Introduction to Categories

EventTracker v6.x
ABSTRACT

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

Introduction to Categories.......................................................................................................................... 3
  How can I use Categories to my advantage?........................................................................................ 3
  Are there any predefined Categories?................................................................................................... 3
  What are the steps involved in creating Categories?........................................................................... 3
  What are the Category related operations available?.......................................................................... 4
Create Category ........................................................................................................................................... 5
Add, Edit, or Remove Events from a Category ........................................................................................ 10
  Add Events to a Category ..................................................................................................................... 10
  Edit Events that belong to a Category ................................................................................................. 12
  Remove Events from a Category ......................................................................................................... 14
Edit a Category ...................................................................................................................................... 15
Delete a Category ................................................................................................................................... 17
Export Categories .................................................................................................................................. 18
Import Categories ...................................................................................................................................... 22
  How to Use Categories........................................................................................................................ 23
Event Categories ....................................................................................................................................... 25
Reports Console ........................................................................................................................................ 27
Appendix .................................................................................................................................................... 38
  Disclaimer .............................................................................................................................................. 38
Introduction to Categories

EventTracker for Windows has an exciting feature called Categories. This feature facilitates you to group related events together under one Category and monitor them collectively as a Category. Categories help you to view event data from a very high level and get instant answers to application/system problems merely by looking at the status of a Category.

How can I use Categories to my advantage?

Windows as well as all applications that run on Windows, log events into the Windows event log. By analyzing the event log at run time, various system/application malfunctions can be identified and resolved. Many a time, it is useful to group related events and analyze them together.

Categories are provided by EventTracker to enable grouping of related events, with each event being assigned a severity. Whenever an event occurs, if it belongs to a Category, then the status of the Category changes based on the event severity. The severity of a Category depends on the severity of the events that occur. You can select these Categories in the EventTracker Reports console to generate Advanced Reports.

When looking at event activity through Categories, it is easy to identify and fix application/system problems, rather than to run through the entire list of events.

Are there any predefined Categories?

EventTracker for Windows provides a set of predefined Categories that is part of its Knowledge Base. Apart from this, EventTracker supports user-defined Categories. You can create ‘n’ number of Categories. Prism Microsystems, Inc keeps adding to the set of predefined Categories.

What are the steps involved in creating Categories?

Category creation is intended to make sense out of event logs. Given below is a process suggested to create Categories:
1. Identify all the events that form the basis of the Category you want to create. Consider a Category that will identify if there is any critical event generated by the Web Server. To create such a Category, you will first have to identify all the critical events that could be generated by the Web Server.

2. Once the events have been identified, open the Manage Categories console and create the Category.

3. Add the details of the identified event details into the Category. Select a Severity for each event. The severity assigned to an event will help the Management console to visually indicate the severity of events in a Category.

4. Click ‘Add’ after providing event details to move onto the next event detail.

5. Click Finish after entering details of all the identified events.

What are the Category related operations available?

The available operations are

- Create Category.
- Add, edit or remove events from a Category.
- Edit Category.
- Delete Category.
- Export Category.
- Import Category.

The detailed description of each of the above operations is described in the following sections.
Create Category

You can create Categories through the Manage Categories console. The Manage Categories console provides options to Create Category, Edit Category, Delete Category and Add, Edit or Remove Events from a Category.

1. From the EventTracker Management Console menu bar, select the ‘Reports’ menu and then click the ‘Manage Categories’ option. Refer Figure 1.

   EventTracker displays the Manage Categories console.

2. Click ‘Create Cat…’. Refer Figure 2.
EventTracker displays the ’Create Event Category Wizard’.

3. Enter valid **Event Category Name** and **Description** and then click ’Next’.

Refer Figure 3.
EventTracker displays the confirmation message box as shown in Figure 4.

4. Click ‘Yes’ to continue.

EventTracker displays ‘Event Details’ window.
5. Choose the ‘Severity’ of the item.

6. Enter appropriate Event Details such as Event Type, Category, Log Type, Event ID, Source, User, Match in Event Descr and Event Descr Exception.

7. Enter any additional information or comments that is available about the event in the More Information field.

8. Click the ‘Add’ button to add the item into the Category.

Refer Figure 5.
EventTracker adds the new Category.

Refer Figure 6.

