Installing and Configuring Syslog Agent for End User Traffic

End User Traffic functionality requires separate Syslog agent to be installed on working stations or domain controller.

NetVizura, by default, includes built-in support for Snare OpenSource agent. Installation and configuration of Snare agent is described in the following steps.

If you have another Syslog agent then you can create a separate rule for that agent: Configuring End Users.

1. Step - Downloading Snare OpenSource

Download Snare OpenSource Syslog agent from the official website, www.intersectalliance.com.

2. Step - Installing Snare agent on Windows

Install Snare OpenSource agent on domain controller and/or Windows working station by following these instructions.

- Run Snare OpenSource installer with administrative privileges
- Accept License Agreement and press **next**
- Leave defaults for EventLog configuration and press **next**
- Select **Use System account** and press **next**
- Choose to **enable** Web access for Snare Remote Control Interface and be sure that you enter password to protect configuration interface and press **next**.
- From now on just click **next** til the end of installation.

3. Step - Configuring Snare

If you have followed previous steps carefully, you will be able to access Remote Control Interface using your browser of choice.

To access Remote Control Interface paste http://localhost:6161/ into your address bar in your browser and press **Enter.**

In order to fully configure Snare OpenSource agent to work correctly with NetVizura follow these steps.

1. ### Network configuration
   Click on **Network Configuration** on the left side of the Control Interface. Locate *Destination Snare Server address* field and put IP address of your NetVizura server here.
   Open NetVizura application, and navigate to **Settings > NetFlow Settings > Configuration** and search for *End users collection port* value.
   By default collection port should be set to 33515. Locate *Destination Port* field in Snare Remote Control Interface and paste the port value from NetVizura Settings configuration.
   To finish network configuration check *Enable Syslog Header* checkbox. Click **Change Configuration** to save changes.

2. ### Objectives Configuration

   Click on **Objectives Configuration** on the left side of the Control Interface.
   Make sure that objective named **Logon_Logoff** exists in the list.
   Other objectives are not needed for NetVizura to work properly and therefore can be deleted from the list.

3. #### Apply new configuration
   In order for new configuration settings to be applied you should restart Snare service by executing following commands inside Windows command prompt.

   > ⚠ Make sure to run Command Prompt with Administrative privileges

   First stop Snare service by running:

   ```
   net stop snare
   ```

   After that, start Snare again by running:

```
net start snare
```

By now, you should have your Snare agent successfully installed and configured to work with NetVizura.

Follow step 4 to make sure that NetVizura is actually receiving Syslog messages from Snare agent.

4. Step - Checking installation and configuration

If you have EventLog module activated, you can easily check if you are receiving Syslog messages by going to **EventLog > Syslog** tab.

Otherwise, login to your NetVizura server over SSH, and first check if NetVizura is listening for Syslog messages on specified port.

In order to perform this check run the following command inside your shell.

```
netstat -lnup | grep 33515
```

33515 is a default port. If you have configured collection port to have another value, put that value in the previous command instead of 33515.

If collection is working fine you should see something similar to the following after running this command.

```
udp   0      0 :::33515        :::*       31414/jsvc.exec
```

Next, check if Snare agent is sending syslog to Netvizura collector by running tcpdump.

```
tcpdump port 33515
```

Once again, default port value is used. In case some other value is configured through Settings, replace that value into provided command.

After running tcpdump command, you shoud see packets incoming to your server from workstations or domain controller.

If tcpdump is not installed on your server do the following:

Debian/Ubuntu

```
sudo apt-get update
sudo apt-get
install tcpdump
```

CentOS

```
sudo yum update
sudo yum install
tcpdump
```