



Feature Guide

Anomalous Login Detection

Publication Date

Nov 20, 2025

Abstract

This guide provides instructions to configure the Anomalous Login Detection feature with Logcollect 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 Logcollect 9.4 or later.

Audience

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

Table of Contents

1	Overview	4
2	Configuring Anomalous Login Detection	4

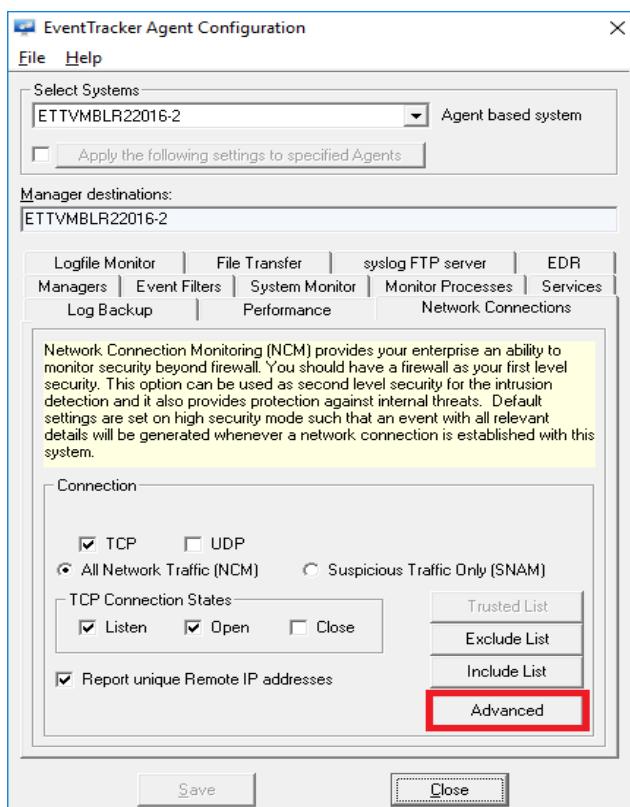
1 Overview

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 Logcollect 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.

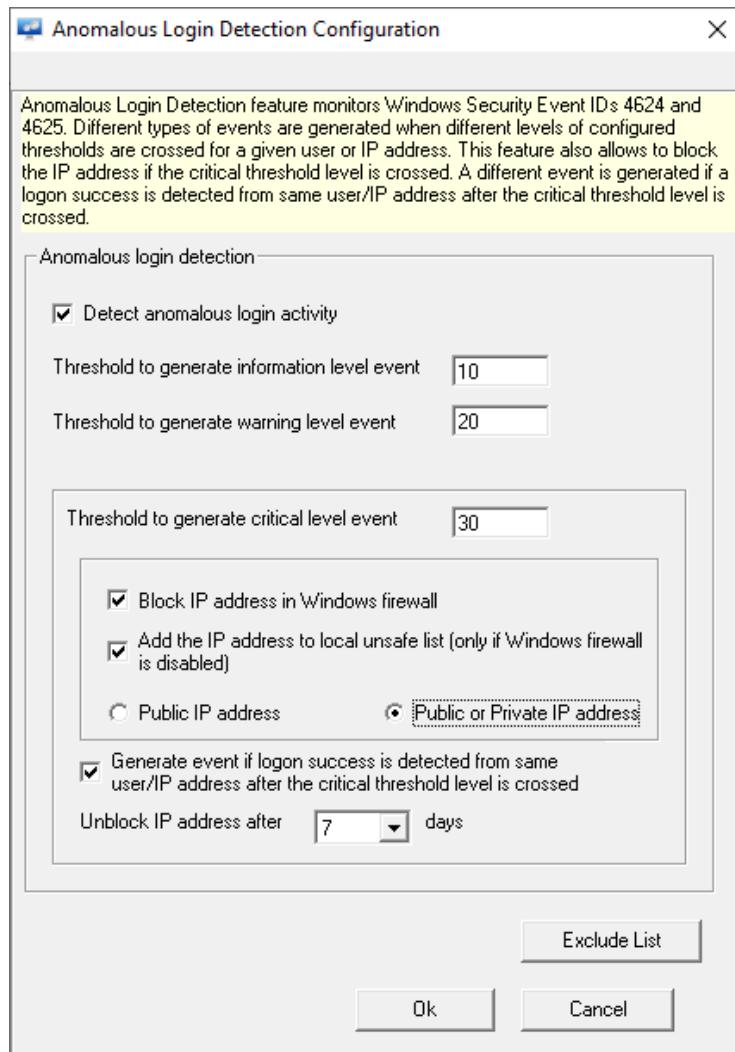
2 Configuring Anomalous Login Detection

1. Go to **Logcollect Agent Configuration**. Select **Network Connections**, and then **Advanced**.



Need to change this image when we change the Title to Logcollect

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



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:

