The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2008 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

About this Guide .......................................................................................................................................... 4
   Who should read this guide ............................................................................................................. 4
   Typographical Conventions ............................................................................................................ 4
Document Revision Control.................................................................................................................... 5
How to Get In Touch ................................................................................................................................ 6
   Documentation Support .................................................................................................................. 6
   Customer Support .......................................................................................................................... 6
Chapter 1 Advanced Reports ...................................................................................................................... 7
   Trend Analysis ..................................................................................................................................... 8
   Configure Log Analysis - Trend - On Demand.................................................................................. 8
      STANDARD / CUSTOM COLUMN ANALYSIS .......................................................................... 8
   Configure Log Analysis - Trend - Queued ...................................................................................... 9
      STANDARD / CUSTOM COLUMN ANALYSIS .......................................................................... 9
   Configure Log Analysis - Trend - Scheduled ............................................................................... 11
      STANDARD / CUSTOM COLUMN ANALYSIS ...................................................................... 11
   Generate Default report in Case no Matching Records Found .................................................... 13
Chapter 2 Virtual Collection Points .......................................................................................................... 14
   Virtual Collection Points ................................................................................................................ 15
      Configure EventTracker Receiver to listen on multiple ports ................................................... 15
Example scenario ...................................................................................................................................... 16
   Computer: Sys1 – Configure Ports ................................................................................................ 16
   Upgrade Agent (Sys2) from Manager (Sys1) ................................................................................. 20
   Upgrade Agent (Sys3) from Manager (Sys1) ................................................................................. 20
   Virtual Collection Points for syslogs ............................................................................................. 21
      Configure the Syslog Service on a UNIX/Linux/Solaris Host ................................................... 23
Chapter 3 System Manager ...................................................................................................................... 24
   System Manager Console ............................................................................................................. 25
   Install Remedial Actions Script ................................................................................................... 25
   Install Agent with Different User Credentials ............................................................................. 26
About this Guide

This guide will help you to use every option of EventTracker and provides detailed procedures for the same.

Who should read this guide

Intended audience:

- Administrators who are assigned the task to monitor and manage events using EventTracker
- Operations personnel who manage day-to-day operations using EventTracker

Typographical Conventions

Before you start, it is important to understand the typographical conventions followed in this guide:

<table>
<thead>
<tr>
<th>This</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Input fields, radio button names, checkboxes, drop-down lists, menus, and menu options, buttons on the screen and keyboard keys.</td>
</tr>
<tr>
<td><code>{Text_to_customize}</code></td>
<td>A placeholder for something that you must customize. For example, <code>{Server_Name}</code> would be replaced with the name of your server/machine name or an IP address.</td>
</tr>
<tr>
<td>Constant width</td>
<td>Text that you enter, program code, files and directory names, function names.</td>
</tr>
<tr>
<td>📚</td>
<td>A Note, providing additional information about a certain topic.</td>
</tr>
</tbody>
</table>
Document Revision Control

This section defines the conventions followed for the document revision control number. The revision control number is an alphanumeric identifier, unique to the document. The components of the acronym identify the following:

- First word – name of the product
- Second word – version of the product
- Third word – document description

The document revision control number for this guide is as given below:

<table>
<thead>
<tr>
<th>Document Revision Control Number</th>
<th>Significance</th>
</tr>
</thead>
<tbody>
<tr>
<td>ET6.2USGD</td>
<td>ET – EventTracker™</td>
</tr>
<tr>
<td></td>
<td>6.2 – version number</td>
</tr>
<tr>
<td></td>
<td>USGD – Document description</td>
</tr>
</tbody>
</table>
How to Get In Touch

The following sections provide information on how to obtain support for the documentation and the software.

