EventTracker
Secure. Comply. Succeed.

Active Watch List and its Usage

EventTracker v8.x

Publication Date: Apr. 28, 2016

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

ABSTRACT

This document describes the usage of entities in Active Watch List. 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

Active Watch List

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, Active Watch List 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 –** User type groups can be created and usernames can be added within the groups.

  Ex: If a spammer is 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 Active Watch List.

- Import entities Automatically via Schedule Action Script
- Import entities via Command Line
- Import entities Manually through Active watch List UI

Create a group in Active Watch List

1. Logon to EventTracker Enterprise.

2. Select the **Admin** menu, and then select **Active Watch List**.

Figure 1

3. To add a new group, select '⊕' symbol in the group pane.

   Group window displays.

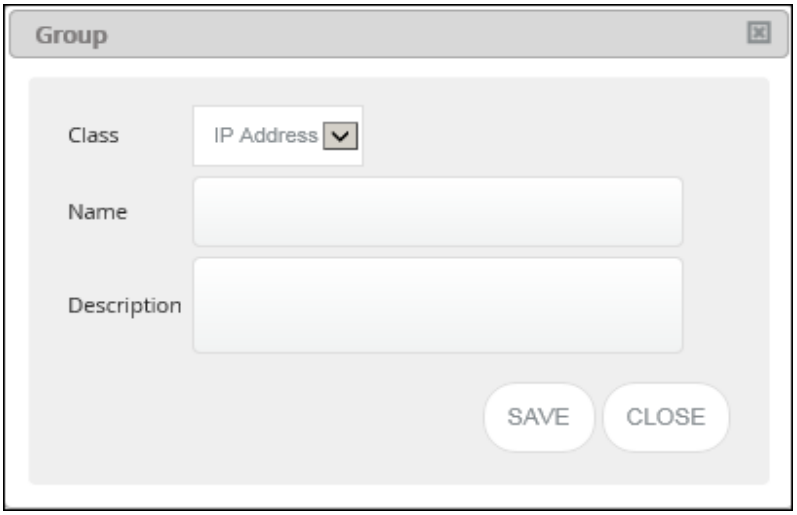


Figure 2

4. To select the respective class, select the **Class:** drop down list.

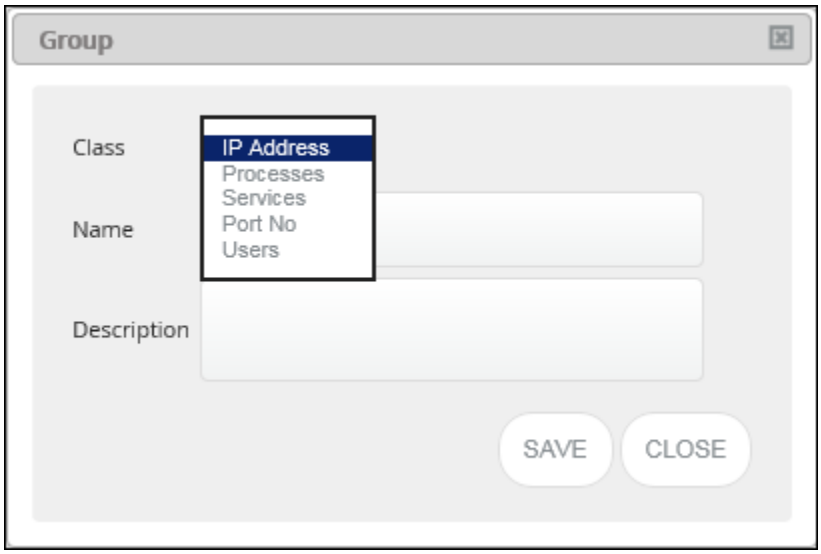


Figure 3

5. Enter the group **Name:** and then select the **Save** button.

Automatic Import of entity to Active Watch List via Schedule Action Scripts

EventTracker users can automatically import the black listed IP addresses and port numbers updated @ 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
- Port Number: http://dshield.org/services.html

The factory setting or EventTracker installation will be provided to the user with two VB scripts (DShieldOrgBlockedIPListImport.vbs and DShieldOrgTrojanServicePortListImport.vbs) to download the black listed IP addresses and Port numbers from dshield and update the same in EventTracker Active Watch List 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 Active Watch List.

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 Active Watch List

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 Active Watch List.

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""" & Space(1) & """\n""" & Space(1) & """1""" & Space(1) & """2""" & Space(1) & """ETAdmin""" & Space(1) & """""""" & Space(1) & """1"""

and

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""" & Space(1) & """" & stroutfile & """" & Space(1) & """\n""" & Space(1) & """\n""" & Space(1) & """0""" & Space(1) & """0""" & Space(1) & """ETAdmin""" & Space(1) & """""""" & Space(1) & """1"""

Schedule Action Script

1. Logon to EventTracker Enterprise.

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

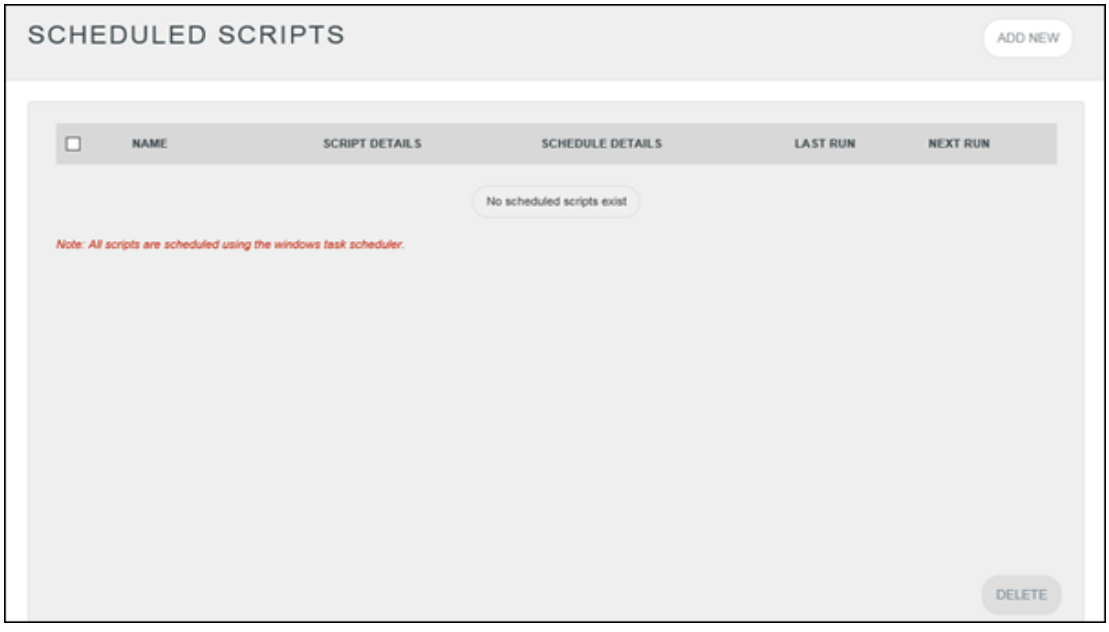


Figure 4

3. Select the **Add New** button.

Script scheduler window displays.

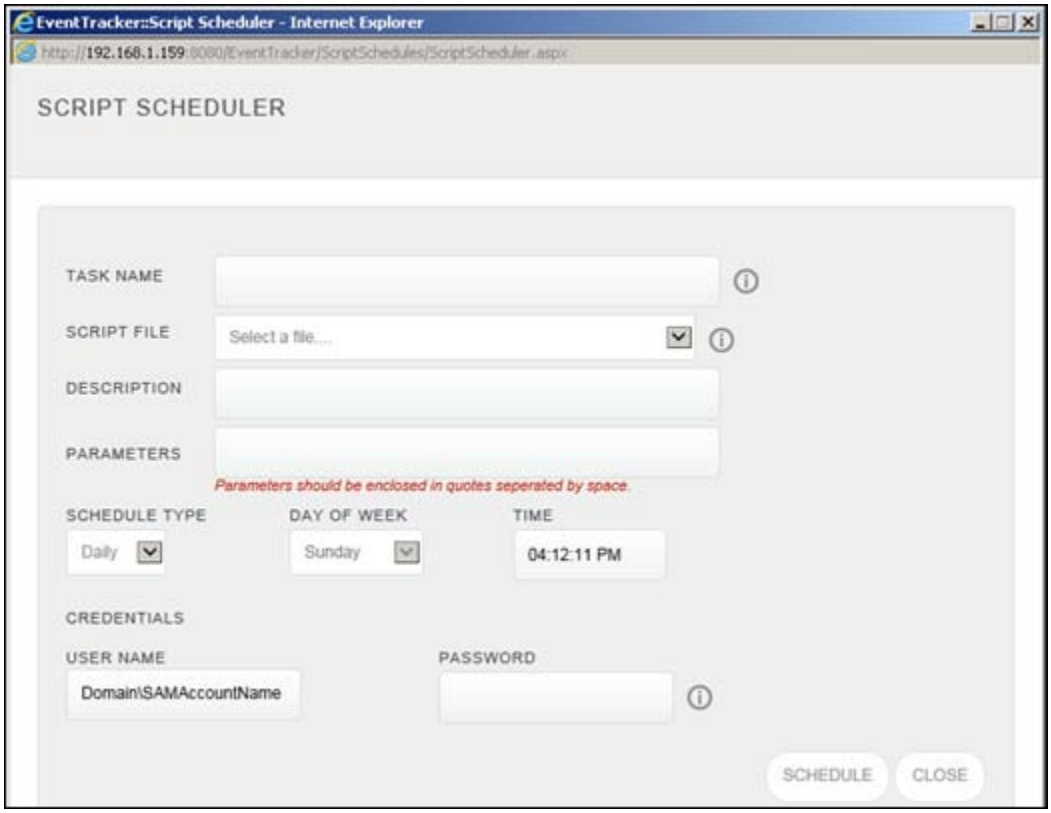


Figure 5

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 Active Watch List.

Verify the imported entities in Active Watch List

1. Select the **Admin** menu and then select **Active Watch List**.

Active Watch List page displays.

