# LiveWire 24.3.0 New Features

# QUICK GUIDE



# 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".

ngines / Capture Engine / Forensic	nipeek Searches / Forensics Capture 3	/ Packets								🌣 - 🛔 adr
Home Captures Forensics Files	Forensic Searches Events Ad	lapters Settings A	dmin							
Packets (502,763)								← → 502748	Go Select 差	0
T - Enter a filter expression										Apr
PACHET SOURCE 502,737 92 122 206 95 502,739 92 122 206 95 502,739 10.244.4.159 502,740 10.244.4.155 502,741 10.244.4.222 502,742 10.10.10.1 502,743 10.10.10.2 502,744 10.10.10 502,745 10.10.10.2	BESTINATION 10 99.27.121 10 99.27.121 10 224.47.142 10 125.30.81 10 10 10.2 10 10 10.1 10 10 10.2 10 10 10.1 10 10 10.2	FLOW ID 6353 6353 6226 6297 6326 6363 6363 6363 6363 6363 6363	size 1,566 1,566 1,560 1,530 82 152 152 152 152 152 152	BLCATHE TIME PROTOCOL           0.04.24.02081           0.04.24.02083           0.04.24.02083           0.04.24.02083           0.04.24.02083           0.04.24.02085           0.04.24.02087 </th <th>APPLICATION TCP TCP TCP TCP TCP TCP ICMP ICMP ICMP ICMP ICMP</th> <th>INMANY         CVERT           Scr. 1935,Dul-50437,A.,5-1005813,.         Scr. 1935,Dul-5047,A.,5-1005818,.           Scr. 1935,Dul-5047,A.,5-1005818,.         Scr. 2012,Dul-2017,A.,5-1005818,.           Scr. 2012,Dul-2017,A.,5-1005818,.         Scr. 2012,Dul-2017,A.,5-1005818,.           Scr. 2012,Dul-2017,S,A.,5-3098779,.         Scr. 2012,Dul-2017,S,A.,5-3098779,.           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106</th> <th></th> <th>1709 1709 1709 1709 1709 1709</th> <th>Brook Hets Sweckert Annu           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)</th> <th>***</th>	APPLICATION TCP TCP TCP TCP TCP TCP ICMP ICMP ICMP ICMP ICMP	INMANY         CVERT           Scr. 1935,Dul-50437,A.,5-1005813,.         Scr. 1935,Dul-5047,A.,5-1005818,.           Scr. 1935,Dul-5047,A.,5-1005818,.         Scr. 2012,Dul-2017,A.,5-1005818,.           Scr. 2012,Dul-2017,A.,5-1005818,.         Scr. 2012,Dul-2017,A.,5-1005818,.           Scr. 2012,Dul-2017,S,A.,5-3098779,.         Scr. 2012,Dul-2017,S,A.,5-3098779,.           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106           Scr. 40002,Dul-8472,L, 106         Scr. 40002,Dul-8472,L, 106		1709 1709 1709 1709 1709 1709	Brook Hets Sweckert Annu           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)           0x000036A (16042)	***
502,747 10.10.10.2 502,748 10.10.10.1 502,749 10.10.10.2	10.10.10.1 10.10.10.2 10.10.10.1	6363 6363 6363	152 152 152	0:04:45.823300 ICMP Echo Reply 0:04:46.824344 ICMP Echo 0:04:46.824344 ICMP Echo Reply	ICMP ICMP ICMP	Src=48002,Dst= 8472,L= 106 Src=48002,Dst= 8472,L= 106 Src=48002,Dst= 8472,L= 106		1709 1709 1709		
John Street 2: Pool      John Street 2: P	Let Number-502746 F-0x00000 202454-001210F-665 5-525.54-00 7.5. Services-10-000 102-100 000000 (SI-401) 000000 (SI-401) 000000 (SI-401) 000000 (SI-401) 00000 (SI-401) 000000 (SI-401) 000	0000 S=0x00000000 1:63:E2:80 ion Flags=%000 S+ xfffff00] 7:58:D5:22 ion Flags=%010 S- Checksum=0x4E58 Ic	L=152 T=11 192.168.1. 19.10.10.10.1 entifier=0	124:24.4336830 00/29/2024 Channel 1 0-192,100,2.1 0-10.10.10.2 1105 Sequence Runber-4 ICMP Data A	=3 rea=.).Uy	×	0 16 32 48 64 80 96 112 128 144	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	RTRT.CE. 	V

