Netsurion®

Feature Guide

Anomalous Login Detection

Publication Date

December 06, 2023

© Copyright Netsurion. All Rights Reserved.

Abstract

This guide provides instructions to configure the Anomalous Login Detection feature with Netsurion Open XDR to identify suspicious activities.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for investigating and managing network security.

Table of Contents

© Copyright Netsurion. All Rights Reserved.

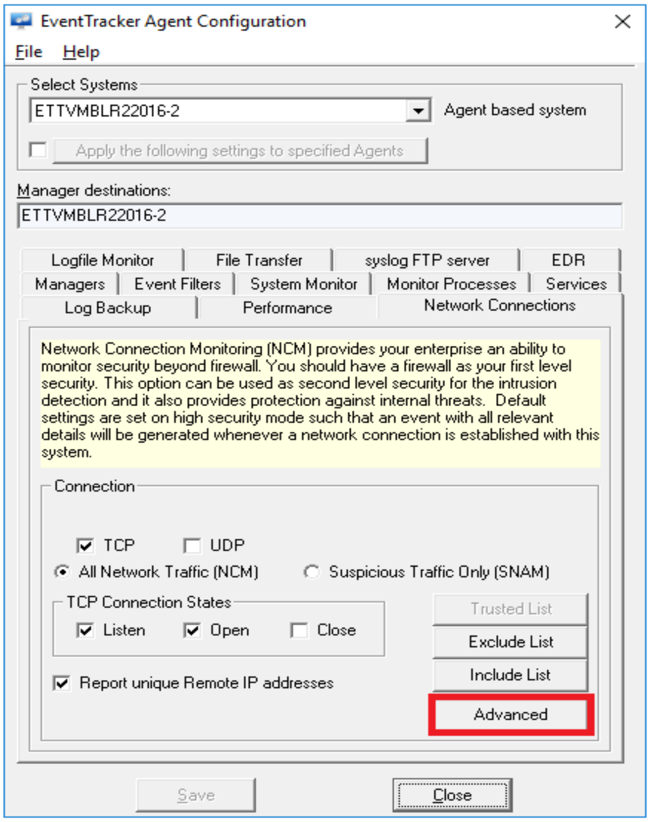
1 Overview

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

The Netsurion Open XDR Windows agent can identify Anomalous Login activity. It detects intrusion, fraud, and fault by the network intruders. The Anomalous Login identification is based on the user name and IP address.

2 Configuring Anomalous Login Detection

1. Go to **Netsurion Open XDR Agent Configuration**. Select **Network Connections**, and then **Advanced**.



Select Systems: ETTVMBLR22016-2 — Agent based system

☐ Apply the following settings to specified Agents

Manager destinations: ETTVMBLR22016-2

Network Connection Monitoring (NCM) provides your enterprise an ability to monitor security beyond firewall. You should have a firewall as your first level security. This option can be used as second level security for the intrusion detection and it also provides protection against internal threats. Default settings are set on high security mode such that an event with all relevant details will be generated whenever a network connection is established with this system.