Documentation Support

Prism Microsystems, Inc. welcomes your comments and suggestions on the quality and usefulness of this document. For any questions, comments, or suggestions on the documentation, you can contact us by e-mail at support@eventtracker.com

Customer Support

If you have any problems, questions, comments, or suggestions regarding EventTracker, contact us by e-mail at support@eventtracker.com. While contacting customer support, have the following information ready:

- Your name, e-mail address, phone number, and fax number
- The type of hardware, including the server configuration and network hardware if available
- The version of EventTracker and the operating system
- The exact message that appeared when the problem occurred or any other error messages that appeared on your screen
- A description of how you tried to solve the problem
Chapter 1
Advanced Reports

In this chapter, you will learn how to:

- Configure Trend Analysis
- Set custom separator and terminator
Trend Analysis

**Trend:** This report provides trend charts for the selected event categories and systems for the selected period.

**Usage:** Trend reports are useful to obtain perspective on performance or occurrence of selected periods. They are useful to focus attention to specific areas of concern.

Configure Log Analysis - Trend - On Demand

STANDARD / CUSTOM COLUMN ANALYSIS

1. Click the Analysis tab.

2. Expand the Log Analysis group, select Trend.

3. Click New On Demand Analysis in the Actions pane.

   (OR)

   Expand the Logs node.

   Right-click Trend.

   Advanced Reporter displays the shortcut menu.

   From the shortcut menu, choose New On Demand Analysis.

4. Click Next >>.

5. Select the Analyze events based on Event categories / Custom Properties option.

6. Select the Category / Categories.

7. Select the System(s) / Group(s) / Site(s).

8. Select the analysis interval.

   **Select the interval for analysis:**

   Select this option, Advanced Reporter considers events occurred during the selected number of days for analysis.
Select this option and select **Limit to time range** option. Advanced Reporter enables the **From** and **To** spin boxes. Set the time range. Advanced Reporter considers only events occurred in that time range for analysis.

**Select custom date range:**

Select this option, Advanced Reporter considers events occurred during the selected number of days for analysis.

Select this option and select **Limit to time range** option. Advanced Reporter enables the **From** and **To** spin boxes. Set the time range. Advanced Reporter considers only events occurred in that time range for analysis.

Note that Advanced Reporter considers only the date range from the **From**, **To** drop-down lists and ignores the time range set in those drop-down lists.

9. Select the Export Type.

10. Type the Refine and Filter criteria.

11. Type the Title, Description, Header, and Footer.

12. Crosscheck the Analysis cost details.

13. Crosscheck the Analysis details.

14. Click **Generate**.

**Configure Log Analysis - Trend - Queued**

**STANDARD / CUSTOM COLUMN ANALYSIS**

1. Click the **Analysis** tab.

2. Expand the Log Analysis group, select **Trend**.

3. Click **New On Demand Analysis** in the Actions pane.

4. Click Next >>.

5. Select the **Analyze events based on Event categories / Custom Properties** option.

6. Select the Category / Categories.

7. Select the System(s) / Group(s) / Site(s).
8. Select the analysis interval.

**Select the interval for analysis:**

Select this option, Advanced Reporter considers events occurred during the selected number of days for analysis.

Select this option and select **Limit to time range** option. Advanced Reporter enables the From and To spin boxes. Set the time range. Advanced Reporter considers only events occurred in that time range for analysis.

**Select custom date range:**

Select this option, Advanced Reporter considers events occurred during the selected number of days for analysis.

Select this option and select **Limit to time range** option. Advanced Reporter enables the From and To spin boxes. Set the time range. Advanced Reporter considers only events occurred in that time range for analysis.

Note that Advanced Reporter considers only the date range from the From, To drop-down lists and ignores the time range set in those drop-down lists.

