LiveAction

LiveWire 25.2.0 New Features

QUICK GUIDE

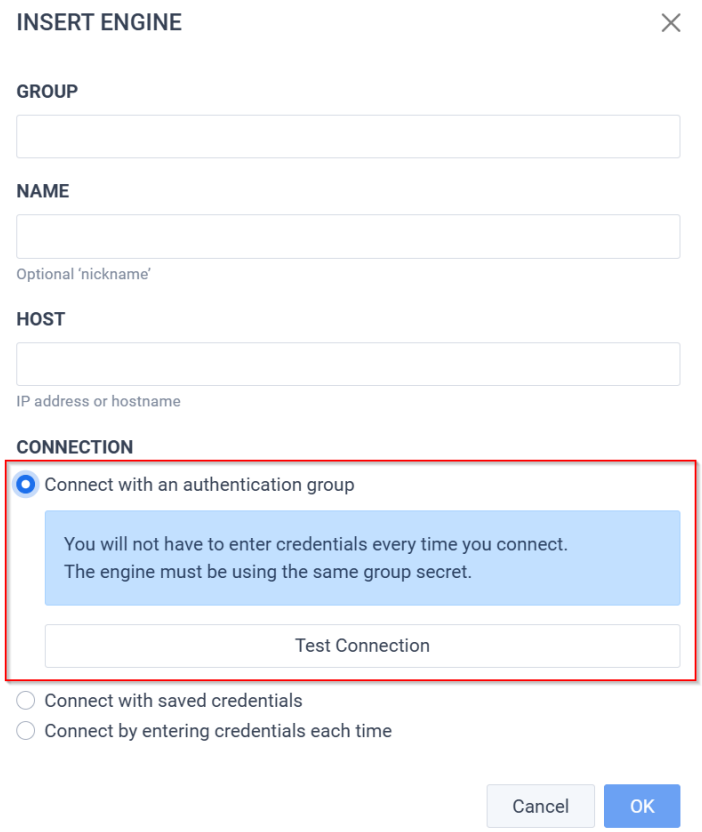
ver. 25.2.0a

Added Windows Remote Capture Engine as a product

Added the Windows Remote Capture Engine as a product and created management views in LiveWire to manage captures across a group of engines.

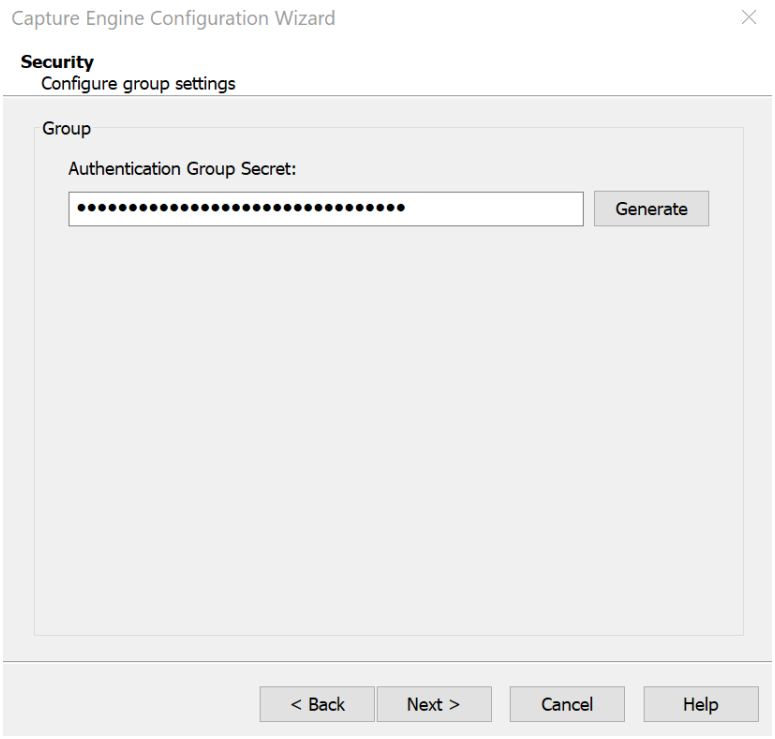
Terminology

A group engine is one for which an authentication group is used for the connection:



Omnipeek Windows

For a LiveWire that has support for the Authentication Group Secret (v24.3.0+), a new tab will be added to the Capture Engine Configuration Wizard. This new tab is called "Security: Configure group settings".



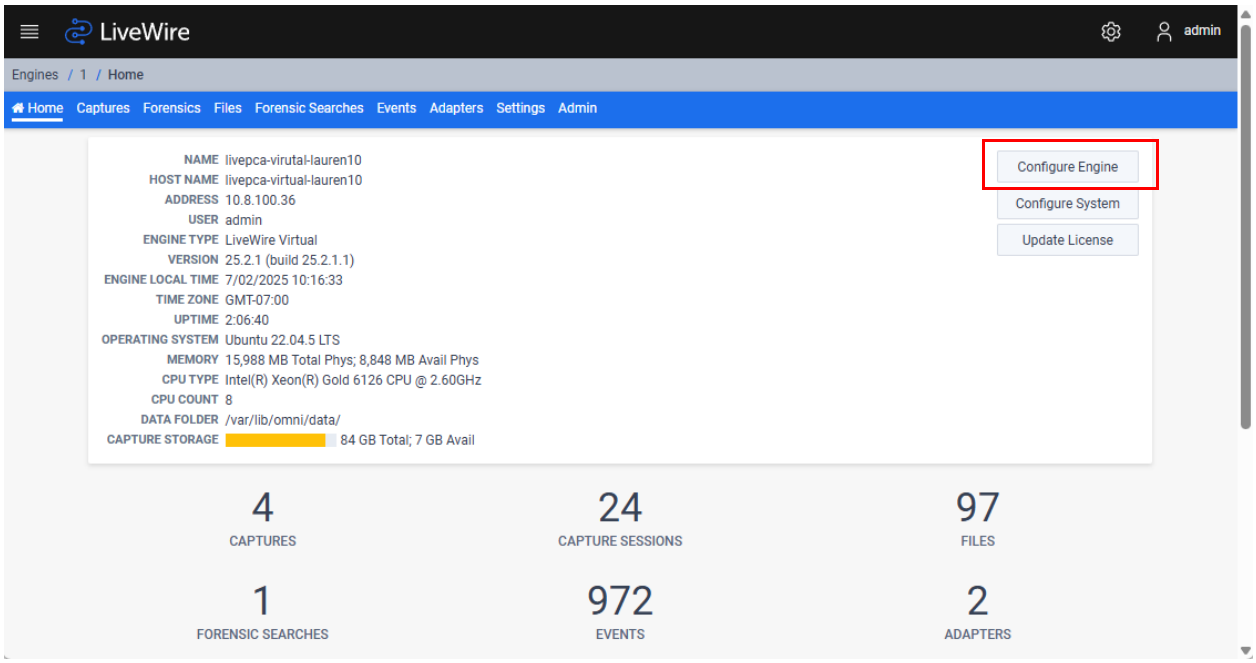
Clicking the "Generate" button will generate a random 32 character group authentication secret.

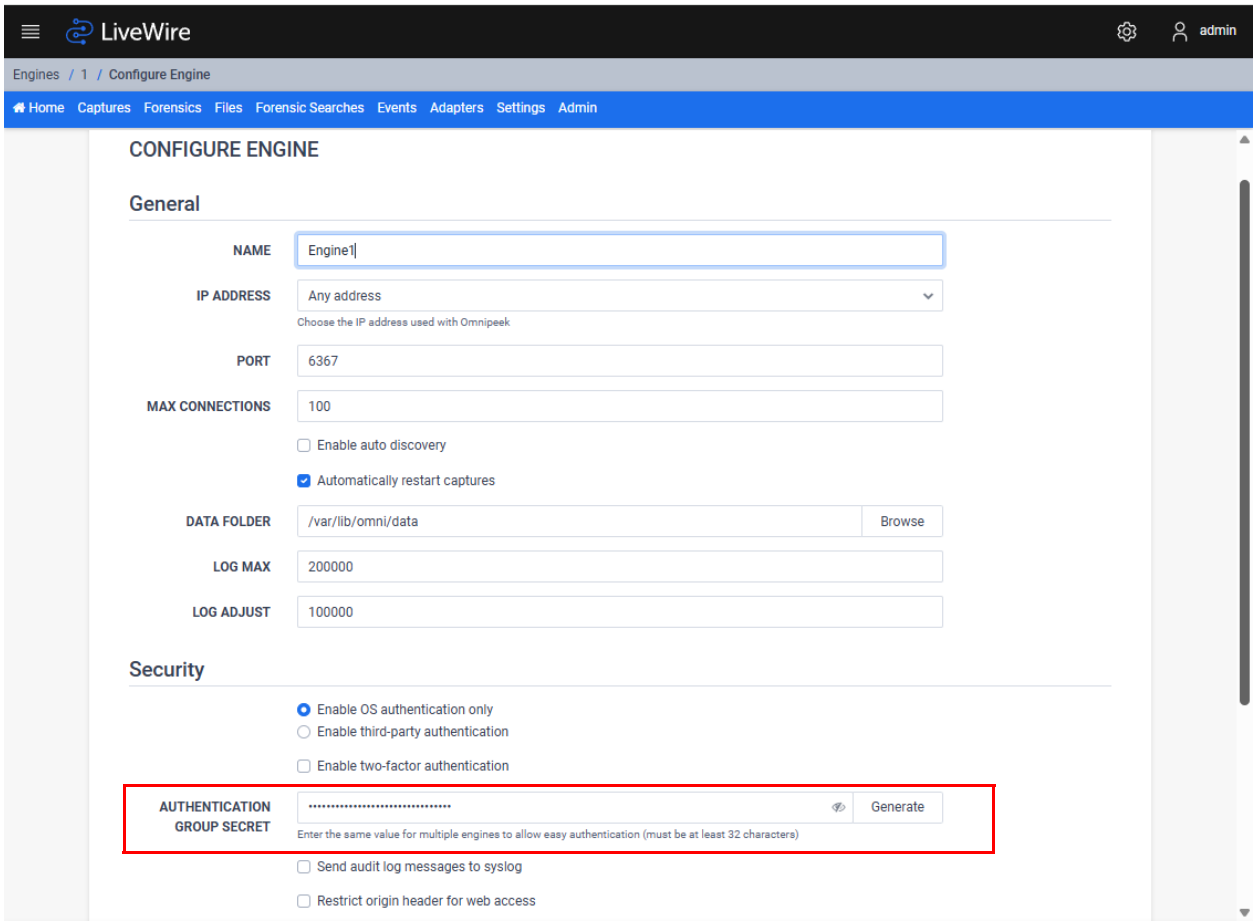
The Authentication Group Secret must be either empty or between 32 characters and 64 characters in length.

LiveWire Omnipeek

Engine Configuration View

The Authentication Group Secret can be modified in the "Security" section of the Engine Configuration View:



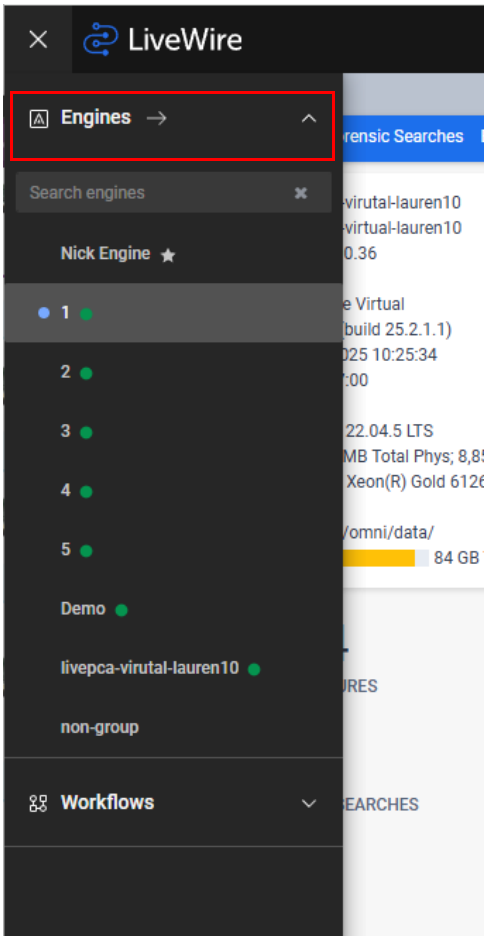


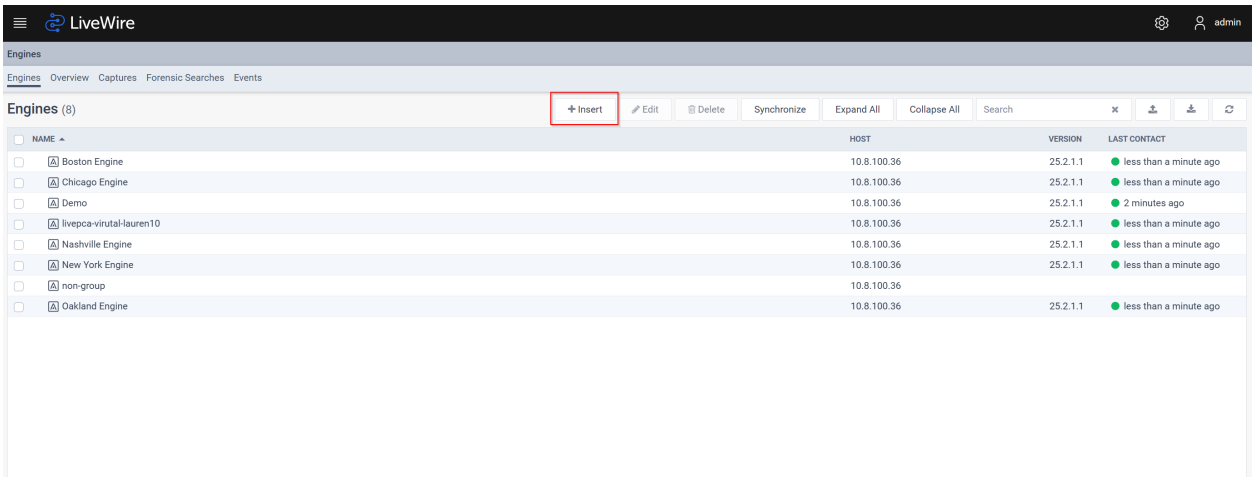
Clicking the "Generate" button will generate a random 32 character group authentication secret.