Connection

☑ TCP ☐ UDP

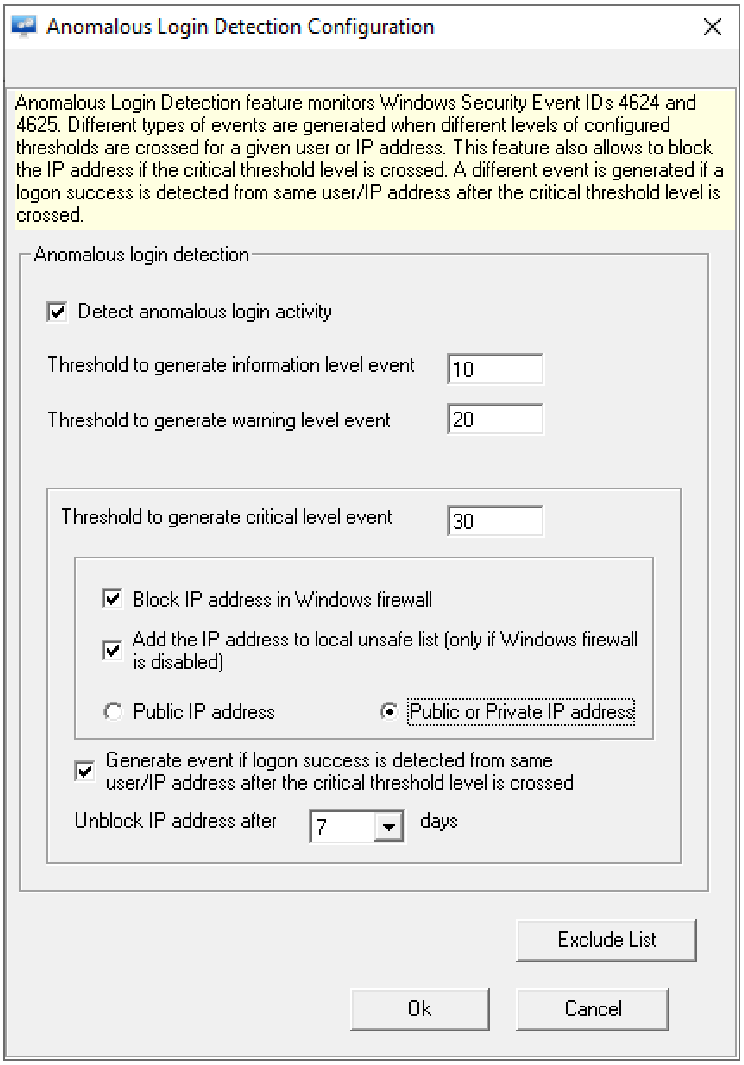
● All Network Traffic (NCM) ○ Suspicious Traffic Only (SNAM)

TCP Connection States

☑ Listen ☑ Open ☐ Close

☑ Report unique Remote IP addresses

2. The Anomalous Login Detection Configuration window opens as shown below:



Anomalous Login Detection Configuration

Anomalous Login Detection feature monitors Windows Security Event IDs 4624 and 4625. Different types of events are generated when different levels of configured thresholds are crossed for a given user or IP address. This feature also allows to block the IP address if the critical threshold level is crossed. A different event is generated if a logon success is detected from same user/IP address after the critical threshold level is crossed.

Anomalous login detection

☑ Detect anomalous login activity

Threshold to generate information level event: 10

Threshold to generate warning level event: 20

Threshold to generate critical level event: 30

☑ Block IP address in Windows firewall

☑ Add the IP address to local unsafe list (only if Windows firewall is disabled)

○ Public IP address ● Public or Private IP address

☑ Generate event if logon success is detected from same user/IP address after the critical threshold level is crossed

Unblock IP address after 7 days

3. Select the **Detect anomalous login activity** check box to enable Anomalous Login Detection.

   Ensure that the value of **Threshold to generate critical level event** is greater than the value of **Threshold to generate information level event** and the value of **Threshold to generate warning level event.**

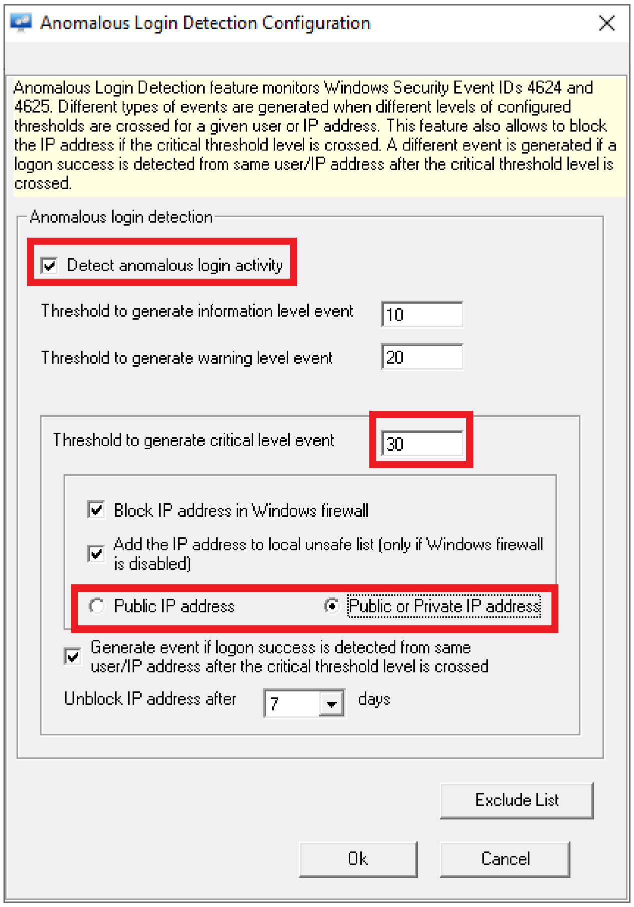
Note:

The Anomalous Login Detection feature works for both Public IP address and Private IP address according to the selected option.

