List Management and its Usage

EventTracker v7.5
ABSTRACT

This document describes the usage of entities in List Management. To monitor and prevent irrelevant activities of users, we have introduced this feature where in all the actions can be monitored and precautionary measures can be taken when required.

TARGET AUDIENCE

EventTracker users who wish to curb the unknown malicious activities.
# Table of Contents

List Management ........................................................................................................................................ 4
Create a group in List Management .......................................................................................................... 5
Automatic Import of entity to List Management via Schedule Action Scripts ............................................ 6
  Prerequisites ............................................................................................................................................ 7
  Create a group ......................................................................................................................................... 7
  Edit VB script file ..................................................................................................................................... 7
  Schedule Action Script ............................................................................................................................ 8
    Verify the imported entities in List Management ................................................................................... 9
Command Line Usage in List Management .................................................................................................... 12
  Prerequisites to import list via command prompt .................................................................................. 12
  Create Group in List Management ........................................................................................................ 12
  Usage of Command Line parameters ..................................................................................................... 13
  Import entity list via command prompt .................................................................................................. 14
  Import entities from text file ................................................................................................................ 16
  Import entities from CSV file ................................................................................................................. 17
  Import entities from excel file ................................................................................................................. 18
    Verify the imported entities in List Management UI ........................................................................... 18
Manual Import of List Management ........................................................................................................... 18
Usage of List Management ....................................................................................................................... 19
  Remedial Action - Monitor Black Listed Port Communicated ................................................................. 19
    Prerequisites ...................................................................................................................................... 19
    Create a group ‘DshieldTrojanportlist’ ............................................................................................... 19
    Configure alert and remedial action for McAfee IPS ........................................................................ 19
    Configure an alert for black listed port communicated ................................................................... 24
    Verify the generated incidents ............................................................................................................ 26
Monitor Behavior Activity Dashboard ....................................................................................................... 27
  Monitor IP Address Activity .................................................................................................................. 27
  Monitor Process Activity ....................................................................................................................... 30
Unauthorized File Access ..................................................................................................................... 34
Prerequisites...................................................................................................................................... 34
To Detect unauthorized file access.................................................................................................. 34
Verify in Incidents Dashboard........................................................................................................ 37
List Management

In large organizations administrators find it difficult to maintain the network when systems are running 24/7. To ease and improve efficiency of network administrators, List Management feature has been introduced. A various list of classes can be maintained and respective activities can be generated from these entities to minimize illegitimate activities of hackers.

The classes that have been provided are,

- **IP Address**
  
  Ex: An external access request from unknown IP address can be tracked.

- **Port No**
  
  Ex: If any external user is trying to connect to your local machine, then blacklisted port numbers can be tracked.

- **Process**
  
  Ex: Malicious processes can be monitored like Trojan.exe.

- **Service**
  
  Ex: If an unknown service is being installed by users, which potentially degrade performance of systems can be monitored.

- **Users** - To avail this, please install the update ET75U13-012.exe that has been provided. Refer [http://www.eventtracker.com/support/software-updates/](http://www.eventtracker.com/support/software-updates/) for more details.
  
  Ex: If a spammer is trying trying to frequently intrude in your network, then a list of users can be maintained to block him/her.

There are three different ways to import entities in List Management.

- Import entities Automatically via Schedule Action Script
- Import entities via Command Line
- Import entities Manually through List Management UI
Create a group in List Management

1. Logon to EventTracker Enterprise.

2. Select the Admin menu, and then select List Management.

3. To add a new group, select ‘+’ symbol.
   
   Group window displays.

4. To select the respective class, select the Class: drop down list.
5. Enter the group **Name:** and then select the **Save** button.

---

### Automatic Import of entity to List Management via Schedule Action Scripts

EventTracker users can automatically import the blacklisted IP addresses and port numbers updated @ [http://dshield.org](http://dshield.org) via Schedule Action Script. It is not meant for other sites and other classes.

The referral links are:

- **IP Address:** [http://feeds.dshield.org/block.txt](http://feeds.dshield.org/block.txt)
- **Port Number:** [http://dshield.org/services.html](http://dshield.org/services.html)

The factory setting or EventTracker installation will be provided to the user with two VB scripts (DShieldOrgBlockedIPLListImport.vbs and DShieldOrgTrojanServicePortListImport.vbs) to download the blacklisted IP addresses and Port numbers from dshield and update the same in EventTracker list management on a daily basis via Schedule Action Scripts.