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

= \	LiveWire Om	nipeek														¢٠	💄 admin 🗵
Engines /	Capture Engine / Forensic:	Searches / Forensics Capture 3 /	Packets	dmin													
Deeke			piera ociunga z														
Раске	<b>IS</b> (502,763)									•	>	502748		GO	Select	•	3
۳.	Enter a filter expression																Apply
	PACKET SOURCE	DESTINATION	FLOW ID	SIZE	RELATIVE TIME PROTOCOL	APPLICATION	SUMMARY EXPERT		D	ECODE/VX	LAN/VXLAI	N NETWORK I	DENTIFIE DE	CODE/MPLS	UNICAST/LABEL		
5	02,736 10.244.4.149	10.244.47.182	6339	82	0:04:24.020826 TCP	TCP	Src=12002,Dst=39712,.A,S=4093783						Channel				<b>^</b>
5	02,737 92.122.206.95	10.93.27.121	6353	1,566	0:04:24.020881 TCP	TCP	Src= 1935,Dst=50437,.A,S=1005813						Adapter				
5	02,738 92.122.206.95	10.93.27.121	6353	1,566	0:04:24.020934 TCP	TCP	Src= 1935,Dst=50437, A, S=1005815						✓ Size				
5	02,739 10.244.4.159	10.244.47.142	6296	716	0:04:24.020953 TCP	TCP	Src=34700,Dst=12002, AP,S=193546						IP Length				
5	02,740 10.244.4.155	10.125.30.11	6297	1,530	0:04:24.020987 TCP	TCP	Src=53262,Dst=12002, A,S=3848277						IP ID				
5	02,741 10.244.4.222	10.125.30.81	6326	82	0:04:24.020987 TCP	TCP	Src=12002,Dst=35975, A,S=3988719						Date				
5	02,742 10.10.10.1	10.10.10.2	6363	152	0:04:43.819235 ICMP Echo	ICMP	Src=48002,Dst= 8472,L= 106		1	709			Time				
5	02,743 10.10.10.2	10.10.10.1	6363	152	0:04:43.819808 ICMP Echo Reply	ICMP	Src=48002,Dst= 8472,L= 106		1	709			Delta Time				
5	02,744 10.10.10.1	10.10.10.2	6363	152	0:04:44.821257 ICMP Echo	ICMP	Src=48002,Dst= 8472,L= 106		1	709			<ul> <li>Relative Ti</li> </ul>	me			
5	02,745 10.10.10.2	10.10.10.1	6363	152	0.04:44.821261 ICMP Echo Reply	ICMP	Src=48002,Dst= 8472,L= 106		1	709			<ul> <li>Protocol</li> </ul>				
5	02,746 10.10.10.1	10.10.10.2	6363	152	0:04:45.823300 ICMP Echo	ICMP	Src=48002,Dst= 8472,L= 106		1	709			<ul> <li>Application</li> </ul>	n			
5	02,747 10.10.10.2	10.10.10.1	6363	152	0:04:45.823300 ICMP Echo Reply	ICMP	Src=48002,Dst= 8472,L= 106		1	709			Filter				
5	02,748 10.10.10.1	10.10.10.2	6363	152	0:04:46.824344 ICMP Echo	ICMP	Src=48002,Dst= 8472,L= 106		1	709			<ul> <li>Summary</li> </ul>				
	Info:         Pac           11-13         IPv4:         Oif           14-33         IPv4:         Oif           34-43         UDP:         Src           34-43         UDP:         Src           67009         Policy ID:         YXLAN - Virtual Xtensib           Flags:         Group Policy ID:         YXLAN Network Identifi           64-83         IPv4:         Oif           64-87         IOP:         IC           148-151         FCS:         FCS	Net Nuber-92746 F-003080 F-154009120746 5-52754400 F-557456-0100 Fregmental weinham Detreev In:100 9322 (4-4-6) 9322 (4-4-	00 S=0x00000000 63:E2:B0 on Flags=X000 S ::::FFFFF00] 58:D5:2C on Flags=X010 S ecksum=0x4E58 L	L=152 T=1: =192.168.1 =10.10.10.1	24124.44334839 00/29/2024 Channel 1 D-102.168.2.1 D-10.10.10.2 sequence Number-4 ICMP Data A	=3 rea=.).Uy	••••••••••••••••••••••••••••••••••••••	0 16 32 48 64 80 96 112 128 144	52 54 00 12 0F 6E 00 66 02 20 00 02 21 88 62 21 18 AD 00 3A CF 9F 8F 45 00 00 54 5C C4 00 00 00 54 5C C4 00 00 00 00 59 57 14 15 16 17 18 19 24 25 26 27 28 29 34 35 36 37 F8 9A	52 54 6 40 11 F 00 72 0 DE 16 F 40 00 4 4E 58 1 00 00 0 1A 18 1 2A 28 2 88 1F	00 63 22 3 32 00 10 00 88 4 04 47 10 01 85 11 D8 00 10 00 00 10 10 1E 10 2D 2E	80 08 0 A8 01 0 55 D5 2 CE 0A 04 A6 29 00 10 11 1 1F 20 21 1 2F 30 31 1	Analysis M Expert Decode/VJ Decode/M 95 55 12 13 22 23 23 588 456	Iodule KLAN/VXL PLS Unica: 	N Network Id 1/Labe .).0  1"= 0123	entifier (v	<b>NI)</b>