The Authentication Group Secret must be either empty or between 32 characters and 64 characters in length.

Engines View

The user may add engines to the Engines List using the Engines View.

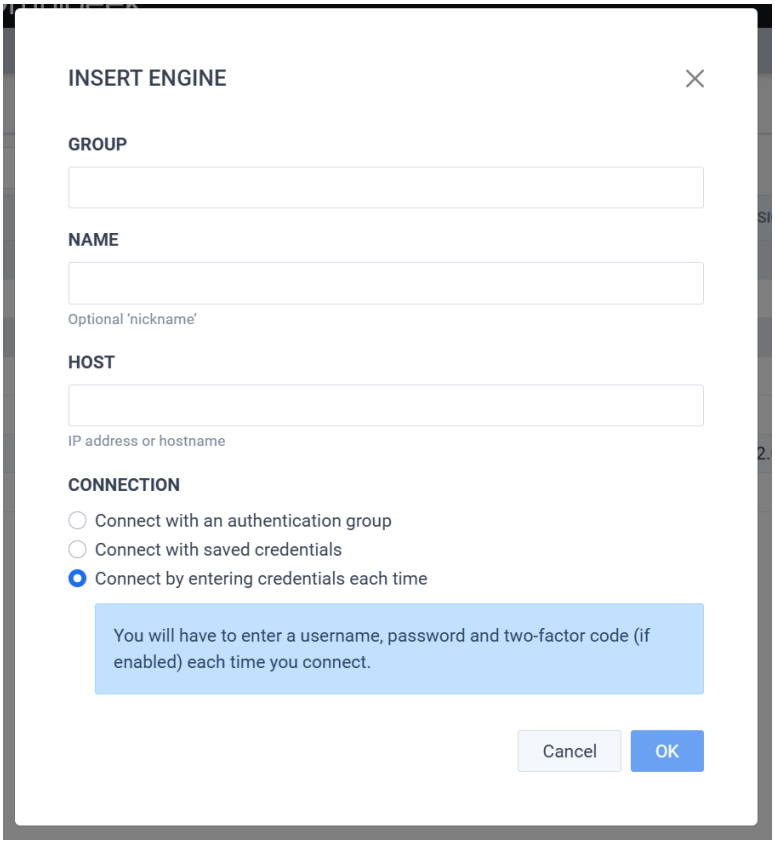




Beginning with LiveWire 25.2.0, the engines will be displayed in the Engines View according to the following rules:

- Non-group engines created by the user will be visible to only that user.
- Group engines will be visible to all users assuming the user has the ACL permission to Configure Group Engines

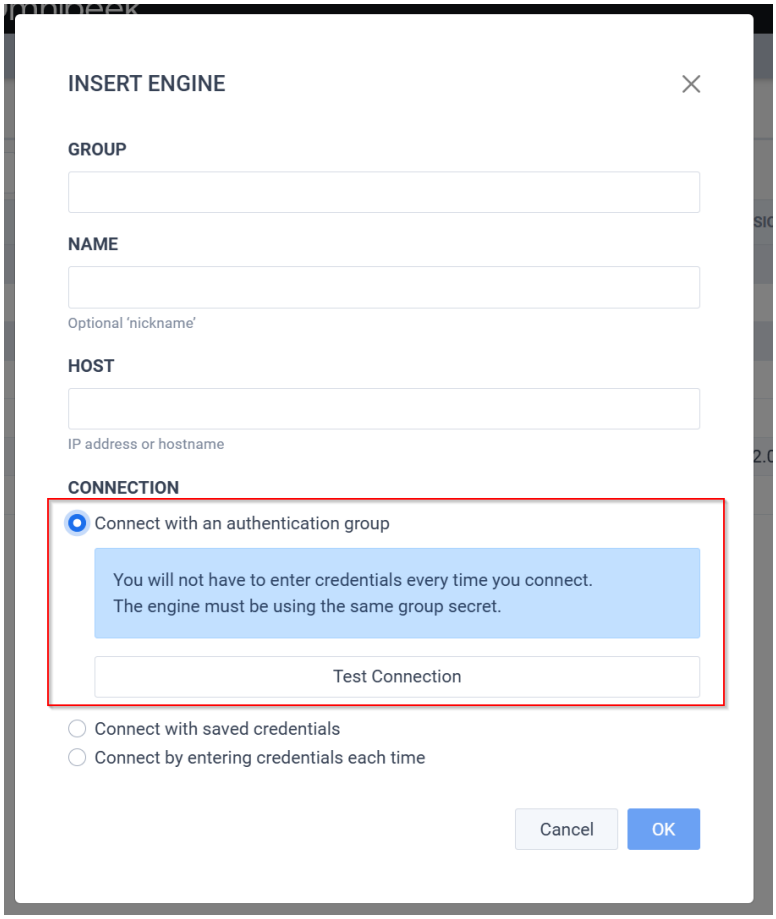
Clicking on the “Insert” button will popup a dialog allowing the user to insert a new engine.



For a LiveWire that has support for the Authentication Group Secret (v24.3.0+), the user will have the option in the “Connection” section for “Connect with an authentication group”. If the LiveWire does not have this support, this option will be hidden and the user will have to select one of the other 2 options. If the user selects the “Connect with an authentication group” option in the “Connection” section, this newly inserted engine will be a group engine.

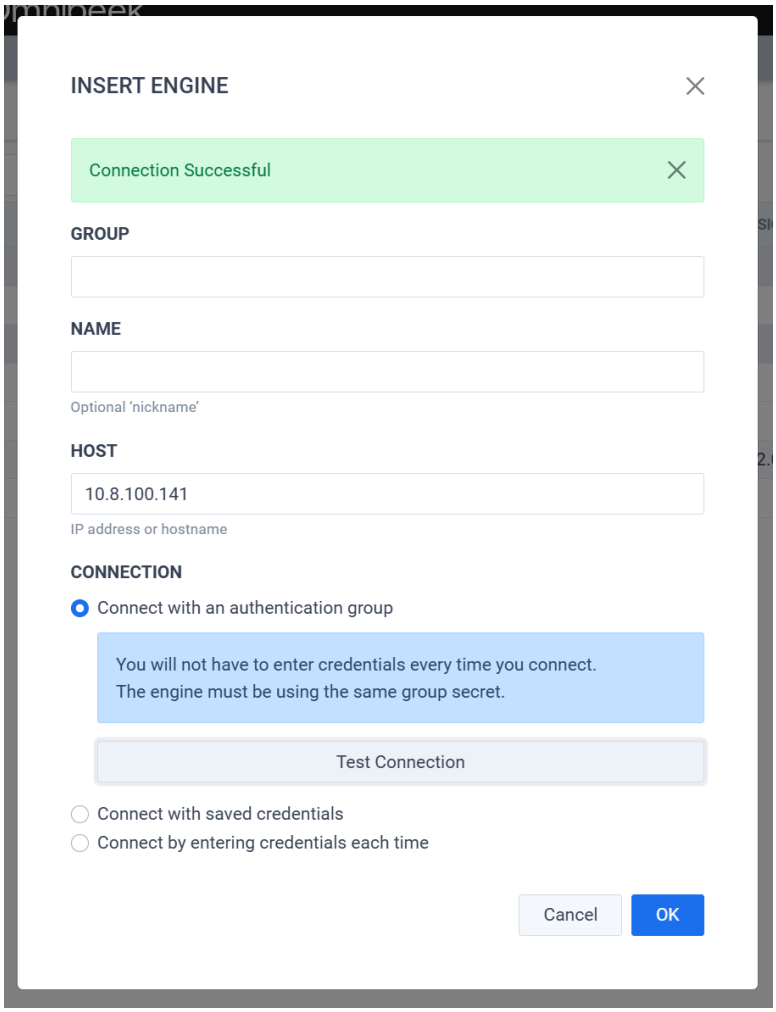
If the host engine has support for the Authentication Group Secret (v24.3.0+) and the Authentication Group Secret is not empty, then the default Connection for new engines will be “Connect with an authentication group”.

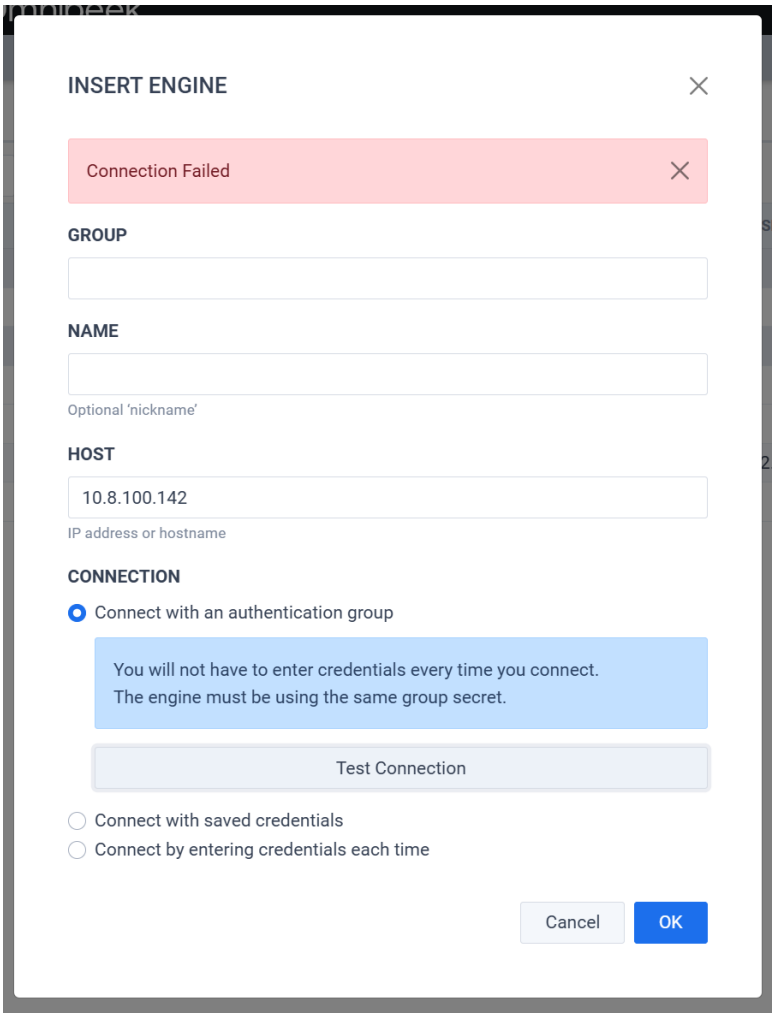
Also, the user will now be restricted to either enter no Name or a unique Name.



For a LiveWire that has support for group engines (v25.2.0+), the "Test Connection" button will be displayed in the "Connection" section when the Connection is "Connect with an authentication group".

Clicking the “Test Connection” button will cause the engine to try and communicate with the LiveWire at the specified host using the Authentication Group Secret. A success or failure message will be displayed to let the user know the test result.





For a LiveWire that has support for group engines (v25.2.0+), inserting a group engine in the Engines List for this LiveWire will also automatically add a group engine for this LiveWire in the group engine's Engines List, assuming the group engine also has support for group engines (v25.2.0+). This automatic insert will occur on the group engine when the first group engine heartbeat is sent (see below).

LiveWire (Group Engine Heartbeat)

For a LiveWire that has support for group engines (v25.2.0+), a hearbeat message will be sent between all group engines at a specified interval.

Every time a heartbeat is sent, information about the group engines will be exchanged. This will effectively update the "Last Contact" time and "Version" for both the group engine on this LiveWire and this LiveWire on the group engine.

Note The group engine must also have support for group engines (v25.2.0+) for this LiveWire to get a response.

Note For a group engine pair, the group engine heartbeat will only be sent from 1 LiveWire. In other words, both engines do not send a group engine heartbeat. Only 1 side will send a heartbeat so as to reduce duplicate communication. If the user added the group engine through this LiveWire's Engines View, then the first group engine heartbeat will come from this LiveWire, but all other group engine heartbeats will come from the group engine that was inserted. If the user added the group engine through the Omnipeek Windows installer, then that Omnipeek Windows engine will send all group engine heartbeats.

The status of group engine heartbeats can be seen in /var/log/omnitrace.log (additional logging can be seen by changing the log level to MEDIUM):

```
root@livepca-virtual-lauren10:/var/log# tail -f omnitrace.log
2025-04-22T11:16:16.894-07:00  Group engine heartbeats, hr=0x00000000
2025-04-22T11:16:46.898-07:00  Group engine heartbeat success for id={6AFD954A-7D2F-4F44-B8FF-2EE4BD4AB6E6}, host='10.8.100.141', name='Nick Engine'
2025-04-22T11:17:16.900-07:00  Group engine heartbeat failed for id={A7DDDA29-3AE3-48C2-A740-D02C74F85350}, host='192.168.31.1', name='Capture Engine', hr=0x80004005, code=0
2025-04-22T11:17:16.900-07:00  Group engine heartbeats, hr=0x00000000
2025-04-22T11:17:46.904-07:00  Group engine heartbeat success for id={6AFD954A-7D2F-4F44-B8FF-2EE4BD4AB6E6}, host='10.8.100.141', name='Nick Engine'
2025-04-22T11:18:16.906-07:00  Group engine heartbeat failed for id={A7DDDA29-3AE3-48C2-A740-D02C74F85350}, host='192.168.31.1', name='Capture Engine', hr=0x80004005, code=0
2025-04-22T11:18:16.907-07:00  Group engine heartbeats, hr=0x00000000
2025-04-22T11:18:46.911-07:00  Group engine heartbeat success for id={6AFD954A-7D2F-4F44-B8FF-2EE4BD4AB6E6}, host='10.8.100.141', name='Nick Engine'
2025-04-22T11:19:16.912-07:00  Group engine heartbeat failed for id={A7DDDA29-3AE3-48C2-A740-D02C74F85350}, host='192.168.31.1', name='Capture Engine', hr=0x80004005, code=0
2025-04-22T11:19:16.913-07:00  Group engine heartbeats, hr=0x00000000
```

When the user deletes a group engine from either side, the corresponding group engine on the other side will be deleted during the next heartbeat.

