ABSTRACT

The purpose of this document is to describe the configuration and usage of Alerts in EventTracker for Windows.
# Table of Contents

Alerts ............................................................................................................................................................ 3  
Alert Groups ............................................................................................................................................. 3  
Modes of notification .............................................................................................................................. 3  
  Monitor Critical Systems or Applications .......................................................................................... 4  
  Reduce the problem caused by geographical distance from your critical systems ...................... 4  
  Automatically start off a contingency process ................................................................................. 4  
Create Alert Groups ..................................................................................................................................... 5  
  Manage Categories ............................................................................................................................... 18  
Add Categories as Alerts .......................................................................................................................... 28  
  Generate Alert Notification Report ...................................................................................................... 28
Alerts

Alerts are a spontaneous notification mechanism implemented in EventTracker to notify the user about the arrival of an event. Say for instance, you are monitoring all events occurring in your enterprise sitting at your work desk through the Management Console, but particularly interested in an error event. In this scenario, manually scanning through zillions of events becomes laborious and next to impossible to be precise.

- What happens when you move out of the desk?
- Who will intimate you that such an event has occurred?
- How will you remedy the issues without even knowing what has happened?

EventTracker Alert mechanism comes to your rescue to pinpoint the issues with scholarly exactitude and keep abreast of the events in absentia. Summarily, Alert mechanism is a watchdog that alleviates the workload of IT personnel to a greater extent.

Alert Groups

Alert Groups are nothing but grouping together of similar events. For example, Administrative log-on Alert Group has events that fall under SECURITY Log Type. Putting together of similar events under one easily identifiable entity helps you to track, modify or delete those events.

Alert Groups are so flexible and scalable like a collapsible canopy wherein you can add, delete or modify event details. EventTracker is shipped with predefined Alert Groups, which are highly configurable according to your needs. You can also define your own Alert Groups as the situations demand.

Modes of notification

This is age of communication and the information fly before anyone could say ‘Jack Robinson’. There is no second chance when it comes to security. EventTracker has implemented a gamut of notification modes from primitive beep sound, console message to sophisticated e-mail and RSS Feeds.

RSS Feeds is a unique feature, whereby you can configure them in EventTracker and get notified via RSS about the count of Alerts raised by EventTracker. To avail this feature you need to have EventLogCentral installed in your enterprise.
You can also link the RSS Feeds with the reports you configure in EventLogCentral. So whenever EventLogCentral generates a report, you will be intimated instantaneously.

You can also forward events as SNMP traps to any SNMP manager such as Tivoli Netview, HP Openview, Unicenter, etc... or automate to run self-healing batch files and applications.

Some real life examples where alerts will help you solve issues.

Monitor Critical Systems or Applications

You have a Window 2000 Advanced Server that is hosting your Oracle database that is the backend for your e-commerce business. You will certainly be interested in knowing every ERROR event that is being logged by this system. This is an ideal situation to configure an EventTracker Alert.

Reduce the problem caused by geographical distance from your critical systems

You work on a system that is on a different floor (or different building/location) and your critical servers are located on another floor (or different building/location). But you have to be up to date on the status of each critical servers and have the responsibility of ensuring 100% uptime. Using EventTracker Alerts you will be able to work on your system and leave EventTracker Alerts to inform you of any critical happening on any important system.

Automatically start off a contingency process

In case your critical application has a problem during your non-working hours you would like to automatically kick-start a contingency plan or initiate a process that will page or fax you. You could configure an EventTracker Alert to automatically execute a custom application.
Create Alert Groups

This section guides you to create a new Alert Group.

1. Open the Management Console.

2. Click the **Configure** menu, and select **Configure Alerts** option.

   EventTracker displays the Alert Groups console.

3. Click **New** on the toolbar.

   EventTracker displays the Alert Group configuration window.

---

**Figure 1: Alert Groups**
4. Type an appropriate name for the new Alert Group in the **Enter Alert Name** field.
   Example: My Alert Group.