# Enable MPLS, VLAN, and VXLAN Expert Events in Omnipeek Windows

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



# 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. Clicking the "Details..." button when the "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 Omnipeek 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.

۶	Omnipeek					<b>5</b> 7
File	Edit View Cap	oture Tools Window He	elp			0
2	New Capture		Ctrl+N			
	New Capture Fro	om Template	•	×		
	New Multi-Segm	nent Analysis Project	Ctrl+Shift+M			
6	Open		Ctrl+O			
	Close		Ctrl+W			
	Save All Packets.		Ctrl+S			
H	Save MPLS/VLA	N/VXLAN Statistics			21.29.57	
8	Save Report			5.43	21:28:57	
	Save Capture Ter	mplate				
	Print Setup			D-I' ID-0		<u></u>
6	Print		Ctrl+P	ip Policy ID: 0	VXLAN VNI: 0	- <b>- - - - - - - - - -</b>
	Print Selected Pa	ackets				
۷	Properties			_		
	1 mpls-vlan.pcap	þ				
	2 sip_with_respo	nse.pcap				
	3 C:\Users\\o36	65_1_flow.pcap				
	4 liveflow_captu	re_4_bad_flow.pcap				
1	5 LiveFlow Captu	ure 4.pcap				
	6 10dot5_Morni	ng.pcap		J		
	7 IPFIX-2024-06	-04T15.58.24.870.pkt				
١.	8 2021-02-25_sł	nire_call_1_flow_needs_rea	ssembly.pcap			
	Exit					
Visu	als	💻 Germar	у			
Pee	er Map ophs	United :	States		_	
File	s	✓ 19				
Stati	istics	IP-4.4.4	.2		_	
Sur	nmary les	IP-3.3.3	8.1			
Pro	tocols	Cisco:1	9:BC:41			
App	olications	Cisco:D	8:28:C1			
Cou	untries	✓ Protocols				
• MPI	LS/VLAN/VXLAN	TELNET				
		✓ Applications				
		🙈 ТСР				

# Statistics Summary page for MPLS/VLAN/VXLAN

Omnipeek     File Edit View     Capture     Capture     Packet: 9     Flow: 1,     File: 0     Event: 3,     Applications: 1:     IP Addresse; 7	Capture Tools Window Help Engines Start Page LiveFlow 502 578 700 59 59 50 57 57 57 50 50 50 50 50 50 50 50 50 50 50 50 50	Capture 4.pcap X Ca	13.01:12	13.01:18	13.01.24	13.01.30	13.01.36	11/6/2024	13.01:00.000 - 11/6/2024	- O × LiveAction 13:01:59.999 Duration: 59.999 13:01:54
Sector a filter €	expression here (use F1 for help)									
Capture										
Packets	Counts I I I I I I I I I I I I									
Events	Statistic			Current						
Notes	Max Utilization (bits/s)			147,989,992						
Expert	> Errors	Packets	Bytes	Value						
Clents/Servers	~ Counts	Packets	Bytes	Value						
Applications	Physical Addresses			907,727						
Web	IP Addresses			800						
Servers	IPv6 Addresses			2						
Clients	Protocols			64,078						
Pages	Appications			1/						
Requests	Countries			7						
Voice & Video	MPLS			15						
Calls	VLAN			55						
Media	VXLAN Group Policy ID			0						
Visuals	VXLAN VNI			0						
Graphs	Fies									
Files	> Size Distribution	Packets	Bytes	value						
Statistics	> Expert	Packets	Bytes	Value						
Summary	> Flow Tracker	Packets	Bytes	Value						
Nodes	> Voice & Video	Packets	Bytes	Value						
Protocols	> Email Analysis	Packets	Bytes	Value						
Applications	> FTP Anarysis	Packets	Bytes	value						
Countries	> ICMP Analysis	Packets	Bytes	Value						
MPLS/VLAN/VXL	> IP Analysis	Packets	Bytes	Value						
Omnipeek Log	* 005 Allalysis	Packets	Dytes	value						a
Eventer 66	<b>10</b> 50 <b>10</b> 7									
Events: 00										
Date	Ime Message									
9/26/2024	10:36:45 6 expired names removed									
10/14/20	14:13:41 4 expired names removed									
10/31/20	9:14:28 1 expired name removed									
11/14/20	16:13:58 1 expired name removed									
11/19/20	13:26:00 89 expired names removed									

