

Enable Decode VXLAN Column in LiveWire Omnipeek

Here are the steps to enable the Decode VXLAN column:

1. Enable "Decode /MPLS/VXLAN Network Identifier" in Expert > Packets.
2. Click the flag for VXLAN > Click the ellipsis and Select "Add as Decode Column".

The screenshot shows the LiveWire Omnipeek interface. The top navigation bar includes 'Engines', 'Capture Engine', 'Forensic Searches', 'Forensics Capture 3', and 'Packets'. The main window displays a list of packets with columns for 'PACKET', 'SOURCE', 'DESTINATION', 'FLOW ID', 'SIZE', 'RELATIVE TIME', 'PROTOCOL', 'APPLICATION', 'SUMMARY', and 'EXPERT'. A packet with ID 502748 is selected. The 'Expert' view for this packet is expanded, showing details for an Ethernet II frame. The 'Flags' section is expanded to show 'VXLAN - Virtual extensible LAN'. The 'VXLAN Network Identifier' flag is selected, and a context menu is open with 'Add as Decode Column' highlighted.

3. A new column will appear in the column on the far right of the Expert/Packets page.

The screenshot shows the LiveWire Omnipeek interface after the configuration change. The main window displays the same list of packets as the previous screenshot. A new column, 'DECODE/VXLAN/VXLAN NETWORK IDENTIFIER...', has been added to the right side of the table. The 'Expert' view for the selected packet is still expanded, showing the 'VXLAN - Virtual extensible LAN' flag.

Enable MPLS, VLAN, and VXLAN Expert Events in Omnicpeek Windows

Right-click the Column header in Expert Events and enable all four options as shown at the bottom of the screenshot below:

The screenshot displays the Omnicpeek interface. At the top, there's a graph showing traffic volume over time. Below the graph is a table of flows. A context menu is open over the table headers, showing options to enable various expert events.

Client Addr	Server Addr	Flows	Events	Packets	Bytes	Duration	3-Way Handshake (sec)	Avg Response Time (sec)	TLS Version	TCP Status	MPLS	VLAN	VXLAN GPOD	VXLAN VNI
4.4.4.2	3.3.3.1	1	237	571	83,798	0:01:35.433000	0.016000	0.010800			19	100		
4.4.4.2	7.7.7.2	1	0	30	3,720	5.697000					20	100		
7.7.7.2	5.5.5.1	2	1	298	74,268	0:01:02.814000	0.018000	0.010266			16, 20	100		
15.1.1.2	15.1.1.1	1	2	12	852	0:01:49.294000		46.251000				100		

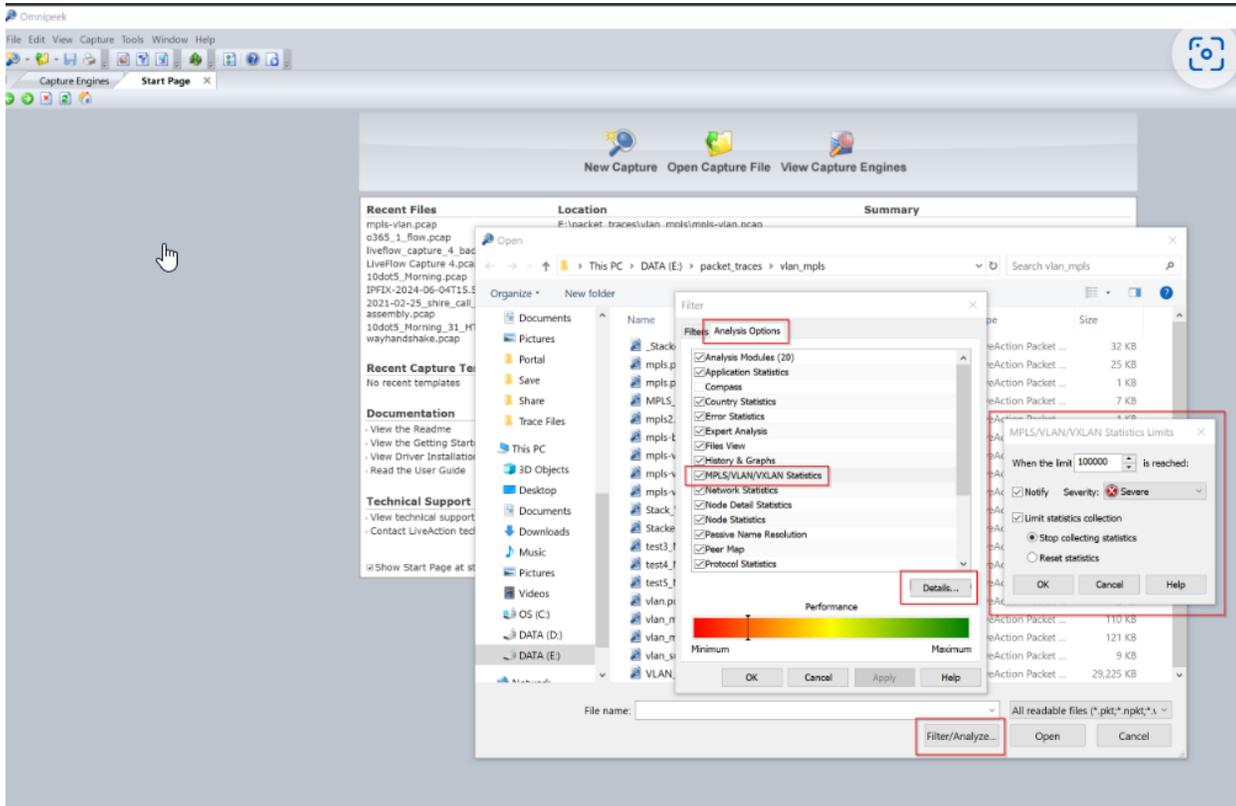
The context menu on the right shows the following options checked:

- Server Addr
- Server Port
- Server Country
- Server City
- Server Latitude
- Server Longitude
- Flow ID
- Flows
- Events
- Protocol
- Application
- Hops
- Packets
- Client Pkts
- Server Pkts
- Bytes
- Client Bytes
- Server Bytes
- Start
- Finish
- Duration
- 3-Way Handshake (sec)
- Network Latency Turn Count
- Best Network Latency (sec)
- Avg Network Latency (sec)
- Worst Network Latency (sec)
- Application Latency Turn Count
- Best Application Latency (sec)
- Avg Application Latency (sec)
- Worst Application Latency (sec)
- Response Time Turn Count
- Best Response Time (sec)
- Avg Response Time (sec)
- Worst Response Time (sec)
- C->S bps Turn Count
- C->S bps Best
- C->S bps Worst
- S->C bps Turn Count
- S->C bps Best
- S->C bps Worst
- TLS Version
- TLS Cert Not Before
- TLS Cert Not After
- TLS Handshake (sec)
- TCP Status
- MPLS
- VLAN
- VXLAN GPOD
- VXLAN VNI

Enable MPLS, VLAN, and VXLAN Statistics in Omnipeek Windows

Local Files

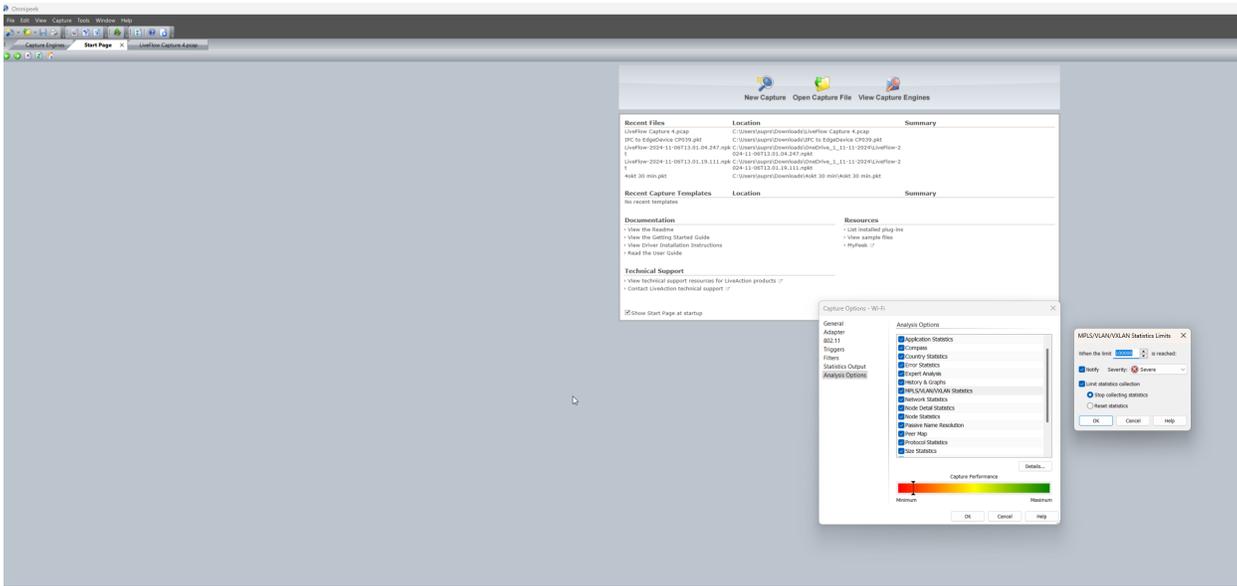
When opening a packet file in Omnipeek Windows, the user may click the Filter/Analyze... button in the open file dialog to see the list of analysis options that will be used to analyze the packet file. A new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the file window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the "Details..." button when the "MPLS/VLAN/VXLAN Statistics" item is selected will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