2. In **IP Address** group, select **DshieldBlockList**.

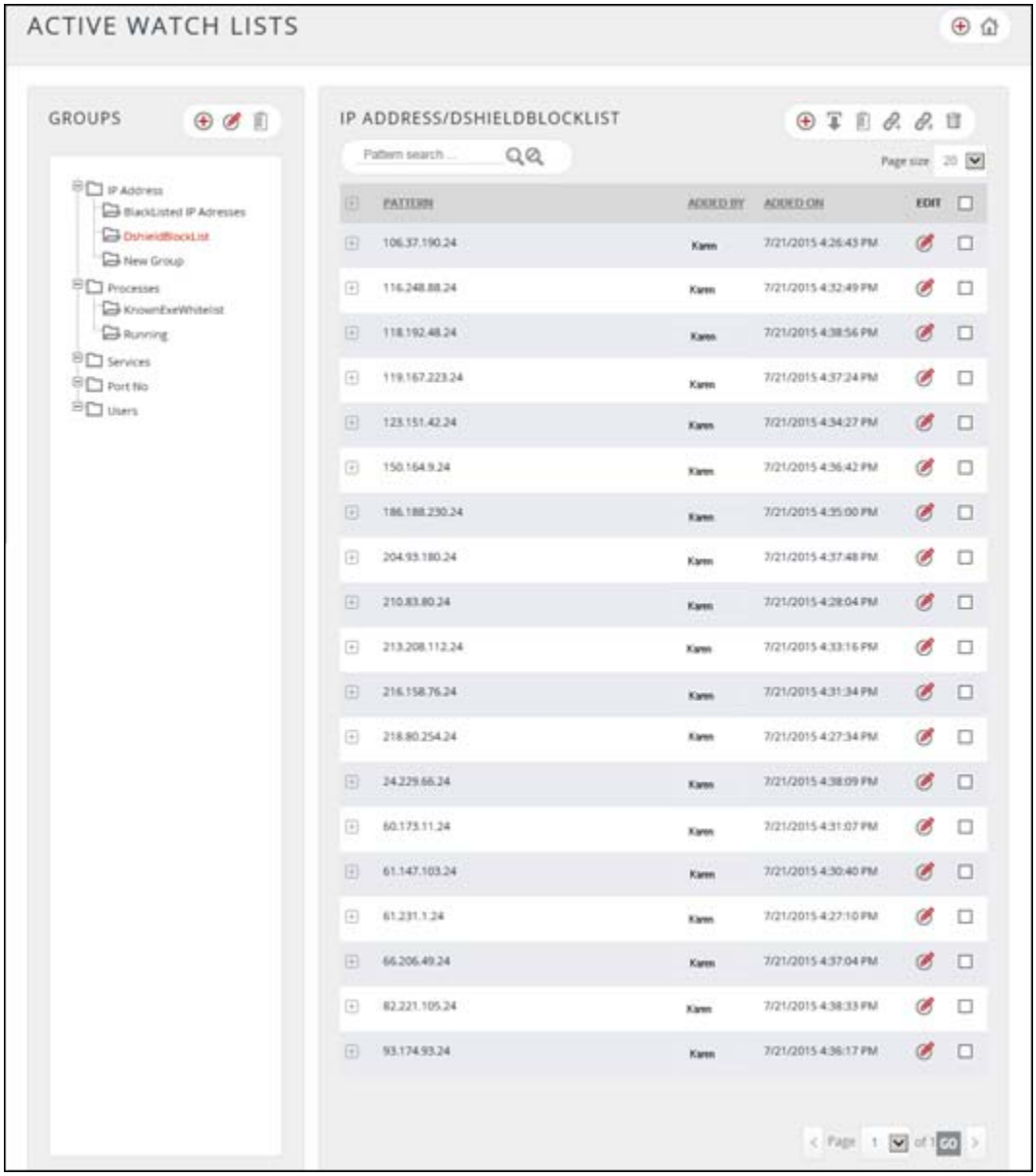


Figure 6

3. In **Port No** group, select **DshieldTrojanportlist**.

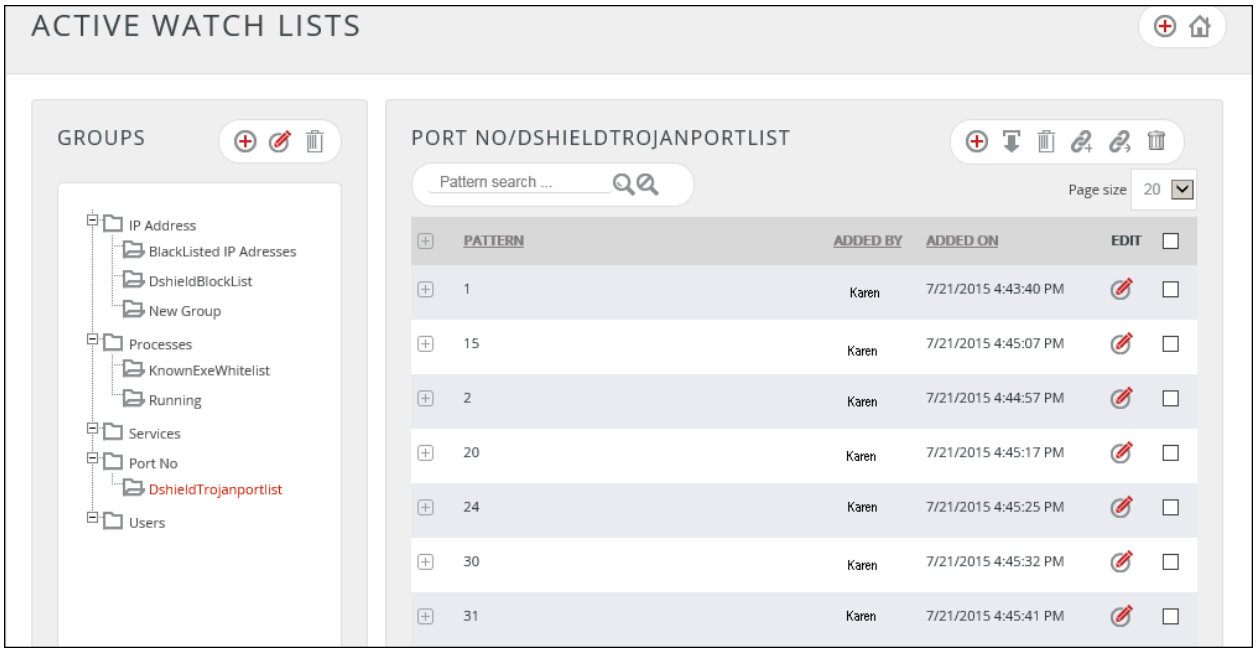

ACTIVE WATCH LISTS
GROUPS
IP Address
BlackListed IP Adresses
DshieldBlockList
New Group
Processes
KnownExeWhitelist
Running
Services
Port No
DshieldTrojanportlist
Users
PORT NO/DSHIELDTROJANPORTLIST
Pattern search ...
Page size 20
PATTERN
ADDED BY
ADDED ON
EDIT
1 Karen 7/21/2015 4:43:40 PM
15 Karen 7/21/2015 4:45:07 PM
2 Karen 7/21/2015 4:44:57 PM
20 Karen 7/21/2015 4:45:17 PM
24 Karen 7/21/2015 4:45:25 PM
30 Karen 7/21/2015 4:45:32 PM
31 Karen 7/21/2015 4:45:41 PM

Figure 7

Command Line Usage in Active Watch List

To import entities under Active Watch List 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 Active Watch List.

Prerequisites to import list via command prompt

The following prerequisites are necessary to execute and import the entities in Active Watch List 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 Active Watch List

NOTE:

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

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

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

   The respective group is created.

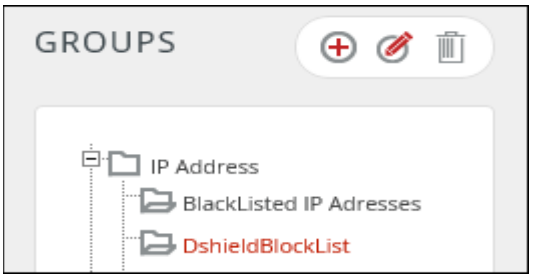
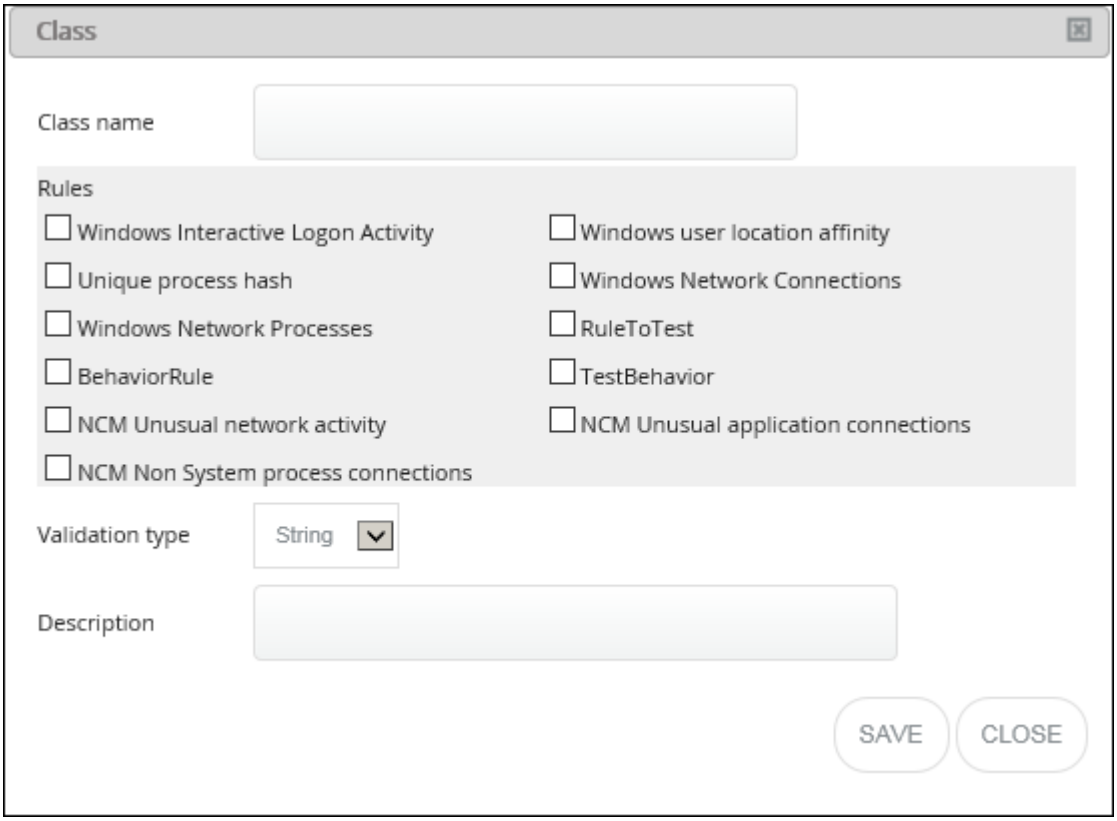