Added new LiveFlow alerts for issues around TLS, Certificates, and Authentication

Several LiveFlow security alerts have been added that are primarily focused around TLS, Certificates, and Authentication. Here's the list of the new alerts:

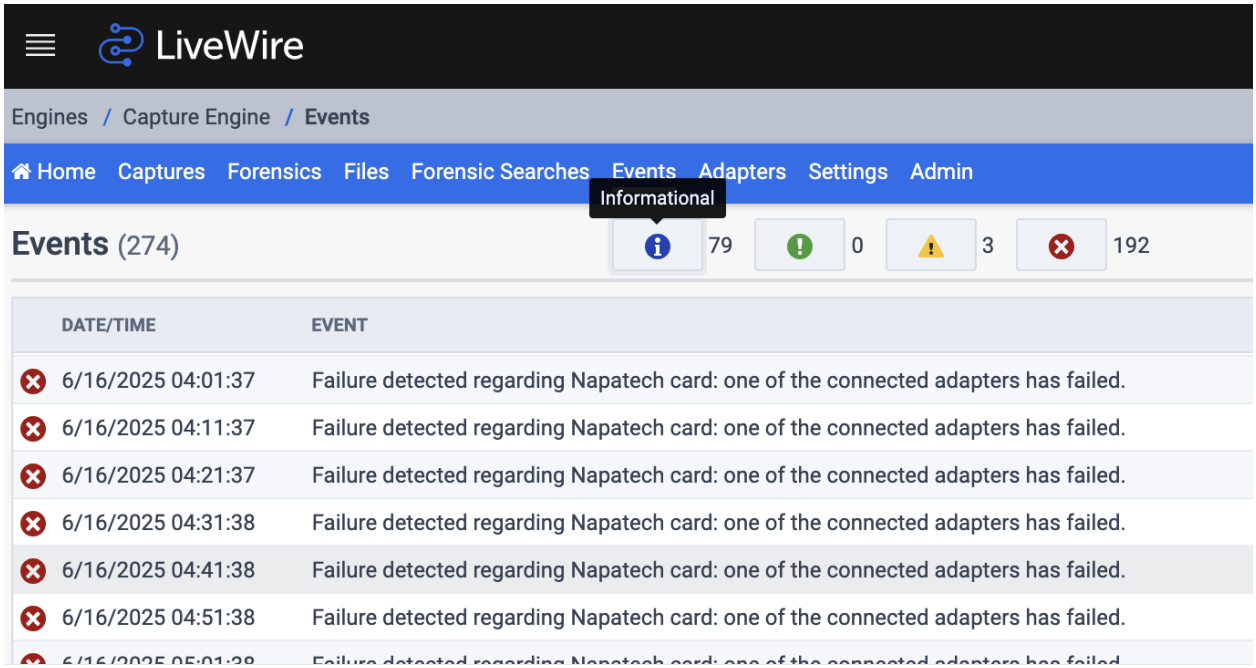
	LiveFlow Alert	Notes
1	Cleartext Credentials Detected	Description: Detection of user credentials (usernames, passwords, API tokens) transmitted in plain text, which is a major security risk. Cause: Allowed ciphers policy is not in place or not enforced. Remedy: Implement and enforce allowed ciphers policy.
2	Kerberos Detected	Description: The Kerberos protocol has been detected. If all machines are running an up-to-date version of Kerberos, this may not be an issue unless Kerberos is disallowed by policy. Cause: Kerberos protocol detected in network traffic. Remedy: If Kerberos is disallowed by policy, update affected machines. Otherwise, verify all machines are running an up-to-date version of Kerberos.
3	Kerberos RC4 Detected	Description: The Kerberos protocol has been detected, and the ticket key is encrypted using insecure RC4 cipher. Cause: Kerberos officially deprecated RC4 long ago. Affected machines are overdue for a Kerberos update. Remedy: If Kerberos is disallowed by policy, update all affected machines. Otherwise, update all affected machines to a new version of Kerberos, and disallow RC4.
4	Malicious IP or Domain Detected	Description: Detection of encrypted traffic to known blacklisted or suspicious IPs/domains. Cause: Newly detected or unblocked known malicious IP/domain. Remedy: Block known malicious IPs/domains. Note: If enabled, the security configuration should be modified as specified in KB #000001409.
5	Microsoft IP Detected	Description: Network traffic to Microsoft domains normally used only by computers running Windows has been detected. For example, "phone home" to telemetry.microsoft.com. Cause: Passive scanning has detected traffic possibly indicating computers running Windows on the network.
6	NTLM Protocol Detected	Description: Network traffic utilizing NTLM may be a security risk due to known vulnerabilities in NTLM. Microsoft has announced NTLM will be phased out after Windows 11 version 24H2. Cause: Passive scanning has detected traffic utilizing the NTLM protocol. Remedy: Microsoft recommends replacing NTLM with the latest Kerberos.
7	TLS Certificate Anomalies Detected	Description: Untrusted or self-signed certificates, expired, or mismatched certificates suggest potential MITM attacks or misconfigurations. Cause: Newly detected or unblocked known issues in Server Certificate. Remedy: Block identified Server Certificate anomalies. Note: If enabled, the security configuration should be modified as specified in KB #000001409.

	LiveFlow Alert	Notes
8	TLS Client Excessive Handshakes	Description: A client machine has attempted an unusually high number of TLS connections (client hello messages). Cause: Possibly comprised machine is attempting to infect other machines. Remedy: The client machine should be thoroughly examined for malware, and any infection mitigated.
9	TLS Long Lived Connection	Description: Long-lived sessions, especially to external destinations, may be indicative of compromised hosts or ongoing data exfiltration. Cause: Possibly compromised machine has a long duration TLS connection to another machine. Remedy: The client and server machines should be thoroughly examined for malware, and any infection removed.
10	Weak TLS Cipher Suite	Description: Detection of TLS encrypted traffic using known weak cipher suites. Cause: Minimum TLS cipher strength not monitored and enforced. Remedy: Analyze SSL/TLS handshakes for the negotiated cipher suites. Identify connections that use outdated or weak ciphers. Use network security tools to enforce minimum cipher standards and monitor for any deviations, especially in encrypted traffic between internal systems and external hosts.

Added an alert when a Napatech card experiences an issue and/or change in state

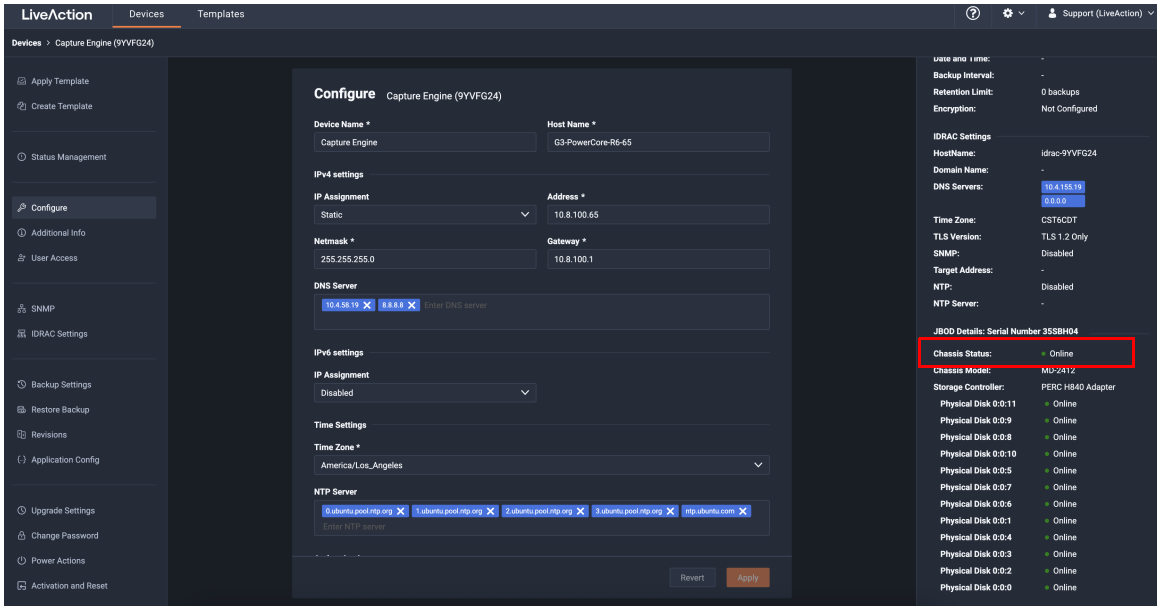
Multiple alerts have been added that are displayed in the ***Events*** view whenever a Napatech card encounters an error or has a hardware failure. Here are the new alerts that have been added:

- *Failure detected regarding Napatech card: number of adapters present has changed*
- *Failure detected regarding Napatech card: one of the connected adapters has failed*
- *Failure detected regarding Napatech card: an adapter sensor has reported an alarm. Packet capture may be degraded or stopped*
- *Failure detected regarding Napatech card: a port sensor has reported an alarm. Packet capture may be degraded or stopped*
- *The adapter monitoring thread is stopping. It may be that this system doesn't contain a Napatech based capturing card*
- *Failure detected regarding a Napatech card: a port is showing that it is in the down state*
- *Napatech capture card is reporting that a port is now in the up state*



Added JBOD status information to Grid reporting

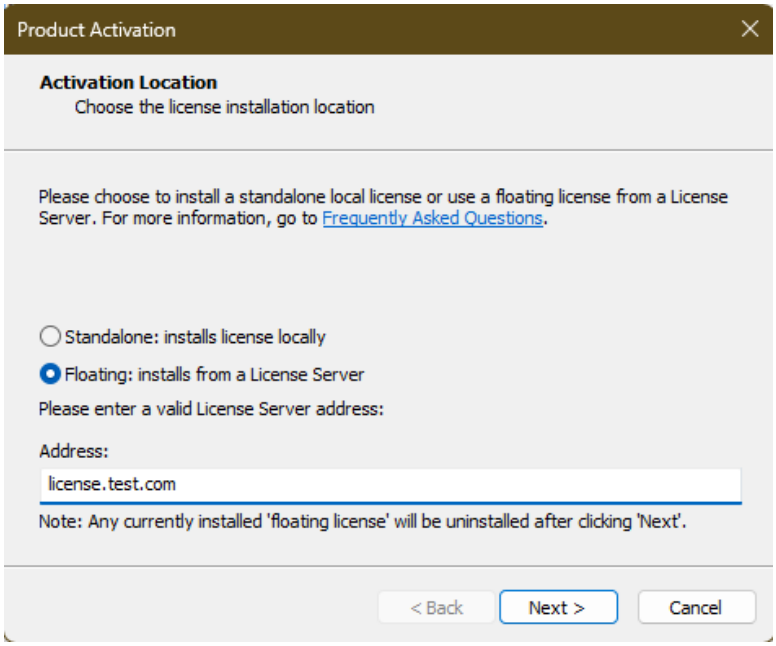
JBOD status information is now available in Grid reporting.



Added Floating License support for both Perpetual and Subscription licenses

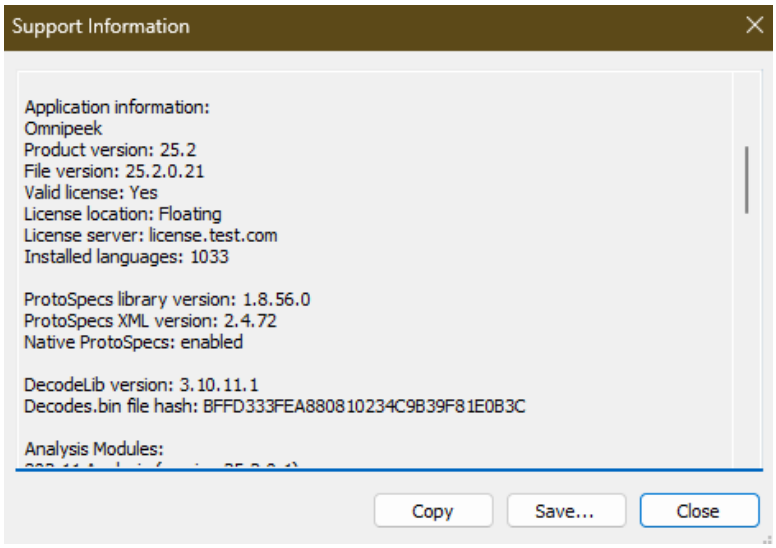
Floating license support has been to the Omnipeek UI for Remote Capture Engine and Omnipeek itself, allowing for centralized management of LiveWire licensing.

Enter the address of your on-prem license server:



LiveWire automatically checks out a license from this server when the application starts, and relinquishes control of this license when the application closes.

As seen below, LiveWire is now in "Floating" mode:



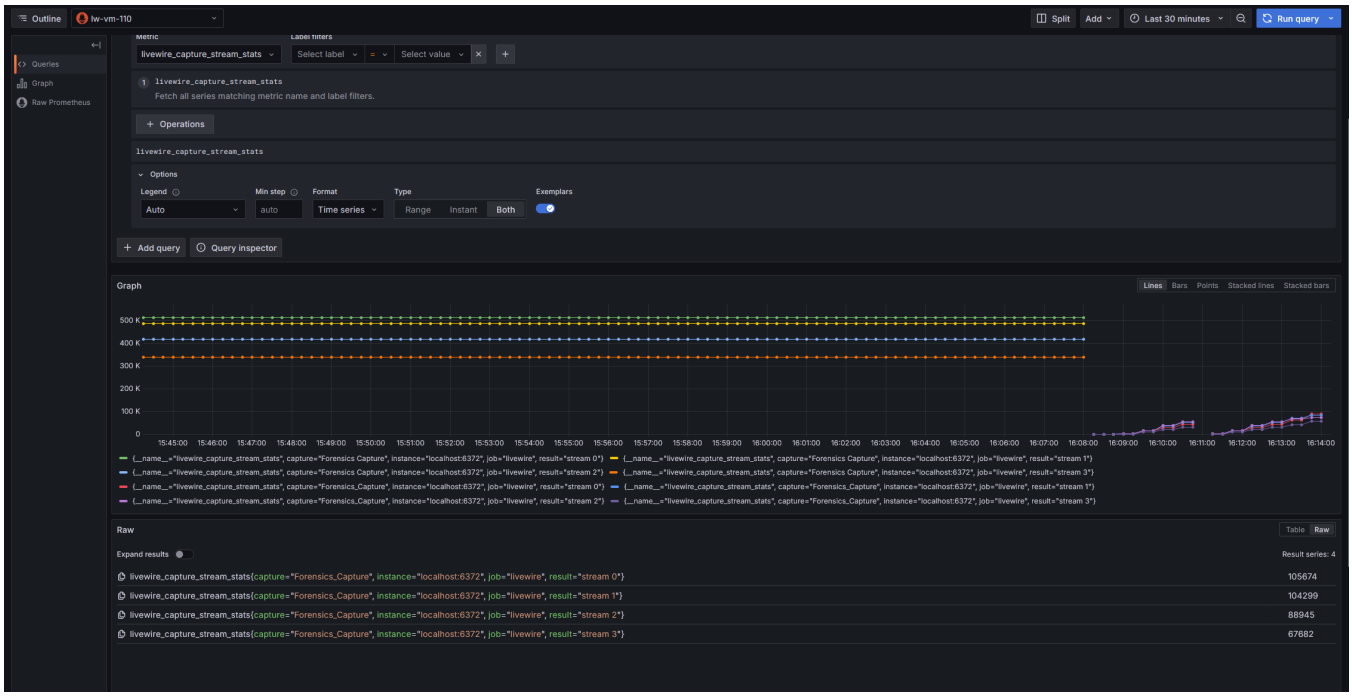
Utilities for managing this license server can be found on MyPeek, under the "Free Utlities" section.