Capture

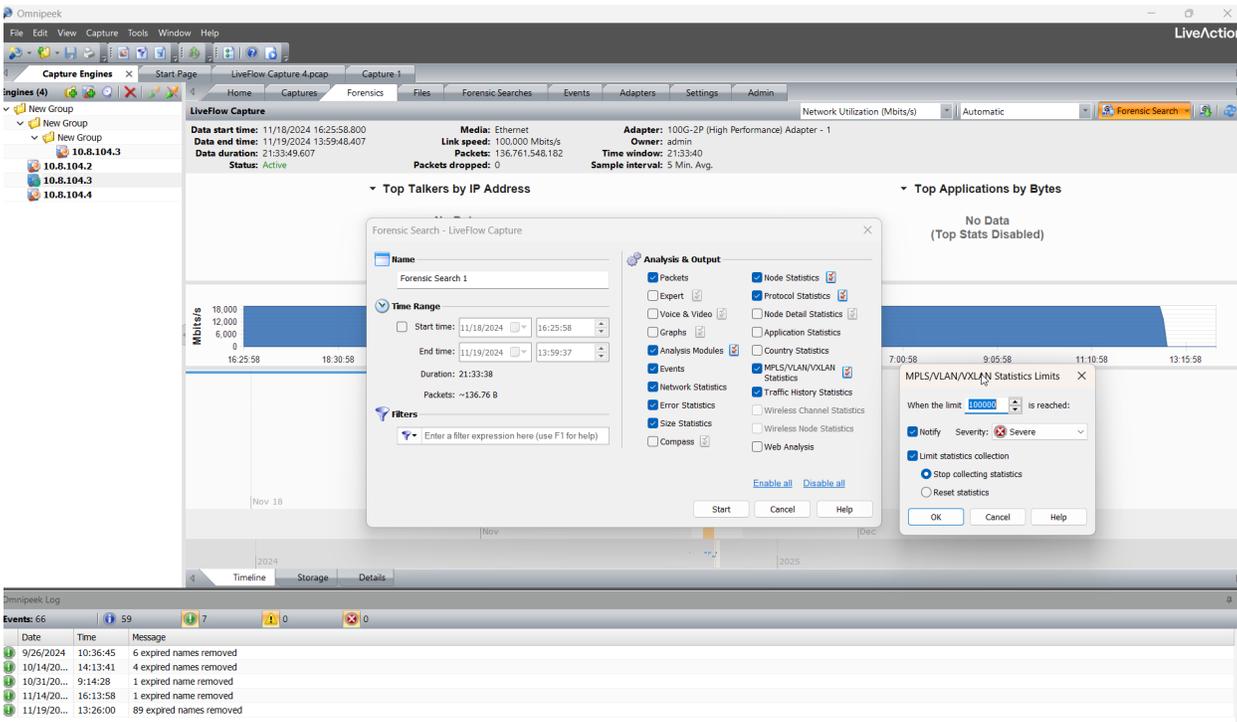
When creating a capture in Omnipeek Windows, the user may click the "Analysis Options" tab in the capture options dialog to see the list of analysis options that will be used to analyze the packets. A new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the capture window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the "Details..." button when the "MPLS/VLAN/VXLAN Statistics" item is selected will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.

Statistics" item is selected will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



Forensic Search

When creating a forensic search in Omnicap Windows, a new option will be present called "MPLS/VLAN/VXLAN Statistics" which will represent this new MPLS/VLAN/VXLAN Statistics view. Enabling this option will show the MPLS/VLAN/VXLAN Statistics view in the forensic search window, while disabling this option will hide the MPLS/VLAN/VXLAN Statistics view. Clicking the configuration button next to the "MPLS/VLAN/VXLAN Statistics" item will display the MPLS/VLAN/VXLAN Statistics Limits dialog and allow the user to modify the statistics limits for this MPLS/VLAN/VXLAN Statistics view.



Statistics Limits

The statistics limits work the same way as the other statistics limits work for other statistic views (such as Nodes, Node Details, Protocols, etc...). The only difference is that for MPLS/VLAN/VXLAN Statistics, the limit pertains to the total number of Nodes for all MPLS Labels, VLAN IDs, VXLAN Group Policy IDs and VXLAN VNIs.

Saving/Exporting MPLS/VLAN/VXLAN Statistics to a text file

The screenshot shows the Omnipcap application interface. The 'File' menu is open, and the option 'Save MPLS/VLAN/VXLAN Statistics...' is highlighted with a red rectangle. The background shows a network flow visualization with nodes and connections. The interface includes a menu bar (File, Edit, View, Capture, Tools, Window, Help), a toolbar, and a main display area with various panels like 'Visuals', 'Statistics', and 'MPLS/VLAN/VXLAN'.

File Menu Options:

- New Capture... (Ctrl+N)
- New Capture From Template
- New Multi-Segment Analysis Project... (Ctrl+Shift+M)
- Open... (Ctrl+O)
- Close (Ctrl+W)
- Save All Packets... (Ctrl+S)
- Save MPLS/VLAN/VXLAN Statistics...**
- Save Report...
- Save Capture Template...
- Print Setup...
- Print... (Ctrl+P)
- Print Selected Packets...
- Properties
 - 1 mpls-vlan.pcap
 - 2 sip_with_response.pcap
 - 3 C:\Users\...\o365_1_flow.pcap
 - 4 liveflow_capture_4_bad_flow.pcap
 - 5 LiveFlow Capture 4.pcap
 - 6 10dot5_Morning.pcap
 - 7 IPFIX-2024-06-04T15.58.24.870.pkt
 - 8 2021-02-25_shire_call_1_flow_needs_reassembly.pcap
- Exit

