Configure IP reputation lookup
How to - Configure IP reputation lookup

About this Guide:

Services such as Reputation Authority (a free service from Watchguard) maintains a database of public IP addresses and associate a reputation score for each, based on observed activity. Resources inside the network may initiate or accept TCP network connections originating from public IP addresses. EventTracker can lookup public IP addresses contained within log entries against this list and generate alerts if a connection is made to a low reputation public address. When properly tuned, these alerts can be useful for IT Security personnel, to focus on possible attacks.

This guide will help the EventTracker Administrators to configure IP reputation lookup using the Watchguard Reputation Authority service. This configuration will check the reputation score of the new IP address detected by EventTracker IP activity monitoring feature and will provide overall reputation details like Reputation Score, Reverse DNS, ISP Location and % of specific type of data sent from that specific IP address.

Scope:

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.X and later.

Audience:

IT/Security or network administrators who is responsible for monitoring and maintaining the security of the network.

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. © 2014 Prism
Table of Contents:

About this Guide: ......................................................................................................................................... 1
Scope: ............................................................................................................................................................ 1
Audience: ...................................................................................................................................................... 1
Introduction: ................................................................................................................................................. 3
Pre-requisite: ................................................................................................................................................ 4
Setting up IP reputation lookup: ................................................................................................................ 6
  Preparing Scripts for use as per your environment ..................................................................................... 6
  Import Alert to Perform Remedial Action in EventTracker ................................................................. 6
  Import Scheduled Reports: ..................................................................................................................... 9
  Import Token Value: .............................................................................................................................. 11
  Configuring Remedial Action for Alerts ............................................................................................... 12
  Configure Scheduled Reports ............................................................................................................... 18
Verify Alerts and Reports ......................................................................................................................... 24
Tuning Alerts and Reports ......................................................................................................................... 26
Introduction

Services such as Reputation Authority (a free service from Watchguard) maintain a database of public IP addresses and associate a reputation score for each based on observed activity. Resources inside the network may initiate or accept TCP network connections originating from public IP addresses. EventTracker can lookup public IP addresses contained within log entries against this list and generate alerts if a connection is made to a low reputation public address. When properly tuned, these alerts can be useful to focus IT Security personnel on possible attacks.

EventTracker alerts IT/Security administrators whenever any network activity is detected in network from or to IP address which has bad reputation score. It provides detailed information about Local system, Port, Process, User and Remote ip address with detailed description of the log where bad reputation ip connection is detected.

Example uses:

- Connection establishment from inside the network to a low reputation outside IP address, a hallmark of virus or trojans.

- Mail server hosted in DMZ accept connections on the SMTP port (25) from low reputation public IP address may attempt to use the mail server as open relay to send spam.

EventTracker alerts and provide reports if any such activity is detected in network so that the administrators can act on that immediately and take proper action.
Pre-requisite

- EventTracker v7.x should be installed with the behavior option enabled
- Windows PowerShell 3.0 and later must be installed. To check the PowerShell version:
  - Launch Windows PowerShell as Administrator.
  - Run command $PSVersionTable.PSVersion
- Script Execution policy must be set to Unrestricted.
  - To change PowerShell execution policy,
    - Launch Windows PowerShell as Administrator.
    - Run command ‘Set-ExecutionPolicy Unrestricted’.
    - Make sure you do this for both x86 and x64 versions.
- Connection to the internet from EventTracker server.
- Network Connection monitoring should be enabled in EventTracker (Windows systems).
How it works?

The Behavior option in EventTracker, maintains lists of previously observed elements including IP v4 address, usernames, systems, USB serial numbers etc. IP addresses contained in log entries are extracted and compared with this list. If the IP address is ‘new’ i.e., not on the list, then a ‘New Activity – IP Address” alert is generated.

This package configures a ‘remedial action’ for such New Activity – IP Address alerts, which look up the IP reputation score of the new public IP address. If the reputation score is higher than 50, a bad-reputation alert is generated with detailed information.

IP address reputation info is queried from http://www.reputationauthority.org
Setting up IP reputation lookup:

Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the IPReputationLookupScript pack.
- Save IPReputationLookupScript.zip (saved to d:\IPReputationLookupScript\ folder in the example below).
- Extract .ps1 file to d:\IPReputationLookupScript\.
- Files in the package are shown below

<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventTracker-Bad reputation IP network connection report.issch</td>
</tr>
<tr>
<td>EventTracker-Bad IP reputation lookup alerts.isalt</td>
</tr>
<tr>
<td>IPReputationLookupScript.ps1</td>
</tr>
<tr>
<td>EventTracker-IP reputation lookup tokens.istoken</td>
</tr>
</tbody>
</table>

Import Alert to Perform Remedial Action in EventTracker

To Import Alert for performing Remedial Action,

- Go to EventTracker Control Panel.
- Select the Export Import Utility feature as displayed in the figure below:
For importing the alert Eventtracker: New ip activity-IP Reputation lookup, select the **Alerts** Option.

![Figure 2](image)

![Figure 3](image)
• Provide the path name and file name of the Alert file.

• For this, click the icon and browse the Alert File i.e. EventTracker-Bad IP reputation lookup alerts from your system and click **Open**.

![Figure 4](image)

Figure: 4

• Now, click the **Import** button.

![Figure 5](image)

Figure: 5
• The success message box of ‘Selected alert configurations imported ‘will be displayed.

![Image](image.png)

Figure 6

• Click OK.

The two Alerts will be imported namely:

1. Eventtracker: New ip activity-IP Reputation lookup
2. EventTracker: Detected New Bad Reputation IP activity

Import Scheduled Reports:

To Import Scheduled Reports, follow the same process:

• Select **Scheduled Report** from the Export Import Utility Window.

