End User Settings

NetVizura is capable of detecting end user activity in the company network. End user traffic is identified by mapping IP address provided in syslog logon event and IP address provided in NetFlow data. Logon events could be generated by Domain Controllers or Work Stations relayed via *Syslog server* to *NetVizura server*. We use Windows Domain Controller in our example.

On this page:

NetVizura comes with predefined matching rules for Snare Open Source Syslog agent:

In blocked URL **> Settings > NetFlow Settings > End Users** there is already predefined logon rules for collecting logon events from Snare syslog agent. You can activate it by clicking *Active* at Status field. Double click on rule opens rule condition where you can change *Source IP* to more specific value to increase performance and check collection of logon events by clicking on *Verify match*.

For detailed explanation on how to install and configure Snare Syslog agent see Installing and Configuring Syslog Agent for End User Traffic.

By default collection port for logon events is set to 33515 so the syslog's should be sent to 33515 port at NetVizura server. If you want to change the port go to blocked URL **> Settings > NetFlow Settings > Configuration** and search for End users collection port value.

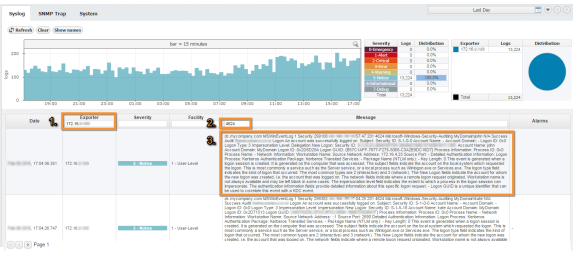
Example of correct match string from Snare

* MSWinEventLog * 4624 Microsoft-Windows-Security-Auditing * Success Audit * Logon Type: 3 * Account Name: <USERNAME> * Account Domain: <DOMAIN> * Source Network Address: <USER-IP> *

Step 1. Select Appropriate Message (Logon Event)

Navigate to Netvizura **Eventlog** module and choose **Syslog** tab. Identify syslog message with logon information. This log should contain:

1. **IP address** of domain controller that exports Syslogs - *type IP address into Exporter text box and press Enter*
2. Windows code **4624** that designates successful logon event - *type 4624 into Message filter text box and press Enter*
3. Select, copy and paste text message in some text editor (Wordpad or similar)
4. Create appropriate **Match string** in text editor



Match String

Steps for creating correct match string :

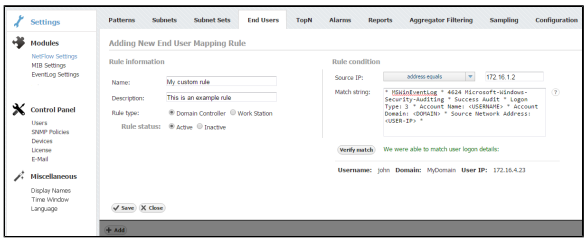
1. Find *Account Name* within the message and **put <USERNAME> instead of real account name** (please refer to picture below)
2. Find *Account Domain* within the message and **put <DOMAIN> instead of real account domain** (please refer to picture below)
3. Find *Source Network Address* within the message and **put <USER-IP> instead of real IP address** (please refer to picture below). No need for this step in case of Work Station type of rule.
4. Find additional information that can help in matching message more precisely like: **MSWinEvent Log, 4624 Microsoft-Windows-Security-Auditing, Success Audit, Logon Type: 3**
5. **IMPORTANT**: Delete any other text and **put * as a wildcard** instead of deleted text (**refer to Example of correct match string**)

Dec 9 16:57:48 dc.mycompany.com MSWinEventLog 1 Security 299108 Thu. Dec. 09 16:57:47 4624 Microsoft-Windows-Security-Auditing MyDomain\john N/A Success Audit dc.mycompany.com Logon An account was successfully logged on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Impersonation Level: Delegation New Logon: Security ID: S-1-5-4104 Account Name: john Account Domain: MyDomain Logon ID: 0x2A8DB41A Logon GUID: {B50C1E00-1688-A170-5068-84D2F9A016D3} Process Information: Process ID: 0x0 Process Name: - Network Information: Workstation Name: Source Network Address: 172.16.4.23 Source Port: - Detailed Authentication Information: Logon Process: Kerberos Authentication Package: Kerberos Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon session is created. It is generated on the computer that was accessed. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.

Step 2. Setup Rule

In upper right corner of Netvizura application navigate to blocked URL **> Settings > NetFlow Settings > End Users**:

1. Click on **+ Add** button
2. Enter your own **Rule Name and Description**
3. Set **Rule type** (in this example set *Domain Controller*)
4. Set **Rule status** (in this example set *Active*)
5. Enter **Source IP** (IP address of Domain Controller)
6. Copy and paste **Match string** from text editor into the *Match string area*
7. Click on ***Verify match*** button
8. Click on ***Save*** button to save your rule (if verification is successful)



To check results of your work, navigate to **NetFlow > End Users**. If the three is empty, refresh your web browser with ctrl+F5.

In order to improve system performance, we recommend to set status as inactive for all rules that are not in use.

Specifying too broad subnet in the **Source IP** field might result in performance penalty. For best results consider changing Source IP to more specific value or concrete IP address.

Use help button: Move your cursor under the question mark on the screen for additional help.

You can easily verify the rule by clicking **Verify**. It will check if any Syslog message from the last 24 hours matches the rule.