The license server address can be synced via Grid, or through LiveWire's native Engine Configuration Sync.

Note LiveWire appliances must remain in constant contact with the License Server, otherwise they risk losing their activation state.

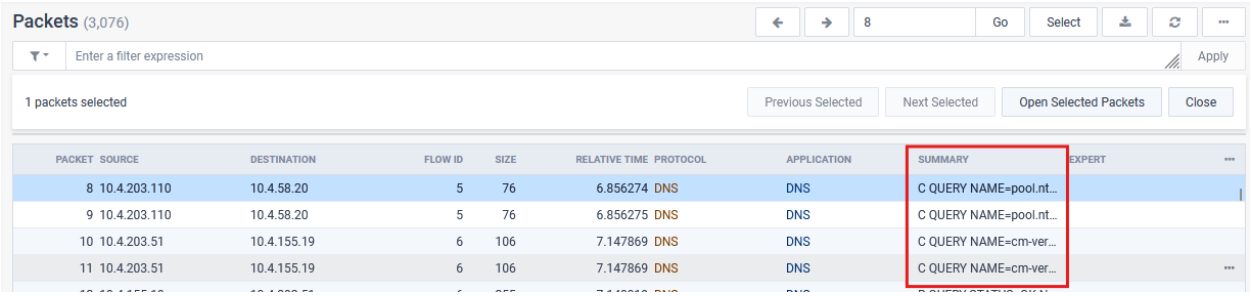
Added additional Prometheus metrics to our existing reporting and support data collection

Promethus metrics for stream packet counts are displayed in admin/support when the capture is active (instead of written to omnitrace). In addition, the packet count stats for the same analysis streams are outputted to prometheus.



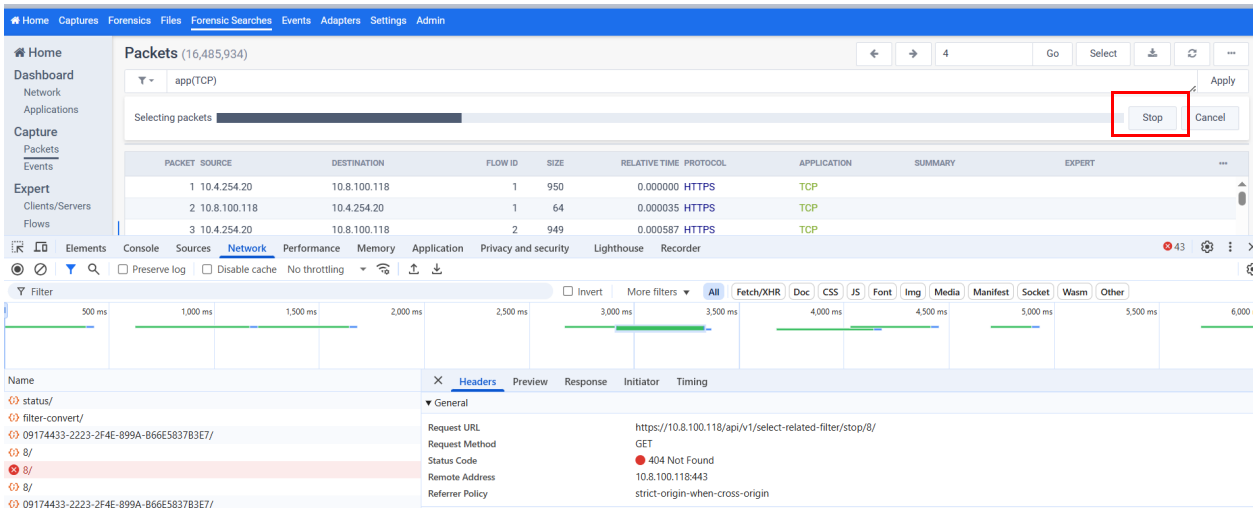
Added Packet Summary to Flow Visualizer

The Packet Summary column was added to the Flow Visualizer (*Forensic Search* > *Expert Flows* > [Select Flow] > *Flow Visualizer*). This helps to provide more context for what the payload of the packets look like.



Added "Stop Selection" to Forensic Search and packet search to show current results

A ***Stop Selection*** button has been added to Forensic Search. When clicked, the selection of packets is stopped and the current results are displayed.

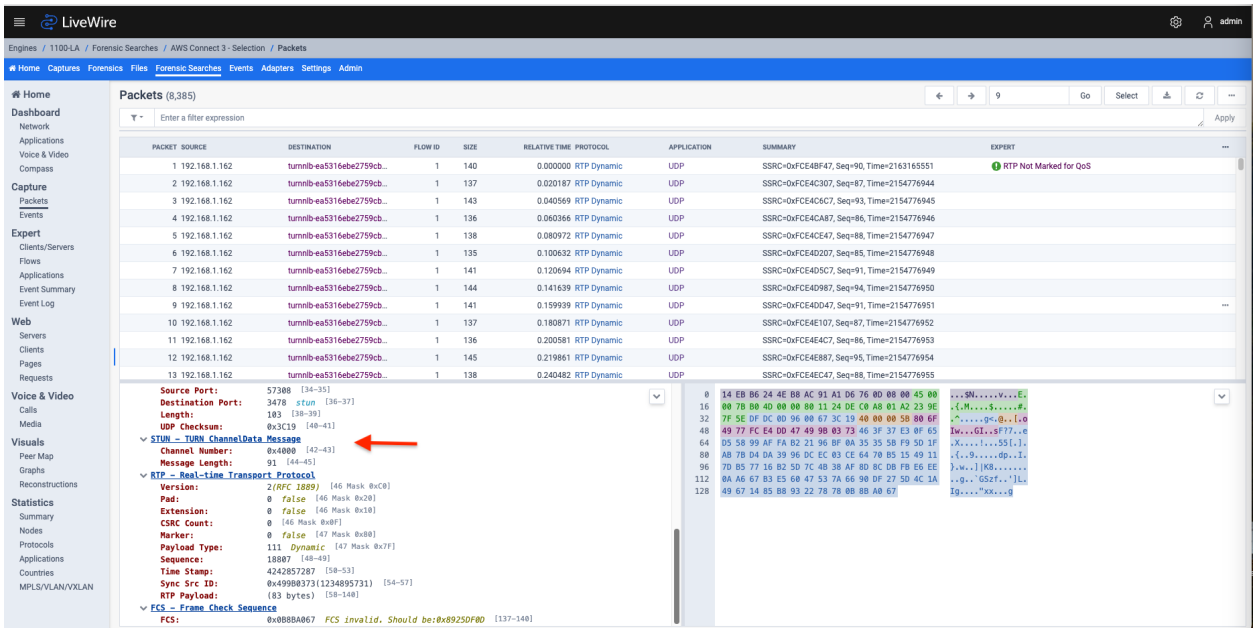


Updated HTTP Host Resolution to not send IP Address

LiveFlow no longer sends IP addresses in HTTP Host Name and SSL Common Name.

Added decoder support for TURN message format

Decoder support for TURN message format has been added to LiveWire. The TURN header and its payload will now be decoded.



Added Details Statistics view to LiveWire

The Details Statistics view has been added to LiveWire.

The rest of this description will describe where and how the Details Statistics View can be opened, and how the Details Statistics View behaves.

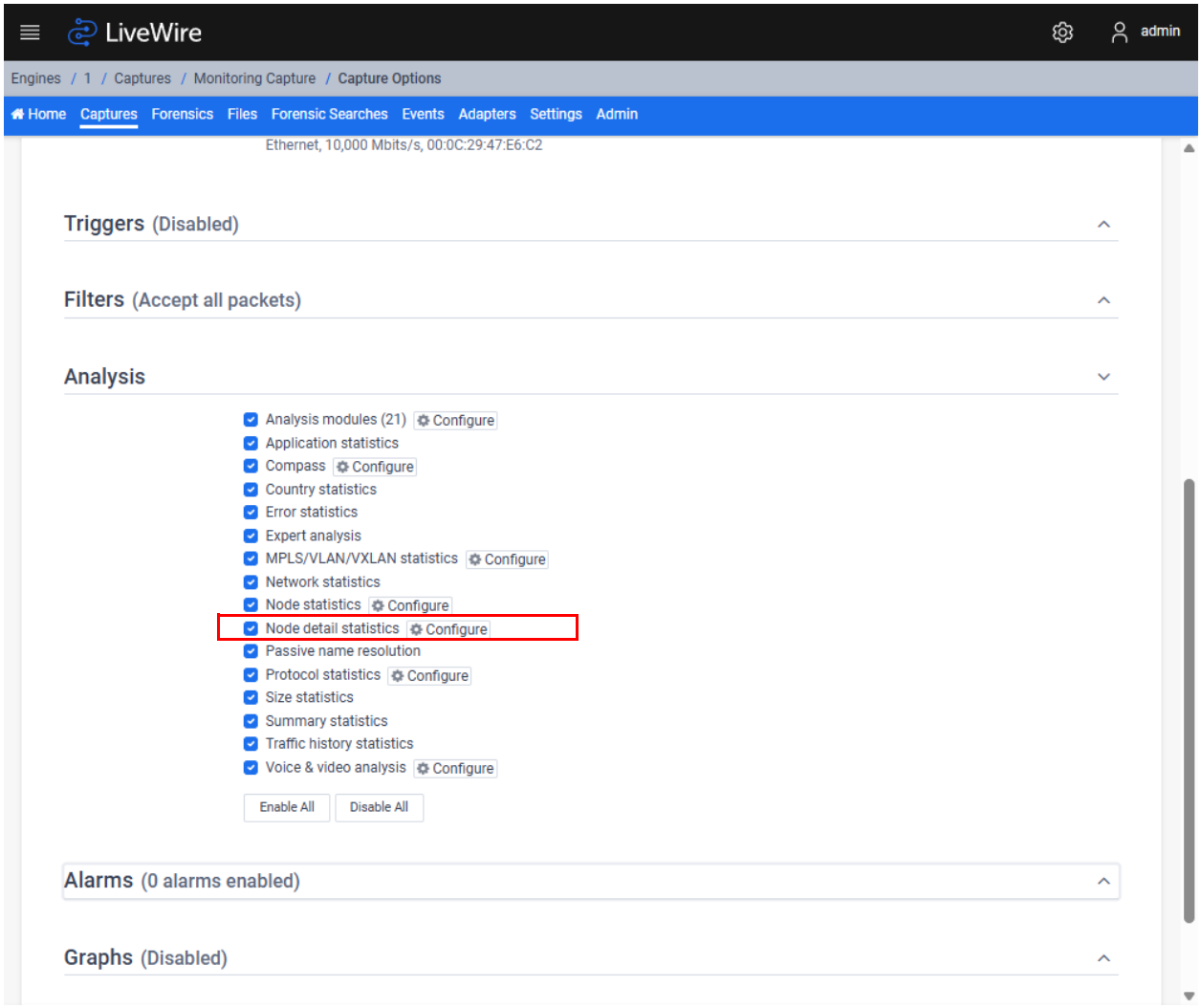
How to enable the Details Statistics View

The Details Statistics View is available in any Capture or Forensic Search, but must be enabled by the user.