Figure 8

Add a New Class

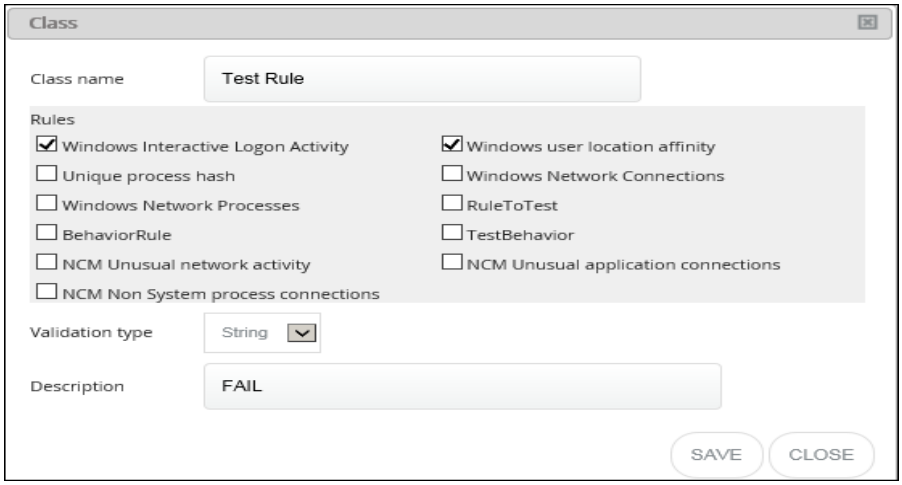
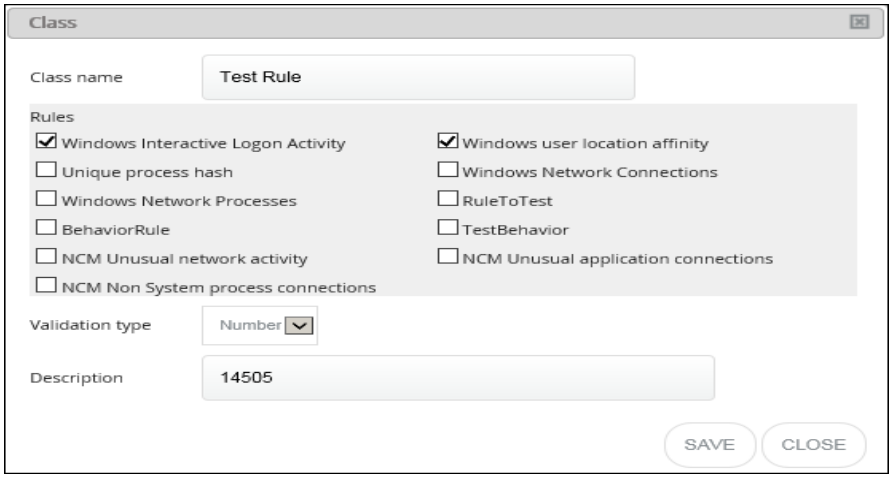
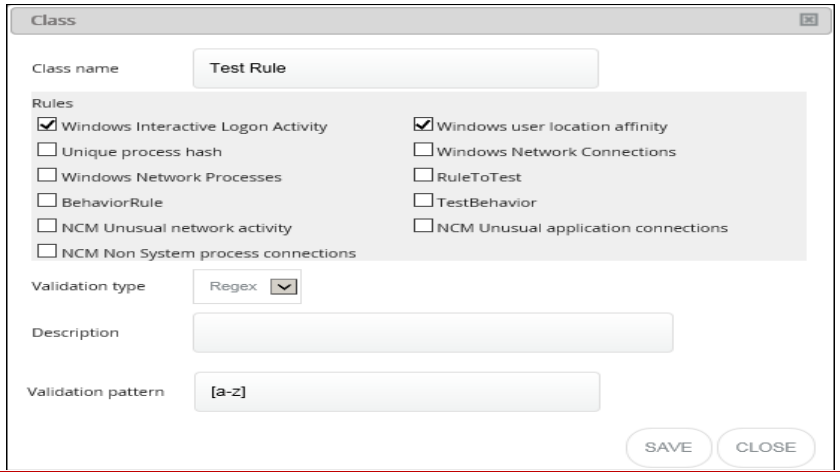
To create a New Class,

- Click the add icon in the right hand corner.
  The Class window gets displayed.



- Enter the Class name and select the Behavior Rule(s) checkbox to be mapped with the class.

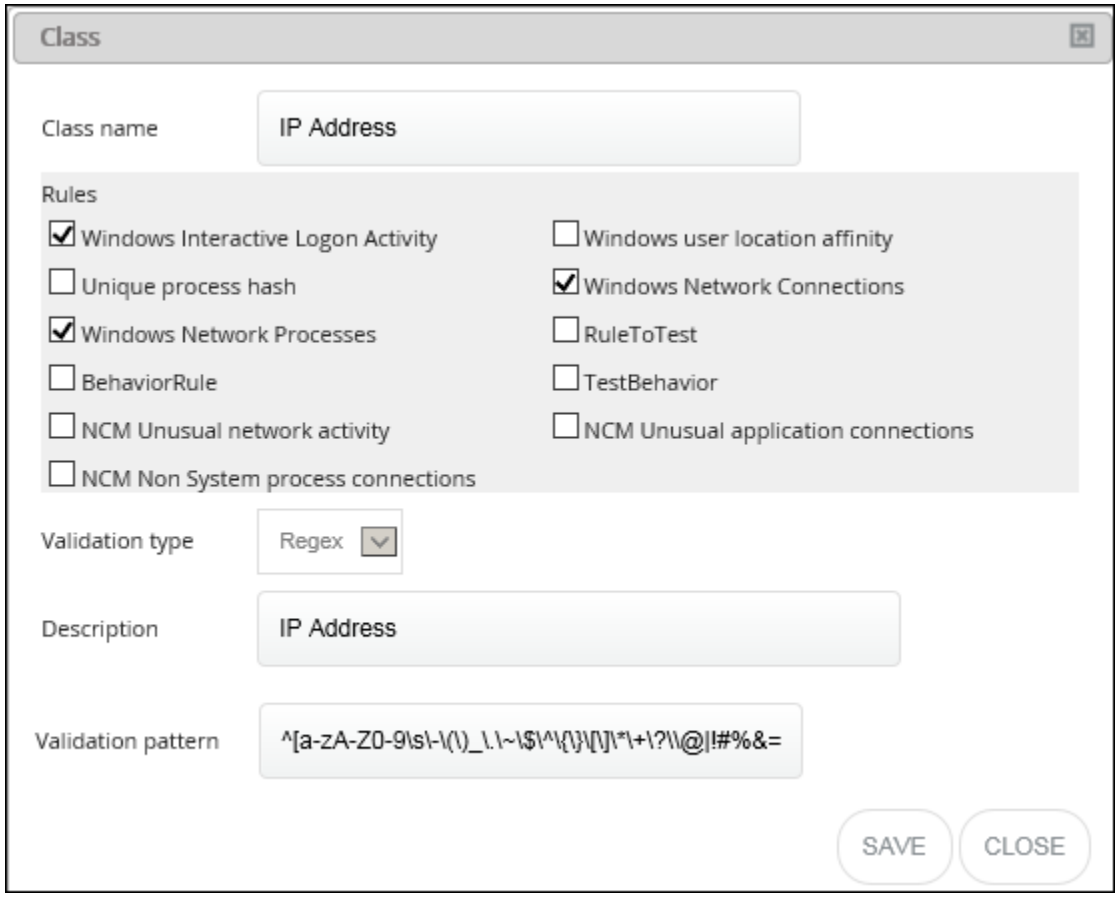
- Select the Validation Type from the dropdown list.

Field	Description
String	**A String can be selected. Ex: FAIL** 
Number	**A Number can be selected. Ex: 14505** 
Regex	**A Regular Expression can be selected. Ex: [a-z]** 

Edit an Existing Class

To edit or modify an existing class,

- Select the class and click the edit icon in the top right hand side corner.
  The edit class window gets displayed.



- Make the changes required and click the **Save** button.

Usage of Command Line parameters

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

Parameter No	Description	Example	
	Prism.ListImportUtility.exe	The file to be executed.	
1	Class name within double quotes	"IP Address" / "Services" / "Port No" /"Processes"	
2	Group name within double quotes	Any alphanumeric characters. Ex: 1abc, blacklisted port. The following special characters are not allowed (i.e. @*^/,:(%)[]$#="<>'|).	
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.
12	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 Active Watch List UI.

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.

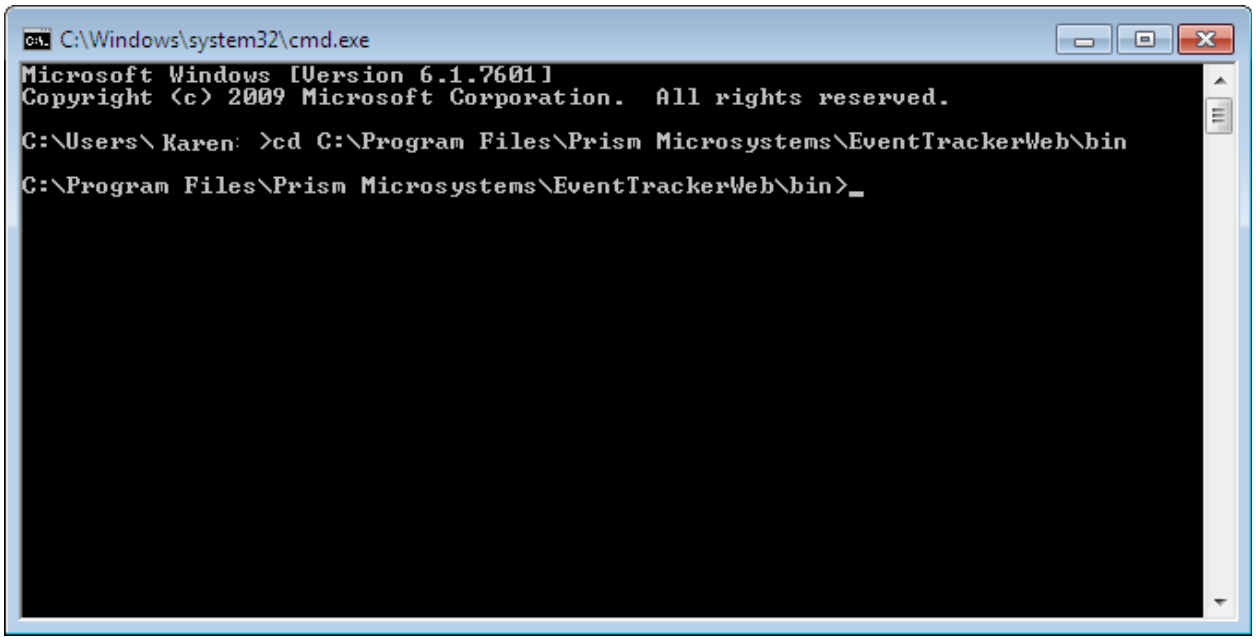


Figure 9

4. Pass the parameters in command prompt as shown below

   Example1:

   In this example below, a group has to be created in Active Watch List 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" "" "" "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.

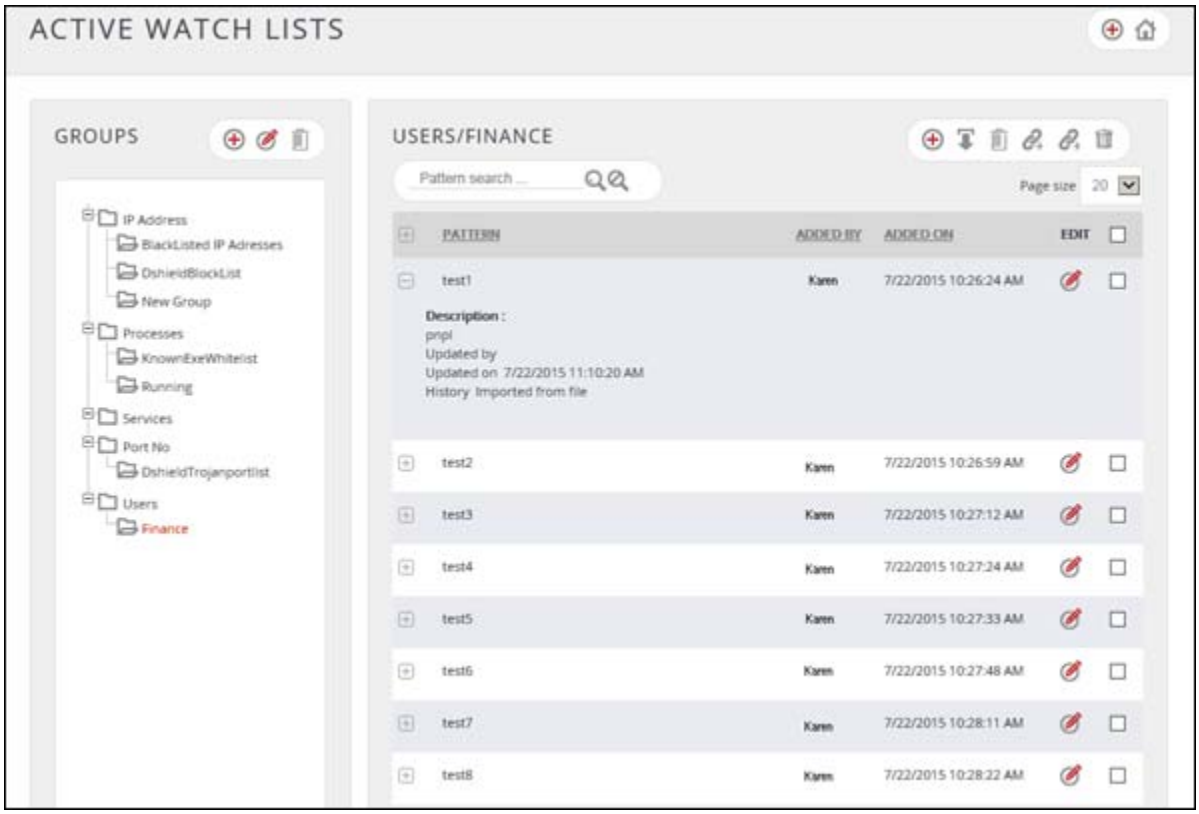


Figure 10

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 Active Watch List UI.

