Netsurion | EventTracker®

Anomalous Login Detection in EventTracker

EventTracker v9.3

Publication Date: May 7, 2020

Abstract

This guide will help you to use Anomalous Login Detection feature configured with EventTracker v9.3 and above to identify suspicious activities.

Anomalous Login Detection feature detects intrusion, fraud and fault by the network intruders. The unauthorized entries can be identified based on user name and IP address.

Audience

This guide is intended for all the EventTracker users responsible for investigating and managing the network security. It is assumed that you have EventTracker access and understanding of networking technologies.

Table of Contents

1. Introduction to Anomalous Login

Anomalous Login is a method of attack such as a brute force attack by which the attacker is identifying the user name and password of the system or web page randomly. By generating the user name or password from a remote location, it can be compromised over time. From an unknown source, an attacker can try this by simulating a random number of passwords.

EventTracker agent is introducing a new kind of capability to identify Anomalous Login activity. Anomalous Login identification is based on user name and IP address.

- Prevention
  - Creation of new firewall rules for the Public and Private IP address.
  - Adding the Public and Private IP address to the EventTracker block list.

2. Configuring Anomalous Login Detection

1. Go to EventTracker Agent Configuration-> Network connections -> Advanced.

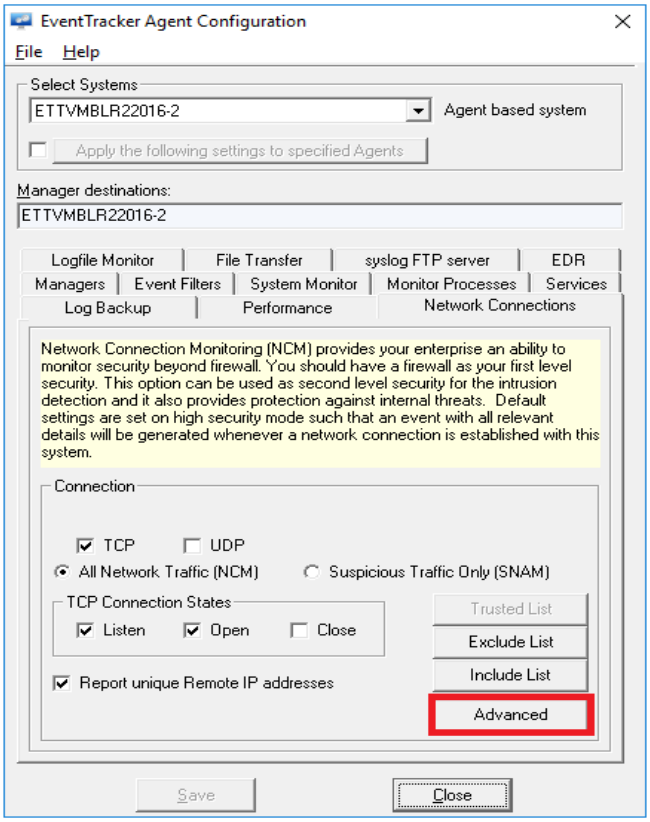

Figure 1

2. **Anomalous Login Detection Configuration** window opens.

