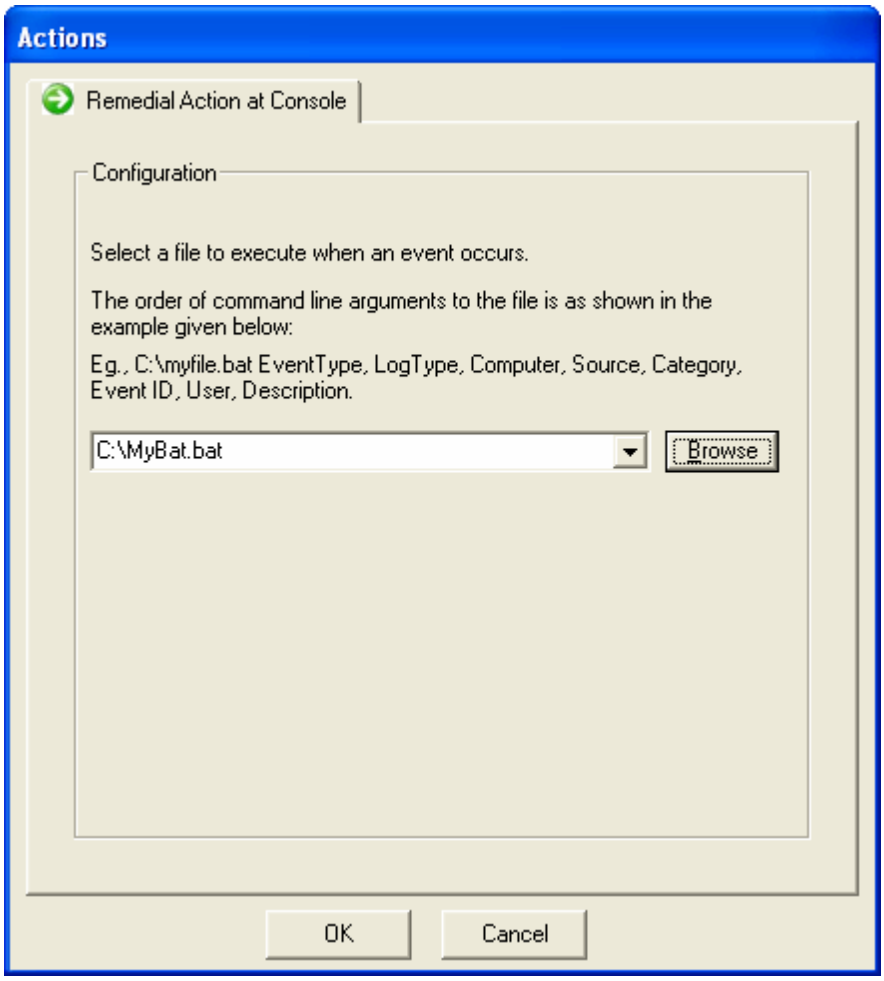

Figure 12

5. Click **OK**, and then click **Save** on the toolbar.
6. Restart the Management Console.