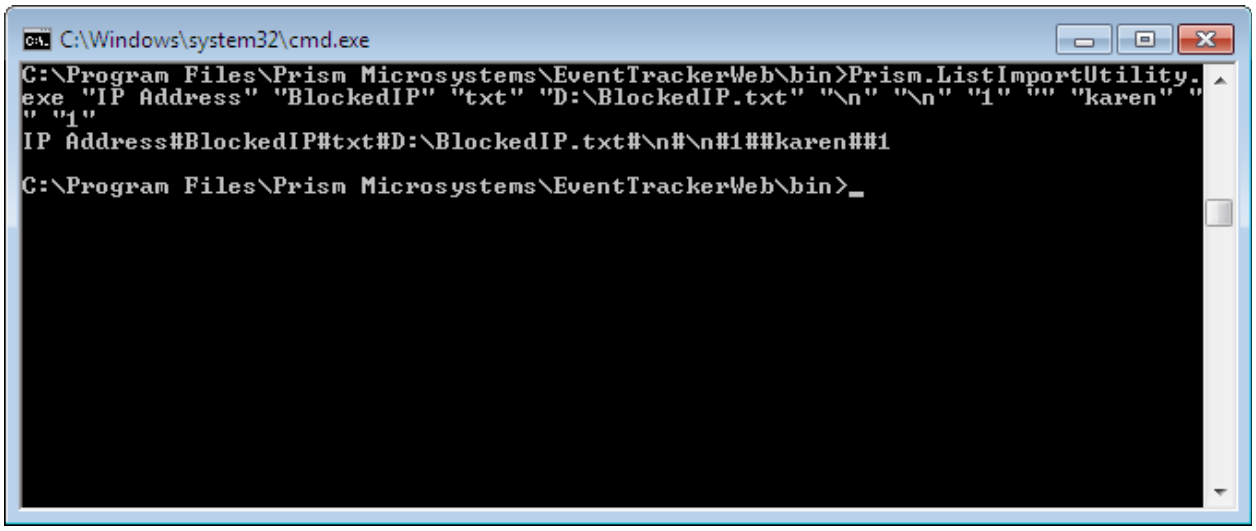


Figure 11

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 Active Watch List UI.

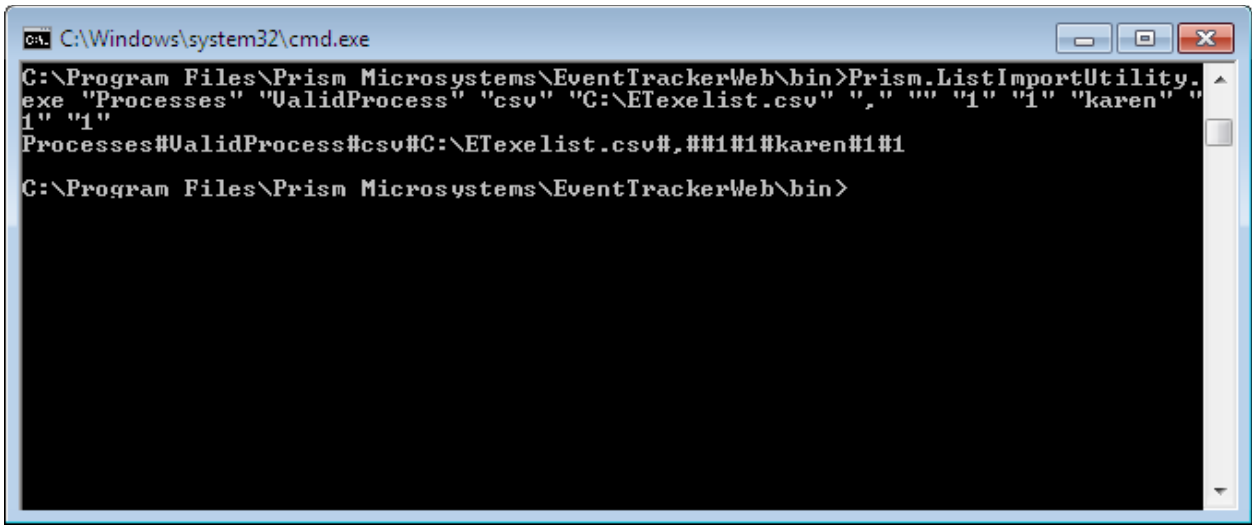


Figure 12

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 Active Watch List UI.

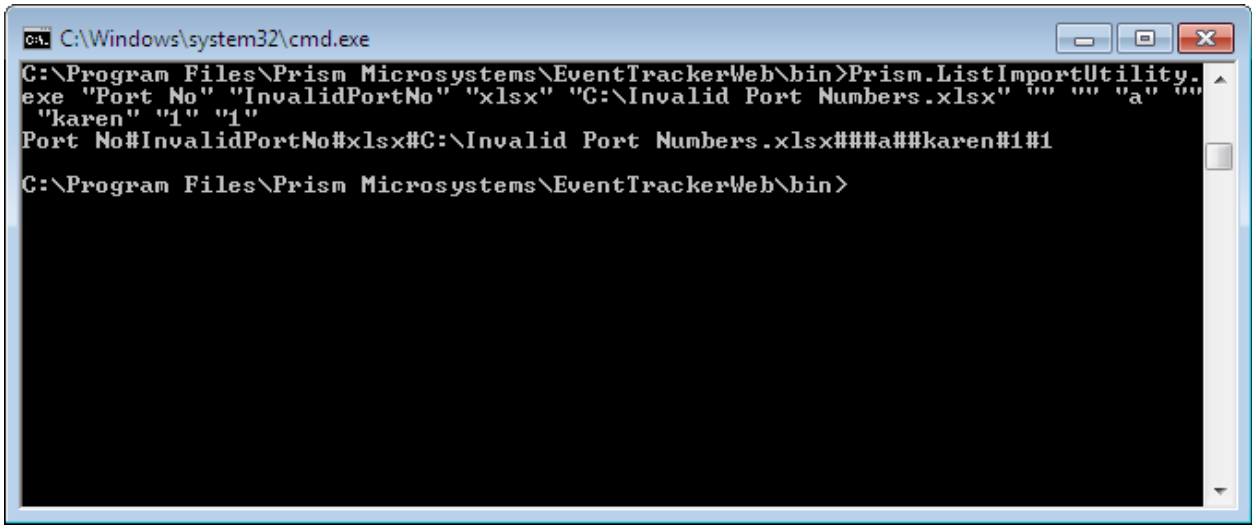


Figure 13

Verify the imported entities in Active Watch List UI

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

Manual Import of Active Watch List

Please refer EventTracker Enterprise v8.0 User Guide – Chapter 20 Active Watch List.

Usage of Active Watch List

This section describes the usage of Active Watch List 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 Active Watch List under **Class** '**Port No'** with Group Name as '**DshieldTrojanportlist**' as described in Create Group.

   The respective blocked port numbers should be listed in Active Watch List.

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.

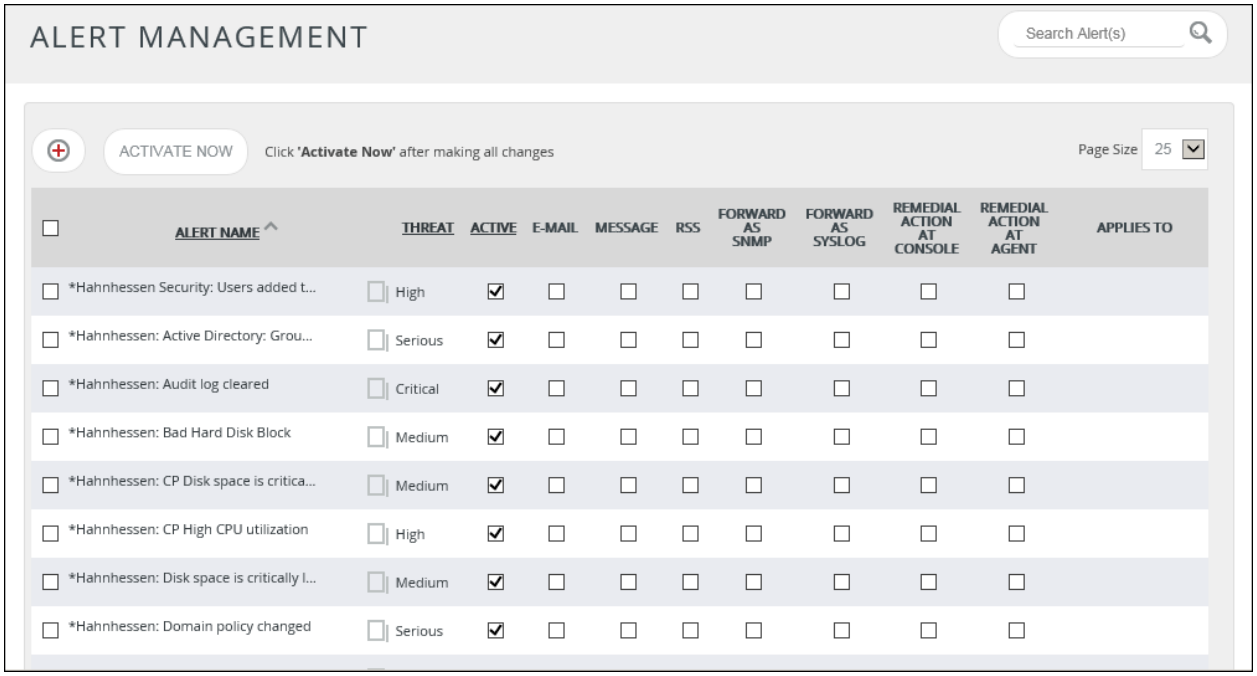


Figure 14

3. Select the **Add Alert** icon .

EventTracker displays the **Alert configuration** page.