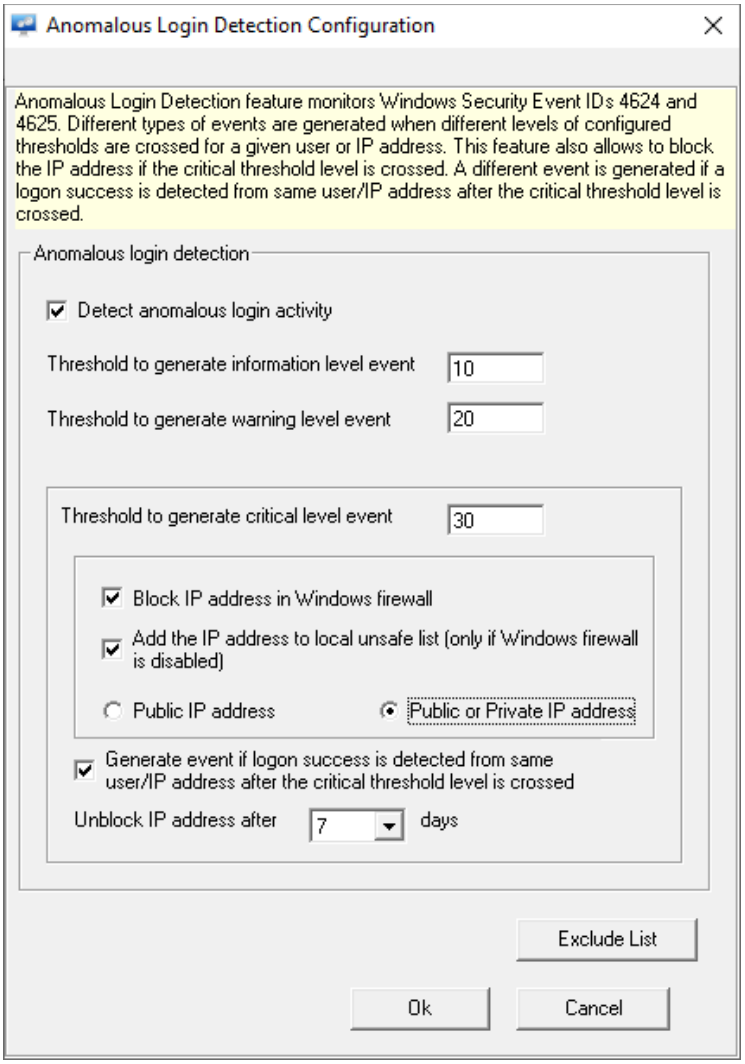

Figure 2

3. Check the option "**Detect anomalous login activity**" to enable Anomalous Login Detection.
   Ensure that the "**Threshold to generate critical level event**" is greater than "**Threshold to generate information level event" and "Threshold to generate warning level event".**

   Note: Anomalous Login Detection feature works for both Public IP addess and Private IP addess according to the options selected, refer figure 3.

4. Event ID 3527 will be generated if logon threshold crosses event levels of information, warning and critical with log levels of information, warning and critical respectively.

NOTE: Anomalous Login Detection will occur only when the threshold crosses the critical level.

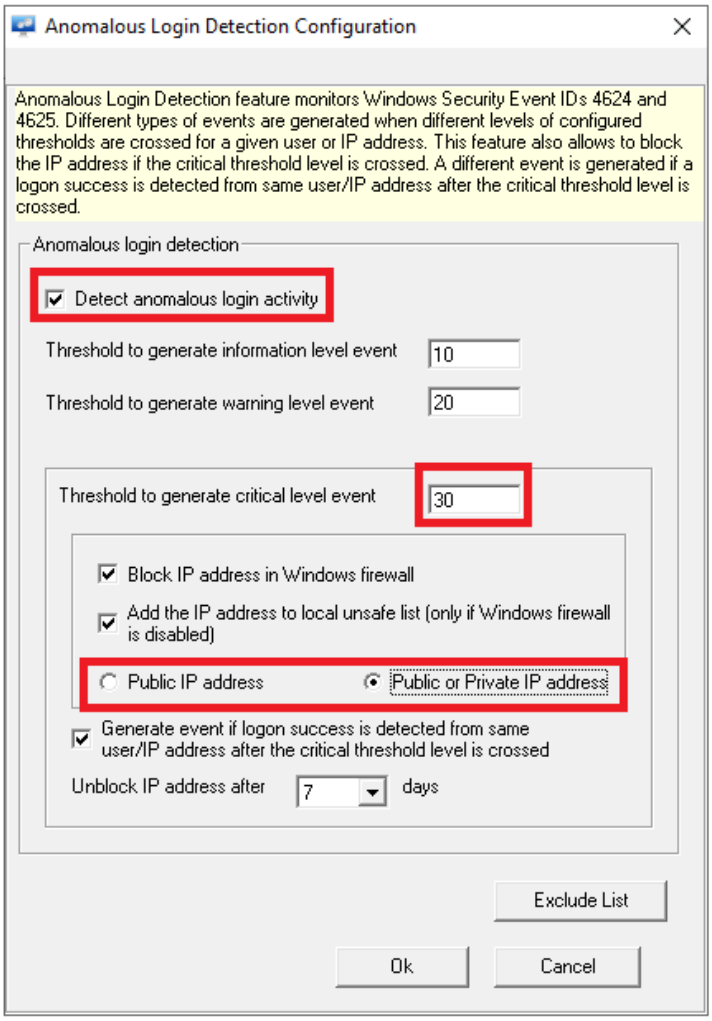

Figure 3

The three criteria to detect and prevent Anomalous Login are to:

- Block IP address in the Windows firewall.
- Add the IP address to the local unsafe list.
- Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed.

