LiveAction

LiveWire 25.1.0 New Features

QUICK GUIDE

ver. 25.1.0b

Added More DHCP/DNS LiveFlow Alerts to LiveFlow

The following DHCP/DNS LiveFlow Alerts have been added to LiveFlow:

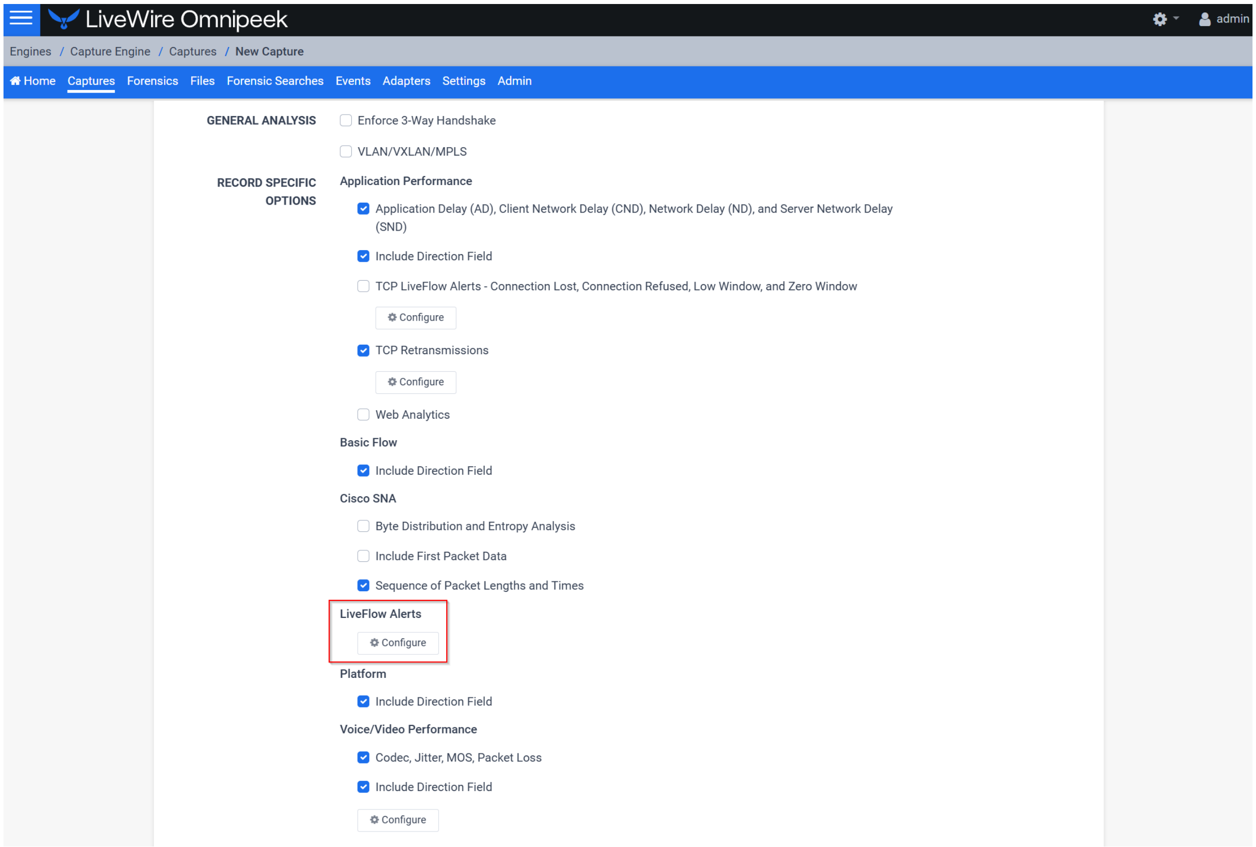
	LiveFlow Alert	Notes
1	DHCP Frequent Retransmissions	**Description**: Repeated DHCPDISCOVER or DHCPREQUEST messages observed from a given client within a short time period. **Cause**: Retransmission occurs when the DHCP client isn't receiving a response from a server in a timely fashion. This may be because the client's message isn't reaching the server, because the server isn't configured to provide leases for the client subnet, or because the subnet has been exhausted of free leases. Retransmissions can also occur when the DHCP client is receiving a DHCPOFFER for a lease it can't accept: for example, the offer may be missing DHCP options critical to the device's operation, such as vendor-specific information (option 43), or options specifying where the device can load a boot image and/or configuration file. Remedy: Determine whether any responses from a DHCP server to the client are seen on the wire. If no responses are observed, verify that the DHCPDISCOVER or DHCPREQUEST are reaching the appropriate DHCP server(s). Check the logs of the DHCP server(s) to verify the server is seeing the message(s) and for a reason why it may not be sending a response. Check the configuration of the DHCP server(s) to ensure they're configured to serve leases for the client's subnet, and verify that DHCP relay(s) are correctly configured on the router(s) in the DHCP client's local subnet. If responses are observed, check the logs of the DHCP client(s) for a reason why the client may be rejecting the lease, and verify that the necessary DHCP options for the client are properly configured on the DHCP server(s).
2	DHCP Low Lease Time	**Description**: The client has been offered an IP address lease in which the lease time is at or below the threshold. **Cause**: The DHCP server's lease time is configured "too low." **Remedy**: Consider an appropriate lease time for your environment, taking into consideration the number of fixed (desktop) nodes, static (server and router) nodes, mobile (laptop wired and wireless) nodes, and the available IP address space for each subnet.
3	DHCP Request Rejected	**Description**: DHCP Request has been rejected by a DHCP server. **Cause**: A client is booting and attempting to renew an IP address that has already been reallocated, or the client has moved to a different subnet and the IP address was statically configured in the DHCP server. **Remedy**: Ensure that there are adequate IP addresses to be dynamically allocated and consider reducing the lease time. Check to see if the client has moved and if its IP address has been statically assigned at the DHCP server to its physical address.
4	DHCP Request Storm	**Description**: A high count of DHCP addresses are being requested. **Cause**: A DoS attack may be in progress with a utility like gobbler, which requests as many DHCP addresses as possible. This blocks legitimate requests from being fulfilled. **Remedy**: Disable the machine if it is accessible. If the machine is not accessible and your switch allows port blocking, block DHCP port traffic on that switch port.