**NOTE:**

The user should create a group named DshieldTrojanportlist under class port no and group named DshieldBlockList under class IP Address. The user must also update the List import section available on the script with the correct path where EventTracker is installed. By default,
the IP and port will be merged to the existing list. This can be changed in the VB script as per the user requirement.

Prerequisites

The following steps have to be followed in order to automatically import entities in List Management.

1. User should have appropriate permission on EventTracker Database.
2. Create a group
3. Edit VB Script file
4. Schedule Action Script
5. Verify imported entities in List management

Create a group

NOTE:

Please create respective groups named ‘DshieldTrojanportlist’ for class ‘Port No’ and ‘DshieldBlockList’ for class ‘IP Address’ as described in Create a Group in List Management.

Edit VB script file

1. Traverse to the path where the VB script file is available (i.e. \InstallDIR\Program Files\Prism Microsystems\EventTracker\ScheduledActionScripts).
2. Locate and edit the VB script files “DShieldOrgTrojanServicePortListImport.vbs”, “DShieldOrgBlockedIPListImport.vbs”.
3. Update the script files with correct path where EventTracker is installed.

The command that has to be modified in “DShieldOrgTrojanServicePortListImport.vbs” file is

```
Listimportcmd= C:\Program Files\Prism Microsystems\EventTrackerWeb\bin\Prism.ListImportUtility.exe "Port No" "DshieldTrojanportlist" "txt" & Space(1) & stroutfile & Space(1) & "t"
```
EventTracker: List Management and its Usage

The command that has to be modified in “DShieldOrgBlockedIPListImport.vbs” file is

```
Listimportcmd="C:\Program Files\Prism Microsystems\EventTrackerWeb\bin\Prism.ListImportUtility.exe" "IP Address" "DshieldBlockList" "txt" & stroutfile & " ETAdmin"
```

Schedule Action Script

1. Logon to EventTracker Enterprise.

2. Select the Tools menu, and then select Scheduled Scripts.

3. Select the Add New button.

   Script scheduler window displays.
4. Enter a **Task Name**.

5. Select the **Script file** from drop down i.e. **DShieldOrgTrojanServicePortListImport.vbs**.

6. Enter a valid **Description** and select the **Schedule Type**.

7. Enter valid credentials and then select the **Schedule** button.

    Similarly schedule the script **DShieldOrgBlockedIPListImport.vbs**. The scheduled scripts will run at the specified time and the list is imported accordingly in List Management.

**Verify the imported entities in List Management**

1. Select the **Admin** menu and then select **List Management**.

    List Management page displays.

2. In **IP Address** group, select **DshieldBlockList**.
3. In **Port No** group, select **DshieldTrojanportlist**.
**List Management**

<table>
<thead>
<tr>
<th>Groups</th>
<th>Port No/DshieldTrojanPortlist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>Groups: HP Address, Blocked IP, DshieldBlockList, Processes, ValidProcess, Services, Port No, DshieldTrojanPortlist, invalidPortno</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Port No</td>
<td>Pattern</td>
</tr>
<tr>
<td>1</td>
<td>Port No</td>
</tr>
<tr>
<td>2</td>
<td>Port No</td>
</tr>
<tr>
<td>15</td>
<td>Port No</td>
</tr>
<tr>
<td>20</td>
<td>Port No</td>
</tr>
<tr>
<td>24</td>
<td>Port No</td>
</tr>
<tr>
<td>30</td>
<td>Port No</td>
</tr>
<tr>
<td>31</td>
<td>Port No</td>
</tr>
<tr>
<td>38</td>
<td>Port No</td>
</tr>
<tr>
<td>41</td>
<td>Port No</td>
</tr>
<tr>
<td>44</td>
<td>Port No</td>
</tr>
<tr>
<td>48</td>
<td>Port No</td>
</tr>
<tr>
<td>55</td>
<td>Port No</td>
</tr>
<tr>
<td>58</td>
<td>Port No</td>
</tr>
<tr>
<td>59</td>
<td>Port No</td>
</tr>
<tr>
<td>66</td>
<td>Port No</td>
</tr>
<tr>
<td>68</td>
<td>Port No</td>
</tr>
<tr>
<td>69</td>
<td>Port No</td>
</tr>
<tr>
<td>81</td>
<td>Port No</td>
</tr>
<tr>
<td>86</td>
<td>Port No</td>
</tr>
<tr>
<td>96</td>
<td>Port No</td>
</tr>
<tr>
<td>110</td>
<td>Port No</td>
</tr>
<tr>
<td>121</td>
<td>Port No</td>
</tr>
<tr>
<td>123</td>
<td>Port No</td>
</tr>
</tbody>
</table>

**Figure 7**
Command Line Usage in List Management

To import entities under List Management via command prompt, the user can have the entity list (input file) in text, CSV or excel format. The user can use command line utility ‘Prism.ListImportUtility.exe’ file available in the install directory to import the entities to list management.