1. Enabling "**Block IP address in Windows firewall**" option will add the IP address to the Windows firewall rule and generates an Event ID 3529.

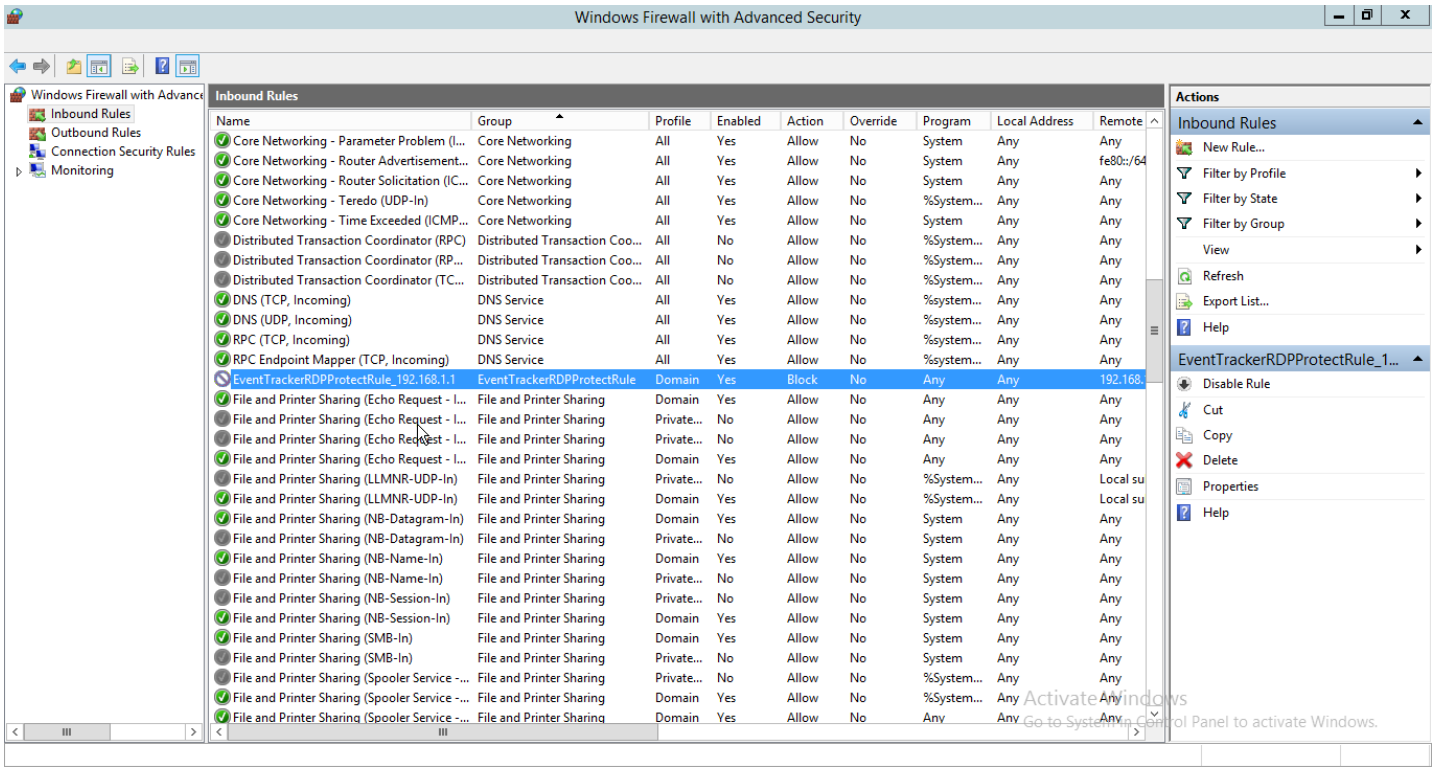

Figure 4

2. Enabling "**Add the IP address to local unsafe list**" option, will add the IP address to the anomalous_data.bin file, which is in the following path %ET_INSTALL_PATH%\Prism MicroSystems\EventTracker\Agent\Cache. When the IP address gets added to the **Anomalous_data.bin** file, Event ID 3530 will be generated**.**

3. Enabling "**Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed**" option will generate Event ID 3528, if the logon is successful from the same user/IP address after the critical threshold level is crossed.