	LiveFlow Alert	Notes
5	DHCP Slow Response Time	**Description**: Slow response time from a DHCP server to a DHCPDISCOVER or DHCPREQUEST message from a client. **Cause**: May be caused by unusual network latency or by the DHCP server itself. The DHCP server may simply be overloaded. Depending on the DHCP server type and configuration, the server may be delayed by (e.g.) attempting to perform dynamic DNS updates on behalf of the DHCP client. DHCP servers can also be configured in a fallback scenario to intentionally delay their response to requests: the expectation is that, in normal operation, another DHCP server (configured without such a delay) should respond to clients. **Remedy**: Determine where the delay is being introduced: on the wire due to latency or network issues from client to server or server to client, or at the DHCP server between the time a message is received and a response is being sent. If the delay is on the wire, perform normal diagnostics of the network path. If at the DHCP server, check the load on the DHCP server. Review the logs of the DHCP server, correlate the inbound request and response, and look for unusual log messages between the two, possibly relating to dynamic DNS. Check the configuration of the DHCP server to see if a delayed response has been configured by intent or accident.
6	DNS Frequent Retransmissions	**Description**: Same DNS query, with same transaction ID, repeatedly issued by a client within a short time period. **Cause**: Caused when the DNS client doesn't receive a (timely) response to a DNS query, and attempts to re-send the same query. May be caused by incorrect DNS resolver configuration on the client, packet loss or network issues between client and server (in either direction), or an overloaded or misconfigured DNS server. **Remedy**: Determine whether this is an intermittent or consistent problem for a given client or server. If intermittent, investigate whether latency or packet loss are occurring on the network path, and investigate the load on the DNS server(s). If consistent, check the load on the DNS server, and check the configuration and logs of the DNS server(s) to see if the server is actively ignoring requests from the client(s) due to (e.g.) an ACL or other configuration issue.
7	DNS Idle Too Long	**Description**: The DNS connection has been idle for longer than the configured threshold. **Cause**: The request is to a caching DNS server that may have to look it up from an Authoritative DNS server, or the network may be congested or have a high round-trip delay from the client or between DNS servers. The DNS request may have been lost due to a congested network. The request may be to a caching DNS server that needs to look it up from an Authoritative DNS server. A malicious actor may also use an unanswered DNS request to beacon to a Command and Control server or to exfiltrate data in the payload. **Remedy**: Ensure the DNS server is pingable and not overwhelmed. Check the contents of the DNS request to ensure it is not malicious.
8	DNS Query Format Error	**Description**: A DNS server sent a Format Error (FORMERR) in response to a DNS request, indicating the request was malformed or not understood. **Cause**: Format Errors can be caused by corruption or manipulation of requests in transit from DNS client to server. If Format Errors are consistently observed in response to queries from the same DNS client(s), the client(s) may be sending problematic requests to the DNS server: the requests may literally be malformed, or they may use a feature (e.g. EDNS) unsupported by the DNS server. **Remedy**: Determine why the Format Errors are occurring. If a persistent network issue, address the source of corruption or manipulation. If specific client(s) are consistently receiving Format Errors, determine whether the issue is a misbehaving client or (e.g.) an outdated server that does not support DNS extensions required by those client(s).