4. **Event ID 3527** will be generated in the following cases:

Event Type	Description
Information	Generated when the login threshold crosses the information event level.
Warning	Generated when the login threshold crosses the warning event level.
Critical	Generated when the login threshold crosses the critical event level.

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



Anomalous Login Detection Configuration

Anomalous Login Detection feature monitors Windows Security Event IDs 4624 and 4625. Different types of events are generated when different levels of configured thresholds are crossed for a given user or IP address. This feature also allows to block the IP address if the critical threshold level is crossed. A different event is generated if a logon success is detected from same user/IP address after the critical threshold level is crossed.

Anomalous login detection

☑ Detect anomalous login activity

Threshold to generate information level event: 10

Threshold to generate warning level event: 20

Threshold to generate critical level event: 30

☑ Block IP address in Windows firewall

☑ Add the IP address to local unsafe list (only if Windows firewall is disabled)

○ Public IP address ● Public or Private IP address

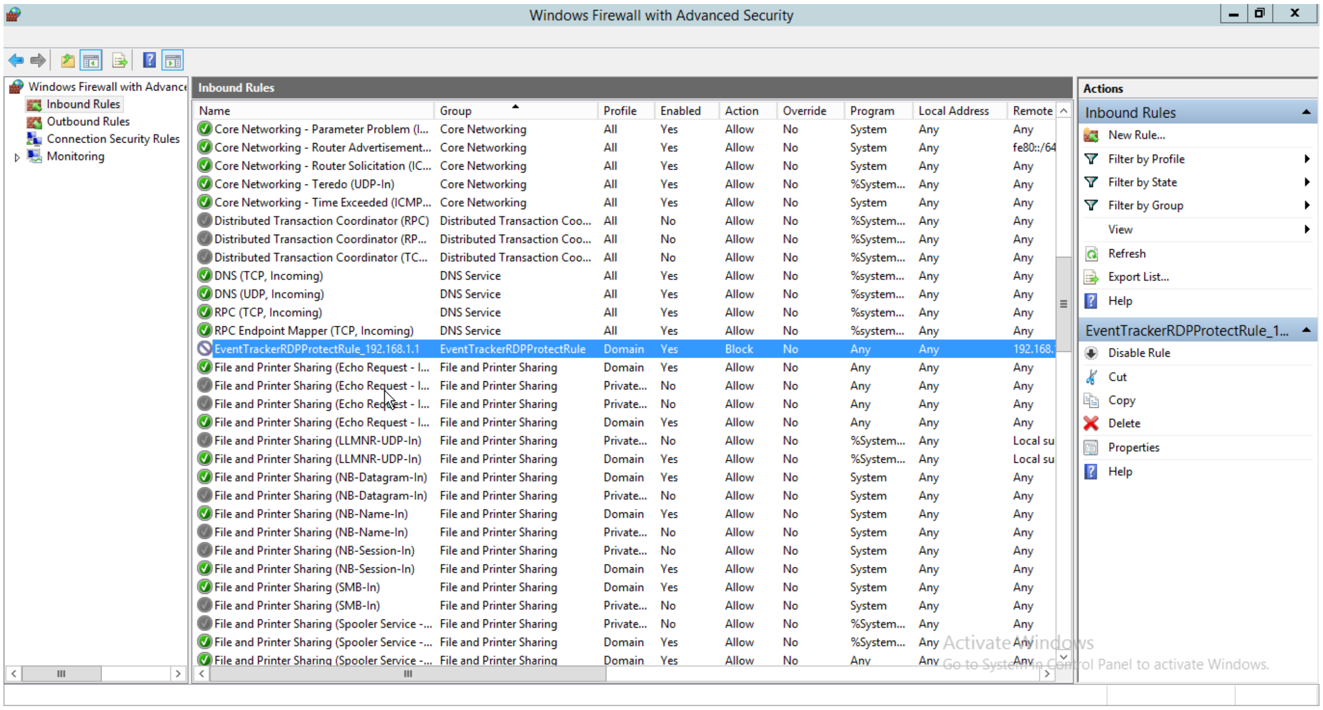
☑ Generate event if logon success is detected from same user/IP address after the critical threshold level is crossed