Prerequisites to import list via command prompt

The following prerequisites are necessary to execute and import the entities in List management via command prompt.

1. Input files should be present in text, CSV or excel format.
2. Create a group under the respective class which is passed as a parameter via command line.
3. Pass the parameters in the same order as mentioned in Usage of command line parameters.
4. User should have appropriate permission on EventTracker Database.

Create Group in List Management

NOTE:

Users have to first create a group name in the List Management UI which will be passed through the command line as a parameter.

1. To create a group in List Management, refer Create Group.

   Example: Class: selected here is IP Address and Name: is DshieldBlockList.

   The respective group is created.
### Usage of Command Line parameters

The details of the parameters that have to be passed via command prompt are mentioned in the table below.

<table>
<thead>
<tr>
<th>Parameter No</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Class name within double quotes</td>
<td>&quot;IP Address&quot; / &quot;Services&quot; / &quot;Port No&quot; / &quot;Processes&quot;</td>
</tr>
<tr>
<td>2</td>
<td>Group name within double quotes</td>
<td>Any alphanumeric characters. Ex: 1abc, blacklisted port. The following special characters are not allowed (i.e. @ * ^ / (%)[ ] # $ = &quot; &lt; &gt;</td>
</tr>
</tbody>
</table>
| 3            | File extension within quotes | Text: "txt"  
CSV: "csv"  
Excel: "xlsx" |
| 4            | File name along with path in double quotes | The correct location of the file has to be entered within double quotes. Ex: "C:\block.txt" |
| 5            | Field separator within double quotes | Text: Tab - "\t", Space - "\s", Comma - ",", Colon - ":", "\n" - Newline  
CSV: Comma only  
Excel: "" - double quotes without space because there is no field separators in excel |
| 6            | Row Terminator within double quotes | Text: "\n" - Newline  
CSV: "\n" - Newline or "" - double quotes without space  
Excel: "" - double quotes without space because there is no row terminator in excel |
| 7            | Data Index within double quotes | Text/CSV: "1", "2" etc – Numeric values  
Excel: "a" or "A", "y" or "Y" etc – Column name  
You can also input any other column name provided that there is valid data in the excel file. |
| 8            | Description Index within double quotes (optional) | Text/CSV: "1", "2", "" etc – Numeric values  
Excel: "a" or "A", "y" or "Y", "" etc – Column name. You can also input any other column name provided that there is valid data in the excel file. |
| 9            | User name within double quotes | Ex: “Karen” |
| 10           | Skip Header Rows within double quotes | Number of header rows that has to be ignored. Ex: "1", "3", "" – double quotes without space if there is no row to skip |
| 11           | Merge/Overwrite within | "1" or "2" |
double quotes | 1 – merge. The existing entity list will be merged with the new entity list.  
2 – overwrite. The existing entity list will be overwritten, hence the previous data will be erased.

Create group | “2”  
This parameter can be used directly to create a group by specifying the input as “2” within double quotes on the command line utility.  
NOTE: If you do not wish to pass this parameter via command line then a group has to be created in List Management UI.  
To avail this parameter to be passed via command line, please install the update ET75U13-012.exe that has been provided. Refer http://www.eventtracker.com/support/software-updates/ for more details.

Please follow the steps given below to import the entity available in the input file.

NOTE:

- All parameters should be passed in correct order.
- The parameters 2 and 3 i.e. class name and group name should be proper and available in UI since it is passed as a parameter via command line.
- Duplicate entities will not be imported.
- .xls format is not supported.
- While passing the parameters, make sure that there is no space between parameters if there is no input for that parameter. Ex: In an excel file, if there are no header rows, then number of header rows to be skipped is placed within empty double quotes without spaces.