# 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.

😑 🤝 LiveWir	re Omnipeek										🗘 - 🔺 admin -
Engines / Capture Engine	/ Forensic Searches / Forensics Captu	are 9 / Expert Flows									
Home Captures Foren	sics Files Forensic Searches Events	s Adapters Setting									
# Home	Expert Flows									Search 🛋	• 2
Dashboard Network Applications										CLIENT ADDRESS	
Voice & Video									3-WAY HANDSHAKE (SEC) AVG NETWORK LATENCY (S., AVG APPLICATION	CLIENT PORT	
Compass			www.google.com	https		50,094	11/15/2024 11:05:37			•	1
Packets		56950	www.google.com					0.238102		SERVER ADDRESS	
Events			www.google.com			50,094	11/15/2024 11:05:37			•	
Expert			www.google.com							SERVER PORT	
Clients/Servers		5340	www.google.com	https		50,094				•	
Flows			www.google.com					0.238099		PROTOCOL	
Applications Event Summary			www.google.com			50,094	11/15/2024 11:05:37			•	
Event Log			www.google.com					0.238098		APPLICATION	
Web			www.google.com	https		50,094	11/15/2024 11:05:37			•	
Servers			www.google.com					0.238097		MPLS	
Clients			www.google.com			50,094				•	
Pages		60998	www.google.com					0.238095		10 414	
Voice 8 Midee			www.google.com			50,094	11/15/2024 11:05:37				
Calls		60998	www.google.com					0.238095			
Media			www.google.com			50,094				VXLAN GPID	
Visuals			www.google.com					0.238094			
Peer Map			www.google.com			50,094	11/15/2024 11:05:37			VXLAN VNI	
Graphs			www.google.com					0.238093		-	
Reconstructions		49645	www.google.com	https	Amazon Web Services	4,688	11/15/2024 11:05:37	0.086162		START	
Statistics			www.google.com			50,094				2024-11-19 14:18:03:50	
Nodes			www.google.com			50,094				FINISH	
Protocols		44305	www.google.com			50,094				2024-11-19 14:18:03.50	
Applications			www.google.com	https		50,094				Canada Canada	
Countries			www.google.com					0.000000		Canon Starc	

# 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.

### **Enable Authentication Group Connection**

Finally, enable **Connect with an authentication group** when inserting or editing an engine in the **Engines** list of the primary engine.

= VLiveWire Omnipeek	
Engines	
Engines	
Search X Determine / Edit 2 Delete	GROUP
NAME -	
	NAME
	Oppional 'nickname'
	но́ят
	IP address or hostname
	CONNECTION
	Connect with an authentication group
	You will not have to enter credentials every time you connect.
	The engine must be using the same group secret.
	Connect with saved credentials     Connect by entering credentials each time
	Cancel

#### Use

#### • Seamless Remote Connection

Connect to remote engines from the primary engine without being prompted for a username or password.

#### • Effortless Distributed Features

Use Distributed Forensic Search or Multi-Segment Analysis without the need to re-enter authentication details.

### **Implementation Details**

The LiveWire Omnipeek UI and back-end now use JSON Web Tokens (JWTs), a widely adopted technology in modern web applications. These tokens contain information such as the expiration time (exp), the time the token was issued (iat), a username (name), a not-valid-before time (nbf), a session id (sess), and a user id (sub). JWTs are signed to verify authenticity.