9. Select the Export Type.

10. Type the Refine and Filter criteria.

11. Type the Title, Description, Header, and Footer.


13. Select the **Add analysis to Queue** check box.

14. Crosscheck the Analysis details.

15. Click **Add To Queue**.
Configure Log Analysis - Trend - Scheduled

STANDARD / CUSTOM COLUMN ANALYSIS

1. Click the Analysis tab.
2. Expand the Log Analysis group, select Trend.
3. Click Scheduled Analysis in the Actions pane.
4. Click New Scheduled Analysis.
5. Click Next >>.
6. Select the Analyze events based on Event categories / Custom Properties option.
7. Select the Category / Categories.
8. Select the System(s) / Group(s) / Site(s).
9. Select the Schedule interval. If you select the Schedule Type as Daily / Weekly, then Advanced Reporter selects the Limit to time range check box.
   - Set the time range. Advanced Reporter considers only events occurred in that specified time range.
10. Select the Export Type.
11. Type the Refine and Filter criteria.
12. Type the Title, Description, Header, and Footer.
13. Crosscheck Analysis cost details.
14. Crosscheck the Analysis details.
15. Click Schedule.

**NOTE**

- In case any EventTracker services are not running a warning message is displayed when you log in. By default Advanced Reports selects the Chart Type as Line.
- Advanced Reports displays the Analysis Format Type drop-down list, if you try to generate On Demand report without selecting the format type in the Logs analysis group.
• You can also select the **Add analysis to Queue** check box and click **Add To Queue** to add the report to the queue. Advanced Reports enables the **Enable Publishing Option** check box and **Update status via RSS** drop-down list. Select an appropriate publishing option to deliver / notify results via E-mail. Type valid To address in the **To e-mail address field**. Select a RSS feed to get notification via RSS.

• **Quick View** Export Type option is not available when you schedule an analysis.

• **Quick View** Export Type option is not available when add a new analysis to queue.

• **Quick View** Export Type option is not available when you select the **Custom column analysis** option.

• You can select any number of Categories.

• Advanced Reports enables **Week Day** drop-down list only when you select the **Weekly** option as **Schedule Type**.

• To generate reports on multiple sites, select the Collection Point Master site from the drop-down list in the toolbar. Select the **Select Sites** option in the Select Systems window. EventTracker displays the available sites.

• By default only managed systems are displayed. You can select any number of managed and unmanaged Systems. Select the **Show all Systems/Groups** check box to view all the enterprise domains and the systems associated with them.

• **Select the All Systems check box** to select all managed and unmanaged systems.

• Advanced Reports pops up the **Options** window, had you not configured the SMTP Server in the E-mail Configuration tab.

• You can also exclude predefined columns from the report. Advanced Reports does not save this exclusion in the database.
Generate Default report in Case no Matching Records Found

![Figure 1](image)

**Reports/Analysis backup directory:**

- Note: On changing the folder, reports have to be manually copied from older to newer folder.
- Folder to keep the copies of generated reports
  - C:\Program Files\Prism Microsystems\EventTracker\Reports
  - Select

**Generate Default Report in case of no matching record found**

**Report/Analysis purge frequency:**

- Note: Uncheck the options to retain reports forever.
- An event will be logged 2 days before file deletion, which can be viewed in the EventTracker Management Console.
- Retain on demand/queued reports for **7** days
- Retain scheduled reports for **90** days

**Prompt to publish on demand Quick View reports**

- On demand ‘Quick view’ reports are not published on hard disk.
- This option will prompt to publish the report before closing.

---

Figure 1
Chapter 2
Virtual Collection Points

In this chapter, you will learn how to:

- Configure EventTracker Receiver to listen on multiple ports
- Upgrade Agents through System Manager
Virtual Collection Points

Virtual Collection Points (VCP) enable the existing receiver to behave like a collection master without having the physical Collection Points installed. The Existing Collection Point (CP-CM model) requires physically organized Collection Points reporting to a Collection Master. CP-CM model requires a number of hardware facilities and a large degree of deployment difficulty.

VCP provides the solution to break down the huge volume of input events using the existing set up with minimal configuration changes, thus helps to process the received data in a short time at the reporting end.

Configure EventTracker Receiver to listen on multiple ports

EventTracker Receiver can be configured to listen on 10 ports for Traps and 20 (10 UDP & 10 TCP) ports for Unix/Linux/Solaris Syslogs.