5. Click **Next** or click the **Event Details** tab.

   EventTracker displays the Event Details tab. In this tab you can add Event details that you want to add in the newly created Alert Group.
6. Click **Add Event**.

   EventTracker displays Event Configuration window.
Figure 4: Event Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td>Select an event type from the drop-down box.</td>
</tr>
<tr>
<td>Log Type</td>
<td>Select a log type from the drop-down box.</td>
</tr>
<tr>
<td>Match in Source</td>
<td>Type the source in this field.</td>
</tr>
<tr>
<td>Category</td>
<td>Type the Category number in this field.</td>
</tr>
<tr>
<td></td>
<td>This field supports numeric data type only.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Type the Event ID in this field.</td>
</tr>
<tr>
<td></td>
<td>This field supports numeric data type only.</td>
</tr>
<tr>
<td>Match in User</td>
<td>Type the user name in this field.</td>
</tr>
<tr>
<td>Match in Event Descr</td>
<td>Type a sub-string of the description that needs to be matched.</td>
</tr>
</tbody>
</table>

"Match in Event Descr" field can take multiple strings separated with && or ||.
- && stands for AND condition. - || stands for OR condition.
Note: If you want to make a match on any of the special characters, like "", """, "$", etc..., then in the search string prefix this char with a backslash. Example: "\\" for a "" and "\\" for a "$".

For more information click here.
EventTracker supports multiple strings separated by the following operands:

**&&** stands for **AND** condition.

**II** stands for **OR** condition.

If you type Successful Logon **&&** New Trusted Domain **II** Removing Trusted Domain, EventTracker will filter out the events that are matching Successful Logon, (AND) New Trusted Domain (OR) Removing Trusted Domain.

| Event Descr Exception | Type a sub-string of the description that needs to be matched. EventTracker checks for event description for match and ignores that event.
Example: Match in Event Descr: EventTracker, Event Desc Exception: ET. EventTracker first checks event description for Event Desc Exception string. If it matches, then EventTracker will ignore the event. |

EventTracker assumes a wildcard match if you leave a field blank. For example, leaving the **Match in User** field blank implies that any value in that field is acceptable.

7. Enter/select appropriate details in the relevant fields.
   Example: Event Type: Error.

8. Click **OK**.
   EventTracker displays the Event Details tab with newly added Event details.
9. Click **Next** or click the **Event Filters** tab.

EventTracker displays the Event Filters tab. Although, you have configured events of Event Type: Error, you can exclude events of minor significance from the Alert Group.
10. Click **Add Event**.

   EventTracker displays the Event Configuration window.
11. Enter/select appropriate details in the relevant fields.

Example: Event Type: Error, Event ID: 45.

12. Click OK.

EventTracker displays the Event Filters tab with newly added event exception.
13. Click **Next** or click the **Custom** tab.

EventTracker displays the Custom tab.

---

**EventTracker**


13
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply at all times</td>
<td>EventTracker selects this option by default. You will get the Alert notification any time in a day when the specified events occur.</td>
</tr>
<tr>
<td>Apply between these times</td>
<td>Select this option when you want to get the Alert notification at a particular time in a day. Set From and To time from the spin boxes. You will be notified when the events occur within this time frame.</td>
</tr>
<tr>
<td>Alert based on Count</td>
<td>This option lets you to raise Alert only if the same event occurs for a specified number of times within the specified duration. EventTracker disables Raise alert for event count and Duration fields by default. To enable, select the Enable check box. The default value for Raise Alert for event count is 2 and Duration is 3600 secs.</td>
</tr>
<tr>
<td>Archive Alert</td>
<td>Store this alert in Alert Archives check box is selected by default. Clear this check box if you wish not to store the Alert in the Alert Archives</td>
</tr>
</tbody>
</table>