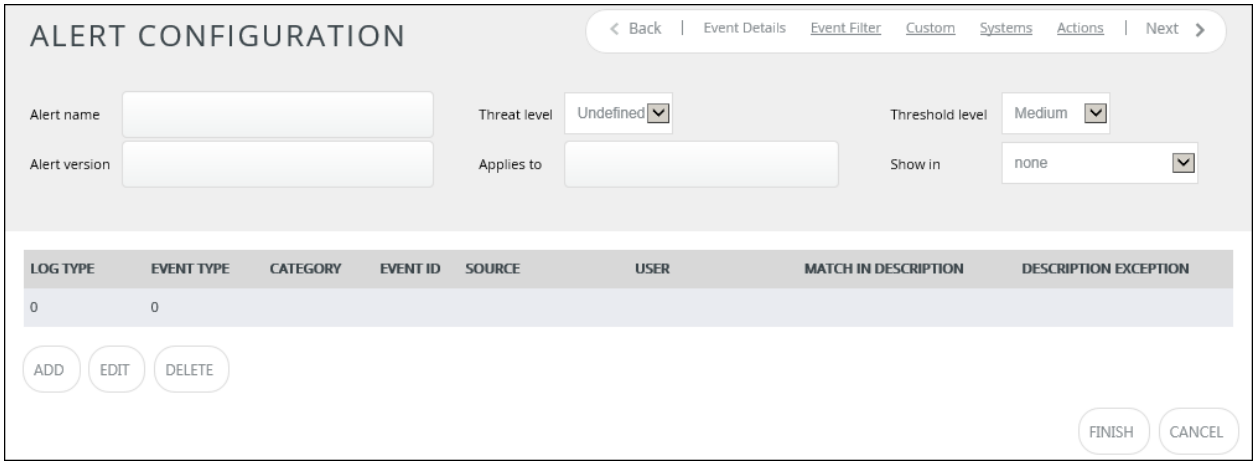


Figure 15

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.

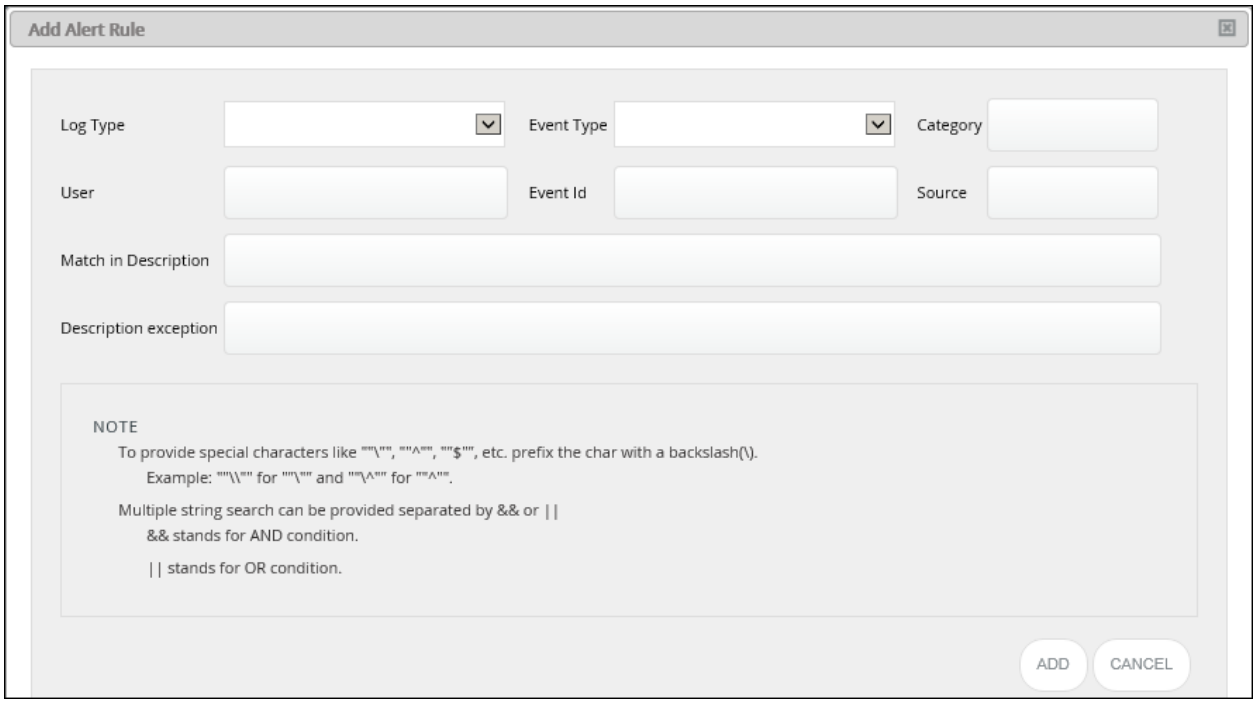


Figure 16

9. Enter **Source:** as **"syslog"**.

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

11. Select the **Add** button.

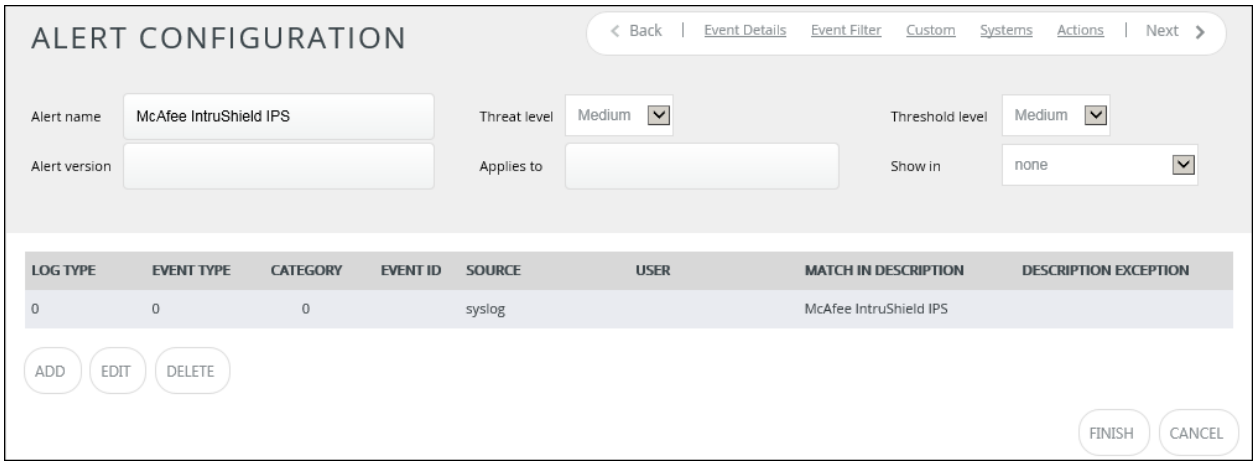


Figure 17

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).

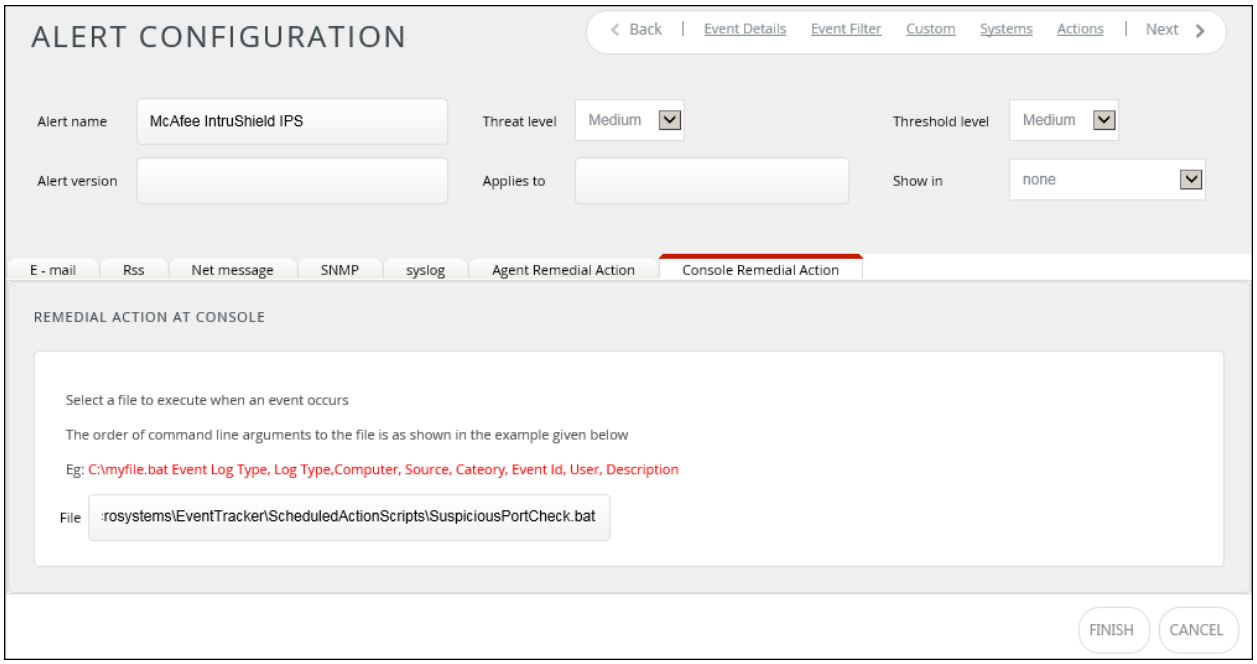


Figure 18

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:

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:

Event Id: 123
Source: Syslog
Event type: Information
User: Karen

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.

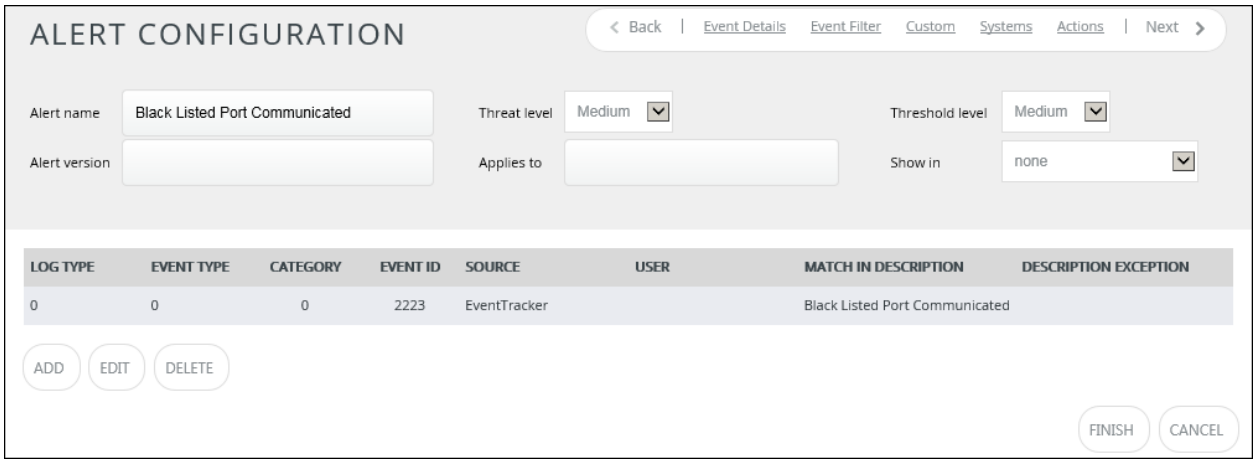


Figure 19

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.