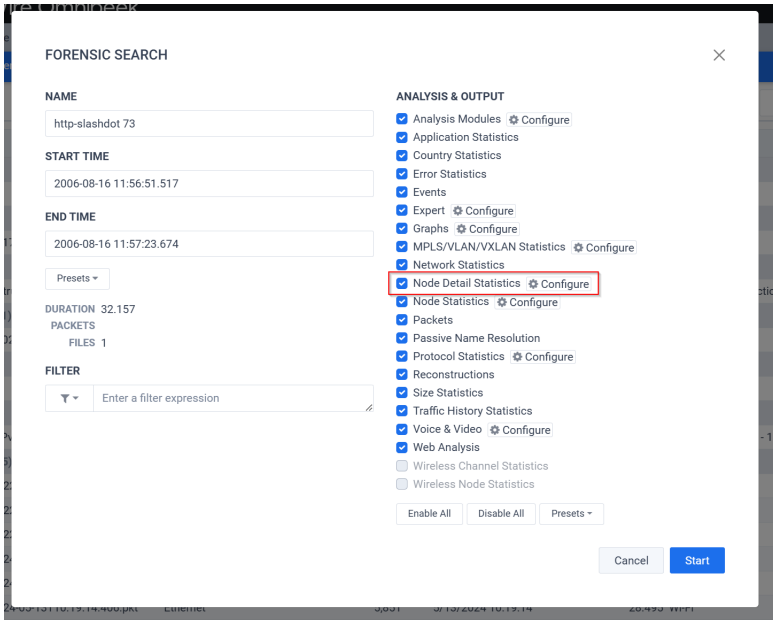
This Details Statistics feature will be unavailable if:

- the Capture or Forensic Search doesn't have "Node Detail Statistics" analysis enabled
- the LiveWire is version 25.1.x or earlier

Capture



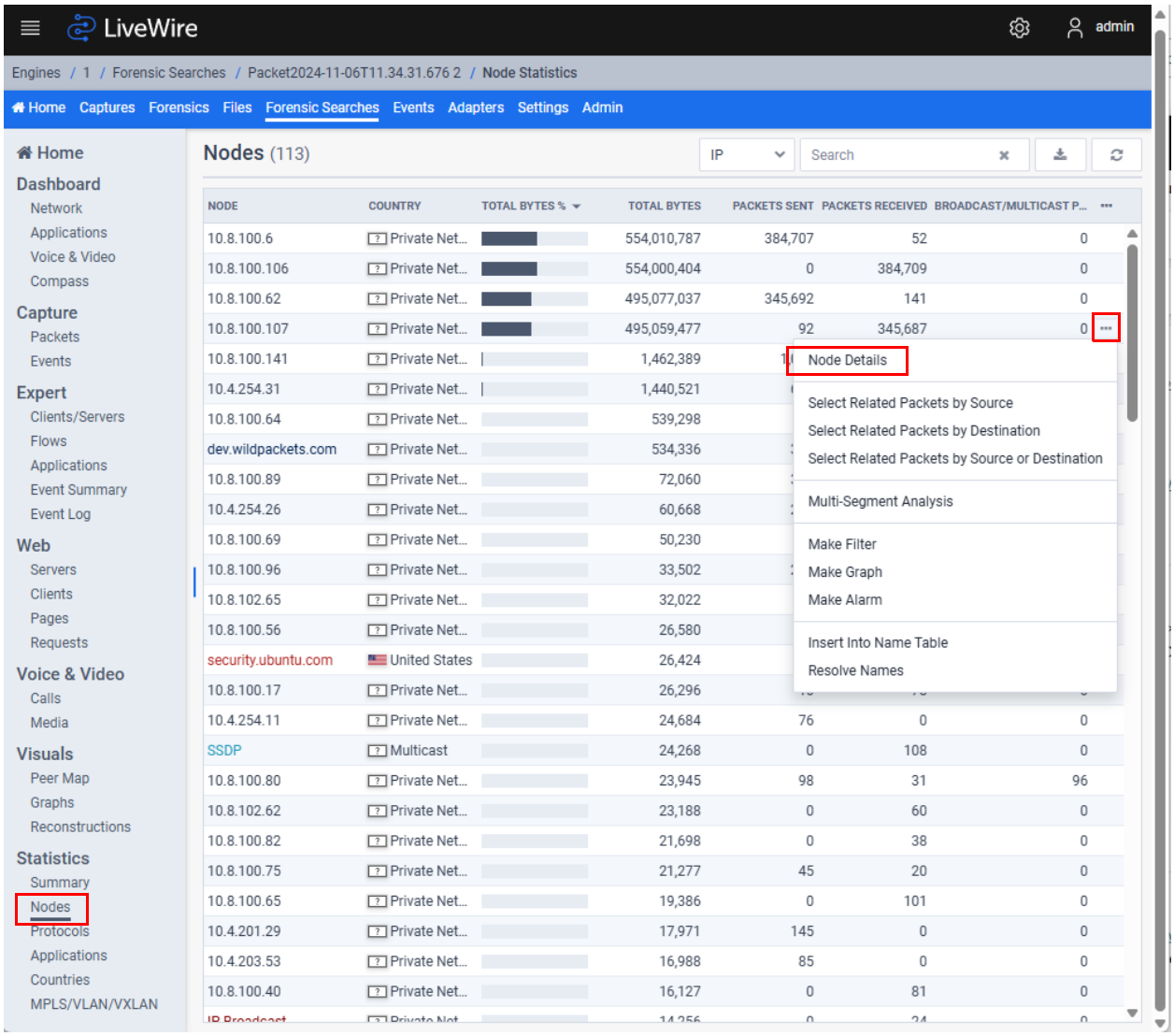
Forensic Search



How to open the Details Statistics View in LiveWire

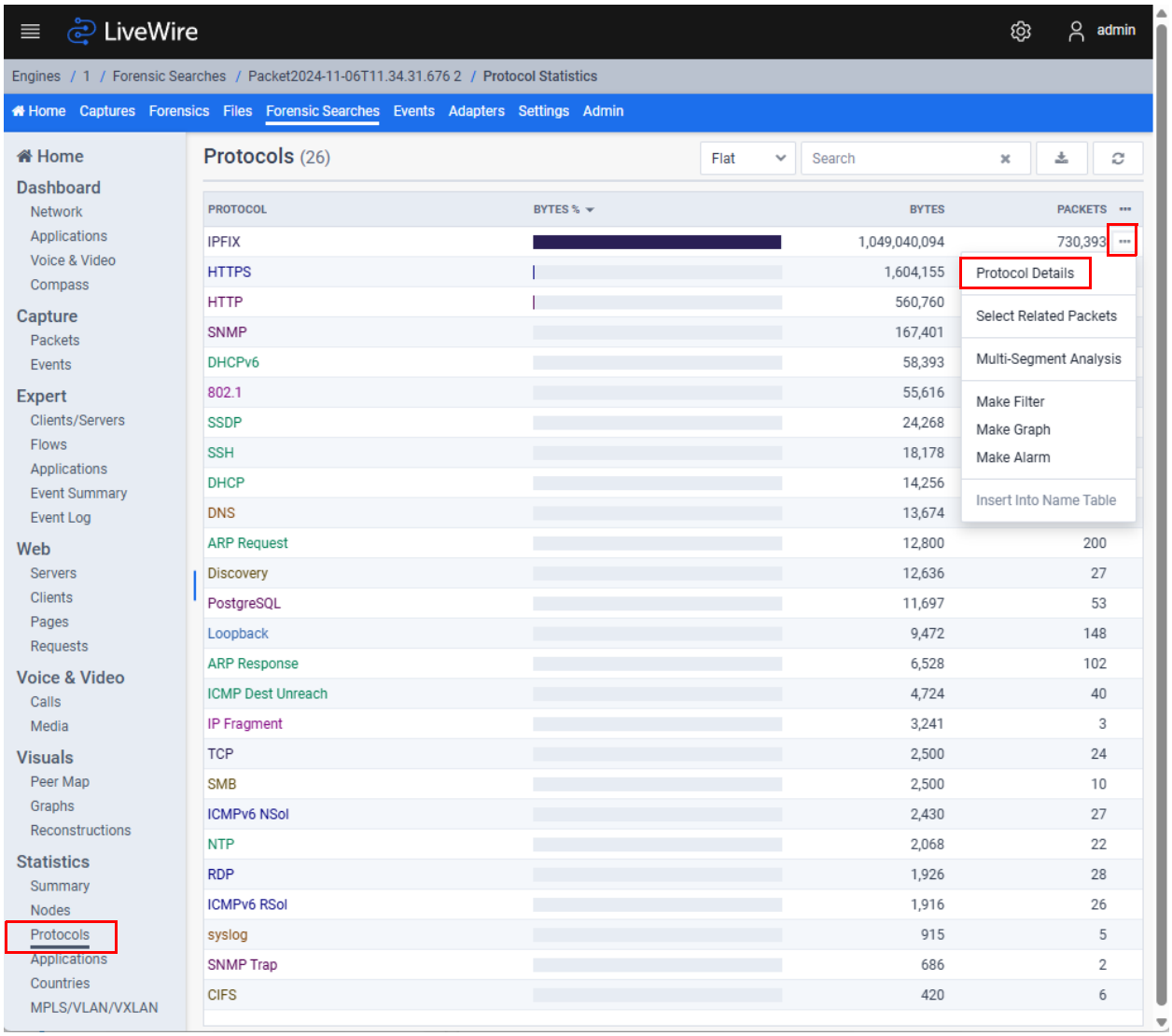
Nodes Statistics View

The user may open the Details Statistics View for a node by clicking the "..." button at the end of each row in the Nodes table and clicking the "Node Details" context menu item. This will work in any of the modes ("IP", "IPv6", "Physical", "Hierarchy"). This "Node Details" feature will be disabled if the Capture or Forensic Search doesn't have "Node Detail Statistics" analysis enabled, or the LiveWire is version 25.1.x or earlier.



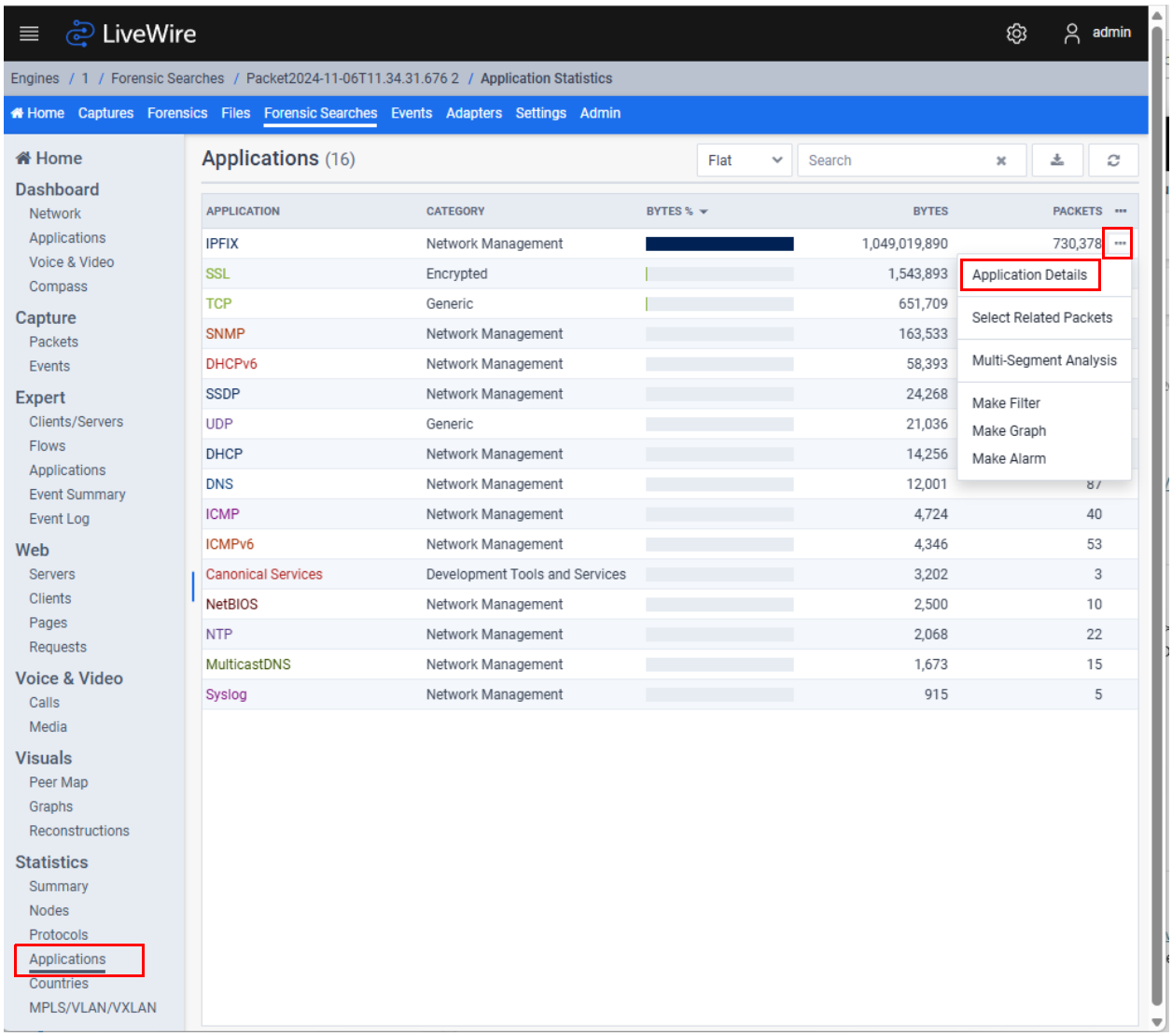
Protocols Statistics View

The user may open the Details Statistics View for a protocol by clicking the "..." button at the end of each row in the Protocols table and clicking the "Protocol Details" context menu item. This will work in any of the modes ("Flat", "Hierarchy"). This "Protocol Details" feature will be disabled if the Capture or Forensic Search doesn't have "Node Detail Statistics" analysis enabled, or the LiveWire is version 25.1.x or earlier.



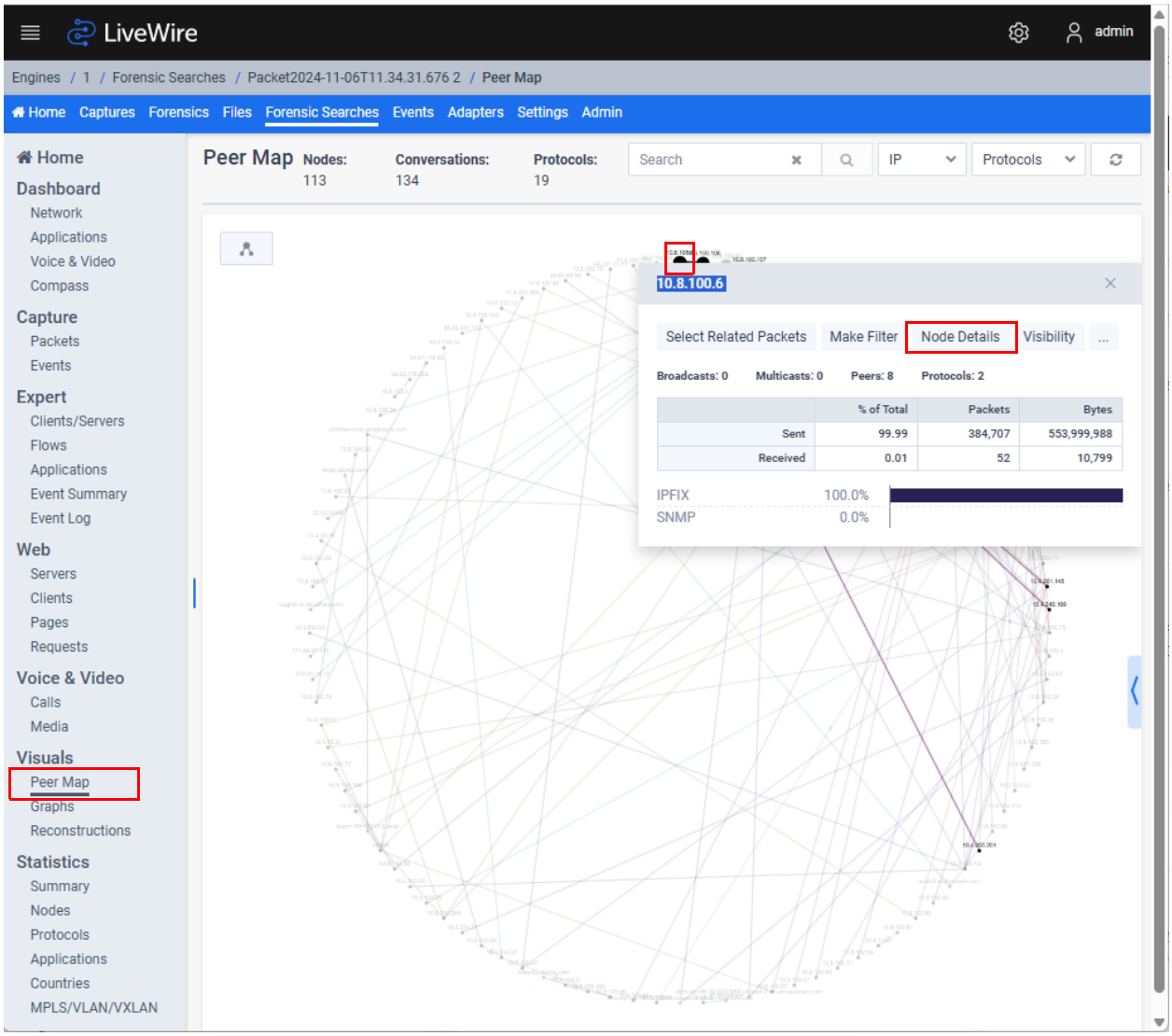
Applications Statistics View

The user may open the Details Statistics View for an application by clicking the "..." button at the end of each row in the Applications table and clicking the "Application Details" context menu item. This will work in any of the modes ("Flat", "Hierarchy"). This "Application Details" feature will be disabled if the Capture or Forensic Search doesn't have "Node Detail Statistics" analysis enabled, or the LiveWire is version 25.1.x or earlier.