Import entity list via command prompt

1. To import entity list via command prompt, run the executable file “Prism.ListImportUtility.exe”.  
   This executable file is available in \InstallDIR\Program Files\Prism Microsystems\EventTrackerWeb\bin folder.

2. Open the command prompt as an administrator, if the target system is Vista and above.
3. Traverse to the path where "Prism.ListImportUtility.exe" file is available.

![Figure 9](image)

4. Pass the parameters in command prompt as shown below

   **Example 1:**
   
   In this example below, a group has to be created in List Management UI as described in [Create a group](#).

   ```
   Prism.ListImportUtility.exe "Processes" "BlackListedProcesses" "txt" "C:\block.txt" "n" "n"
   "0" "0" "Karen" "1"
   ```

   **Example 2:**
   
   ```
   Prism.ListImportUtility.exe "users" "Finance" "xlsx" "C:\users.xlsx" "n" "a" "b" "Karen" "1" "1"
   "2"
   ```
   In this example a group is created directly via command line and list of users are imported to the list.
This update has been provided for ET75U13-012.exe file only as described in [http://www.eventtracker.com/support/software-updates/] for v7.5 - Build 29.

**Import entities from text file**

**Example:**
The command mentioned below imports IP addresses to a group named ‘BlockedIP’ from the respective Text file.

```
Prism.ListImportUtility.exe "IP Address" "BlockedIP" "txt" "D:\BlockedIP.txt" "\n" "\n" "1" "0" "Karen" "" "1"
```

On successful execution of the command, the screen will appear as shown below.

The entities will be updated in the List Management UI.
Import entities from CSV file

Example:
The command mentioned below imports some executable files to a group named 'ValidProcess' from the respective CSV file.

```
Prism.ListImportUtility.exe "Processes" "ValidProcess" "csv" "C:\ETexelist.csv",", "1" "1"

karen""1""1"
```

The output is shown below and respective entities will be updated in List Management UI.
Import entities from excel file

**Example:**

The command mentioned below imports port numbers to a group named ‘InvalidPortNo’ from the respective excel file.

```
Prism.ListImportUtility.exe "Port No" "InvalidPortNo" "xlsx" "C:\Invalid Port Numbers.xlsx"
    "" "" "a" " " "Karen" "1" "1"
```

The output is shown below and respective entities will be updated in List Management UI.

![Figure 13](image)

**Verify the imported entities in List Management UI**

1. To view the output in List Management UI, logon to EventTracker Enterprise.
2. Select **Admin** drop-down and then select **List Management**.
3. Select the respective **Groups** and the **Class Name**.

**Manual Import of List Management**

Please refer [EventTracker Enterprise v7.5 User Guide](#) – Chapter 20 List Management.
EventTracker: List Management and its Usage

Usage of List Management

This section describes the usage of List Management in

- Remedial Action - Monitor Black Listed Ports Communicated
- Behavior Activity - Monitor IP Address and Process Activity

Remedial Action - Monitor Black Listed Port Communicated

Prerequisites

To monitor the black listed ports communicated in the network, please follow the steps mentioned below.

- Update the VB script file with correct path where EventTracker is installed
- Create a Group with name 'DshieldTrojanportlist'
- Automate importing of black listed port from Dshield
- McAfee IPS logs should be present to monitor black listed ports

Create a group ‘DshieldTrojanportlist’

A group has to be created to import all the black listed ports from Dshield (http://dshield.org/services.html).

1. Please create a group in List Management under Class ‘Port No’ with Group Name as 'DshieldTrojanportlist' as described in Create Group.

   The respective blocked port numbers should be listed in List Management.

2. Edit DShieldOrgTrojanServicePortListImport.vbs file as described in Edit VB Script file with the correct path where EventTracker is installed.

Configure alert and remedial action for McAfee IPS

1. Logon to EventTracker Enterprise.

2. Select Admin dropdown, and then select Alerts.
EventTracker displays Alert Management page.

![Alert Management Page](image1)

**Figure 14**

3. Select the **Add Alert** button.

EventTracker displays the **Alert configuration** page.

![Alert Configuration Page](image2)

**Figure 15**
4. Type the new alert name in the **Alert Name** field.
   
   Example: McAfee IntruShield IPS

5. Select the severity of threat from the **Threat level** drop-down list.

6. Select the threshold from the **Threshold level** drop-down list.

7. If required, to view the alert in compliance dashboard, select ‘**Show in**’ dropdown, and then select ‘**Compliance Dashboard**’.