	LiveFlow Alert	Notes
9	DNS Server Failure	**Description**: A DNS server sent a Server Failure (SERVFAIL) error in response to a DNS request, indicating the server could not process the request. **Cause**: The Server Failure error is a catch-all error returned when a DNS server is unable to respond to a request for any reason outside of the more specific standard errors such as FORMERR (query format error), NOTIMP (function not implemented), or REFUSED (request/access denied). Because of this, it's impossible to define a generic cause for a Server Failure error. That said, probably the most common cause of Server Failure errors is an inability of the DNS server to communicate with other DNS servers to retrieve information required to answer the query. For example, a Secondary DNS server may have been unable to receive a Zone Transfer from its Primary, a Recursive DNS server may be unable to route to the Internet, or a Forwarding DNS server may be unable to contact any of the configured forwarding targets. **Remedy**: Check the connectivity of the DNS server returning Server Failure errors to ensure that it can reach all necessary upstream servers. Check the logs of the DNS server returning Server Failures to discover the specific reason why a Server Failure is being returned.
10	DNS Server Refused Query	**Description**: A DNS server sent a Refused (REFUSED) error in response to a DNS request, indicating the server refused to service the request. **Cause**: The Refused error is returned when a DNS server is asked by a client to perform an operation that is disallowed by a configured policy. Common causes are denial due to explicit allow-query ACLs, recursive queries being sent to an authoritative-only server, requesting a full (AXFR) or incremental (IXFR) zone transfer without permission, or attempting to perform a dynamic DNS update without permission. **Remedy**: Determine whether the request being Refused should or should not be allowed. If the operation should be allowed, modify the configuration of the DNS server to permit the operation. If the operation is being correctly denied, investigate the client(s) to determine why they attempted to perform a disallowed action.

LiveFlow Capture Options

No changes were made to the LiveFlow Capture Options UI other than the additional LiveFlow Alerts now appear in the LiveFlow Alerts Configuration UI:


LiveWire Omnipeek
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin

GENERAL ANALYSIS

☐ Enforce 3-Way Handshake

☐ VLAN/VXLAN/MPLS

RECORD SPECIFIC OPTIONS

Application Performance

☑ Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)

☑ Include Direction Field

☐ TCP LiveFlow Alerts - Connection Lost, Connection Refused, Low Window, and Zero Window