14. Enter/select appropriate details in the relevant fields.

15. Click Next> or click the Systems tab.

EventTracker displays the Systems tab.
EventTracker: Configure Alerts

Figure 10: Alert Group Configuration - Systems

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply to all Systems</td>
<td>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.</td>
</tr>
<tr>
<td>Apply to selected Systems</td>
<td>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.</td>
</tr>
<tr>
<td>System Groups</td>
<td>Select this option, if you want to apply the Alert to all monitored systems in a group. When you select this option, EventTracker...</td>
</tr>
</tbody>
</table>
EventTracker: Configure Alerts

<table>
<thead>
<tr>
<th><strong>System Groups</strong></th>
<th><strong>Behaviors</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>EventTracker enables this drop-down box only when you select the Apply to selected systems option.</td>
</tr>
<tr>
<td></td>
<td>Select a group of systems for which you want to apply the Alert from the drop-down box.</td>
</tr>
<tr>
<td></td>
<td>Select the systems and click the arrow buttons to add the selected systems to the List of selected systems list box.</td>
</tr>
</tbody>
</table>

16. Select the systems.

17. Click **Next** or click the **Actions** tab.

EventTracker displays the Actions tab.

![Alert Group Configuration - EventTracker Console](image)

**Figure 11: Alert Group Configuration – Actions**
### EventTracker: Configure Alerts

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate sound from my PC speaker</td>
<td>Select this option to configure audible Alert notification.</td>
</tr>
<tr>
<td>Send E-mail to specified recipient</td>
<td>Select this option to configure E-mail Alert notification.</td>
</tr>
<tr>
<td>Update RSS feed</td>
<td>Send Alerts via RSS Feeds.</td>
</tr>
<tr>
<td>Send net message</td>
<td>Select this option to configure console message notification.</td>
</tr>
<tr>
<td>Forward Events as SNMP trap</td>
<td>Select this option to forward events as SNMP traps to the specified location.</td>
</tr>
<tr>
<td>Forward Events as SYSLOG message</td>
<td>Select this option to forward events as SYSLOG messages to the specified location.</td>
</tr>
<tr>
<td>Execute remedial action at EventTracker Console</td>
<td>Select this option to execute scripts at the Manager console system.</td>
</tr>
<tr>
<td>Execute remedial action at EventTracker Agent</td>
<td>Select this option to execute remedial action at the system where EventTracker Windows Agent has been deployed.</td>
</tr>
</tbody>
</table>

You can set actions now or later.

18. Click **OK**.

   EventTracker displays EventTracker Console message box, had you not set any actions.

![EventTracker Console](image)

Figure 12

19. Click **Yes**.

   EventTracker displays the Alerts Group console with the newly added Alert group.
18

20. Click **Save** on the toolbar.


### Manage Categories

1. Click the **Configure** menu and select the **Manage Categories** option.

   (OR)

   In the Management Console, right-click any Alerts Group by expanding the All Categories hive.

   EventTracker displays the shortcut menu.

   From the shortcut menu, choose **Manage Categories**.
EventTracker: Configure Alerts

EventTracker displays the Manage Categories console.

Expand the **All Categories** hive.

Expand the **Alerts** group.

Click the **Alerts** Category.

**(OR)**

Right-click **Correlated Alerts & Incidents** Category.

EventTracker displays the shortcut menu.

From the shortcut menu, choose **Manage Categories**.

EventTracker displays the Manage Categories console.

Expand the **All Categories** hive.

Expand the **Alerts** group.

Click the **Alerts** Category.

![Figure 14: Manage Categories - Alerts](image-url)
2. Scroll the right pane.

EventTracker displays the events configured for the new Alert (My Alert Group).

You can edit and delete the new event details in ***Alerts*** Category. These manipulations would not affect the event details of the new Alert that is My Alert in the Alert Groups console.

3. Select the event.

4. Click **Edit Event**.

   (OR)

   Double-click the Event.

   EventTracker displays the Edit Event Detail window.
5. Enter appropriate details in the relevant fields.
   Example: Log Type: Application.