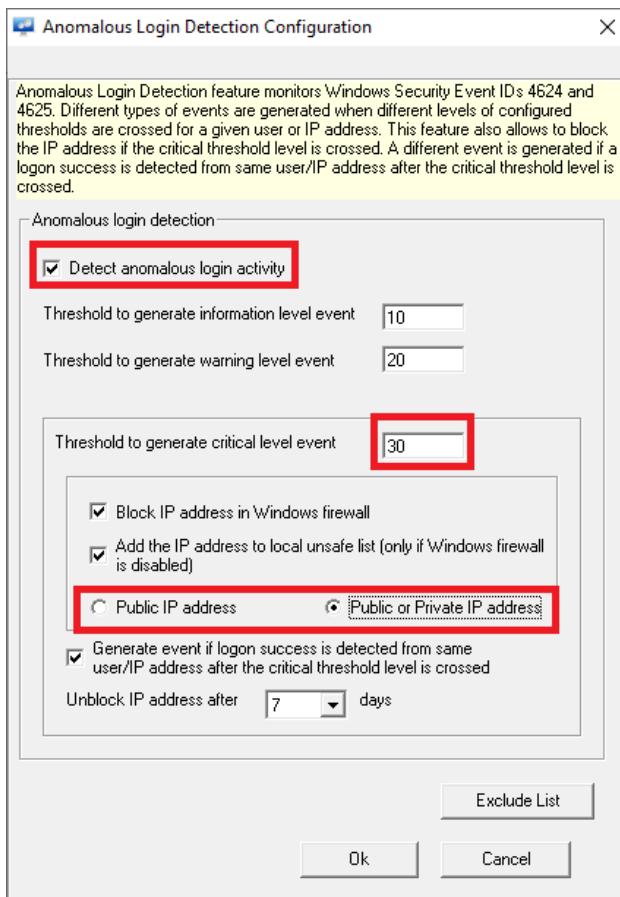
The Anomalous Login Detection feature works for both Public IP address and Private IP address according to the selected option.

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:

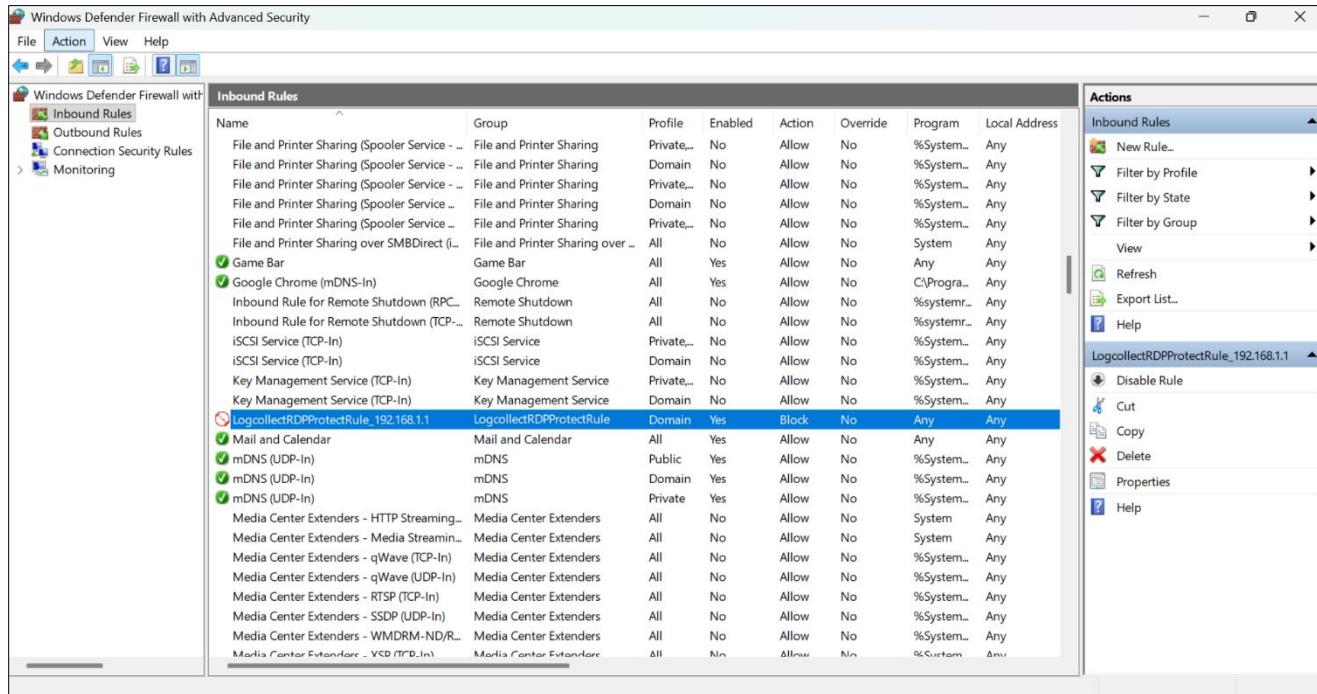
Anomalous Login Detection will occur only when the login threshold crosses the critical level.