4. "**Unblock IP address after __ days"** option, with this option the IP address added in the Windows firewall or unsafe list will be unblocked after the enforcement period and it will generate Event ID 3529 for unblocking the rule and Event ID 3530 for unblocking the IP address.

5. **Exclude List:** To exclude the users or the IP address from being monitored by Anomalous Login Detection, click **Exclude List.**

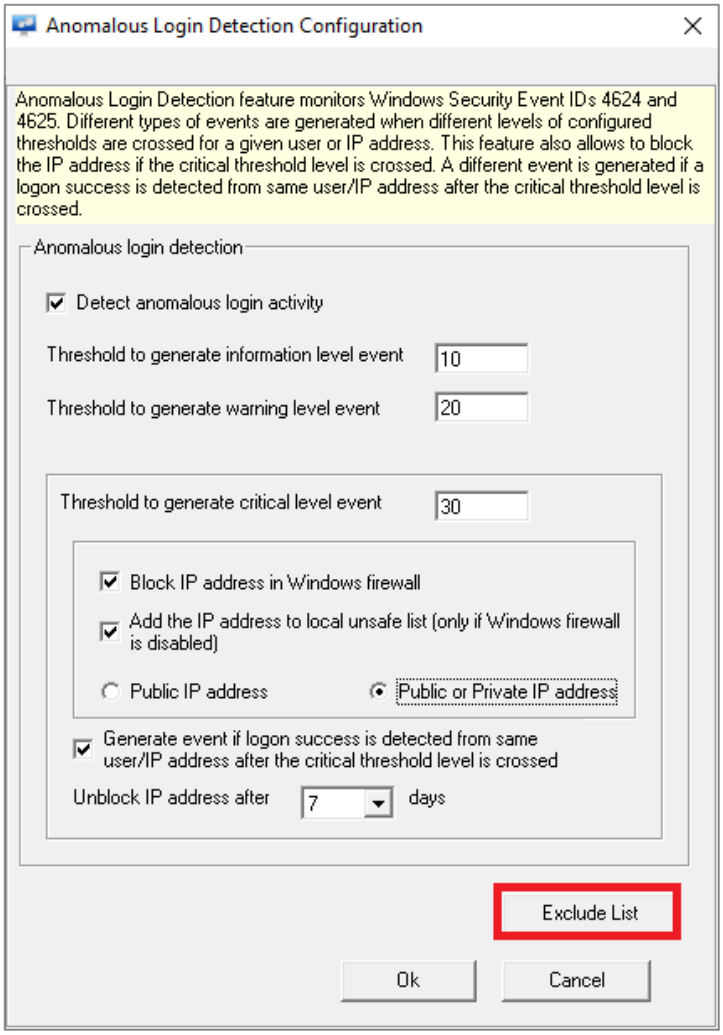

Figure 5

a. To do that, click **Exclude List**---- **Anomalous Trusted Connections List** window opens

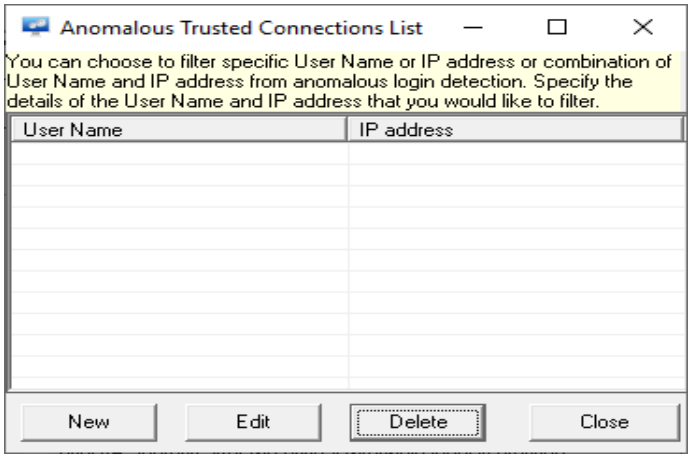

Figure 6

b. Click **New,** the **New Anomalous Filter Details** window opens. Enter the User Name and the IP Address that you want to exclude.