Unblock IP address after 7 days

The three criteria to detect and prevent Anomalous Login are:

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

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



Inbound Rules

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
Core Networking - Parameter Problem (I...	Core Networking	All	Yes	Allow	No	System	Any	Any
Core Networking - Router Advertisement...	Core Networking	All	Yes	Allow	No	System	Any	fe80::/64
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	No	System	Any	Any
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	No	%System...	Any	Any
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes	Allow	No	System	Any	Any
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	All	No	Allow	No	%System...	Any	Any
Distributed Transaction Coordinator (RP...	Distributed Transaction Coo...	All	No	Allow	No	%System...	Any	Any
Distributed Transaction Coordinator (TC...	Distributed Transaction Coo...	All	No	Allow	No	%System...	Any	Any
DNS (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%system...	Any	Any
DNS (UDP, Incoming)	DNS Service	All	Yes	Allow	No	%system...	Any	Any
RPC (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%system...	Any	Any
RPC Endpoint Mapper (TCP, Incoming)	DNS Service	All	Yes	Allow	No	%system...	Any	Any
EventTrackerRDPProtectRule_192.168.1.1	EventTrackerRDPProtectRule	Domain	Yes	Block	No	Any	Any	192.168.
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domain	Yes	Allow	No	Any	Any	Any
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Private...	No	Allow	No	Any	Any	Any
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Private...	No	Allow	No	Any	Any	Any
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	Domain	Yes	Allow	No	Any	Any	Any
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Private...	No	Allow	No	%System...	Any	Local su
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	Domain	Yes	Allow	No	%System...	Any	Local su
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private...	No	Allow	No	System	Any	Any
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private...	No	Allow	No	System	Any	Any
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private...	No	Allow	No	System	Any	Any
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	Yes	Allow	No	System	Any	Any
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	No	Allow	No	System	Any	Any
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	Private...	No	Allow	No	%System...	Any	Any
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	Domain	Yes	Allow	No	%System...	Any	Any
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	Domain	Yes	Allow	No	Any	Any	Any

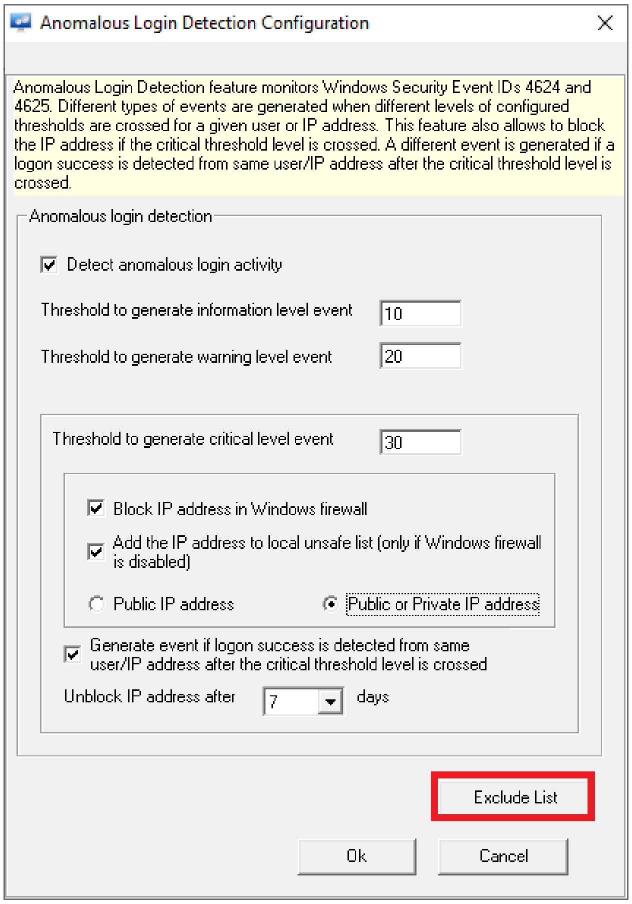
Activate Windows
Go to System in Control Panel to activate Windows.