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Suggested Trap Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Receiver</td>
<td>14505 - Default Port</td>
</tr>
<tr>
<td></td>
<td>14515, 14525, 14535, 14545, 14555, 14565, 14575, 14585,</td>
</tr>
<tr>
<td></td>
<td>14595 (max 10 ports)</td>
</tr>
<tr>
<td></td>
<td>514 default UDP for Syslogs.</td>
</tr>
<tr>
<td></td>
<td>1470 default TCP for Syslogs.</td>
</tr>
<tr>
<td></td>
<td>You can add max 10 UDP and 10 TCP ports.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Suggested Trap Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Activity (Incoming)</td>
<td>14556, 14557, 14558, 14559, 14560, 14561, 14562, 14563,</td>
</tr>
<tr>
<td></td>
<td>14564, 14565, 14566, 14567, 14568, 14569, 14570, 14571,</td>
</tr>
<tr>
<td></td>
<td>14572, 14573, 14574, 14575</td>
</tr>
</tbody>
</table>

The following ports are internally fixed. You cannot edit these ports. Communication through these ports is taken care internally, which means the number of ports utilized by the respective modules will be in proportion to the number of trap ports set.

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Suggested Trap Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correlator (Incoming)</td>
<td>14655, 14656, 14657, 14658, 14659, 14660, 14661, 14662, 14663,</td>
</tr>
<tr>
<td></td>
<td>14664, 14665, 14666, 14667, 14668, 14669, 14670, 14671,</td>
</tr>
<tr>
<td></td>
<td>14672, 14673, 14674, 14675</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Suggested Trap Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker Receiver</td>
<td>32001, 32002, 32003, 32004, 32005, 32006, 32007, 32008,</td>
</tr>
<tr>
<td></td>
<td>32009, 32010, 32011, 32012, 32013, 32014, 32015, 32016,</td>
</tr>
<tr>
<td></td>
<td>32017, 32018, 32019, 32020</td>
</tr>
</tbody>
</table>
Example scenario

Consider EventTracker Agents in computers Sys2 and Sys3 are forwarding events to Sys1 (ET Manager). By default, the communication happens through port 14505. Suppose you want to configure different ports 14515 and 14525 for Sys2 and Sys3 respectively, do the following:

Computer: Sys1 – Configure Ports

1. Double-click Manager Configuration on the Control Panel.

   EventTracker displays the Manager Configuration window.

   ![Manager Configuration window](image)

   Figure 2
2. Select the **Multiple processing stacks** check box.

EventTracker displays the Virtual Collection Points dialog box.

![Virtual Collection Points](image)

**Figure 3**

3. Click **Add**.

EventTracker displays the Receiver Port dialog box.

![Receiver Port](image)

**Figure 4**

4. Add Receiver ports and then click **OK**.

(Example: 14515, 14525) EventTracker adds the newly configured ports.
5. Click **Close**.

6. Click **OK** on the Manager Configuration window.

   EventTracker displays the EventTracker Console confirmation message box.

   ![EventTracker Console](image)

    **Figure 6**

7. Click **Yes** to save the changes.

   EventTracker displays the Console Message box.
8. Restart the Management Console as advised on the message box.

EventTracker updates these changes in evtrxer.ini file (..\Program Files\Prism Microsystems\EventTracker)

![Figure 7](image)

![Figure 8](image)

**NOTE**

EventTracker creates *EtaConfig_14515.ini* & *EtaConfig_14525.ini* files in RemotInstaller folder (..\Program Files\Prism Microsystems\EventTracker\RemotInstaller).