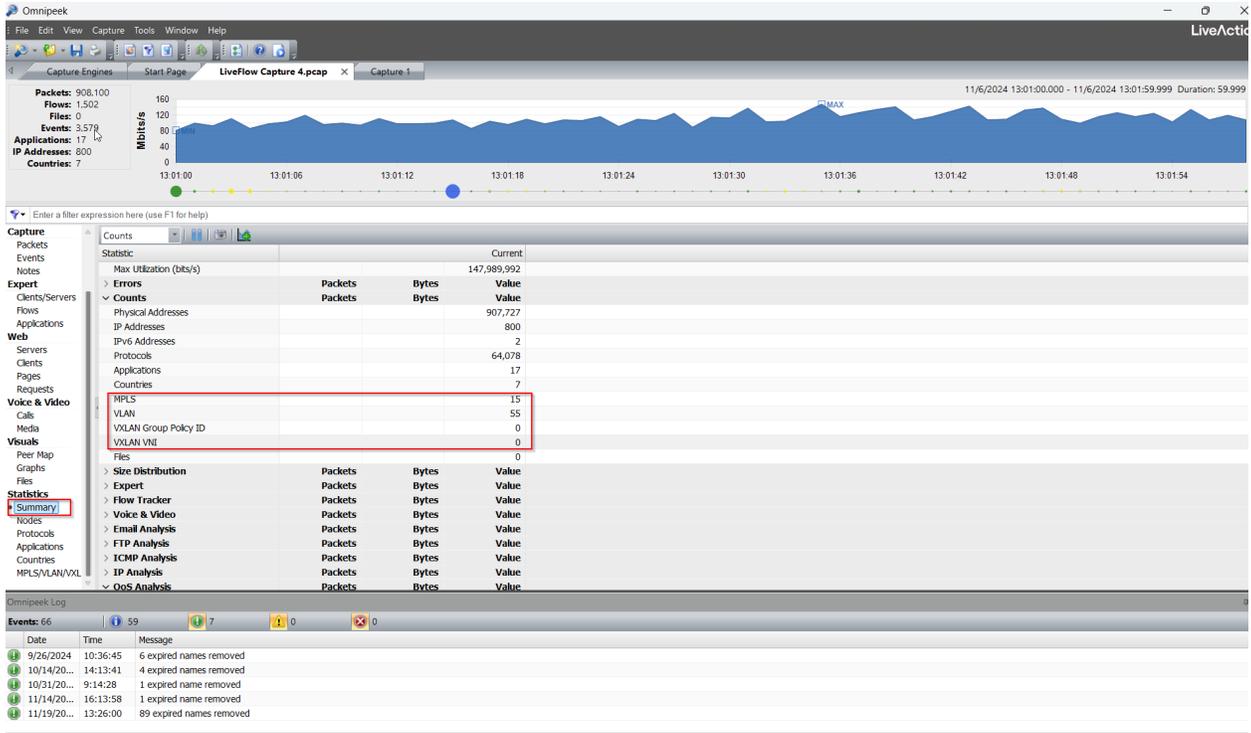
Visuals Panel:

- Peer Map
- Graphs
- Files

Statistics Panel:

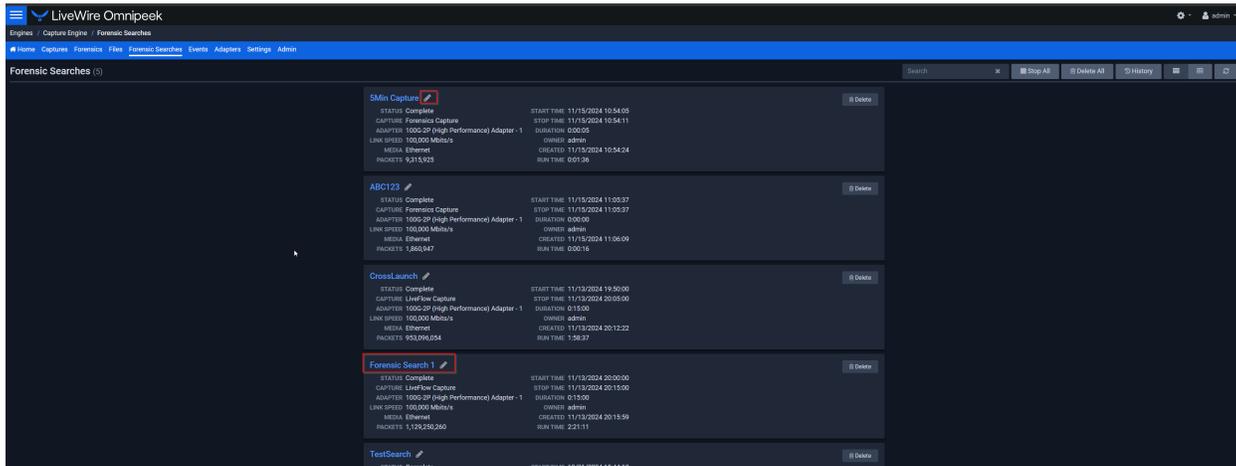
- Summary
- Nodes
 - Germany
 - United States
 - 19
 - Nodes
 - IP-4.4.4.2
 - IP-3.3.3.1
 - Protocols
 - Cisco:19:BC:41
 - Cisco:D8:28:C1
 - Protocols
 - TELNET
 - Applications
 - TCP

Statistics Summary page for MPLS/VLAN/VXLAN



Rename Forensic Search after creating/running the search

- Click the pencil next to the name of the Forensic Search you want to change the name of. In the screenshot below, the name of Forensic Search was changed to *5Min Capture*.