The three criteria to detect and prevent Anomalous Login are:

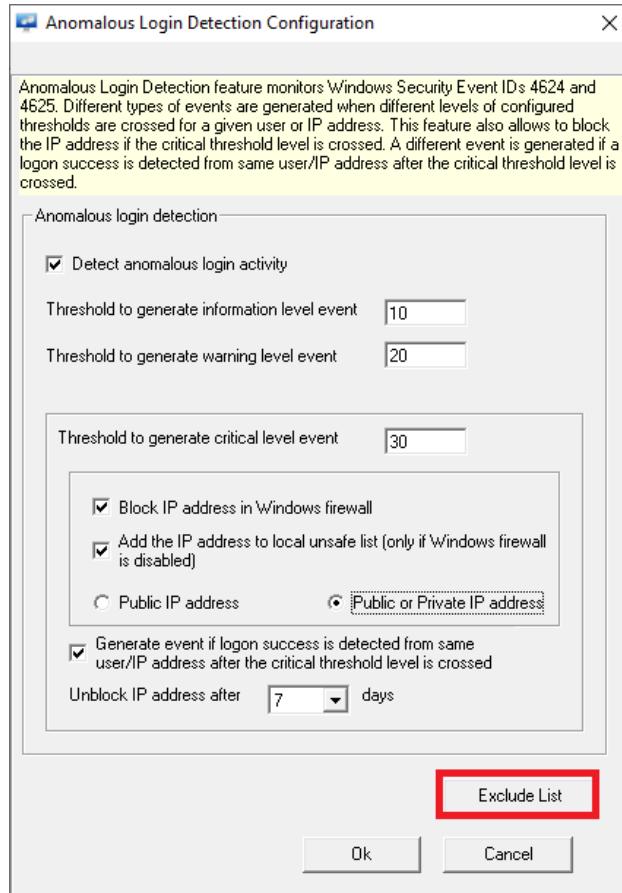
- Block the IP address in the Windows firewall.
- Add the IP address to the local unsafe list.
- Generate an event if a successful login is detected from the same user/IP address after the critical threshold level is crossed.

- 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**.