9. Restart the EventTracker Receiver service.
### EventTracker v6.2 New Features Guide

<table>
<thead>
<tr>
<th>ET Modules</th>
<th>Trap Ports Utilized</th>
</tr>
</thead>
<tbody>
<tr>
<td>You ought to add ports to the <strong>Firewall exceptions</strong> list.</td>
<td></td>
</tr>
<tr>
<td>EventTracker Receiver (Incoming)</td>
<td>14505, 14515, 14525</td>
</tr>
<tr>
<td>User Activity (Incoming)</td>
<td>14556, 14557, 14558</td>
</tr>
<tr>
<td>Correlator (Incoming)</td>
<td>14656, 14657, 14658</td>
</tr>
<tr>
<td>EventTracker Receiver (Outgoing - for viewers)</td>
<td>32001, 32002, 32003</td>
</tr>
</tbody>
</table>

**Upgrade Agent (Sys2) from Manager (Sys1)**

1. Open the System Manager console.
2. Click **Upgrade Agent** on the toolbar.
3. Select and Add> Sys2 to Selected Computers list.
4. Select an appropriate **Upgrade Method**.
5. Click **Advanced**.
6. Select **Custom Config** option.
7. Click **Browse** and locate EtaConfig_14515.ini file in the RemoteInstaller folder.
8. Click **Upgrade**.

   EventTracker overwrites etaconfig.ini file with new settings.

**Upgrade Agent (Sys3) from Manager (Sys1)**

1. Open the System Manager console.
2. Click **Upgrade Agent** on the toolbar.
3. Select and Add> Sys3 to Selected Computers list.
4. Select an appropriate **Upgrade Method**.
5. Click **Advanced**.
6. Select **Custom Config** option.
7. Click **Browse** and locate EtaConfig_14525.ini file in the RemoteInstaller folder.

8. Click **Upgrade**.

   EventTracker overwrites etaconfig.ini file with new settings.

---

**Virtual Collection Points for syslogs**

EventTracker Receiver can be configured to listen on 20 (10 UDP & 10 TCP) ports for Unix/Linux/Solaris Syslogs.
1. Click **Edit Ports**.

EventTracker displays the Virtual Collection Points for Syslogs window.

![Virtual Collection Points for Syslogs](image)

<table>
<thead>
<tr>
<th>Click</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td>Add UDP, TCP ports.</td>
</tr>
<tr>
<td><strong>Edit</strong></td>
<td>Edit ports.</td>
</tr>
<tr>
<td><strong>Remove</strong></td>
<td>Remove ports.</td>
</tr>
</tbody>
</table>

2. Click **Add**.

EventTracker displays the Syslog Receiver Port window.

![Syslog Receiver Port](image)
3. Type appropriate port details and then click OK.
   EventTracker adds new configured ports.

4. Click Close.

5. Click OK on the Manager Configuration window.

Configure the Syslog Service on a UNIX/Linux/Solaris Host

1. Login as root user and edit the syslog.conf file in the /etc directory.

2. Append *.* @<server_name> at the end, where <server_name> is the name of the machine on which EventTracker is running.

3. Save the configuration and exit the editor.

4. SYSLOG service port number 514 is the default listener port of EventTracker. However, if you choose a different port other than 514 then edit the services file in the /etc directory.

5. Save the file and exit the editor.

6. Restart the syslog service on the host.

NOTE

Configuring Syslog service might differ from flavour to flavour kindly refer the respective man pages for more details.
Chapter 3
System Manager

In this chapter, you will learn how to:

- Install Agent with different user credentials
- Generate System Report
- Install Remedial Actions script
System Manager Console

New column to display the ports through which the Agent and EventTracker Receiver service communicate has been added.

![Figure 12](image)

Install Remedial Actions Script

Option to install remedial action scripts while deploying agents.

1) Select the Install Remedial Action scripts check box to install the scripts in the EventTracker install directory, typically (`...\Program Files\Prism Microsystems\EventTracker\Agent\Script`).
Install Agent with Different User Credentials

To deploy Agents on remote systems, you should have local admin privilege on that computer. You can also choose a user that is member of ‘Domain Admins’ group to deploy Agent on remote computers.

To install agent with different user credentials

1) Open the System Manager.

2) Click the Options menu and select the Add System option.

   (OR)

   Click Add System on the toolbar.

   (OR)

   Right-click the system where you want to install the agent.

   EventTracker displays the shortcut menu.
From the shortcut menu, choose the **Add System** option.

EventTracker displays the Add Agent window.