Specific Expert Flows in LiveWire Omnipeek

Here are the steps to search for specific flows in the *Expert Flows* section in LiveWire Omnipeek.

Go to *Forensic Search > Expert > Flows > Search* in the upper right corner of the screen.

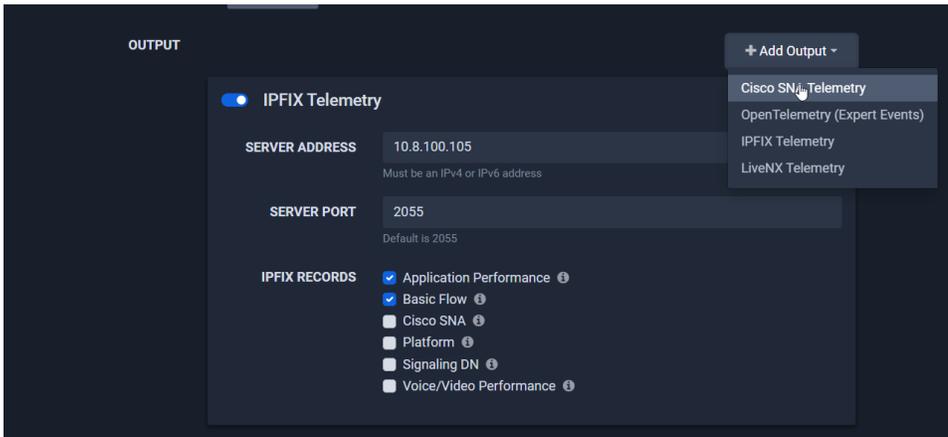
From there you can search by specific network data in the flow that you want to see instead of searching the flows manually.

The screenshot displays the LiveWire Omnipeek interface. The main window shows a table of Expert Flows with the following columns: FLOW ID, CLIENT HOST, SERVER HOST, SERVER PORT, EVENTS, PROTOCOL, APPLICATION, PACKETS, BYTES, START, DURATION, and APPLICATION. The table lists 24 flows, all originating from 193.176.124.115 and mostly destined to www.google.com. A search sidebar is open on the right, with a search bar at the top containing the text '2024-11-19 14:18:03.506'. The sidebar includes filters for CLIENT ADDRESS, CLIENT PORT, SERVER ADDRESS, SERVER PORT, PROTOCOL, APPLICATION, MPLS, VLAN, and VLAN ID. The search results are displayed in a table below the filters.

FLOW ID	CLIENT HOST	SERVER HOST	SERVER PORT	EVENTS	PROTOCOL	APPLICATION	PACKETS	BYTES	START	DURATION	APPLICATION
1	66.1.0.234	2071	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
2	193.176.124.115	56905	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238102
3	193.176.124.48	5475	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
4	66.1.0.217	56618	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238101
5	193.176.124.48	5340	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
6	193.176.124.117	26296	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238099
7	66.1.0.226	2047	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
8	193.176.124.117	28143	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238098
9	193.176.124.50	40114	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
10	66.1.0.19	28054	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238097
11	193.176.124.50	40312	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
12	193.176.124.119	60998	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238096
13	66.1.0.228	37073	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
14	193.176.124.119	60998	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238095
15	193.176.124.52	9532	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
16	66.1.0.21	60711	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238094
17	193.176.124.52	9532	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
18	193.176.124.121	30281	www.google.com	https	1	HTTPS	TCP	13	15,916	11/15/2024 11:05:37	0.238093
19	193.176.124.43	49645	www.google.com	https	1	HTTPS	TCP	5	4,088	11/15/2024 11:05:37	0.088162
20	66.1.0.240	5356	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
21	66.1.0.207	21487	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177474
22	193.176.124.54	44305	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177473
23	193.176.124.21	59774	www.google.com	https	0	HTTPS	TCP	33	50,094	11/15/2024 11:05:37	0.177474
24	66.1.0.88	47750	www.google.com	https	0	HTTPS	TCP	1	1,518	11/15/2024 11:05:37	0.000000

Send IPFIX Flow data to multiple targets

You can configure multiple locations/targets to send IPFIX/Flow data to. Either IPv4 or IPv6 IP addresses must be entered in the *Server Address* field.



You can also specify more than one location to send IPFIX flow data to.

You'll be able to configure LiveNX, IPFIX, OpenTelemetry, and Cisco SNA Telemetry instead of just a singular location.

LiveWire Group Authentication

LiveWires can be added to a “group” that shares the same authentication settings, allowing access without needing to enter or save a username and password.

The primary use case for this feature is to make using Distributed Forensic Search and the Multi-Engine feature easier.