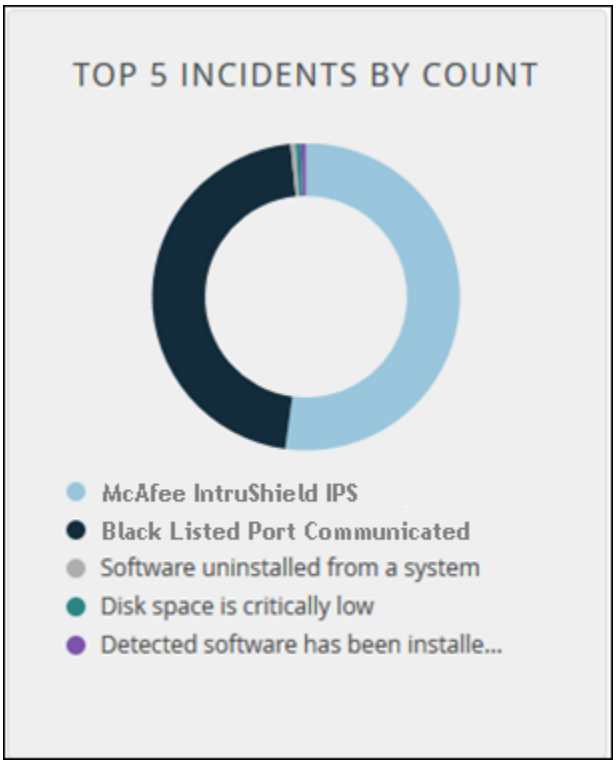


Figure 20

Monitor Behavior Activity Dashboard

Active Watch List 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 Active Watch List 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** donut chart to view behavior details for IP address activities.

   (OR)

   In **View details for** dropdown, select **IP Address Activity** option and then click GO icon.

   EventTracker displays the '**Enterprise Activity Detail'** page.

   By default, **IP Class** dropdown displays all IP addresses.

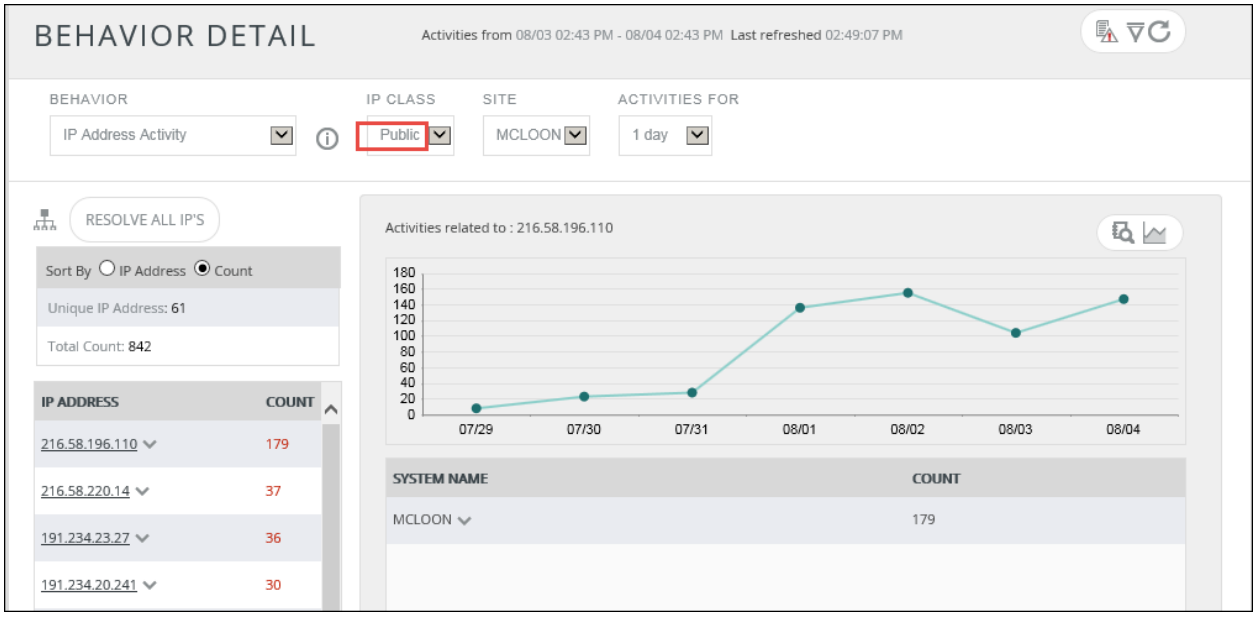


Figure 21

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.

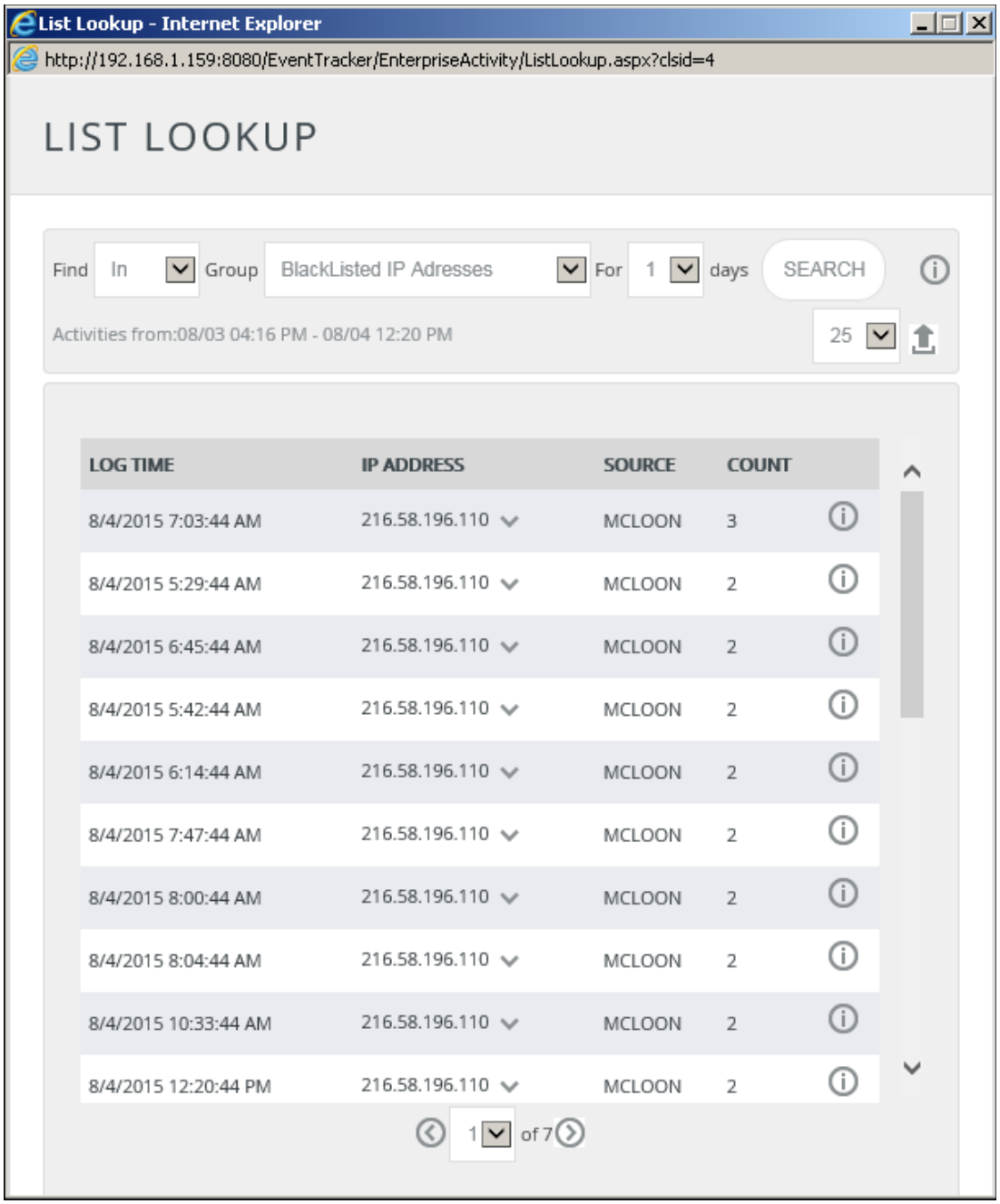


Figure 22

6. If you select '**In**' from **Find:** drop down, the processes that are found in Active Watch List

group displays.

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

8. To view IP Addresses that are not available in Active Watch List, select **Not in** from **Find:** drop down.

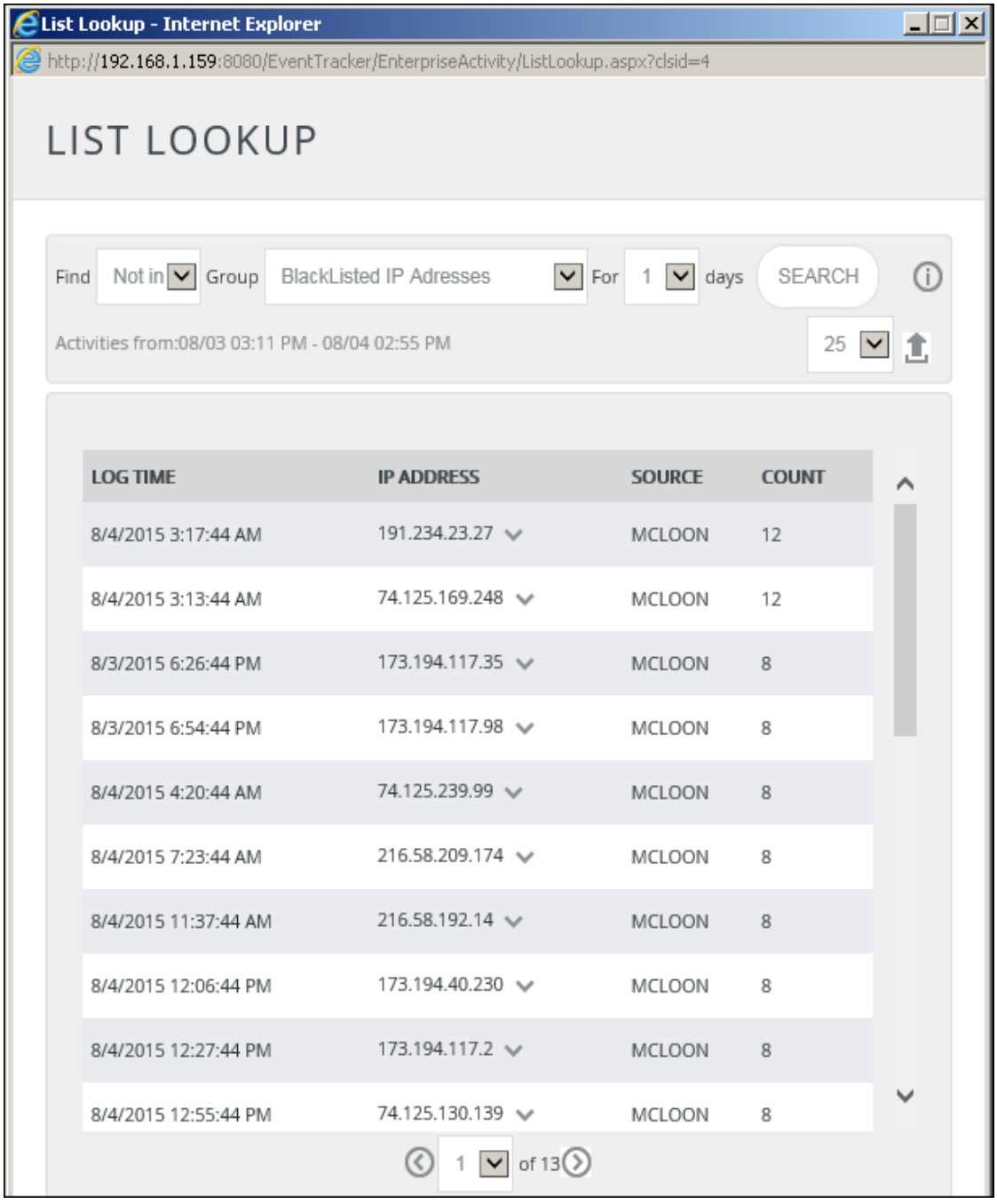


Figure 23

Monitor Process Activity

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

1. Create the respective group in Active Watch List 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 details for** dropdown, select **Windows Process Activity** option, and then click 

icon.