3) Select the systems.

4) Click **Next**.

5) Click **Next**.

6) Select the **Agent based (Full featured)** option.

7) Select the **Install Remedial Action scripts** check box to install the scripts in the EventTracker install directory, typically (…\Program Files\Prism Microsystems\EventTracker\Agent\Script).

8) Click **Next**.

9) Click **Install**.

EventTracker displays the message box indicating that the current user has no privilege to install on the remote system.

10) Click **Yes** to install with a different user credentials that has domain admin privilege. EventTracker displays the Login dialog box.
Type valid user credentials and then click Login.

EventTracker starts installing the Agent and displays the progress bar.

After installing the Agent, EventTracker displays the EventTracker – System Manager message box.

11) Click OK.

EventTracker displays the successful installation message.

12) Click Finish.

System Report

System Report helps to keep track of Managed and Unmanaged systems. Filter option is provided to view the ports used by Managed systems.

To generate system report

1. Open the System Manager.

2. Click the View menu and then select the System Report option.

EventTracker displays the System Report console.

![System Report Console](image.png)

Figure 16
Managed System Report

This option helps to generate O/S wise, group wise and port wise report.

To generate system type wise report

1. Select the Managed option.
2. Select System Type option to view Managed systems by operation systems.
3. Select an O/S type from the System Type drop-down list.
4. Click Show Report.

To generate group wise report

1. Select the Managed option.
2. Select the Group option to view Managed systems by group.
3. Select a group from the Group Name drop-down list. All monitored enterprise system groups are listed in this drop-down list.
4. Click Show Report.
To generate port wise report

1. Select the **Managed** option.
2. Select the **Port Number** option to view Managed systems by port. All configured ports are listed in this drop-down list.
3. Select a port from the **Port Number** drop-down list.
4. Click **Show Report**.

**Unmanaged System Report**

This option helps to generate O/S wise and group wise report.

**To generate system type wise report**

1. Select the **Managed** option.
2. Select **System Type** option to view Managed systems by operation systems.
3. Select an O/S type from the **System Type** drop-down list.
4. Click **Show Report**.

**To generate group wise report**

1. Select the **Managed** option.
2. Select the **Group** option to view Managed systems by group.
3. Select a group from the **Group Name** drop-down list.
4. Click **Show Report**.

**All System Report**

This option helps to generate O/S wise, group wise and port wise Managed / Unmanaged system report.
Chapter 4
EventVault Warehouse Manager
New columns have been added to the EventVault Warehouse Manager console for better understanding of the CAB files.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path</td>
<td>Path of the CAB file.</td>
</tr>
<tr>
<td>Size(KB)</td>
<td>Size of the CAB file in KB.</td>
</tr>
<tr>
<td>Total Events</td>
<td>Total number of events in the CAB file.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Port through which those events were received.</td>
</tr>
</tbody>
</table>
Chapter 5
Remedial Action at Agent System

In this chapter, you will learn how to:

- Enable and Configure Remedial Actions
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.

![Manager Configuration Window](image-url)
EventTracker displays the Caution dialog box.

![Remedial Action Configuration](image)

Figure 19

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.

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

7. 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.

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.

**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.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restart Service</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Restart System</strong></td>
<td>EventTracker disables the Script Name field. Type appropriate description in the Notes field for future reference.</td>
</tr>
<tr>
<td><strong>Shut Down System</strong></td>
<td>EventTracker disables the Script Name field. Type appropriate description in the Notes field for future reference.</td>
</tr>
<tr>
<td><strong>Stop Service</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Terminate Process</strong></td>
<td>EventTracker enables this option only when you set an alert for the specified Events.</td>
</tr>
</tbody>
</table>

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 22](image)
4. Select an appropriate option and then click OK.

![Figure 23](image)

5. Click **Save** on the toolbar.

   EventTracker displays the Management Console message box.

6. Restart the Management Console as advised on the message box.

   Although all predefined Alerts are applicable to all monitored systems, remedial actions will be initiated only on systems where Remedial Action is enabled.
You can also exclude systems where remedial actions have been enabled.