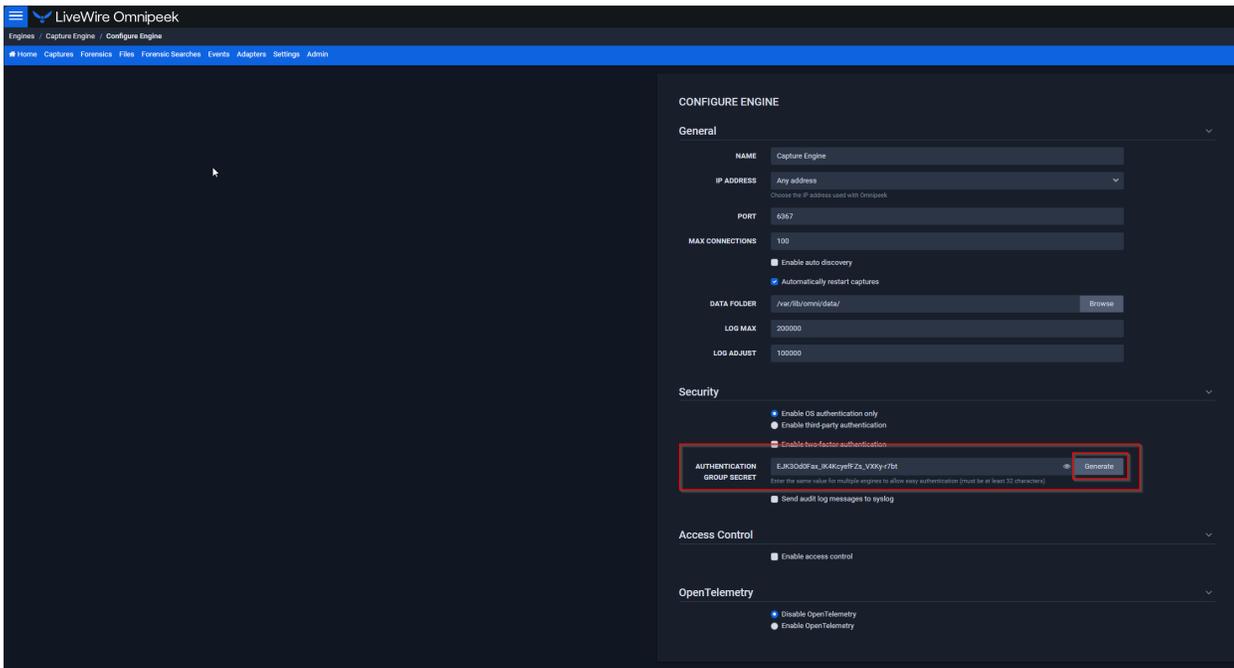
This feature was introduced in LiveWire 24.3 and requires this version or higher for LiveWires accessed remotely from the primary LiveWire.

Note This feature is only available in the LiveWire OmnipEEK and is not present in OmnipEEK Windows.

Configuration

Set up the Authentication Group Secret

On the **Configure Engine** page for your primary engine (the one you connect to directly), enter or generate an Authentication Group Secret. The primary engine maintains the list of engines you connect to remotely.



Apply the Secret to Other Engines

Next, enter the same Authentication Group Secret in the settings for each additional engine you want to access remotely from the primary engine. You can either:

- Use **Apply to Other Engines** to push the same settings (including other authentication and access control settings) to multiple engines, or
- Visit the **Configure Engine** page for each engine individually.

LiveWires are part of the same “authentication group” when they have the same Authentication Group Secret.

Compatibility

JWTs are now the default authentication method for the LiveWire Web UI by requesting a `tokenType` of "Bearer" in the login API. However, the previous authentication method is still supported by engines that do not support JWTs, ensuring backward compatibility.

Security

Since JWTs carry sensitive information, they are always transmitted over encrypted channels (TLS) to prevent eavesdropping. However, if an attacker gains access to a JWT, they could use it to obtain unauthorized access. To mitigate this risk, JWTs used by LiveWire have a short expiration time (15 minutes) and must be periodically renewed using a "refresh token".

Expiration & Refresh Tokens

When the LiveWire UI requests a JWT from the login API, the engine returns an access token with a short expiration time (15 minutes by default) along with a "refresh token". The refresh token is used to obtain new access tokens when the current one nears expiration. The web UI will automatically request a new access token about 1 minute before the current token expires.

- **Remote Engine Connections**

The access token is used to connect to remote engines, with the session identified by the session ID in the token. The session will remain active even after a new token is issued.

- **Refresh Token Lifetime**

The refresh token also has an expiration time, typically set to 1 day. Both the refresh token and access token lifetimes can be configured in *omni.conf* by adjusting the `refreshTokenLifetime` and `accessTokenLifetime` settings, respectively.

References

[JWT RFC](#)