☑ TCP Retransmissions

☐ Web Analytics

Basic Flow

☑ Include Direction Field

Cisco SNA

☐ Byte Distribution and Entropy Analysis

☐ Include First Packet Data

☑ Sequence of Packet Lengths and Times

LiveFlow Alerts

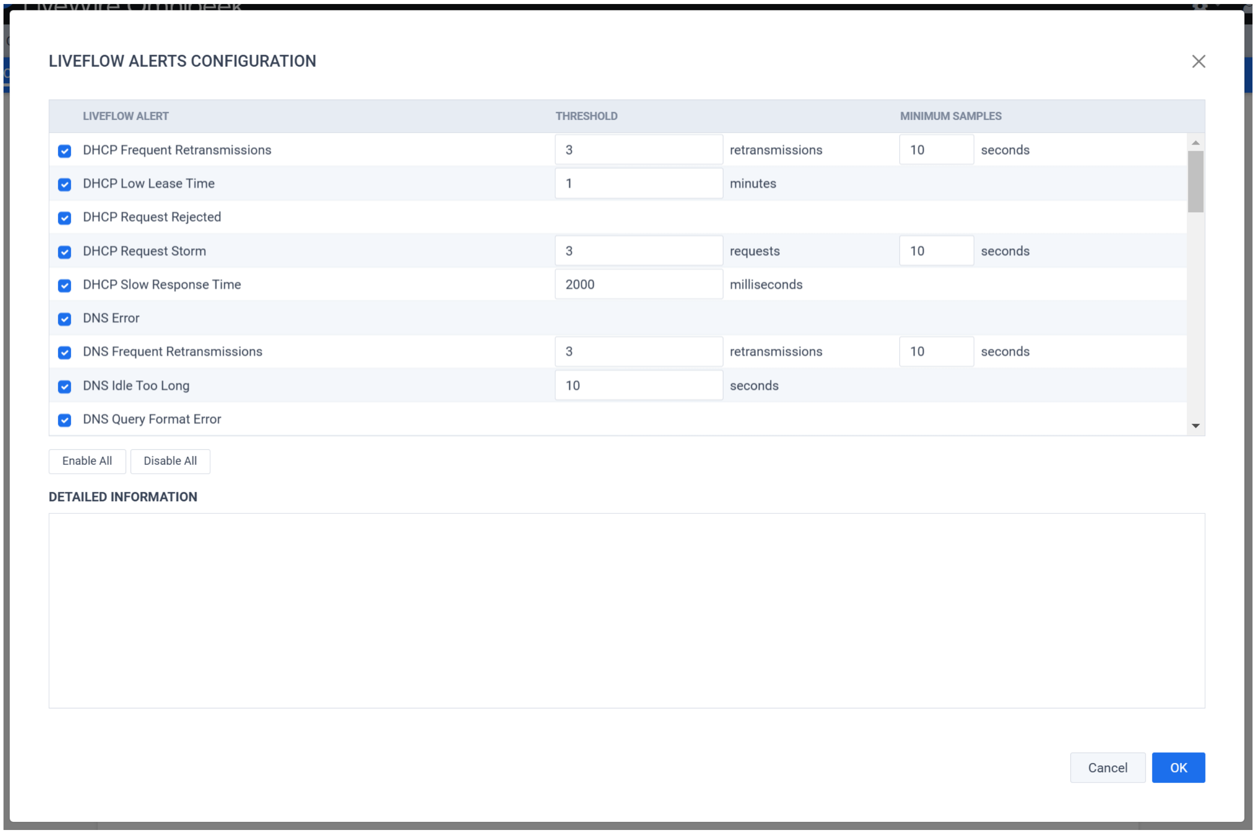
Platform

☑ Include Direction Field

Voice/Video Performance

☑ Codec, Jitter, MOS, Packet Loss

☑ Include Direction Field



LIVEFLOW ALERTS CONFIGURATION

	LIVEFLOW ALERT	THRESHOLD		MINIMUM SAMPLES	
☑	DHCP Frequent Retransmissions	3	retransmissions	10	seconds
☑	DHCP Low Lease Time	1	minutes		
☑	DHCP Request Rejected				
☑	DHCP Request Storm	3	requests	10	seconds
☑	DHCP Slow Response Time	2000	milliseconds		
☑	DNS Error				
☑	DNS Frequent Retransmissions	3	retransmissions	10	seconds
☑	DNS Idle Too Long	10	seconds		
☑	DNS Query Format Error				