   EventTracker displays the '**Enterprise Activity Detail**' page.

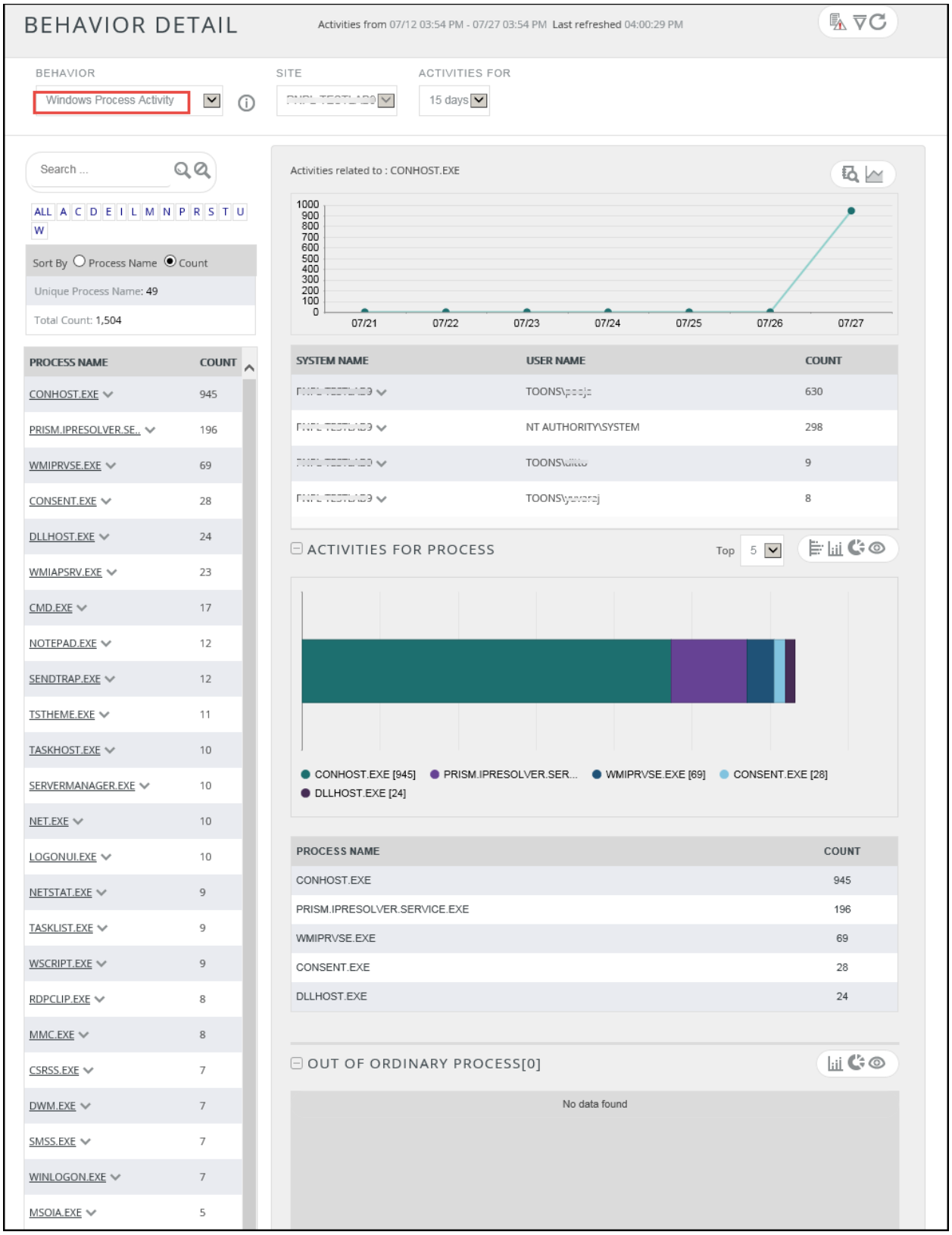

BEHAVIOR DETAIL
Activities from 07/12 03:54 PM - 07/27 03:54 PM Last refreshed 04:00:29 PM
BEHAVIOR
Windows Process Activity
SITE
ACTIVITIES FOR
15 days
Search ...
ALL A C D E I L M N P R S T U W
Sort By Process Name Count
Unique Process Name: 49
Total Count: 1,504
PROCESS NAME COUNT
CONHOST.EXE 945
PRISM.IPRESOLVER.SE.. 196
WMIPRVSE.EXE 69
CONSENT.EXE 28
DLLHOST.EXE 24
WMIAPSRV.EXE 23
CMD.EXE 17
NOTEPAD.EXE 12
SENDTRAP.EXE 12
TSTHEME.EXE 11
TASKHOST.EXE 10
SERVERMANAGER.EXE 10
NET.EXE 10
LOGONUI.EXE 10
NETSTAT.EXE 9
TASKLIST.EXE 9
WSCRIPT.EXE 9
RDPCLIP.EXE 8
MMC.EXE 8
CSRSS.EXE 7
DWM.EXE 7
SMSS.EXE 7
WINLOGON.EXE 7
MSOIA.EXE 5
Activities related to : CONHOST.EXE
1000 900 800 700 600 500 400 300 200 100 0
07/21 07/22 07/23 07/24 07/25 07/26 07/27
SYSTEM NAME USER NAME COUNT
TOONS\ 630
NT AUTHORITY\SYSTEM 298
TOONS\ 9
TOONS\ 8
ACTIVITIES FOR PROCESS
Top 5
CONHOST.EXE [945] PRISM.IPRESOLVER.SER... WMIPRVSE.EXE [69] CONSENT.EXE [28]
DLLHOST.EXE [24]
PROCESS NAME COUNT
CONHOST.EXE 945
PRISM.IPRESOLVER.SERVICE.EXE 196
WMIPRVSE.EXE 69
CONSENT.EXE 28
DLLHOST.EXE 24
OUT OF ORDINARY PROCESS[0]
No data found

Figure 24

4. Click **ListLookup** icon to view malicious processes that can harm the system.

   ListLookup window displays.

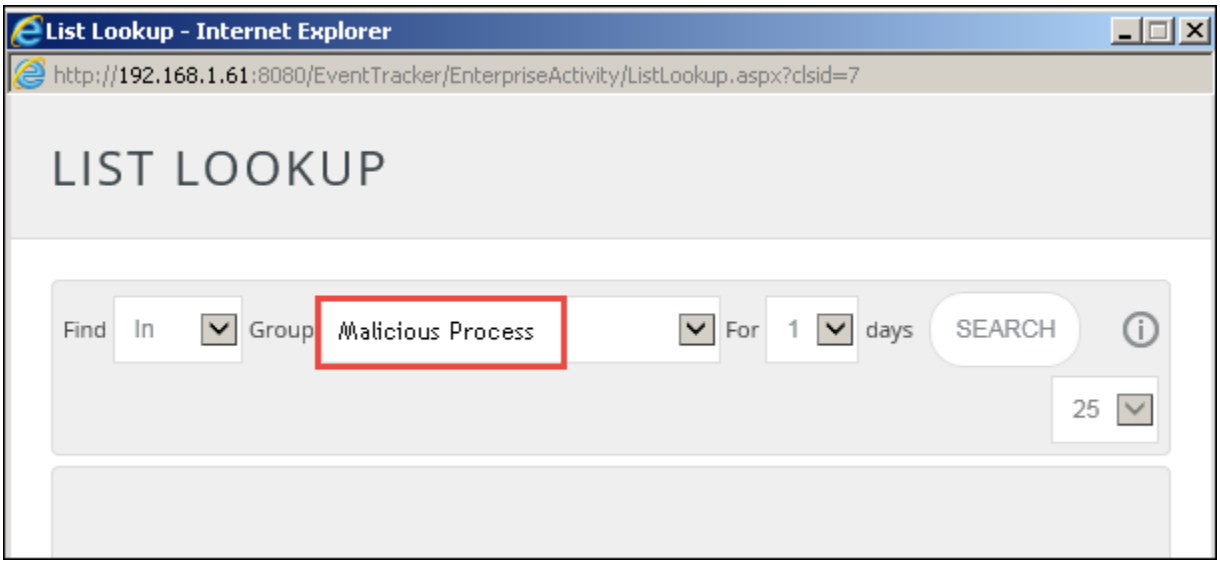


Figure 25

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 Active Watch List group displays.

6. Select the **Search** button.

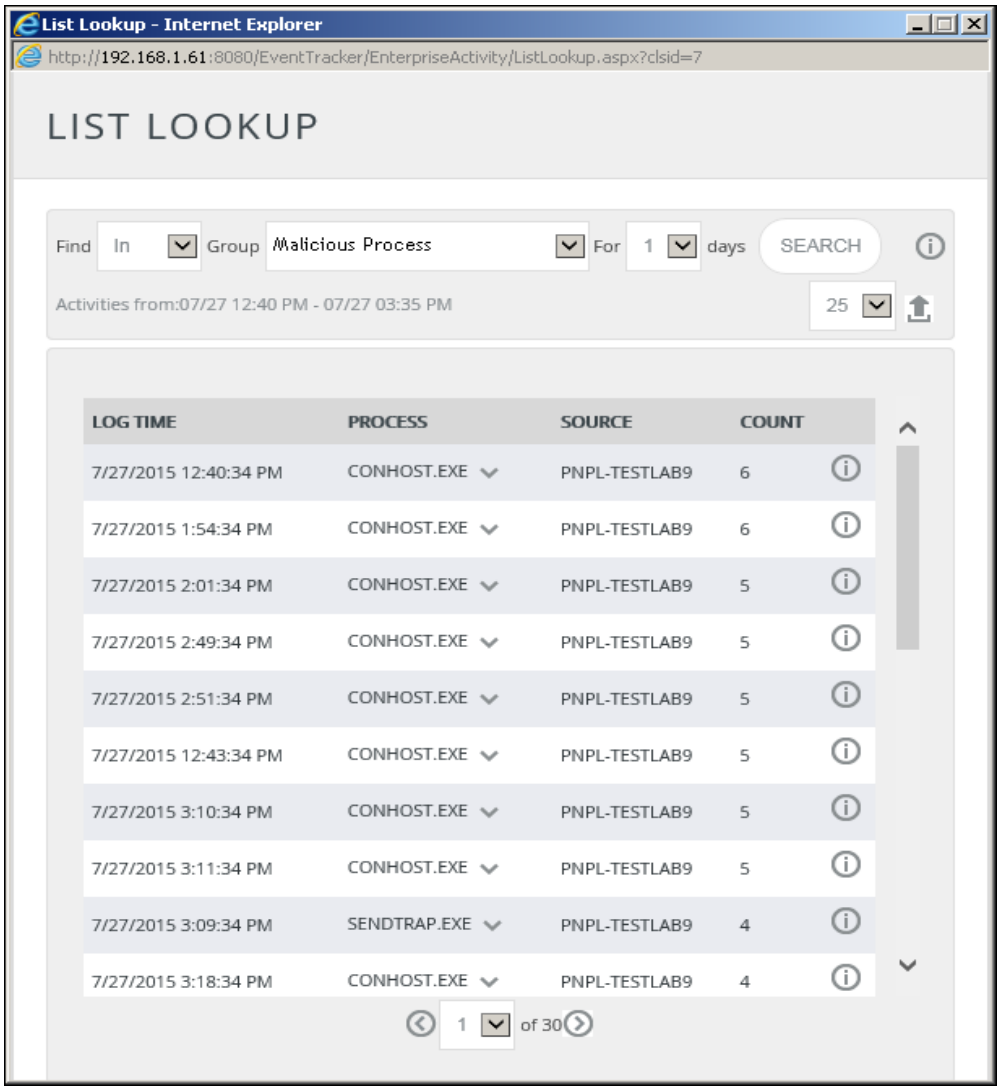


Figure 26

7. Click **Information** ⓘ icon to view additional information.

Figure 27

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 Active Watch List group display.