![Figure 6: Manage Categories – New Category]
Add, Edit, or Remove Events from a Category

Add Events to a Category

Open the Manage Categories console and select the Category to which you want to add more events.

1. Click the ‘Add Events’ button.
   Refer Figure 7.

   ![Add Events](image)
   
   EventTracker displays the ‘Add Event Details’ dialog box.

2. Select the ‘Severity’ of the event.

3. Enter appropriate details in the relevant fields.
4. Click the ‘Add’ button to add the event details into the selected Category. Refer Figure 8.
Edit Events that belong to a Category

To edit the properties of an event, bring up the Manage Categories screen, follow the steps as mentioned below.

1. Select the Category on the left pane and select the Event that you want to edit on the right pane.

2. Click ‘Edit Event’ button.

Refer Figure 9.

EventTracker displays the ‘Edit Event Detail’ dialog box.

3. Modify the Event Details and then click ‘OK’ to save or ‘Cancel’ to ignore the changes.

Refer Figure 10.
Remove Events from a Category

1. To remove an event from a category, open the Manage Categories console.
2. Select the Category on the left pane.
3. Select the Event Detail that you want to delete on the right pane.
4. Click the ‘Remove Events’ button.
   EventTracker displays the Confirmation message box.
   Refer Figure 11.
5. Click ‘Yes’ to delete or ‘No’ to cancel.
Edit a Category

To edit a Category, open the Manage Categories console and do the following procedures in the same sequence.

1. Select the Category; click the ‘Edit cat...’ button.

Refer Figure 12.

EventTracker displays the Edit Event category window.

2. Edit the Event Category ‘Description’, and then click ‘OK’ to save or ‘Cancel’ to discard the changes.

Refer Figure 13.
Figure 13: Edit Event Category

This Category reflects important events that need immediate attention.
Delete a Category

1. To delete a Category, open the Manage Categories console.
2. Select the Category that you want to delete on the left pane.
3. Click the ‘Delete Cat...’ button.
   
   EventTracker displays the Confirmation message box.
4. Click ‘YES’ to delete or ‘NO’ to cancel.
   
   Refer Figure 14.

![Delete Category - Confirmation](image-url)
Export Categories

1. To export a Category to a file, open the Management Console, click the **Tools** menu and select the **Import and Export** option.

Refer Figure 15.

**NOTE:**

The file extension for Category files is .iscat.

Figure 15

EventTracker displays Export Import Utility.

Refer Figure 16.
2. Select the Categories that you want to export.

3. Click Add to add the selected Categories to the Selected list.

Refer Figure 17.
4. Click the 'Export' button.

EventTracker displays the Select Export File window. Refer Figure 18.
EventTracker: Introduction to Categories

EventTracker displays the Export Import Utility message box. Refer Figure 19.

Figure 18: Export Categories Screen

1. Select the directory where you want to save
2. Enter the file name.
3. Click Save

Figure 19
Import Categories

1. To Import a Category from a file, open the **Export Import Utility** and then click the **Import** tab.

2. Click ![browse_icon] to browse the source folder, where the iscat file resides.

   EventTracker displays the Select *iscat File window and displays all existing Category files that exist in the default EventTracker installation directory.

3. Select the Category file that you want to import and the click the **Open** button.

   Refer Figure 20.

4. Click the **Import** button on the Export Import Utility console.

   EventTracker displays the Export Import Utility message box indicating that the selected Category is imported successfully as shown in Figure 21.
How to Use Categories

Categories is a feature available in EventTracker for Windows whereby a set of related events are grouped together into a Category and whenever an event that belongs to a Category occurs, the Management Console will highlight that particular Category in appropriate event severity color indicator.

This feature enables easy identification of critical events that could have been generated by an application/system and belongs to a specific Category.

The steps involved in using categories are:

- Create a Category
- Add the events to the Category
- Define the Event Severity for each event added
- Monitor the status of the Category from the Management Console.

Example:

Take the case of a Category that monitors all critical events generated from a system that hosts a Web Server. This Category will contain all the important events that could be generated by the Web server. Each event will have its own severity. When the user monitors the status of this Category using the Management Console, the Category will be highlighted with the color code of the event with maximum severity that has been generated by the Web server.
If the Category contains 2 events,

- First event with Event ID = 1, Event Source = Web Server, Severity = Major
- Second event with Event ID = 2, Event Source = Web Server, Severity = Critical

If the Web Server generates an event that has Event ID = 1 then the Management Console will indicate the presence of a Major Severity event.