DETAILED INFORMATION

Added More DHCP/DNS Expert Events to Omnipeek

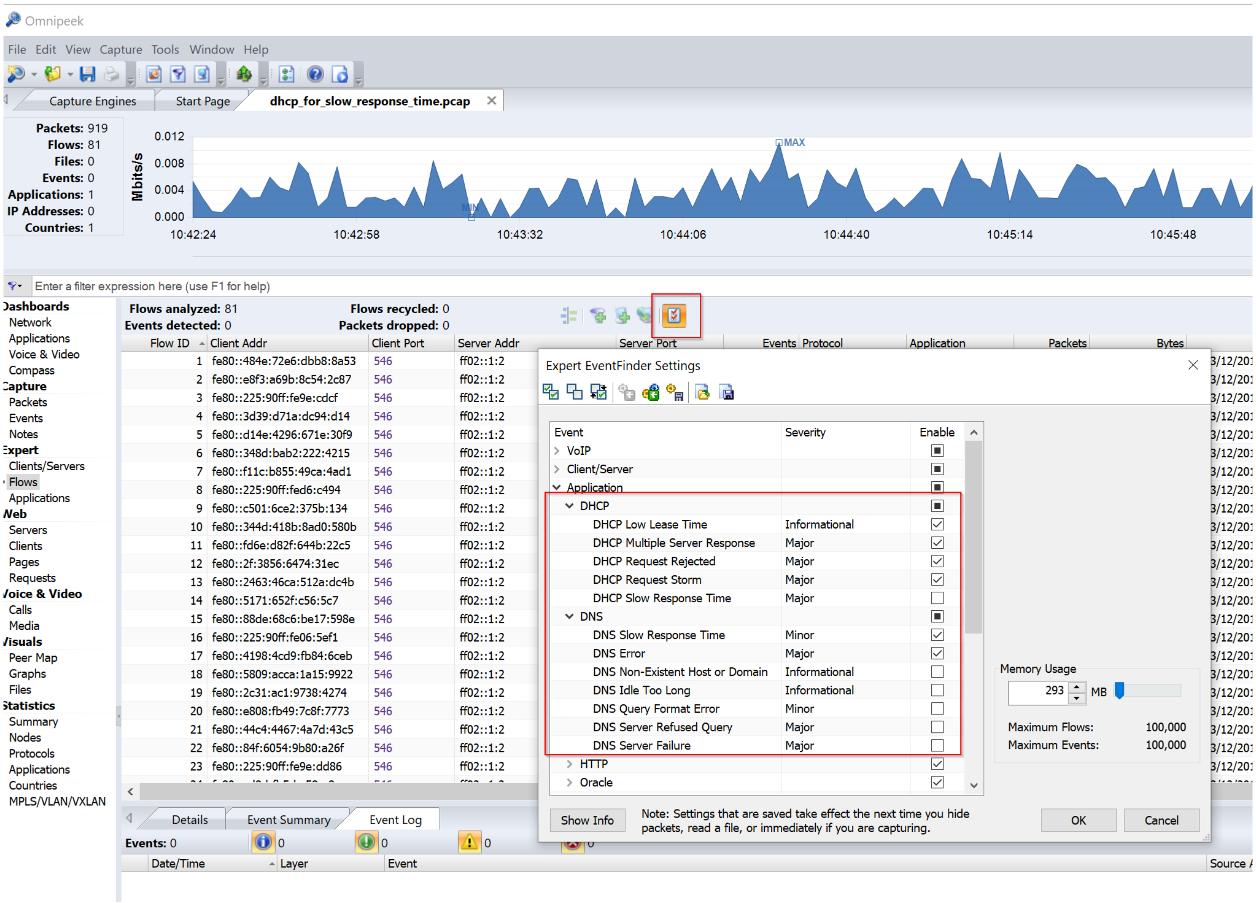
The following DHCP/DNS Expert Events have been added to Omnipeek:

	Expert Events	Notes
1	DHCP Slow Response Time	**Description**: Slow response time from a DHCP server to a DHCPDISCOVER or DHCPREQUEST message from a client. **Cause**: May be caused by unusual network latency or by the DHCP server itself. The DHCP server may simply be overloaded. Depending on the DHCP server type and configuration, the server may be delayed by (e.g.) attempting to perform dynamic DNS updates on behalf of the DHCP client. DHCP servers can also be configured in a fallback scenario to intentionally delay their response to requests: the expectation is that, in normal operation, another DHCP server (configured without such a delay) should respond to clients. **Remedy**: Determine where the delay is being introduced: on the wire due to latency or network issues from client to server or server to client, or at the DHCP server between the time a message is received and a response is being sent. If the delay is on the wire, perform normal diagnostics of the network path. If at the DHCP server, check the load on the DHCP server. Review the logs of the DHCP server, correlate the inbound request and response, and look for unusual log messages between the two, possibly relating to dynamic DNS. Check the configuration of the DHCP server to see if a delayed response has been configured by intent or accident.
2	DNS Query Format Error	**Description**: A DNS server sent a Format Error (FORMERR) in response to a DNS request, indicating the request was malformed or not understood. **Cause**: Format Errors can be caused by corruption or manipulation of requests in transit from DNS client to server. If Format Errors are consistently observed in response to queries from the same DNS client(s), the client(s) may be sending problematic requests to the DNS server: the requests may literally be malformed, or they may use a feature (e.g. EDNS) unsupported by the DNS server. **Remedy**: Determine why the Format Errors are occurring. If a persistent network issue, address the source of corruption or manipulation. If specific client(s) are consistently receiving Format Errors, determine whether the issue is a misbehaving client or (e.g.) an outdated server that does not support DNS extensions required by those client(s).