#### Example

In this screenshot of the Chrome Developer Tools Network Tab, the login API returns a JWT for the authToken in the response along with the tokenType "Bearer". This is otherwise known as an **access token**.



#### The complete JWT returned is

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjY4NDIzNzgsImlhdCI6MTcyNjg0MTQ3OCwibmFtZ SI6ImFkbWluIiwibmJmIjoxNzI2ODQxNDc4LCJzZXNzIjoiNjY5M2UzN2FhNDQ2ZDlkNjBkNmUxYTMyNGYzMzk2OTU iLCJzdWIiOiJhZG1pbiJ9.HHTNCdyWKe7inqS8ZA2D5hzWLySRHp4IbXqgbsj5pC4.

The token is in 3 parts: the header, payload, and signature. It is signed using the Authentication Group Secret, mGyHk81TmH4YwIN\_qxaFQASKPI9QusfY.

#### The token can decoded and verified online <a href="https://jwt.io/#debugger-">https://jwt.io/#debugger-</a>

io?token=eyJhbGciOiJIUzI1NilsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjY4NDIzNzgsImlhdCI6MTcyNjg0MTQ3OCwibmFtZSI 6ImFkbWluliwibmJmljoxNzI2ODQxNDc4LCJzZXNzljoiNjY5M2UzN2FhNDQ2ZDlkNjBkNmUxYTMyNGYzMzk2OTUiLCJz dWliOiJhZG1pbiJ9.HHTNCdyWKe7inqS8ZA2D5hzWLySRHp4IbXqgbsj5pC4.

### 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 I 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

Omnipeek													*
- File - File - Mar	. Cashing	Table Monday, 1	late										Client City
: File Edit Vie	w Capture	Tools Window F	нер	-									Client Latitude
😥 - ધ - 🖡	- 😂 🚽	2 🛐 😟 🚽 🏤	- E C	<b>3</b>									
4 Capture	Engines	Start Page	LiveFlow Cant	ure 4 pcap X								_	Llient Longitude
				and opening to								~	Server Addr
Packets:	) (of 908,10) 1	))										<	Server Port
Files:	5												Server Country
Events:	D												Server City
Applications:	) 1								No Data				Family Latitude
Countries:	5												Server Latitude
													Server Longitude
												<	Events
• • • • • • • • • • • • • • • • • • •												✓	Protocol
Y Enter a filte	expression	tere (use r i tor neip)										~	Application
Dashboards	Flows	analyzed: 860	Pa	Flows recycled: 0		- 🗄 😵 😵 🕏	2   🗵					_	Hoos
Applications		Application	Dackate	Butoc		Chart	Duration 2 Way Handsha	ko (r. Conuor	Natwork Data (c	Cleant Natwork Dalay (coc) Ava Natwork Latance	(c Ava Application Late	-	
Voice & Video		Appication	POLICES	20.252	11/0/2024 12	3tart	20 C22	ske (S Server	Network Delay (S	Clent Network Deay (sec) Avg network Latency	(S Wy Appleadon Late	×	Packets
Compass	amic	DTD	320	7 571	11/6/2024 13	01:00	20.555						Client Pkts
Capture	iumic.			1,011	11/0/2024 15		19.991						Server Pkts
Packets	1 /	Datalla Eur		Current La cu	_			) •	· · · · · · · · · · · · · · · · · · ·			<b>v</b>	Bytes
Notes	× /	Details Eve	ent summary	Event Log								Ξ.	Client Bytes
Expert	Event	s: 1,660	9 406	727	509	18							Farmer Britan
Clents/Servers	0	ate/Time	<ul> <li>Layer</li> </ul>	Event		Source Addr	Dest Addr	Source Port	Dest Port	Packet		_	server bytes
<ul> <li>Flows</li> </ul>	1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.235.17	10.200.8.23	50004	15044	4		~	Start
Applications	1	1/6/2024 13:01:00	VOIP	RTP Not Mark	ed for QoS	10.203.3.14	10.200.8.23	50000	17766	8			Finish
Servers		1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.246.19	10.200.8.23	50000	15864	9		✓	Duration
Clients		1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.249.13	10.200.8.22	50000	16934	10		<b>v</b>	3-Way Handshake (sec)
Pages		1/6/2024 13:01:00	VOIP	RTP NOL Mark	ed for QoS	10.203.5.15	10.200.8.23	50000	1/8/0	12		1	Server Network Delay (ser)
Requests		1/6/2024 13:01:00	VOIP	RTP NOL Mark	ed for QoS	10.202.241.25	10.200.8.25	50000	16640	12		÷	Server methods being (see)
Voice & Video	1 8 1	1/6/2024 13:01:00	VOIP	RTP Not Mark	ed for QoS	10 202 229 18	10 200 8 22	50000	17642	14		v	client Network Delay (sec)
Calls	l ä i	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.235.21	10.200.8.21	50000	15042	16			Network Latency Turn Count
Visuals	l ŏ i	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.203.2.15	10.200.8.23	50000	18506	19			Best Network Latency (sec)
Peer Map	1 👸 1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.203.0.14	10.200.8.23	50000	17176	21		<ul> <li>Image: A second s</li></ul>	Avg Network Latency (sec)
Graphs	1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.238.16	10.200.8.21	50000	16050	31			Norst Network Latency (sec)
Files	1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.232.13	10.200.8.22	50000	18344	35			Anniantina Latana Tum Count
Statistics	1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.230.16	10.200.8.23	50004	17702	39			Application catericy furn Count
Nodes	1	1/6/2024 13:01:00	VoIP	RTP Not Mark	ed for QoS	10.202.233.12	10.200.8.23	50000	18110	48			Best Application Latency (sec)
Omnineek Log	- // -									-		<	Avg Application Latency (sec)
Ommipeek cog													Worst Application Latency (sec)
Events: 65		58 🕖	7 💋	0	30								Response Time Turn Count
Date	Time	Message											Best Personne Time (ser)
9/26/2024	10:36:45	6 expired names r	removed										Seat response time (SEC)
10/14/20	14:13:41	4 expired names r	removed										avg kesponse Time (sec)
10/31/20	9:14:28	1 expired name re	emoved										Worst Response Time (sec)
11/14/20	16:13:58	1 expired name re	emoved										C->S Mbps Turn Count
11/22/20	11:43:52	89 expired names	removed										C->S Mbps Best
			_		_			_					