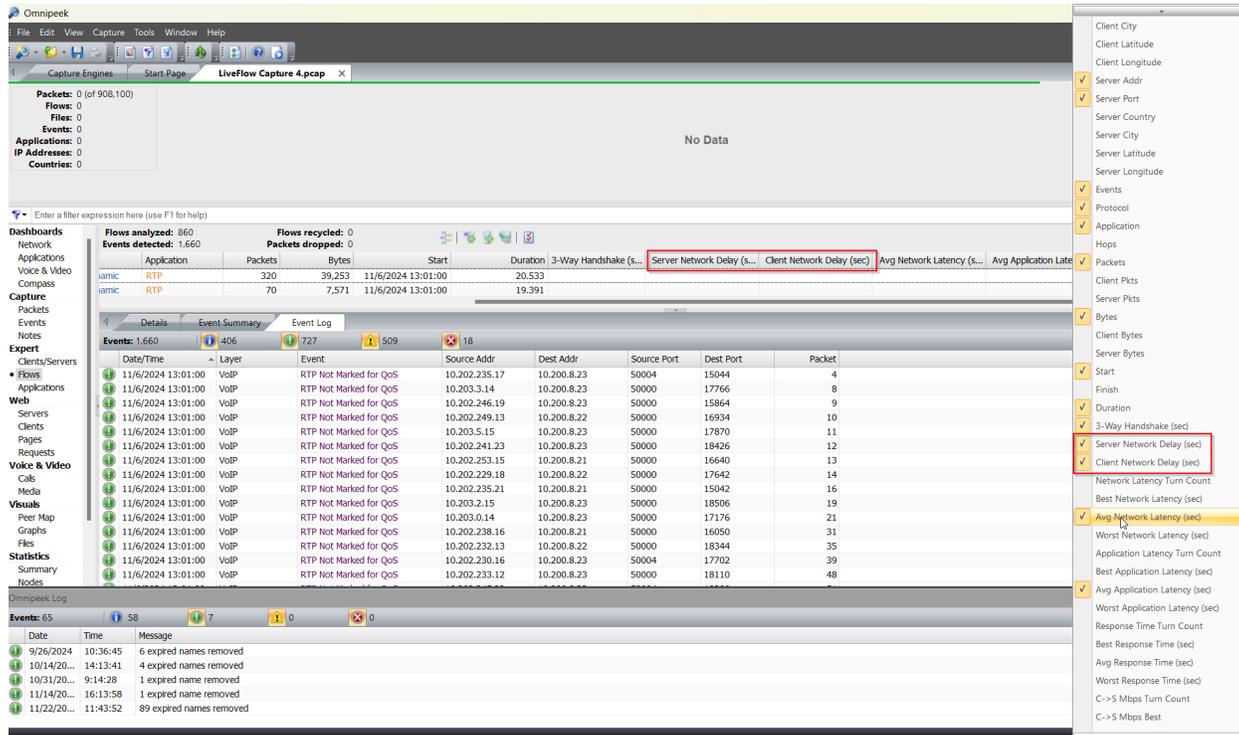
[Token Best Practices](#)

[Refresh Tokens](#)

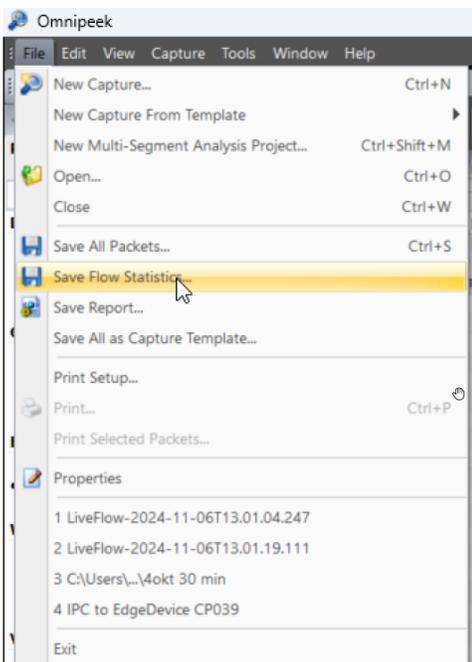
New Expert Events have been added to Omnipeek Windows

The following values have been added to Expert:

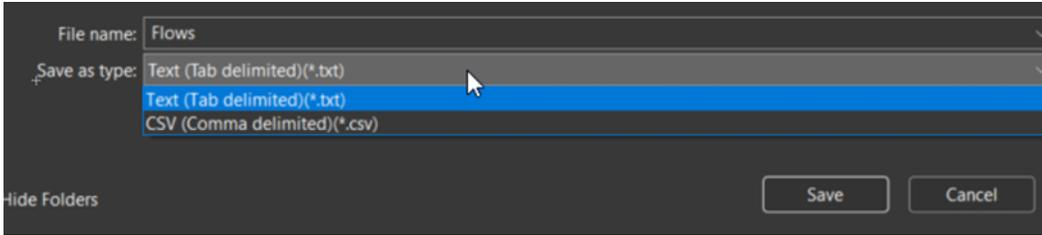
- *Server Network Delay (sec)* - the packet time difference between the TCP SYN packet and the TCP SYN-ACK packet in a TCP 3-way Handshake
- *Client Network Delay (sec)* - the packet time difference between the TCP SYN-ACK packet and the TCP ACK packet in a TCP 3-way Handshake



You can also export the data in *Save Flow Statistics* in the **File** menu.



This will save the Server/Network Delay statistics in a comma separated value file or text file.



