Viewing End User Traffic

> In order to view End User Traffic, you first need to configure NetVizura to collect syslog logon messages and map users to IP addresses. After that, end users will automatically appear in the node tree as they logon to their workstations and start making traffic. To learn more go to Setting End User Traffic.
>
> End User Traffic is visible only to Admin users with Write permission on the NetFlow module.

When you investigate atypical behavior or a threat in the network, information about IP address often does not provide precise identification of the responsible person. Linking an address to a username is very important because it allows administrators to determine exactly who used the IP address at the specific time. This significantly improves situational awareness and reduces incident response/resolution time - help desk agent can quickly call the responsible person to ask if he/she logged on to the device, and cross-check suspicious behavior.

Traffic for one user is presented as the sum of the traffic from all IP addresses he used during a certain time window.

End Users Traffic shows top talkers for:

- All Users Traffic
- Domain Users Traffic
- End User Traffic by Hosts
- End User Traffic by Conversations
- End User Traffic by Services
- End User Traffic by Protocols
- End User Traffic by QoS
- End User Traffic by AS