7. Select the **Apply to selected Systems** option.

EventTracker displays the monitored computers.
8. Select the systems from the Computer(s) list and then click Add ->.

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

Figure 26

9. Click Finish.

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.

   EventTracker displays the Systems tab.
5. Select and add the systems to the List of selected systems.

6. Click Next >.

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

EventTracker displays the Actions window.
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.
Chapter 6
Management Console
Agent Configuration – Track / Monitor USB and Other Devices

Device Changes feature in earlier versions has been enhanced to monitor file transaction activities that occur in the inserted media (USB and other devices).

![EventTracker Agent Configuration](image_url)

**Figure 31**
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Insert/Remove</td>
<td>Select this check box to track insertion or removal of USB or other devices. This check box is selected by default.</td>
</tr>
<tr>
<td>Record activity</td>
<td>Select this check box to monitor file transactions occur in the inserted devices. If you enable this option, EventTracker displays the caution message box.</td>
</tr>
</tbody>
</table>

EventTracker Agent Configuration - USU Tracking

Caution: If enabled, the EventTracker Agent will passively but continuously monitor USB devices thereby causing the "Safely Remove Hardware" feature of Windows to always return "Device in Use". The message can be ignored, the USB device is not affected.

Click OK to continue.

<table>
<thead>
<tr>
<th>Disable USB Devices</th>
<th>Select this check box to disable USB devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Exception List</td>
<td>This button is enabled when you select the Disable USB Devices check box. Click this button to add USB devices that you wish to enable.</td>
</tr>
</tbody>
</table>

USB Exception List

While disabling USB Devices on a particular computer, you can also exempt and enable USB devices from monitoring.

1. Click **USB Exception List**.

EventTracker displays the USB Exception List dialog box.
2. Type the serial no in decimal format in the **Enter USB Serial No** field.

3. To type the serial no in hexadecimal format, select the **Hex** option and then type the serial no in the **Enter USB Serial No** field.

4. Click **Add**.

EventTracker adds the newly entered serial number.
5. Select a serial number in the list and then click **Edit** to edit the serial number.

![USB Exception List](image)

**Figure 34**

6. Click **Edit Ok** to update the changes or **Edit Cancel** to cancel the changes. If you click Edit Ok without making any changes, EventTracker will display a message box with appropriate message.

![EventTracker Agent Configuration](image)

**Figure 35**

7. Select a serial number in the list and then click **Remove** to delete the serial number.

8. Click **Cancel** to close the window without saving.

9. Click **Save & Close** to save the changes and close the window.
Agent Configuration – SNAM

SNAM configuration supports wild card search.

You can use wild cards to search processes. For example, had you configured Virtual Collection Points and wish to add all EventTracker Receiver processes, it is enough to provide the Process name as EtReceiver*.exe.

Auto focus on Alerts Category

If there is any alert event to display, EventTracker auto focuses on Alerts Category while opening Management Console. Otherwise, the focus remains on the default ‘All Categories” group.

Alerts category is a systematic assortment of events and system status that require user's immediate attention and corrective action.
Event-O-Meter

Event-O-Meter is an analytical graphical chart that helps quickly visualize per port trends of events against specified time range. In addition, numerical data has also been provided in a tabular format.
User Activity

Activity Detail dialog in User Activity Viewer to view individual events.

Figure 40

Figure 41
Splash screen

EventTracker displays the Splash screen whenever you open the Management Console.

EventTracker displays the logs collected information in the About box.

Figure 42
Uninstall Options

Following dialog box is displayed while uninstalling EventTracker.

1. Click **Yes** to remove EventTracker completely.
2. Click **Yes** to remove everything.

   EventTracker displays the confirmation message box.

   ![Uninstall EventTracker](image)
   
   **Figure 45**

3. Click **No** to retain data, reports, and configuration.

   ![Uninstall EventTracker](image)
   
   **Figure 46**