2. **Add the IP address to local unsafe list**: Enabling this option will add the IP address to the **anomalous_data.bin** file, which is in the 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. **Generate event if logon success is detected from the same user/IP address after the critical threshold level is crossed**: Enabling this option will generate the **Event ID 3528** if the login is successful from the same user/IP address after the critical threshold level is crossed.

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

5. **Exclude List:** Click **Exclude List** to exclude the users or the IP address from being monitored by Anomalous Login Detection.



Anomalous Login Detection feature monitors Windows Security Event IDs 4624 and 4625. Different types of events are generated when different levels of configured thresholds are crossed for a given user or IP address. This feature also allows to block the IP address if the critical threshold level is crossed. A different event is generated if a logon success is detected from same user/IP address after the critical threshold level is crossed.

Anomalous login detection

☑ Detect anomalous login activity

Threshold to generate information level event: 10

Threshold to generate warning level event: 20

Threshold to generate critical level event: 30

☑ Block IP address in Windows firewall

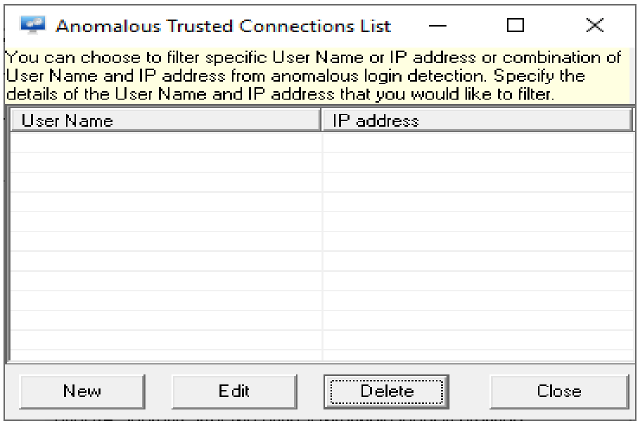
☑ Add the IP address to local unsafe list (only if Windows firewall is disabled)

○ Public IP address ● Public or Private IP address

☑ Generate event if logon success is detected from same user/IP address after the critical threshold level is crossed

Unblock IP address after 7 days

a. The **Anomalous Trusted Connections List** window opens after clicking Exclude List as shown below:



You can choose to filter specific User Name or IP address or combination of User Name and IP address from anomalous login detection. Specify the details of the User Name and IP address that you would like to filter.

User Name	IP address

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

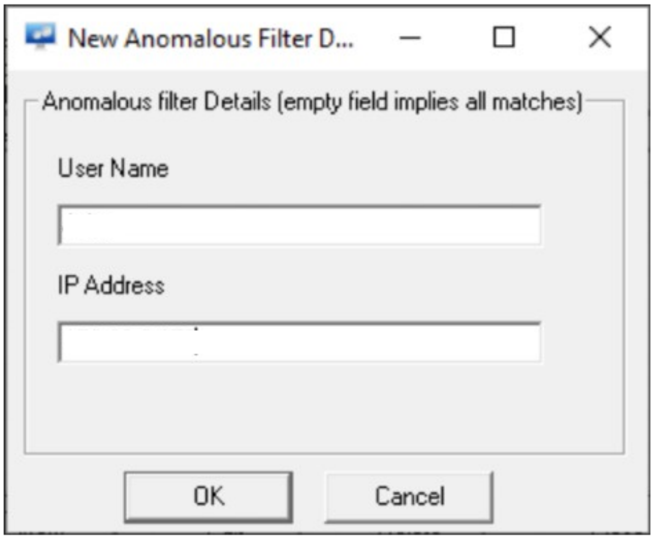
Note:

You can provide the Flat or CIDR IP address.