9. Select the **Search** button.

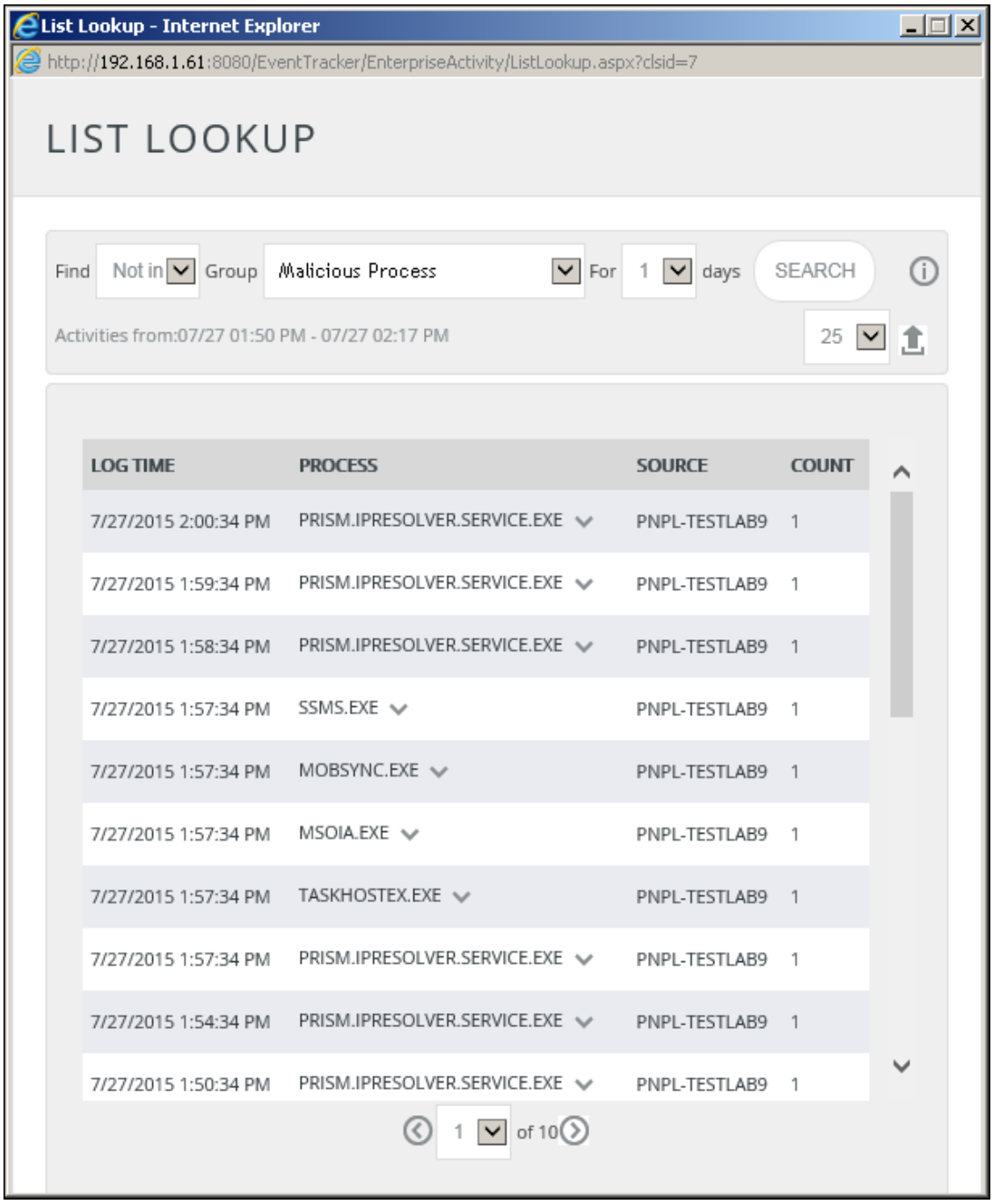


Figure 28

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.

b. Edit the UnauthorizedFileAccess.bat and UnauthorizedFileAccess.vbs files.

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=.\sqlexpress) and GroupName.

1. Create an alert as described in Create alert with **Source:** as"**Microsoft-Windows-Security-Auditing"** and **Event Id:** as"**5145**".

   NOTE:

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

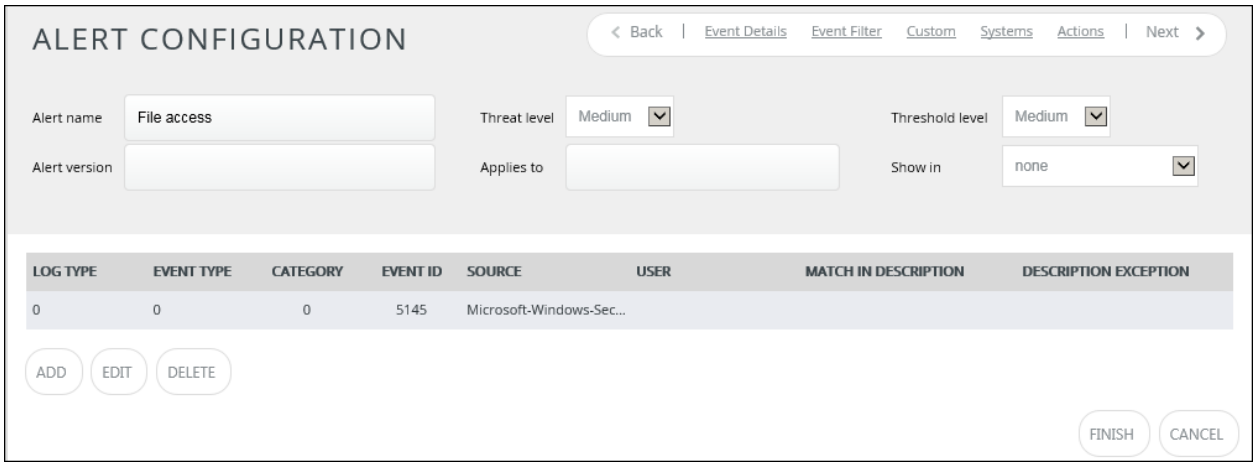


Figure 29

2. In **Console Remedial Action,** enter the correct path of the file.

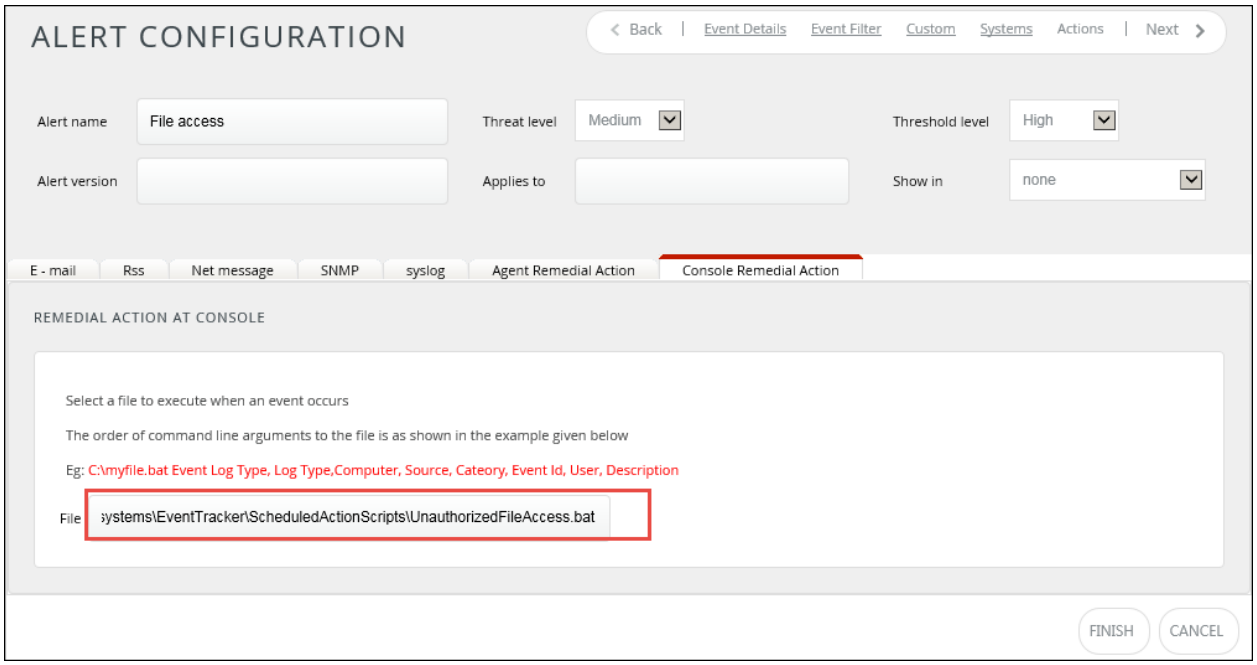


Figure 30

3. Similarly create another alert with the **Event Id** as **2220** and activate the alert.

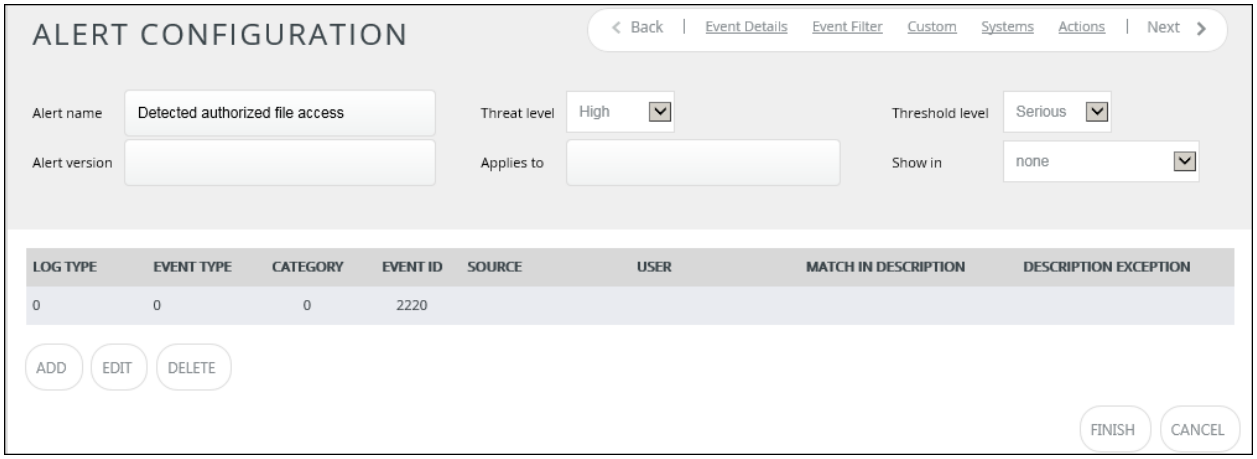


Figure 31