6. Click OK.

EventTracker displays the Confirmation message box.
7. Click **Yes** to save the changes.

   EventTracker displays the Manage Categories console with new settings.

![Manage Categories Console](image)

8. Click **OK**.

9. Open the Alert Groups console.

10. Double-click **My Alert Group**.

   EventTracker displays the Event Details tab with event details unaltered.
When you edit the event details of My Alert in Alert Group Configuration window, it will be reflected in ***Alerts*** Category in the Manage Categories console.

11. Double-click the event or click Edit Event.

EventTracker displays the Event Configuration window.
12. Enter/select appropriate details in the relevant fields.
13. Click **OK**.

EventTracker displays the Alert Group Configuration window with the modified event details.
14. Click **Finish**.

15. Click **Save** on the toolbar.

16. Open the Manage Categories console.

   EventTracker displays the modified event details of My Alert Group.
The advantages of adding new Alert Group’s event details along with the event details of pre-defined ***Alerts*** Category are as follows:

- Apart from alert notifications, reports can be generated for the new Alerts along with the pre-defined ***Alerts*** Category.
- Event analysis can be done for the newly added Alerts.
- Event severity for the new Alerts can be viewed in the Navigation pane etc.,
Add Categories as Alerts

1. Open the EventTracker Management Console.
2. Right-click the Category that you want to configure as Alert.
   EventTracker displays the shortcut menu.
   From the shortcut menu, choose Add As Alert...
   (OR)
   Open the Manage Categories console.
   Right-click the Category that you want to configure as Alert.
   EventTracker displays the shortcut menu.
   From the shortcut menu, choose Add As Alert...
   EventTracker displays the Alert Group Configuration window.
3. Under each tab, enter appropriate details in the relevant fields and then click OK.
4. Click OK on the Manage Categories console.
5. Open the EventTracker Management Console.
6. Click the Configure menu and select the Configure Alerts option.
   EventTracker displays the Alert Groups console.

Generate Alert Notification Report

Alerts Notification report helps you to identify success and failure status of configured Alert Actions for both predefined and user-defined Alerts Groups.

1. Open the Reports Console.
2. Click the Advanced tab, click the Operations tab.
3. Expand the Alerts node, double-click Alert Notification.
   Reports Console displays the Reports Wizard.
4. Click **Next>>**.

5. Select Alert(s) from the Available Alerts list.
   Example: My Alert Group.

6. Click **Add >>** to add the selected Alerts to the **Selected Alerts** list.

7. Select the **Actions type(s)**.

8. Select the report generation **Interval**.

9. Select the **Export Type**.

10. Type the **Report Information** in the appropriate fields.

11. Click **Generate**.

---

**Figure 24: Quick View**

---

**Summary Report:**

<table>
<thead>
<tr>
<th>Computer:</th>
<th>Beep</th>
<th>Email</th>
<th>Message</th>
<th>Forward</th>
<th>Remedial[Msg]</th>
<th>Remedial[Aqt]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>My Alert Group</td>
<td>1022</td>
<td>0</td>
<td>148</td>
<td>955</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

---

**Figure 25: Summary Report**
## Detail Report

**Computer:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event Id</th>
<th>Beep</th>
<th>Email</th>
<th>Message</th>
<th>Forward</th>
<th>Remedial [Nur]</th>
<th>Remedial [Aqt]</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
<tr>
<td>2/27/2009 4:21:00PM</td>
<td>45</td>
<td>Action Not Configured</td>
<td>Successfully sent email to <a href="mailto:nirmal@prismmicrosys.com">nirmal@prismmicrosys.com</a></td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
<td>Action Not Configured</td>
</tr>
</tbody>
</table>

Figure 26: Detail Report
**Disclaimer**

Use of this document is subject to the End User License Agreement (EULA) distributed with this Program. A copy of this EULA is available in the directory where the program is installed.