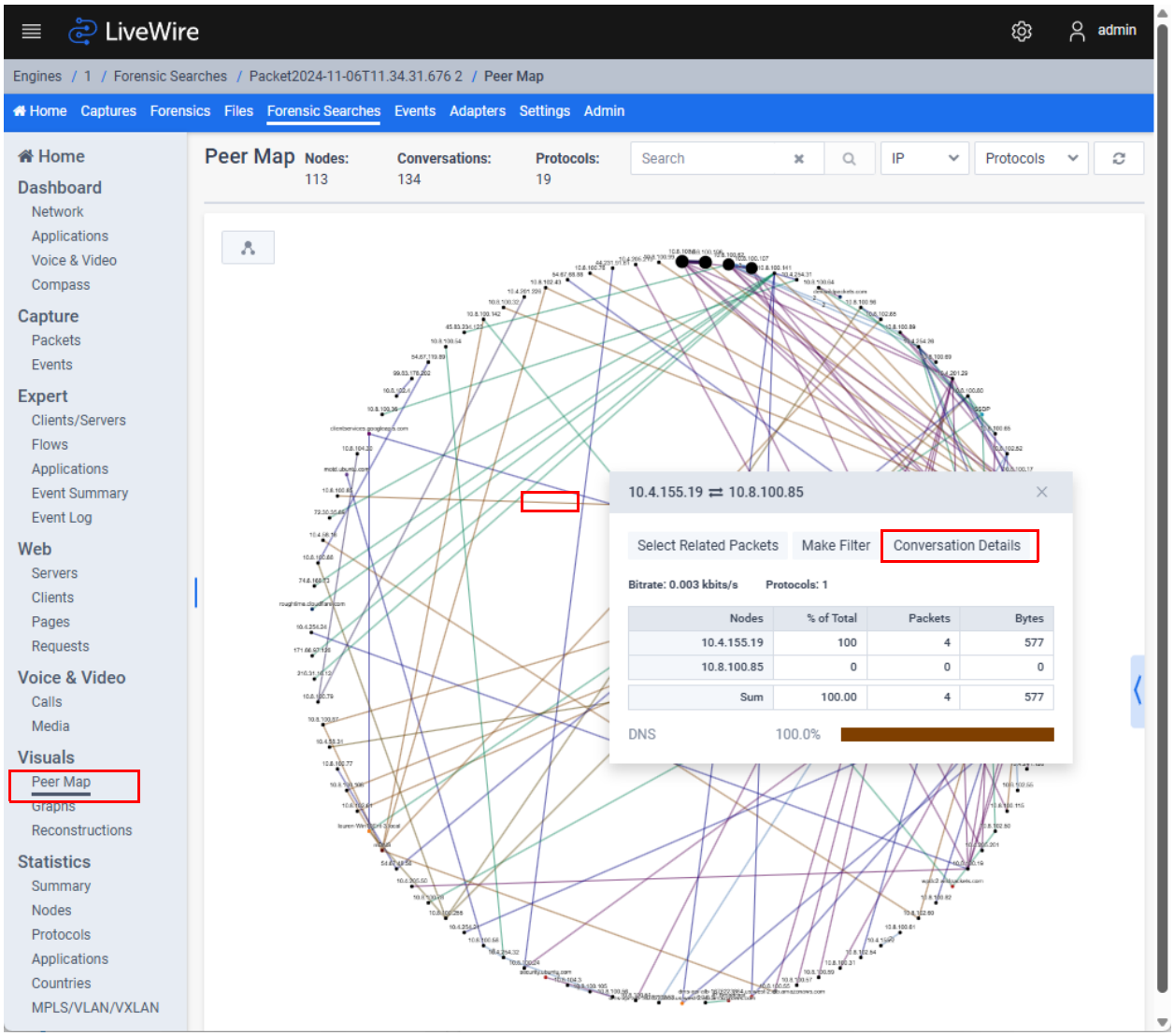


Peer Map View

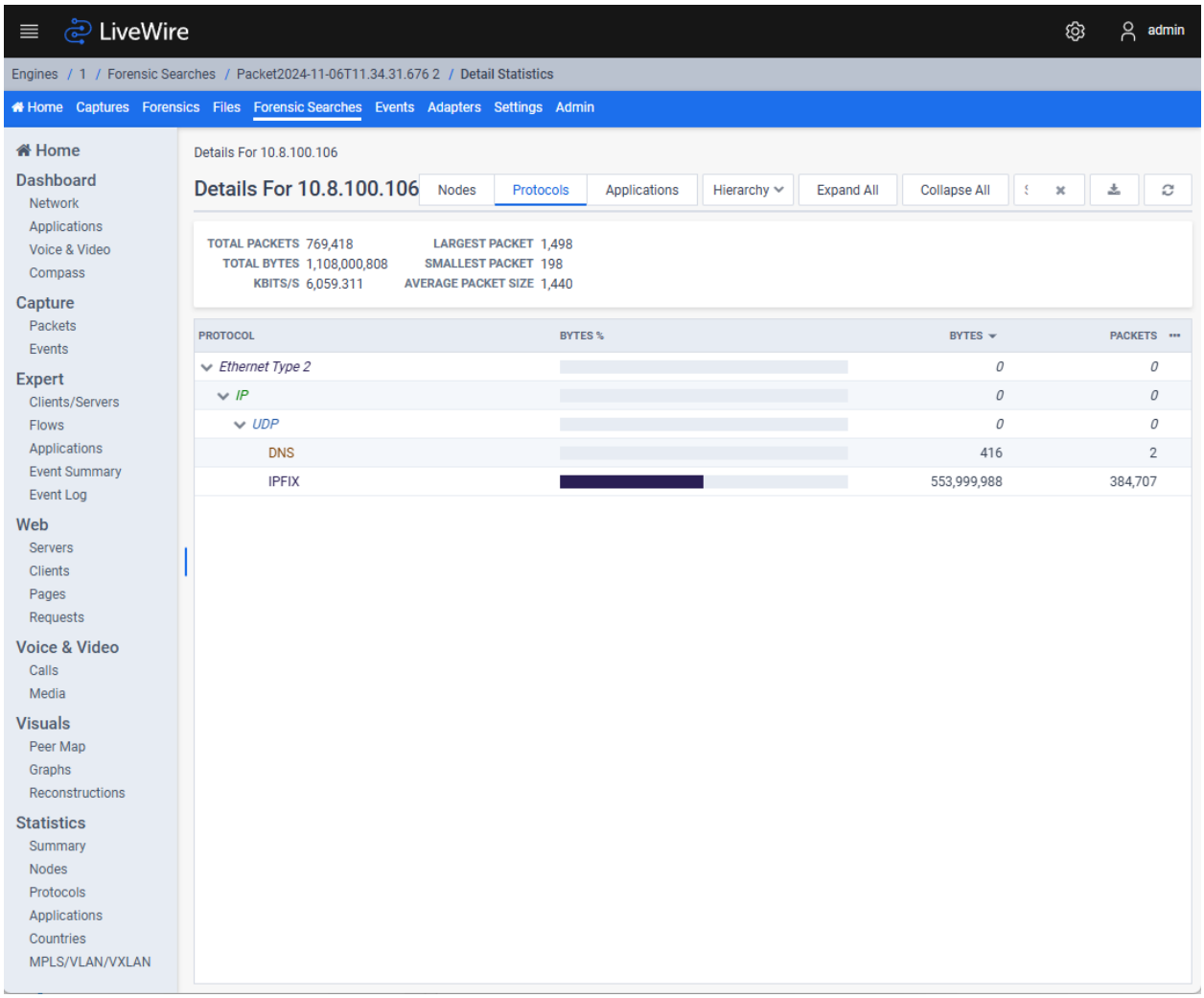
The user may open the Details Statistics View for a node by clicking on it and clicking the “Node Details” button. This “Node Details” feature will be disabled if the Capture or Forensic Search doesn’t have “Node Detail Statistics” analysis enabled, or the LiveWire is version 25.1.x or earlier.



The user may also open the Details Statistics View for a conversation by clicking on a conversation line and clicking the "Conversation Details" button. This "Conversation Details" feature will be disabled if the Capture or Forensic Search doesn't have "Node Detail Statistics" analysis enabled, or the LiveWire is version 25.1.x or earlier.



The Details Statistics View



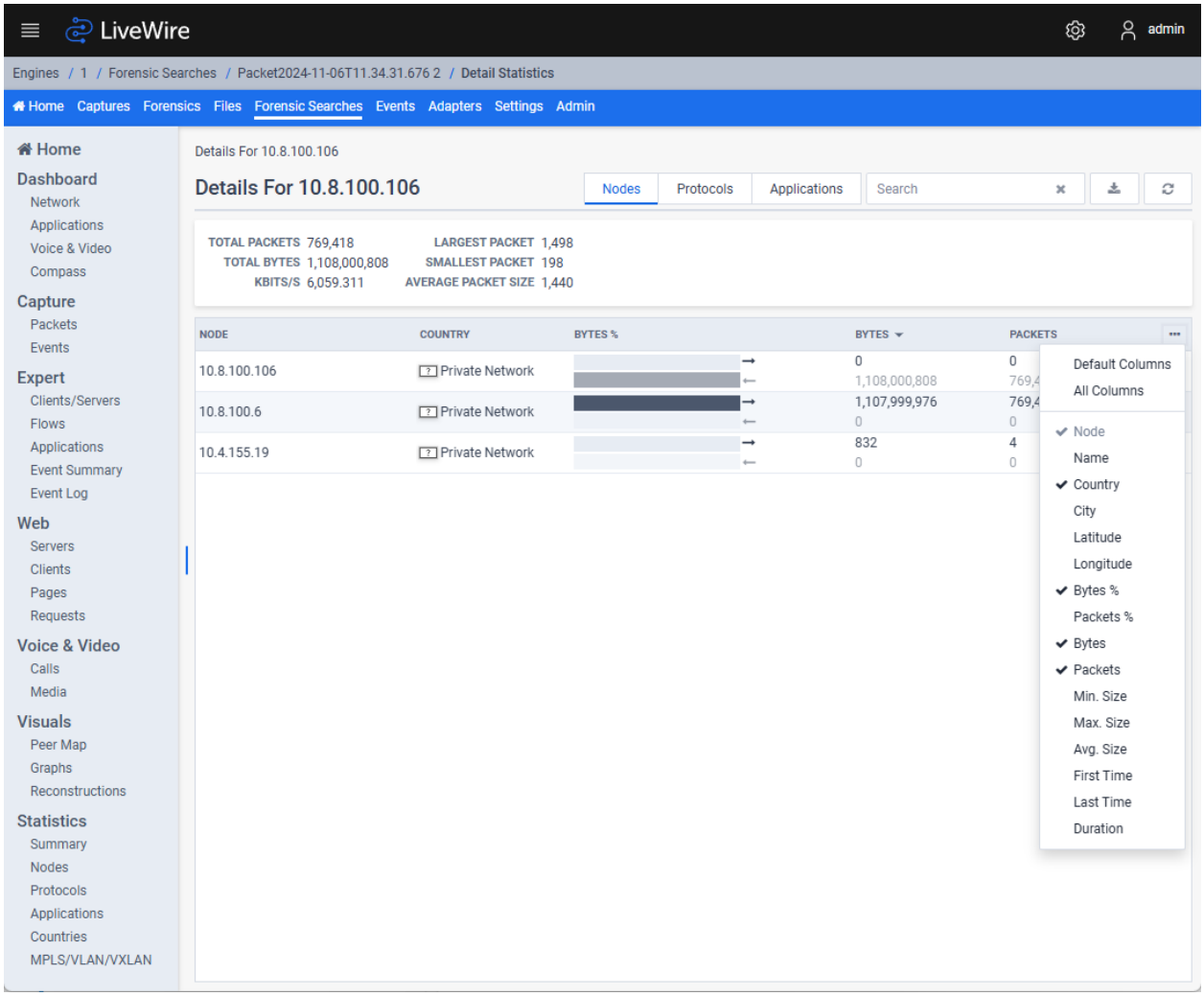
The Details Statistics View Features:

- When in the Details Statistics View, the user has the option of picking any node, protocol or application and requesting the details for it as well. Because of this, this view can become nested as the user continues to request details. For this reason, the very top of the view features a breadcrumb path showing all of the Details Statistics Views the user has viewed since launching from the initial request to see details from one of the Statistics views or Peer Map. The most recent Details Statistics View is shown on the far right , and the less recent Details Statistics View is shown on the far left. All breadcrumb items are a clickable link that will take the user back to that Details Statistics View, except for the most recent Details Statistics View on the far right since that's the view the user is currently viewing.
- Directly under the breadcrumbs and to the left is the title of the Details Statistics View. This title will vary depending on whether the user is viewing the details for a node, protocol, application, nodes conversation, node + protocol conversation or node + application conversation.
- Directly under the title of the Details Statistics View is the Statistics Panel which displays statistics about the nodes in the view:
  - "Total Packets": The total number of packets
  - "Total Bytes": The total number of bytes
  - "kbits/s": The utilization
  - "Largest Packet": The largest packet size
  - "Smallest Packet": The smallest packet size

- "Average Packet Size": The average packet size

- Directly under the breadcrumbs and to the right are controls to modify the view:
  - If there are any nodes to display, a "Nodes" button will be displayed. Clicking this "Nodes" button will display a list of nodes below the Statistics Panel.
  - If there are any protocols to display, a "Protocols" button will be displayed. Clicking this "Protocols" button will display a list of protocols below the Statistics Panel.
  - If there are any applications to display, a "Applications" button will be displayed. Clicking this "Applications" button will display a list of applications below the Statistics Panel.
  - When the user is viewing protocols or applications:
    - The user will be able to specify whether to view them in a "Flat" layout or "Hierarchy" layout from a dropdown. This setting will be remembered between Details Statistics Views.
    - The user will be able to click the "Expand All" button to expand all items in the tree view.
    - The user will be able to click the "Collapse All" button to collapse all items in the tree view.
  - A Search bar will allow the user to filter the nodes, protocols or applications displayed. This setting will be remembered between Details Statistics Views.
    - When displaying protocols in "Hierarchy" mode, the filter will only apply to the items without children in the tree view.
    - When displaying applications in "Hierarchy" mode, the filter will only apply to the items without children in the tree view.
    - Any items in the tree view with no children due to the filter will be hidden.
  - An Export button will export the current view as configured and displayed into a CSV file and automatically download it to the host machine. This CSV file will be named one of the following based on which statistics are currently displayed when the export action is executed: "Application Details Statistics", "Node Details Statistics" or "Protocol Details Statistics".
  - A Refresh button will refresh the Details Statistics View.
- For Captures, the Details Statistics View will refresh every 30 seconds.