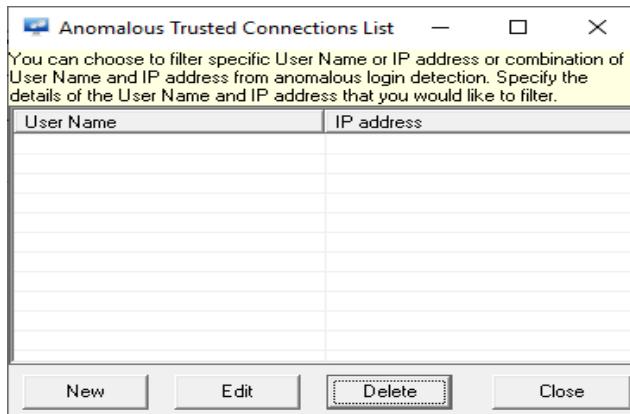


Name	Group	Profile	Enabled	Action	Override	Program	Local Address
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Private,...	No	Allow	No	%System...	Any
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Domain	No	Allow	No	%System...	Any
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Private,...	No	Allow	No	%System...	Any
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Domain	No	Allow	No	%System...	Any
File and Printer Sharing (Spooler Service - ...)	File and Printer Sharing	Private,...	No	Allow	No	%System...	Any
File and Printer Sharing over SMBDirect (i...	File and Printer Sharing over ...	All	No	Allow	No	System	Any
Game Bar	Game Bar	All	Yes	Allow	No	Any	Any
Google Chrome (mDNS-In)	Google Chrome	All	Yes	Allow	No	C:\Progra...	Any
Inbound Rule for Remote Shutdown (RPC-In)	Remote Shutdown	All	No	Allow	No	%systemr...	Any
Inbound Rule for Remote Shutdown (TCP-In)	Remote Shutdown	All	No	Allow	No	%systemr...	Any
iSCSI Service (TCP-In)	iSCSI Service	Private,...	No	Allow	No	%System...	Any
iSCSI Service (TCP-In)	iSCSI Service	Domain	No	Allow	No	%System...	Any
Key Management Service (TCP-In)	Key Management Service	Private,...	No	Allow	No	%System...	Any
Key Management Service (TCP-In)	Key Management Service	Domain	No	Allow	No	%System...	Any
LogcollectRDPProtectRule_192.168.1.1	LogcollectRDPProtectRule	Domain	Yes	Block	No	Any	Any
Mail and Calendar	Mail and Calendar	All	Yes	Allow	No	Any	Any
mDNS (UDP-In)	mDNS	Public	Yes	Allow	No	%System...	Any
mDNS (UDP-In)	mDNS	Domain	Yes	Allow	No	%System...	Any
mDNS (UDP-In)	mDNS	Private	Yes	Allow	No	%System...	Any
Media Center Extenders - HTTP Streaming...	Media Center Extenders	All	No	Allow	No	System	Any
Media Center Extenders - Media Streamin...	Media Center Extenders	All	No	Allow	No	System	Any
Media Center Extenders - qWave (TCP-In)	Media Center Extenders	All	No	Allow	No	%System...	Any
Media Center Extenders - qWave (UDP-In)	Media Center Extenders	All	No	Allow	No	%System...	Any
Media Center Extenders - RTSP (TCP-In)	Media Center Extenders	All	No	Allow	No	%System...	Any
Media Center Extenders - SSDP (UDP-In)	Media Center Extenders	All	No	Allow	No	%System...	Any
Media Center Extenders - WMDRM-ND/R...	Media Center Extenders	All	No	Allow	No	%System...	Any
Marisa Cantor Extenders - VSD (TCP-In)	Marisa Cantor Extenders	All	No	Allow	No	%System...	Any

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



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



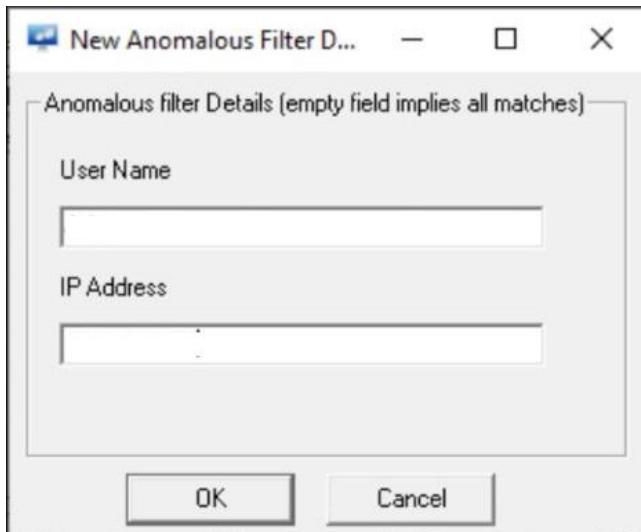
b. Click **New**, and the **New Anomalous Filter Details** window opens. Enter the User Name and the IP Address that you want to exclude.