For Example:

172.27.100.37

172.27.100.45/32



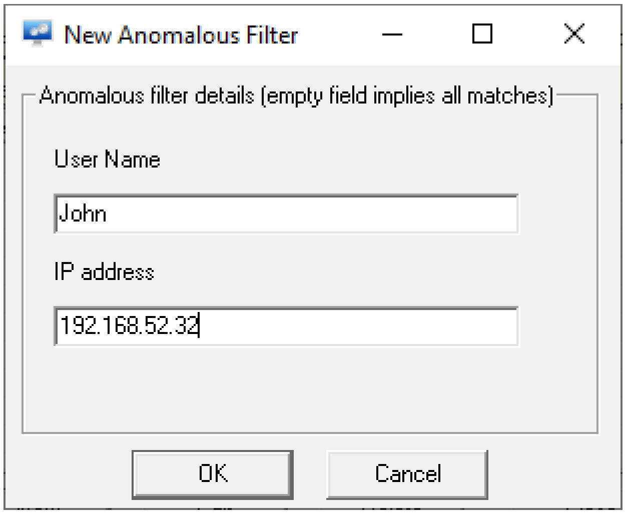
New Anomalous Filter D...
Anomalous filter Details (empty field implies all matches)
User Name
IP Address
OK
Cancel

c. After entering the details, click **OK**.

Note:

- You can also enter only the user name or the IP address to be excluded.
- If only the Username is added to the **New Anomalous Filter**, then the EventID 3527 will not be generated for the IP Address/Username.
- If only the IP Address is added to the **New Anomalous Filter**, then the EventID 3527 will not be generated for the Username/IP Address.

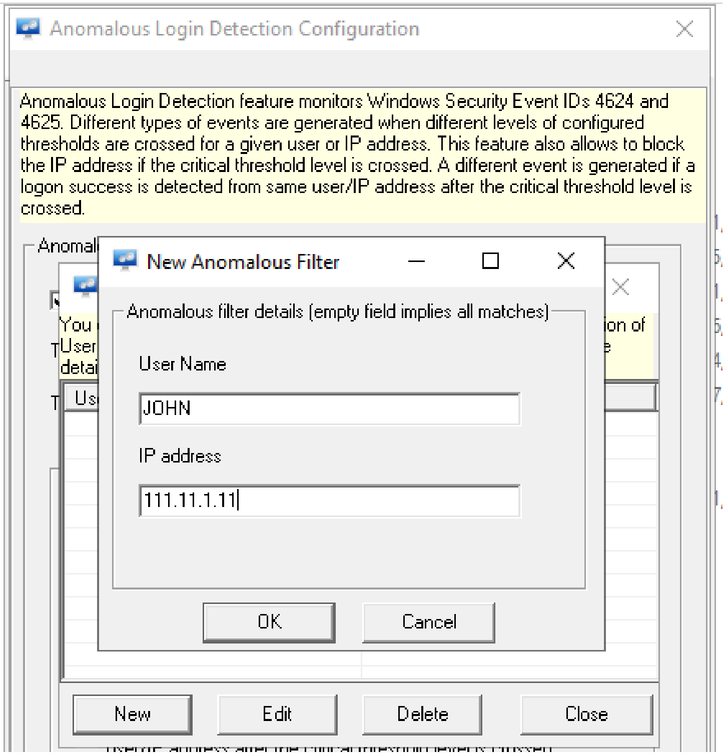
d. The entered user name and the IP address will be seen in the **Anomalous Trusted Connections List** window.



User Name: John

IP address: 192.168.52.32

e. The user can perform the following functions:
New: Add a new user name/IP address.
Edit: Edit the user name/IP address.
Delete: Delete the existing user name/IP address.



Anomalous Login Detection Configuration

Anomalous Login Detection feature monitors Windows Security Event IDs 4624 and 4625. Different types of events are generated when different levels of configured thresholds are crossed for a given user or IP address. This feature also allows to block the IP address if the critical threshold level is crossed. A different event is generated if a logon success is detected from same user/IP address after the critical threshold level is crossed.

New Anomalous Filter

Anomalous filter details (empty field implies all matches)

User Name: JOHN

IP address: 111.11.1.11

f. Click **Close** to exit the Anomalous Login Detection Configuration window.

g. Finally, click **Save** on the Netsurion Open XDR Configuration window.

Note:

- After the agent service restarts, enabling the option **Block IP address in Windows firewall** blocks the IP address at the firewall level. Adding the user name 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 the username and IP address in the **New Anomalous filter exclude filter list** will generate **the Event ID 3530** (stating removed from unsafe list because it is found in anomalous filter list).

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers managed threat protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection & Response (MXDR). Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support

© Copyright Netsurion. All Rights Reserved.