Nodes



The nodes table can display the following values, which the user can toggle by clicking the "..." button on the far right of the table header:

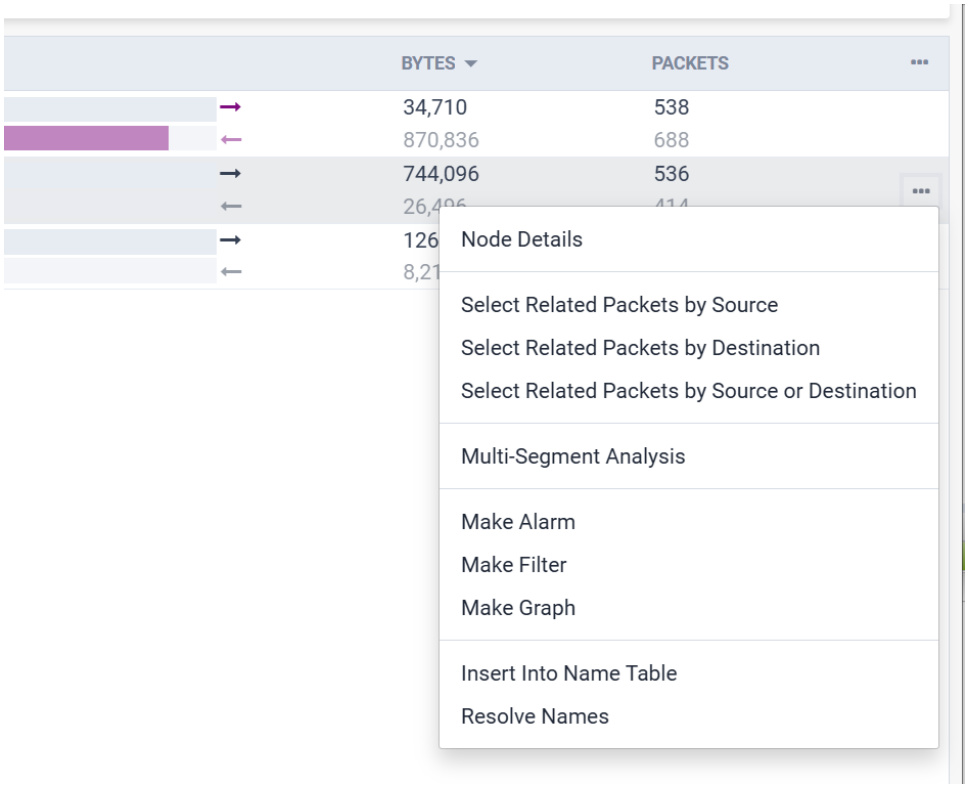
- "Node" (default): If the "Show Address Names" is enabled in the configuration options (gear icon in the top left), the name of the node is shown if there is one. Otherwise, the IP, IPv6 or physical address of the node is displayed. If a color is associated with this node, the text will be displayed in that color.
- "Name": The name of the node is shown if there is one. If a color is associated with this node, the text will be displayed in that color.
- "Country": The country for the node is displayed if it can be calculated.
- "City": The city for the node is displayed if it can be calculated.
- "Latitude": The latitude for the node is displayed if it can be calculated.
- "Longitude": The longitude for the node is displayed if it can be calculated.
- "Bytes %": 2 bars will be displayed along with a direction arrow
  - The percentage of bytes sent in comparison with all nodes in the Details Statistics View is displayed on the top (the left arrow indicates "sent")
  - The percentage of bytes received in comparison with all nodes in the Details Statistics View is displayed on the bottom (the left arrow indicates "sent")
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this node, the text will be displayed in that color

- Sorting this column will sort based on the sum of both bytes sent and bytes received
- "Packets %":
  - The percentage of packets sent in comparison with all nodes in the Details Statistics View is displayed on the top (the left arrow indicates "sent")
  - The percentage of packets received in comparison with all nodes in the Details Statistics View is displayed on the bottom (the left arrow indicates "sent")
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this node, the text will be displayed in that color
  - Sorting this column will sort based on the sum of both packets sent and bytes received
- "Bytes" (default):
  - The bytes sent in comparison with all nodes in the Details Statistics View is displayed on the top
  - The bytes received in comparison with all nodes in the Details Statistics View is displayed on the bottom
  - If a color is associated with this node, Omnipeek Windows will display the text in this color, but LiveWire Omnipeek will not
  - Sorting this column will sort based on the sum of both bytes sent and bytes received
- "Packets" (default):
  - The packets sent in comparison with all nodes in the Details Statistics View is displayed on the top
  - The packets received in comparison with all nodes in the Details Statistics View is displayed on the bottom
  - If a color is associated with this node, Omnipeek Windows will display the text in this color, but LiveWire Omnipeek will not
  - Sorting this column will sort based on the sum of both packets sent and bytes received
- "Min. Size":
  - The minimum packet size sent for this node is displayed on the top
  - The minimum packet size received for this node is displayed on the bottom
  - Sorting this column will sort based on the minimum of both minimum packet size sent and minimum packet size received
- "Max. Size":
  - The maximum packet size sent for this node is displayed on the top
  - The maximum packet size received for this node is displayed on the bottom
  - Sorting this column will sort based on the maximum of both maximum packet size sent and maximum packet size received
- "Avg. Size":
  - The average packet size sent for this node is displayed on the top
  - The average packet size received for this node is displayed on the bottom
  - Sorting this column will sort based on the average of both bytes and packets sent and received
- "First Time":
  - The timestamp of the first packet sent for this node is displayed on the top
  - The timestamp of the first packet received sent for this node is displayed on the top
  - Sorting this column will sort based on the minimum of both first packet sent and first packet received
- "Last Time":
  - The timestamp of the last packet sent for this node is displayed on the top
  - The timestamp of the last packet received sent for this node is displayed on the top

- Sorting this column will sort based on the maximum of both last packet sent and last packet received

- "Duration": The duration of time in which the packets for this node were captured

Context Menu Operations:

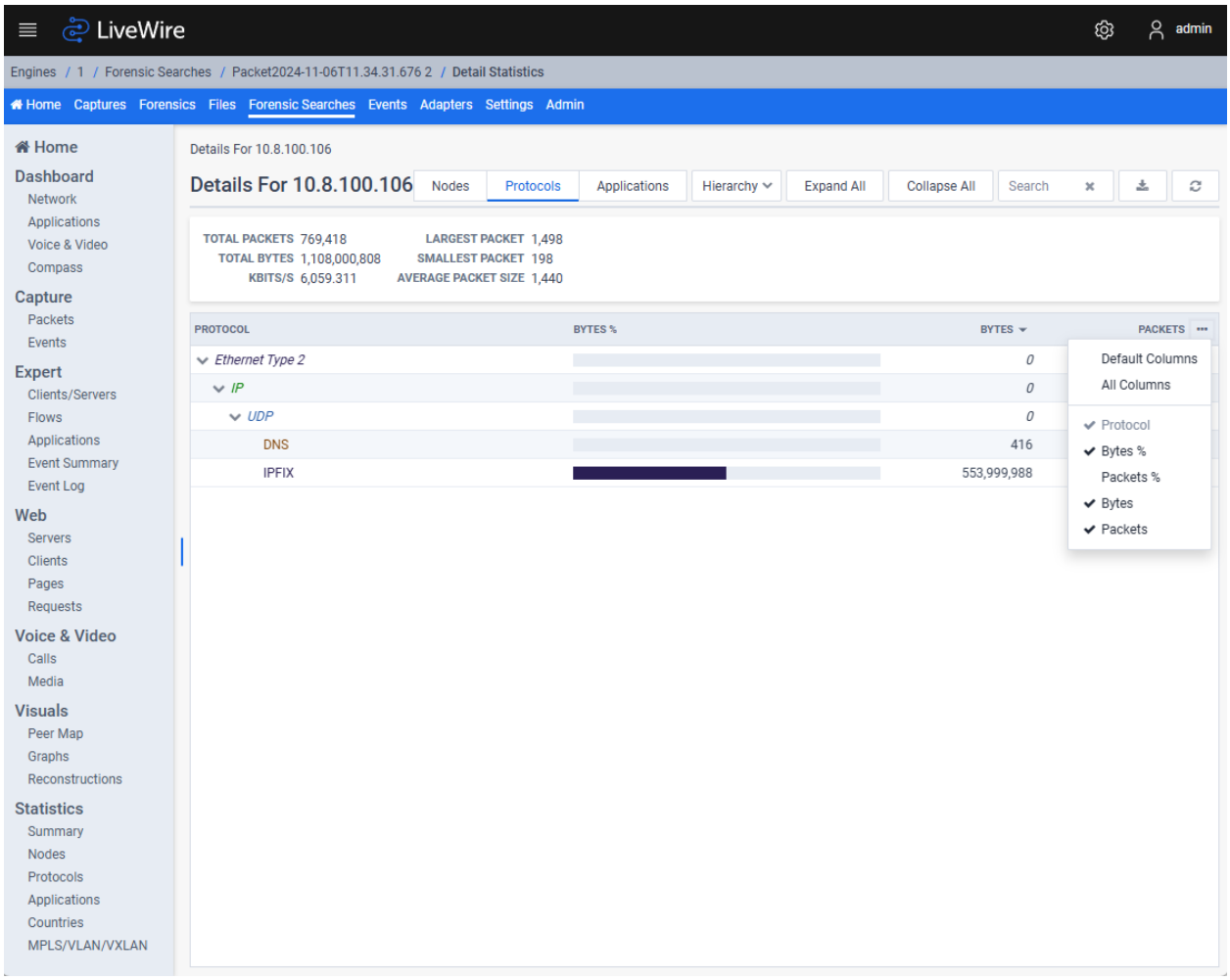


Clicking the "..." button at the end of each row in the table will display the context menu for each node with the following options:

- "Node Details":
  - Clicking this item will open a new Details Statistics View for the node in addition to the current nodes, protocols or applications for the current Details Statistics View
  - This item will be disabled if the node is already a part of the current Details Statistics View
- "Select Related Packets by Source": This item will redirect to the Packets View and select all packets in the Packets View that match the node as source. This item is disabled if the user cannot view packets or there are no packets in this Capture or Forensic Search.
- "Select Related Packets by Destination": This item will redirect to the Packets View and select all packets in the Packets View that match the node as destination. This item is disabled if the user cannot view packets or there are no packets in this Capture or Forensic Search.
- "Select Related Packets by Source or Destination": This item will redirect to the Packets View and select all packets in the Packets View that match the node as source or destination. This item is disabled if the user cannot view packets or there are no packets in this Capture or Forensic Search.
- "Multi-Segment Analysis": This item will redirect to the Multi-Segment Analysis View with the start and end time being the first and last time the node was captured (respectively), and the filter pre-populated with a filter for the node. This item is disabled if the user cannot upload files or create a forensic search.
- "Make Alarm": This item will redirect to the Alarms View with the name of the new alarm being the node, and the units being "Total Bytes Per Second"
- "Make Filter": This item will redirect to the Filters View with an address filter pre-populated with a filter for the node to any other address in both directions
- "Make Graph": This item will redirect to the Graphs View with the name of the new graph being the node, and the units being "Bytes", and the graph table pre-populated with the node and "Total Bytes"

- "Insert Into Name Table": This item will pop up a dialog allowing the user to insert this node into the name table (the name will be pre-populated to the node name, the node type pre-populated to the best match, and the entry pre-populated to the IP, IPv6 or physical name of the node)
- "Resolve Names": This item will attempt to auto-resolve the node and add it to the name table

Protocols



The protocols table can display the following values, which the user can toggle by clicking the "..." button on the far right of the table header:

- "Protocol" (default): If the "Show Port Names" is enabled in the configuration options (gear icon in the top left), the name of the protocol is shown if there is one. Otherwise, the protocol is displayed. If a color is associated with this node, the text will be displayed in that color.
- "Bytes %" (default):
  - The percentage of bytes sent and received in comparison with all protocols in the Details Statistics View
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this protocol, the text will be displayed in that color
- "Packets %":
  - The percentage of packets sent and received in comparison with all protocols in the Details Statistics View
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this protocol, the text will be displayed in that color
- "Bytes" (default):

- The bytes sent and received in comparison with all protocols in the Details Statistics View is displayed on the top