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

Ş	0	mnipeek	
1	File	Edit View Capture Tools Window	Help
	5	New Capture	Ctrl+N
4		New Capture From Template	
I		New Multi-Segment Analysis Project	Ctrl+Shift+M
-	ø	Open	Ctrl+O
4		Close	Ctrl+W
1	H	Save All Packets	Ctrl+S
	H	Save Flow Statistice	
	8	Save Report	
٩		Save All as Capture Template	
		Print Setup	
	8	Print	Ctrl+P
I		Print Selected Packets	
	2	Properties	
IJ		1 LiveFlow-2024-11-06T13.01.04.247	
1		2 LiveFlow-2024-11-06T13.01.19.111	
		3 C:\Users\\4okt 30 min	
		4 IPC to EdgeDevice CP039	
١		Exit	

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

File name:	Flows ~
_Save as type:	Text (Tab delimited)(*.txt) ~
	Text (Tab delimited)(*.txt)
	CSV (Comma delimited)(*.csv)
Hide Folders	Save Cancel

### Example of flows.text file contents:

Press 0								
a statistics	file cre	ated Tuesday, November	12, 2024 16:53	3:01				
lient Addr Cli	ent Port	Server Addr Server Por	t Events Prot	tocol Applicat	tion Packets Byt	es Start Durati	on 3-Way Handshake	s (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 16:3	8:54 0:05:01.885	0.025 1.586	Open
RAY01.local	60563	self.events.data.micro	soft.com http	ps 0 HTTPS	SSL 173 166083	11/12/2024 16:38:5	5 0:05:18.897 0.0	013 0.019 Open
RAY01.local	57291	52.96.36.82 https 0	HTTPS UDP	322 153416 11/1	12/2024 16:38:55	0:05:06.086		
RAY01.local	63361	35.83.181.24 https	0 HTTPS	SSL 150 16940	11/12/2024 16:3	8:55 0:05:10.114	0.088 0.000	Open
RAY01.local	57646	170.114.1.184 https	1 HTTPS	SSL 34 3602	11/12/2024 16:3	8:55 0:05:03.364	0.012 0.792	Open
RAY01.local	51872	23.222.241.151 https	0 HTTPS	UDP 5 415 11/1	12/2024 16:38:56	9.998		
RAY01.local	63447	44.238.43.4 https 3	HTTPS SSL	219 25510 11/1	12/2024 16:38:56	0:05:10.133 0.0	083 0.146 Ope	n .
RAY01.local	59291	192.168.1.168 nvme-d	isc 0 nvm	e-disc SSL 192	25600 11/12/2	024 16:38:56 0:05:1	5.991 0.006 0.0	000 Open
RAY01.local	61028	104.192.138.12 https	0 HTTPS	Atlassian 15	6650 11/12/2	024 16:38:58 2.571	0.070 0.081 0.0	005 Closed
RAY01.local	63994	192.168.1.1 domain 0	DNS DNS 28	4391 11/12/20	024 16:38:58 0:0	3:11.208 0.025	0.000	
49.184.14 612	33 RM-	BGRAY01.local 49914	51 TCP-499	14 SSL 905 1434	439 11/12/2024	16:38:58 0:05:16.27	7 0.033 1.629	Open