If the Web Server generates an event of Event ID = 1 and another event of Event ID =2, then the Management Console will indicate the presence of a Critical Severity event.

If either of these two events were not generated then the Management Console would make no indication for this Category.

NOTE:

The Event ID's and Event Source mentioned in this example are hypothetical. This example is used only to give clarity the priority levels of Event severity.
Event Categories

Event Categories are a powerful concept wherein you can group a set of events into a Category and use the Category for other operations such as for current and historical views.

EventTracker comes with a preconfigured set of Categories and this can be seen by selecting Reports > Manage Categories from the Management Console.

![Image of Manage Categories interface](image)

The left side pane shows the list of available Categories and the right pane shows the event combinations that make up a specific Category. For example, in the screen above, the Category ‘My Category’ consists of one event of Event Type Warning with its own severity.

An event combination consists of the following fields:

- **Event Type**, which is one of Success, Error, Warning, Information, Audit Success, Audit Failure.

- **Log Type**, which is one of System, Security, Application, and DNS Server, File replication Service or Directory Service.
The event Source.

Category number of the event.

The Event Id.

Severity of the event.

The user, depending on the relevance of the event to the operations, configures the severity. There are 5 levels of severity Clear, Minor, Information, Major, Warning and Critical in ascending level precedence. EventTracker displays the Computer Groups, Computers, Category Groups and Categories on the Navigation pane that are with Clear, Minor or Information events in green indicating low priority, Major events in blue, Warning events in orange, Critical events in red and with no events in yellow.
Reports Console

EventTracker for Windows has a major component called the Advanced Report console. The Advanced Report console presents a very simplified picture of all the event activity in your enterprise or any specific system. Using a combination of predefined Categories and user-defined Categories the Advanced Report console provides quick insight about the event activity that has occurred between any time frames.

User-defined Categories can be created and will appear in the Advanced Report console. Using a combination of Alerts, Categories and the Advanced Report console, you can easily isolate and resolve application/system problems based on the event information available. Advanced Report console works in a simple explorer style user interface that requires a zero learning curve.

The Categories Selection tab expands to show all the available Categories, both predefined and user-defined. Event activity is depicted Category wise enabling the user to understand the exact impact of the any of the event in a Category on a specific application or system. This view can be used to identify, analyze and resolve application/system malfunctioning.

The System Groups tab expands to show the Computer groups and their associated computers whilst highlighting the Categories with events of higher severity. This view enables better understanding of the health of a system/application and enables quick isolation and resolution of problems that caused the system/application to behave abnormally.

More customization is possible if more Event Categories are formed. With more Categories, you can easily use separate reports and distribute it to separate personnel such as to the ‘Exchange Admin’, ‘Security-in-Charge’ etc.

To generate an Advanced Report do the following procedures.

1. Open the Advanced Report console.
EventTracker displays the Advanced Reports console. Refer Figure 24.
2. Select a report type (ex: Summary Report) and then click Start Wizard.

EventTracker displays the New Report Wizard. Refer Figure 25.
3. Click **Next>>** and select a chapter.

Refer Figure 26.
4. Select the Category and then click 'Add' button to add it to the 'List of selected Categories'.

5. Click the 'Next' button.

Refer Figure 27.
6. Select the ‘Computers’ for which the report is needed.

   Refer Figure 28.
7. Click the ‘Add’ button and add to the ‘List of selected Computer(s)’.

8. Click the ‘Next’ button.

9. Select the report generation interval.

Refer Figure 29.
10. Click **Generate Report**.

EventTracker displays the Resource Estimation message box as shown in the following Figure 30.

11. Click **Yes**.

EventTracker generates and displays the Summary Report. Refer Figure 31.
Summary Report (WEBDOC1 (Collection Point Master))

Summary Report By Computer

This report gives you information on the selected Categories sorted by Computers in your enterprise. The report can be used to track system activity in relation to a Category thereby giving you an insight into the security and other implications.