8. Click the **Add** button to add event details.

   Add Event window displays.

   ![](image)

   **Figure 16**

9. Enter **Source**: as “syslog”.

10. Enter **Match in Description**: as “McAfee IntruShield IPS”.

11. Select the **Add** button.
12. Click **Next** button or **Actions** link.

   EventTracker displays the **Actions** page.

13. Select **Console Remedial Action** tab.

14. Enter the correct path of the file ‘**SuspiciousPortCheck.bat**’

   (i.e. `\InstallDIR\Program Files\Prism Microsystems\EventTracker\ScheduledActionScripts\SuspiciousPortCheck.bat`).
NOTE:

Make sure that the VB script file (i.e. \InstallDIR\Program Files\Prism Microsystems\EventTracker\ScheduledActionScripts\SuspiciousPortCheck.vbs) contains the correct path where EventTracker is installed.

a. Edit the SuspiciousPortCheck.vbs file.

b. Search for the command ‘eventCmd = """"C:\Program Files\Prism Microsystems\EventTracker\ScheduledActionScripts\sendtrap.exe"""" + eventCmd’.

c. Enter the correct path where EventTracker is installed.

15. Click Finish.

EventTracker adds the newly created alert and displays it on the Alert Management page.

16. Click the Activate Now button.

NOTE:
EventTracker: List Management and its Usage

The remedial action configured compares the black listed port against the McAfee IPS logs. If a match is found an event 2223 will be generated.

**Sample McAfee IntruShield IPS log:**

<table>
<thead>
<tr>
<th>Event Id:</th>
<th>123</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source:</td>
<td>Syslog</td>
</tr>
<tr>
<td>Event type:</td>
<td>Information</td>
</tr>
<tr>
<td>User:</td>
<td>Karen</td>
</tr>
</tbody>
</table>

**Description:** McAfee IntruShield IPS | ATTACK TIME=Jan 25 16:22:31;ATTACK ID=0x41a02f02;ATTACK NAME=Over Threshold;SOURCE IP=193.14.1.7;SOURCE PORT=3451;DESTINATION IP=195.16.74.53;DESTINATION PORT=20;NETWORK PROTOCOL=TCP;INTERFACE=1A;APPLICATION PROTOCOL=HTTP;RESULT STATUS=Blocked;DIRECTION=Inbound;CATEGORY=DDos;SUB CATEGORY=DDos;ATTACK SEVERITY=High;ATTACK CONFIDENCE=Low;ADMIN DOMAIN=domain;SENSOR NAME=sensor1;ALERT TYPE=$IV_ALERT_TYPE$;DETECTION MECHANISM=signature;ATTACK SIGNATURE=Over Threshold

**Configure an alert for black listed port communicated**

An alert needs to be configured to notify black listed ports.

1. Logon to EventTracker Enterprise.
2. Select the **Admin** menu, and then select **Alerts**.
   
   EventTracker displays Alert Management page.
3. Select the **Add Alert** button.
   
   EventTracker displays the **Alert configuration** page.
4. Type the new alert name in the **Alert Name** field.
   
   Example: Black Listed Port Communicated.
5. Select the severity of threat from the **Threat level** drop-down list.
6. Select the threshold from the **Threshold level** drop-down list.
7. If required, to view the alert in compliance dashboard, select ‘**Show in**’ dropdown, and then select ‘**Compliance Dashboard**’.
8. Click the **Add** button to add event details.
   
   Add Event window displays.

9. Enter **Source**: as “**EventTracker**” and **Event Id**: as “**2223**”.

10. Select the **Add** button.

   ![Add Event Window](image)

   **Figure 19**

11. Click **Finish**.

   EventTracker adds the newly created alert and displays it on the **Alert Management** page.

12. Click the **Activate Now** button.

   **Sample event description when a blacklisted port is communicated**

   - **Event Id**: 2223
   - **Source**: EventTracker
   - **Event type**: Information
   - **User**: system
   - **Description**: Port No 1838 detected in network which is listed in Group DshieldTrojanportlist Known to be used by Trojan.
Verify the generated incidents

The alert has been configured to check for suspicious ports and hence it is compared with McAfee IPS logs. If suspicious ports are detected, then the incident is displayed in Incidents Dashboard.