RAY01.local	64542	192.168.1.1 domain 0	DNS DNS 28	4203 11/12/20	024 16:38:58 0:0	3:15.315 0.025	0.000	
RAY01.local	58203	192.168.1.1 domain 0	DNS DNS 22	3416 11/12/20	024 16:38:58 0:0	3:11.205 0.032	0.000	
RAY01.local	65044	192.168.1.1 domain 0	DNS DNS 26	3166 11/12/20	024 16:38:58 0:0	3:15.315 0.027	0.000	
RAY01.local	54864	192.168.1.1 domain 0	DNS DNS 28	4563 11/12/20	024 16:38:58 0:0	3:15.315 0.026	0.000	
RAY01.local	64750	192.168.1.1 domain 0	DNS DNS 26	3994 11/12/20	024 16:38:58 0:0	3:15.315 0.030	0.000	
RAY01.local	61029	108.138.246.80 https	0 HTTPS	Atlassian 14	3330 11/12/2	024 16:38:58 2.415	0.067 0.066 0.0	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	Atlassian 14	3365 11/12/2	024 16:38:58 2.252	0.065 0.067 0.0	000 Closed
RAY01.local	56221	3.128.195.20 https	0 HTTPS	SSL 148 15824	11/12/2024 16:3	8:59 0:05:10.073	0.038 0.000	Open
RAY01.local	63541	52.112.84.177 https	0 HTTPS	Microsoft Servic	ces 24 2168	11/12/2024 16:38:5	9 0:04:40.107 0.0	042 0.000 Open
68.1.193 535	3 mDN	S mdns 0 DNS Mu	lticastDNS	7 2242 11/1	12/2024 16:38:59	0:04:00.534		
:18d8:fcal:eaa	ic:b2c4	5353 mDNSv6 mdns	0 DNS Mult	ticastDNS 6	1966 11/12/2	024 16:38:59 0:04:0	0.534	
RAY01.local	60373	104.192.138.12 https	15 HTTPS	SSL 48 6208	11/12/2024 16:3	9:00 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	
RAY01.local	60911	170.114.52.2 https	0 HTTPS	TCP 4 274 11/1	12/2024 16:39:00	0.007	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 0.0	009 0.016 Open
RAY01.local	60374	104.192.138.12 https	15 HTTPS	SSL 48 6208	11/12/2024 16:3	9:00 0:05:02.045	0.066 20.064	Open
68.1.163 535	3 mDN	S mdns 0 DNS Mu	lticastDNS	45 24590 11/1	12/2024 16:39:01	0:05:13.646		
:1259:32ff:fe7	3:3576	5353 mDNSv6 mdns	0 DNS Mult	ticastDNS 45	25490 11/12/2	024 16:39:01 0:05:1	3.648	
RAY01.local	57674	170.72.245.140 https	1 HTTPS	SSL 100 14235	11/12/2024 16:3	9:01 0:05:00.675	0.045 1.066	Open
RAY01.local	59712	172.64.148.154 https	23 HTTPS	Cloudflare 72	6350 11/12/2	024 16:39:02 0:05:1	0.631 0.008 13.	.496 Open
RAY01.local	61007	wxt-general-ingressgat	eway.acmhwxt-j	prd-2.prod.infra	.webex.com htt	ps 0 HTTPS TC	P 6 409 11/12/2024	16:39:02 27.651 0.030