Extended Summary Report sorted by Computer

From: 08-Feb-2007 2:49:59 pm  
To: 09-Feb-2007 2:49:59 pm

Categories Selected: ***ALERTS***

Computers Selected: MICKEY, WEBDOC1

Total Computers analyzed: 2
Total Events found: 94
Total Event IDs found: 9

Top 2 Computers with Top 10 Event IDs

Computer: MICKEY  Total Events: 68

Computer: WEBDOC1  Total Events: 26
### Summary Report (WEBDOC1 (Collection Point Master))

<table>
<thead>
<tr>
<th>Computer Name:</th>
<th>MICKEY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Events:</td>
<td>68</td>
</tr>
<tr>
<td>Total Event IDs:</td>
<td>8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Count</th>
<th>Sample Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3207</td>
<td>21</td>
<td>Detected High CPU Usage. More than 80 percent in use for last 180 seconds. CPU Usage: 93 percent</td>
</tr>
<tr>
<td>3202</td>
<td>10</td>
<td>Detected Service &lt;WinHTTP Web Proxy Auto-Discovery Services&gt; is not running. Name: WinHTTP Web Proxy Auto-Discovery Service Type: Service</td>
</tr>
<tr>
<td>3201</td>
<td>3</td>
<td>Detected free space in drive C is less than 20 percent. Drive: C Disk Size: 20000 MB Free: 1456 MB Free (in percent): 7 percent</td>
</tr>
<tr>
<td>2008</td>
<td>1</td>
<td>Detected system PNPL-123-NOV is not reachable. No reply received on ping poll.</td>
</tr>
<tr>
<td>3204</td>
<td>1</td>
<td>Detected Service &lt;Event Archiver&gt; could not be restarted. Name: Event Archiver Type: Service</td>
</tr>
<tr>
<td>3218</td>
<td>1</td>
<td>Process &lt;vbs.exe&gt; has crossed the CPU usage limit. Process: vbs.exe Limit: 30 % Actual: 92 %</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computer Name:</th>
<th>WEBDOC1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Events:</td>
<td>26</td>
</tr>
<tr>
<td>Total Event IDs:</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Count</th>
<th>Sample Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3218</td>
<td>2</td>
<td>Process &lt;WINWORD.EXE&gt; has crossed the CPU usage limit. Process: WINWORD.EXE Limit: 30 % Actual: 96 %</td>
</tr>
</tbody>
</table>

**Figure 32**
### Quick View

Summary of all computers analyzed.

| Event ID | Count | Sample Event Description*
|----------|-------|-----------------------------
| 3208     | 1     | Detected software <Event Correlator> has been installed on this system. Name: Event Correlator
| 3201     | 3     | Detected free space in drive C: is less than 20 percent. Drive: C:
|          |       | Disk Size: 20000 MB
|          |       | Free: 1456 MB
|          |       | Free(% in percent): 7 percent
| 3202     | 10    | Detected Service <WinHTTP Web Proxy Auto-Discovery Service> is not running. Name: WinHTTP Web Proxy Auto-Discovery Service Type: Service
| 3204     | 1     | Detected Service <Event Archiver> could not be restarted. Name: Event Archiver Type: Service
| 3206     | 17    | Detected High Memory Usage. More than 80 percent in use for last 180 seconds. Peak Memory: 83 percent Total Physical: 503 MB Total Paging: 1498 MB
|          |       | Available: 84 MB
|          |       | Available Paging: 1038 MB
| 3207     | 21    | Detected High Cpu Usage. More than 80 percent in use for last 180 seconds. CPU Usage: 99 percent
| 3208     | 1     | Detected software <Event Correlator> has been installed on this system. Name: Event Correlator
| 3218     | 3     | Process <WINWORD.EXE> has crossed the CPU usage limit. Process: WINWORD.EXE Limit: 96 % Actual: 96 %

* Description shown is an example of this type of event. Actual descriptions may vary. To see the exact description of each occurrence, run a Detailed 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.
Appendix

Disclaimer

Prism Microsystems, Inc. ("Prism") makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Prism reserves the right to revise this publication. No part of this publication may be reproduced, transmitted, transcribed and stored in a retrieval system without the prior written consent of Prism Microsystems Inc.

This document is for informational purposes only. Microsoft, Windows NT, Windows 2000 and Windows 2003 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Other product or company names mentioned herein might be trademarks of their respective owners.