Note: You can provide the Flat or CIDR IP address.

Example. 172.27.100.37

172.27.100.45/32

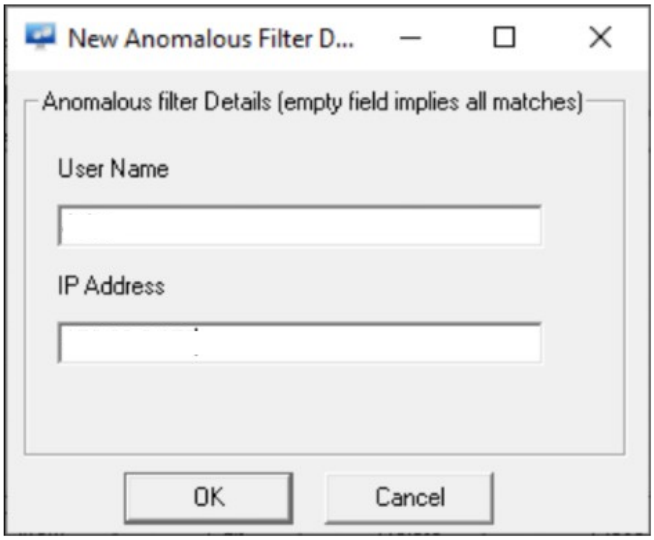

Figure 7

c. Once the user name and the IP address are entered, click **OK**.

Note

- You can also enter only the user name or the IP address to be excluded.
- If only the user name is added to the **New Anomalous Filter,** then EventID 3527 is generated for the IP address and if the option "**Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed**" is enabled Event ID 3528 is generated for IP address.
- If only the IP address is added to the **New Anomalous Filter,** then EventID 3527 is generated for the user name and if the option "**Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed**" is enabled Event ID 3528 is generated for the user name.

d. The entered user name and the IP address is seen in the **Anomalous Trusted Connections List** window.

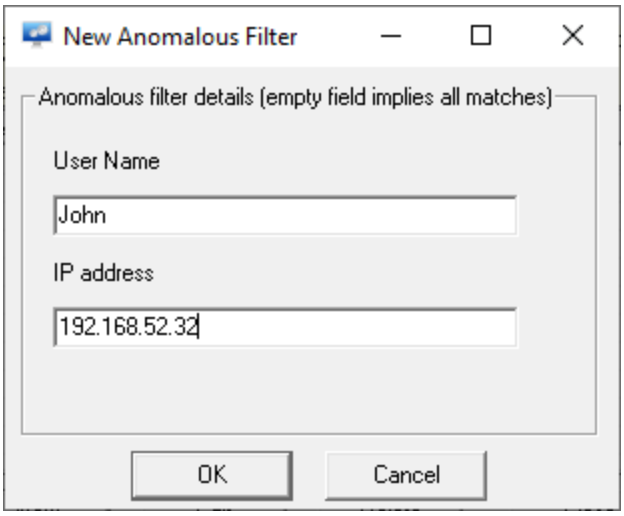

Figure 8

Note: Click New to add new user name and IP address
Click Edit to edit the user name or the IP address.
Click Delete to Delete the user name and IP address
Click Close to exit out of the **Anomalous Trusted Connections List** window.

e. To save the configuration changes, click **Close** to exit out of the **Anomalous Trusted Connections List** window refer figure 8, then click **ok** to exit out of the **Anomalous Login Detection Configuration** window refer figure 2, and click save on the EventTracker Agent Configuration window refer figure 1

Note:

- After the agent service restarts, enabling the option **"Block IP address in Windows firewall"** blocks the firewall. Adding username and the IP address in the **New Anomalous filter exclude** list will generate the Event ID 3529 (stating removal of the rule from the firewall/Found in anomalous filter list)

- After the agent service restarts, adding the IP address in the Anomalous_data.bin file, enabling the option **"Add the IP address to local unsafe list"** and then adding username and IP address in the **New Anomalous filter exlude filter list** will generate the Event ID 3530 (stating removed from EventTracker unsafe list because it is Found in anomalous filter list)