1. In **Incidents Dashboard**, select the **Incidents** menu.

![Top 5 incidents by count](image)

*Figure 20*
Monitor Behavior Activity Dashboard

List Management provides a List Lookup feature where you can analyze and gather information regarding malicious IP addresses and Processes.

Monitor IP Address Activity

To analyze malicious IP addresses (black listed) that are detected, please follow the steps mentioned below.

1. Create the respective group in List Management as described in Create a Group.
   For Example: Name of the group created is 'Black Listed IP Addresses'.

2. Select the Behavior menu, select Security or Operations.

3. Click the IP Address Activity pie chart to view behavior details for IP address activities.
   (OR)
   In View behavior details for dropdown, select IP Address Activity option and then click icon.

   EventTracker displays the ‘Enterprise Activity Detail’ page.

   By default, IP Class dropdown displays all IP addresses.
4. To view public IP addresses, click the **IP Class** drop-down and then select **Public**.

5. Click **ListLookup** icon to monitor unknown/blacklisted IP addresses that have logged into the network.
6. If you select 'In' from **Find:** drop down, the processes that are found in List Management group displays.

7. Click **Information** icon to view detail information.

8. To view IP Addresses that are not available in List Management, select **Not in** from **Find:** drop down.
Monitor Process Activity

The List Lookup option helps you analyze malicious processes that are detected.

1. Create the respective group in List Management as described in Create a Group.
   For Example: Name of the group created is ‘Malicious Processes’.

2. Select the Behavior menu, select Security or Operations.

3. Click Windows Process Activity pie chart to view behavior details for process activities.
   (OR)
   From View behavior details for dropdown, select Windows Process Activity option, and then click icon.

   EventTracker displays the ‘Enterprise Activity Detail’ page.
4. Click **ListLookup** icon to view malicious processes that can harm the system. ListLookup window displays.
5. In **Find**: drop down, select **In** or **Not in**, select the required **Group**: and duration. If you select "In", the processes that are found in List Management group displays.

6. Select the **Search** button.

![Figure 26](image_url)

7. Click **Information** 🔄 icon to view additional information.
8. In **Find**: drop down, select **Not In**, select the required **Group** and the duration.

   If you select *Not in*, the processes that are NOT available in List Management group display.

9. Select the **Search** button.
Unauthorized File Access

This feature has been provided to track unauthorized file access so that restricted users do not have the privilege to tamper data.

Prerequisites

- Apply the update ET75U13-012.exe for v7.5 Build 29 as described in http://www.eventtracker.com/support/software-updates/
- Update UnauthorizedFileAccess.bat and UnauthorizedFileAccess.exe files with the correct path where EventTracker is installed.
- In UnauthorizedFileAccess.vbs file, enter the correct SQL Server Name and Group Name.
- Configure the alert to enable auditing for file access i.e. Event ID 4656 and enable Remedial action at console for UnauthorizedFileAccess.bat file.
- Configure an alert for Event ID 2220 to detect unauthorized file access.

To Detect unauthorized file access

To detect unauthorized file access, please follow the steps mentioned below.

NOTE:

a. Make sure that the files UnauthorizedFileAccess.bat and UnauthorizedFileAccess.exe (i.e. \InstallDIR\Program Files\Prism Microsystems\EventTracker\ScheduledActionScripts\) contain the correct path where EventTracker is installed.


c. Replace the correct path in the files where EventTracker is installed.

d. While editing UnauthorizedFileAccess.vbs file, also enter the correct SQL Server Instance name (i.e. Server=\sql express) and GroupName.
1. Create an alert as described in Create alert with \textbf{Source} as “\textit{Microsoft-Windows-Security-Auditing}” and \textbf{Event Id} as “5145”.

\textbf{NOTE:}

On Vista and above machines, users can configure the event ID ‘4656’ to detect file/object access.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{alert_configuration.png}
\caption{Figure 29}
\end{figure}

2. In \textbf{Console Remedial Action}, enter the correct path of the file.
3. Similarly create another alert with the **Event Id** as **2220** and activate the alert.
Verify in Incidents Dashboard

1. Select the **Incidents** Menu.

   Incidents Dashboard displays by default.

2. In **Top 5 incidents by count**, click on the graph.

   (OR)

   Select the **Tabular** tab and then select the **Advance Search** icon.

   Select the relevant alert **Detected Unauthorized File Access** and then select the **Search** button.

---

**Figure 32**
EventTracker: List Management and its Usage

Figure 33