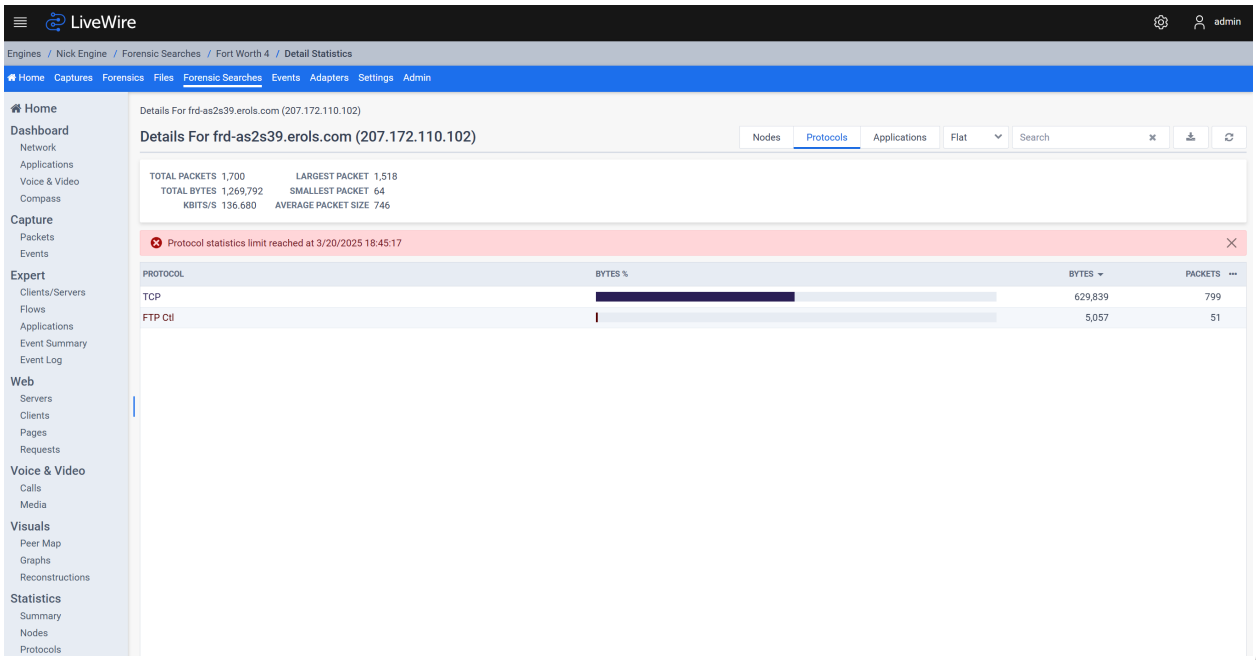
- "Packets" (default):
  - The packets sent and received in comparison with all protocols in the Details Statistics View is displayed on the top

The Hierarchy Mode:

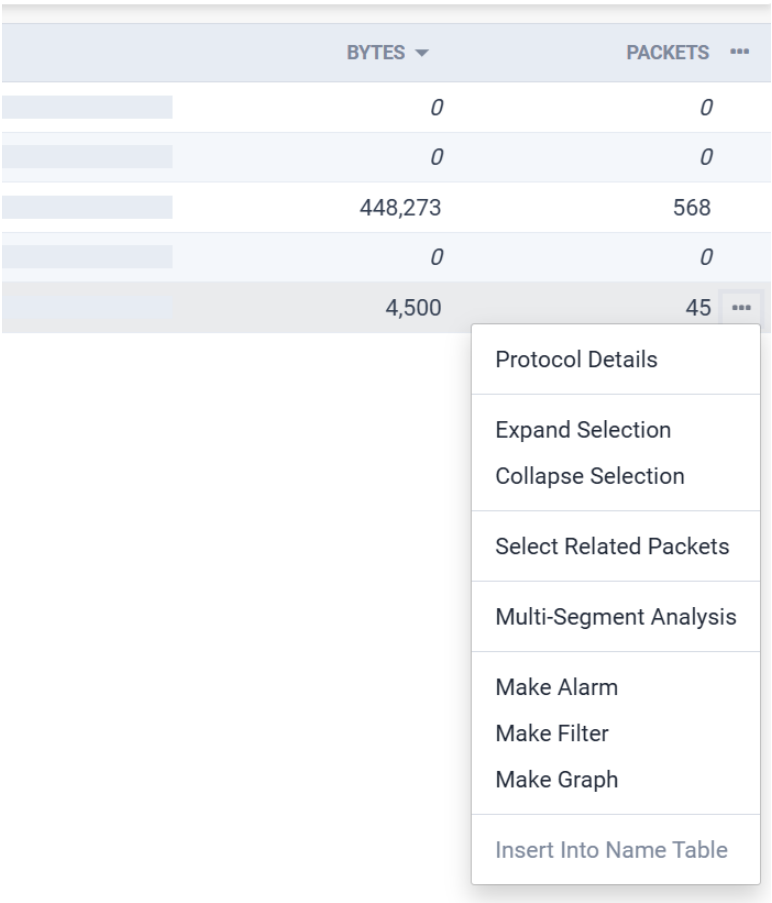
- When showing protocols in hierarchy mode, if a tree item is expanded then the "Bytes %", "Packets %", "Bytes" and "Packets" values describe packets whose most specific protocol is that protocol. If it is collapsed, the "Bytes %", "Packets %", "Bytes" and "Packets" values include all packets that include that protocol in its protocol hierarchy.

Limit Message:

- If the protocol statistics limit has been reached, the user will see a red error banner above the protocols table detailing the limit that was reached.



Context Menu Operations:

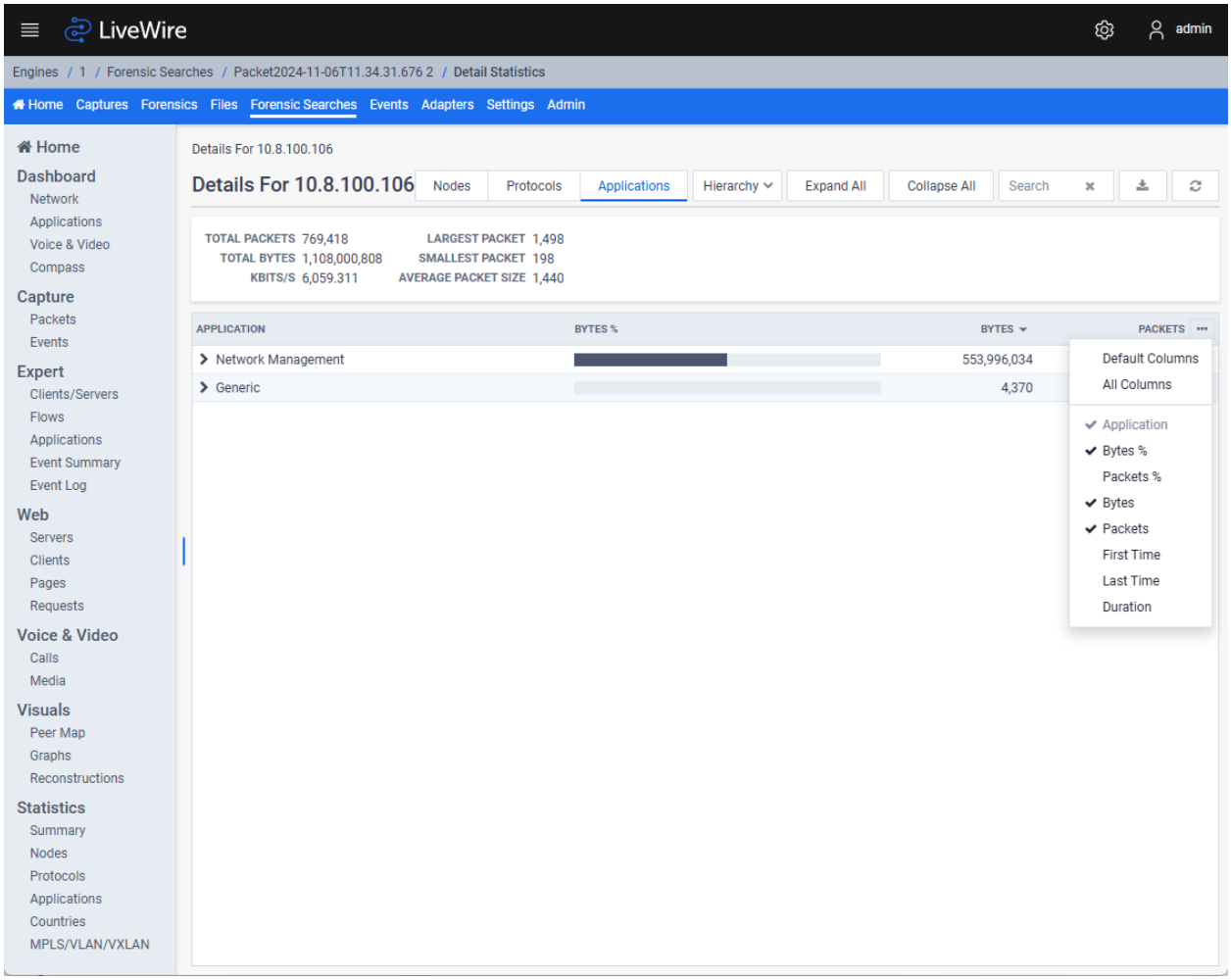


Clicking the "..." button at the end of each row in the table will display the context menu for each protocol with the following options:

- "Protocol Details":
  - Clicking this item will open a new Details Statistics View for the protocol in addition to the current nodes, protocols or applications for the current Details Statistics View
  - This item will be disabled if the protocol is already a part of the current Details Statistics View
- "Expand Selection": This item will expand all child items in the tree view for this protocol (only visible if viewing protocols in "Hierarchy" Mode)
- "Collapse Section": This item will collapse all child items in the tree view for this protocol (only visible if viewing protocols in "Hierarchy" Mode)
- "Select Related Packets": This item will redirect to the Packets View and select all packets in the Packets View that match the protocol. This item is disabled if the user cannot view packets or there are no packets in this Capture or Forensic Search.
- "Multi-Segment Analysis": This item will redirect to the Multi-Segment Analysis View with the start and end time being the first and last time the protocol was captured, and the filter pre-populated with a filter for the protocol. This item is disabled if the user cannot upload files or create a forensic search.
- "Make Alarm": This item will redirect to the Alarms View with the name of the new alarm being the protocol, and the units being "Total Bytes Per Second"
- "Make Filter": This item will redirect to the Filters View with a protocol filter pre-populated with a filter for the protocol

- "Make Graph" (not in Omnipeek Windows): This item will redirect to the Graphs View with the name of the new graph being the protocol, and the units being "Bytes", and the graph table pre-populated with the protocol and "Total Bytes"
- "Insert Into Name Table" (only enabled for protocols that aren't already identified by protospecs): This item will pop up a dialog allowing the user to insert this protocol into the name table (the protocol type will be pre-populated to the best match, and the entry pre-populated to the protocol name)

Applications



The applications table can display the following values, which the user can toggle by clicking the "..." button on the far right of the table header:

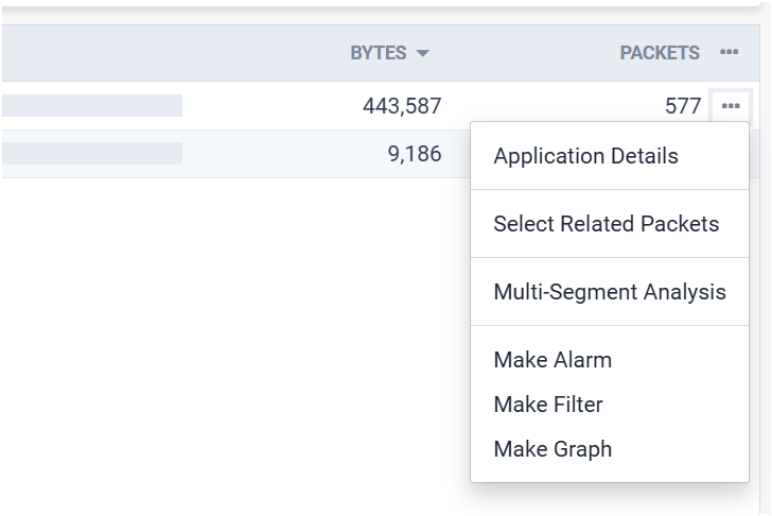
- "Application" (default): The name of the application. If a color is associated with this application, the text will be displayed in that color.
- "Category" (default, only in "Flat" Mode): The category of the application
- "Bytes %" (default):
  - The percentage of bytes sent and received in comparison with all applications in the Details Statistics View
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this application, the text will be displayed in that color
- "Packets %":
  - The percentage of packets sent and received in comparison with all applications in the Details Statistics View
  - Hovering over the bar graph will display the numerical percentage value in a tooltip
  - If a color is associated with this application, the text will be displayed in that color

- "Bytes" (default):
  - The bytes sent and received in comparison with all applications in the Details Statistics View is displayed on the top
- "Packets" (default):
  - The packets sent and received in comparison with all applications in the Details Statistics View is displayed on the top
- "First Time": The timestamp of the first packet for this application
- "Last Time": The timestamp of the last packet for this application
- "Duration": The duration of time in which the packets for this application were captured

The Hierarchy Mode:

- When showing applications in hierarchy mode, the only parent item is the category for the children items.

Context Menu Operations:



Clicking the "..." button at the end of each row in the table will display the context menu for each application with the following options:

- "Application Details":
  - Clicking this item will open a new Details Statistics View for the application in addition to the current nodes, protocols or applications for the current Details Statistics View
  - This item will be disabled if the application is already a part of the current Details Statistics View
- "Select Related Packets": This item will redirect to the Packets View and select all packets in the Packets View that match the application. This item is disabled if the user cannot view packets or there are no packets in this Capture or Forensic Search.
- "Multi-Segment Analysis": This item will redirect to the Multi-Segment Analysis View with the start and end time being the first and last time the application was captured, and the filter pre-populated with a filter for the application. This item is disabled if the user cannot upload files or create a forensic search
- "Make Alarm": This item will redirect to the Alarms View with the name of the new alarm being the application, and the units being "Total Bytes Per Second"
- "Make Filter": This item will redirect to the Filters View with an application filter pre-populated with a filter for the application
- "Make Graph": This item will redirect to the Graphs View with the name of the new graph being the application, and the units being "Bytes", and the graph table pre-populated with the protocol and "Total Bytes"