![Image](image.png)

Figure: 7
- Provide the path and file name of the scheduled report file i.e. EventTracker-Bad reputation IP network connection report by browsing the Report file from your system.

- Open the Report file and click the **Import** button.
The report file EventTracker-Bad reputation IP network connection report will be successfully imported.

**Import Token Value:**

For importing Token Values:

- Select the **Token Value** Option.

  ![Figure: 10](image)

- Provide the path and file name of the Token value file EventTracker-IP reputation lookup tokens.

  ![Figure: 11](image)
• Open the Token Value file and click the **Import** button.

![Import Utility Window](image)

**Figure: 12**

The Token Value file EventTracker-IP reputation lookup tokens will be successfully imported.

---

### Configuring Remedial Action for Alerts

- Go to EventTracker
- Click **Admin** dropdown and click **Alerts**. EventTracker displays the **Alert Management** page.
• Enter the Alert Name Eventtracker: New ip activity-IP Reputation lookup in the Search box.

• Click the Go button. The Alert Name with specified details will be displayed.

• Click on the alert Eventtracker: New ip activity-IP Reputation lookup hyperlink to make changes in the Alert Configuration.
• Click the **System** hyperlink to choose the EventTracker Manager system. In the figure shown below, the example is taken for the local machine i.e. McLOON

For assigning Remedial Action based on a particular Alert,

• Click the **Action** hyperlink and then click the **Console Remedial Action**.

**NOTE:** To assign remedial action for the first alert, the user must select the **Console Remedial Action**.
• Enter the file name with the mentioned path as shown below:

"C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe" -File "D:\IPReputationLookupScript\IPReputationLookupScript.ps1"

**NOTE:** In case if you have stored script in different path, replace d:\IPReputationLookupScript\ with the path where you have stored the script

• Click the **Finish** button.
• Now click the **Active Now** button after confirming all the changes made and activate the Alert Eventtracker: New ip activity-IP Reputation lookup.
Similarly, for configuring the alert Detected New Bad Reputation IP activity,

- Enter the alert name Detected New Bad Reputation IP activity in the Search box and click the Go button.

![Figure 19](image)

- Click on the Detected New Bad Reputation IP activity hyperlink.

![Figure 20](image)

- The Alert Configuration dialog box displays.
- Select the EvenTracker Manager system by clicking the hyperlink Systems

Here, in the figure below, the McLOON system is selected.
• For assigning action, click the **Action** button and choose E-mail Configuration, to generate an e-mail for the alert.

• **Click Finish.**
How to - Configure IP reputation lookup

1. Click **Activate Now** button to activate the alerts.

Configure Scheduled Reports

To assign remedial action to Scheduled Reports,

- Go to EventTracker
- Click on **Reports** and select the **Configuration** option from the dropdown box
- Select the **Scheduled** option

The Report file (EventTracker-Bad IP Reputation Network connections report) is displayed.
• Click the hyperlink **EventTracker-Bad IP Reputation Network connections report** for configuring changes.

![EventTracker:: Flex Report Wizard window](image)

**Figure: 25**

The **EventTracker:: Flex Report Wizard** window displays

• Click on **Next** to continue the steps.

![EventTracker:: Flex Report Wizard window](image)

**Figure: 26**
• Click on the **Next** option to continue.

![Image of a dropdown box with Systems selected](image1.png)

**Figure: 27**

• From the drop down box select **Systems** and click on your EventTracker Manager System name. Here, the local system McLOON is selected.

• Click **Next**.

![Image of a report duration selection](image2.png)

**Figure: 28**

• Select the duration or time range of the report and click **Next**.
How to - Configure IP reputation lookup

- Select Rules (if required) to display and click **Next**.

- Add specific details, if you want to narrow down your criteria and click **Next**.
• Enter Title and Description and click Next.

• Review the cost details, configure the publishing options and click Next.
• Enter the Retention Period and click Next.

• A message box displays notifying the disk space needed, which depends on the retention period selected.
• Click Ok and then click Next.
How to - Configure IP reputation lookup

Verify Alerts and Reports

- Click on the Schedule button.
  The process of configuring report is successfully completed.

- Login to EventTracker web.
- Go to Incidents menu and select Dashboard from the drop down box.
• To view the Alerts in a tabular format, you can click the Tabular option.

![Image](image.jpg)

Figure: 37

• You can also extract the Report files in excel format. Go to Report and select Dashboard.

• Click the icon to extract the excel file for the report.

![Image](image.jpg)

Figure: 38
Tuning Alerts and Reports

Once IP reputation lookup is configured and you receive alerts and reports for few days. You might feel like filtering out few connections which might be false positive, or maybe which you don’t want to get alerted if reputation score is lesser than 75 or so. You may feel that you don’t want to see the alert if it is observed on a specific server.

All this can be done easily by adding filter in Bad reputation alert or reports.

Sample description generated for IP reputation lookup is shown below. You can filter out by adding Filter exception rule by any of the columns listed below.

Network connection established between Contoso-Webserv and 123.192.1.166

Connection Details:-

- Local Address: Contoso-Webserv
- Local Port: 80
- Remote Port: 99786
- User Name: N/A
- Process Name: w3wp.exe
- Process ID: 1012
- Image File Name: c:\windows\systems32\w3wp.exe

Overall Reputation Details:-

- Reputation Score: 60
- ISP Location: Taipei, Tai-wan, Taiwan, Province Of China

Reputation Detail [Email]:-

- Clean: 0%
- Viruses: 0%
- Spam: 0%
- Malformed Messages: 0%
- Suspicious Messages: 0%

Source Description: -