Note:

You can provide the Flat or CIDR IP address.

For Example:

172.27.100.37
 172.27.100.45/32

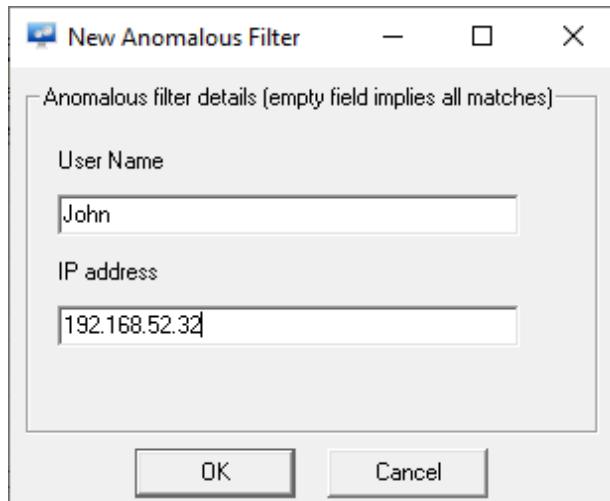


c. After entering the details, click **OK**.

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 Event ID 3527 will not be generated for the IP Address/Username.
- If only the IP Address is added to the **New Anomalous Filter**, then the Event ID 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.

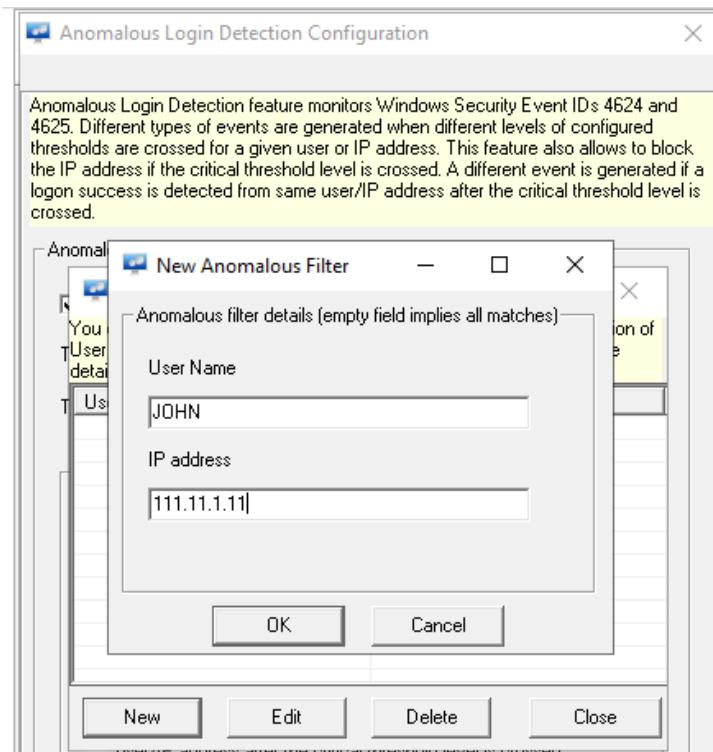


e. The user can perform the following functions:

New: Add a new user name/IP address.

Edit: Edit the user name/IP address.

Delete: Delete the existing user name/IP address.



f. Click **Close** to exit the Anomalous Login Detection Configuration window.
g. Finally, click **Save** on the Logcollect 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 Logcollect

Logcollect is a software-only telemetry pipeline which supports the collection, enrichment, transformation and routing of security data from sources to multiple destinations. It is targeted to security operations that are struggling with distributing large volumes of disparate data, high operational costs, alert fatigue and missed threats. It is available as a software license or hosted in AWS. It is backed by a team that has extensive experience with security logging, SIEM and regulatory compliance. Collect once, analyze everywhere.

Headquartered in Ft. Lauderdale, FL, Logcollect is a leader in Log Collection. Learn more at www.Logcollect.com.

Contact Us

Corporate Headquarters

Prism Microsystems
920 NE 17th Way
Fort Lauderdale, FL 33304

<https://www.Logcollect.com/support>