Example of flows.text file contents:

```

a statistics file created Tuesday, November 12, 2024 16:53:01
Client Addr Client Port Server Addr Server Port Events Protocol Application Packets Bytes Start Duration 3-Way Handshake (sec) Avg Network Latency (sec)
cation Latency (sec) TLS Version TCP Status
RAY01.local 56157 52.40.255.127 https 0 HTTPS Amazon Services 157 17699 11/12/2024 16:38:54 0:05:20.131 0.086 0.000 Open
RAY01.local 57687 170.114.4.223 https 1 HTTPS SSL 60 9517 11/12/2024 16:38:54 0:05:01.885 0.025 1.586 Open
RAY01.local 60563 self.events.data.microsoft.com https 0 HTTPS SSL 173 166083 11/12/2024 16:38:55 0:05:18.897 0.013 0.019 Open
RAY01.local 57291 52.96.36.82 https 0 HTTPS UDP 322 153416 11/12/2024 16:38:55 0:05:10.086 0.088 0.000 Open
RAY01.local 63361 35.83.181.24 https 0 HTTPS SSL 150 16940 11/12/2024 16:38:55 0:05:10.114 0.012 0.792 Open
RAY01.local 57646 170.114.1.184 https 1 HTTPS SSL 34 3602 11/12/2024 16:38:55 0:05:03.364 0.012 0.792 Open
RAY01.local 51872 23.222.241.151 https 0 HTTPS UDP 5 415 11/12/2024 16:38:56 9.998 0.083 0.146 Open
RAY01.local 63447 44.238.43.4 https 3 HTTPS SSL 219 25510 11/12/2024 16:38:56 0:05:10.133 0.006 0.000 Open
RAY01.local 59291 192.168.1.168 nvme-disc 0 nvme-disc SSL 192 25600 11/12/2024 16:38:56 0:05:15.991 0.070 0.081 0.005 Open
RAY01.local 61028 104.192.138.12 https 0 HTTPS Atlasian 15 6650 11/12/2024 16:38:58 2.571 0.000 Closed
RAY01.local 63994 192.168.1.1 domain 0 DNS DNS 28 4391 11/12/2024 16:38:58 0:03:11.208 0.025 0.000 Open
49.184.14 61233 RM-BGRAY01.local 49914 51 TCP-49914 SSL 905 143439 11/12/2024 16:38:58 0:05:16.277 0.033 1.629 Open
RAY01.local 64542 192.168.1.1 domain 0 DNS DNS 28 4203 11/12/2024 16:38:58 0:03:15.315 0.025 0.000 Open
RAY01.local 58203 192.168.1.1 domain 0 DNS DNS 22 3416 11/12/2024 16:38:58 0:03:11.205 0.032 0.000 Open
RAY01.local 65044 192.168.1.1 domain 0 DNS DNS 26 3166 11/12/2024 16:38:58 0:03:15.315 0.027 0.000 Open
RAY01.local 54864 192.168.1.1 domain 0 DNS DNS 28 4563 11/12/2024 16:38:58 0:03:15.315 0.026 0.000 Open
RAY01.local 64750 192.168.1.1 domain 0 DNS DNS 26 3994 11/12/2024 16:38:58 0:03:15.315 0.030 0.000 Open
RAY01.local 61029 108.138.246.80 https 0 HTTPS Atlasian 14 3330 11/12/2024 16:38:58 2.415 0.067 0.066 0.000 Closed
RAY01.local 61030 3.169.182.215 https 0 HTTPS Amazon Cloud 14 3307 11/12/2024 16:38:58 2.422 0.074 0.075 0.000 Closed
RAY01.local 61031 18.244.214.21 https 0 HTTPS Atlasian 14 3365 11/12/2024 16:38:58 2.252 0.065 0.067 0.000 Closed
RAY01.local 56221 3.128.195.20 https 0 HTTPS SSL 148 15824 11/12/2024 16:38:59 0:05:10.073 0.038 0.000 Open
RAY01.local 63541 52.112.84.177 https 0 HTTPS Microsoft Services 24 2168 11/12/2024 16:38:59 0:04:40.107 0.042 0.000 Open
68.1.193 5353 mDNS mdns 0 DNS MulticastDNS 7 2242 11/12/2024 16:38:59 0:04:00.534
:18d8:fca1:eaac:b2c4 5353 mDNSv6 mdns 0 DNS MulticastDNS 6 1966 11/12/2024 16:38:59 0:04:00.534
RAY01.local 60373 104.192.138.12 https 15 HTTPS SSL 48 6208 11/12/2024 16:39:00 0:05:01.978 0.066 20.060 Open
RAY01.local 60950 us.telemetry.zoom.us https 0 HTTPS TCP 4 274 11/12/2024 16:39:00 0.009 Closed Closed
RAY01.local 60911 170.114.52.2 https 0 HTTPS TCP 4 274 11/12/2024 16:39:00 0.007 Closed Closed
RAY01.local 61032 us.telemetry.zoom.us https 43 HTTPS Zoom 56 12573 11/12/2024 16:39:00 0:05:06.888 0.009 0.009 0.016 Open
RAY01.local 60374 104.192.138.12 https 15 HTTPS SSL 48 6208 11/12/2024 16:39:00 0:05:02.045 0.066 20.064 open
68.1.163 5353 mDNS mdns 0 DNS MulticastDNS 45 24590 11/12/2024 16:39:01 0:05:13.646
:1259:32ff:fe73:3576 5353 mDNSv6 mdns 0 DNS MulticastDNS 45 24590 11/12/2024 16:39:01 0:05:13.648
RAY01.local 57674 170.72.245.140 https 1 HTTPS SSL 100 14235 11/12/2024 16:39:01 0:05:00.675 0.045 1.066 Open
RAY01.local 59712 172.64.148.154 https 23 HTTPS Cloudflare 72 6350 11/12/2024 16:39:02 0:05:10.631 0.008 13.496 Open
RAY01.local 61007 wxt-general-ingressgateway.acmhwxt-prd-2.prod.infra.webex.com https 0 HTTPS TCP 6 409 11/12/2024 16:39:02 27.651 0.030
    
```