	Expert Events	Notes
3	DNS Server Failure	**Description**: A DNS server sent a Server Failure (SERVFAIL) error in response to a DNS request, indicating the server could not process the request. **Cause**: The Server Failure error is a catch-all error returned when a DNS server is unable to respond to a request for any reason outside of the more specific standard errors such as FORMERR (query format error), NOTIMP (function not implemented), or REFUSED (request/access denied). Because of this, it's impossible to define a generic cause for a Server Failure error. That said, probably the most common cause of Server Failure errors is an inability of the DNS server to communicate with other DNS servers to retrieve information required to answer the query. For example, a Secondary DNS server may have been unable to receive a Zone Transfer from its Primary, a Recursive DNS server may be unable to route to the Internet, or a Forwarding DNS server may be unable to contact any of the configured forwarding targets. **Remedy**: Check the connectivity of the DNS server returning Server Failure errors to ensure that it can reach all necessary upstream servers. Check the logs of the DNS server returning Server Failures to discover the specific reason why a Server Failure is being returned.
4	DNS Server Refused Query	**Description**: A DNS server sent a Refused (REFUSED) error in response to a DNS request, indicating the server refused to service the request. **Cause**: The Refused error is returned when a DNS server is asked by a client to perform an operation that is disallowed by a configured policy. Common causes are denial due to explicit allow-query ACLs, recursive queries being sent to an authoritative-only server, requesting a full (AXFR) or incremental (IXFR) zone transfer without permission, or attempting to perform a dynamic DNS update without permission. **Remedy**: Determine whether the request being Refused should or should not be allowed. If the operation should be allowed, modify the configuration of the DNS server to permit the operation. If the operation is being correctly denied, investigate the client(s) to determine why they attempted to perform a disallowed action.

Capture Options

No changes were made to the Capture Options UI other than the additional Expert Events now appear in the Expert Event Finder:



Packets: 919
Flows: 81
Files: 0
Events: 0
Applications: 1
IP Addresses: 0
Countries: 1

Flows analyzed: 81 **Flows recycled:** 0
Events detected: 0 **Packets dropped:** 0

Flow ID	Client Addr	Client Port	Server Addr
1	fe80::484e:72e6:dbb8:8a53	546	ff02::1:2
2	fe80::e8f3:a69b:8c54:2c87	546	ff02::1:2
3	fe80::225:90ff:fe9e:cdcf	546	ff02::1:2
4	fe80::3d39:d71a:dc94:d14	546	ff02::1:2
5	fe80::d14e:4296:671e:30f9	546	ff02::1:2
6	fe80::348d:bab2:222:4215	546	ff02::1:2
7	fe80::f11c:b855:49ca:4ad1	546	ff02::1:2
8	fe80::225:90ff:fed6:c494	546	ff02::1:2
9	fe80::c501:6ce2:375b:134	546	ff02::1:2
10	fe80::344d:418b:8ad0:580b	546	ff02::1:2
11	fe80::fd6e:d82f:644b:22c5	546	ff02::1:2
12	fe80::2f:3856:6474:31ec	546	ff02::1:2
13	fe80::2463:46ca:512a:dc4b	546	ff02::1:2
14	fe80::5171:652f:c56:5c7	546	ff02::1:2
15	fe80::88de:68c6:be17:598e	546	ff02::1:2
16	fe80::225:90ff:fe06:5ef1	546	ff02::1:2
17	fe80::4198:4cd9:fb84:6ceb	546	ff02::1:2
18	fe80::5809:acca:1a15:9922	546	ff02::1:2
19	fe80::2c31:ac1:9738:4274	546	ff02::1:2
20	fe80::e808:fb49:7c8f:7773	546	ff02::1:2
21	fe80::44c4:4467:4a7d:43c5	546	ff02::1:2
22	fe80::84f:6054:9b80:a26f	546	ff02::1:2
23	fe80::225:90ff:fe9e:dd86	546	ff02::1:2

Server Port | Events | Protocol | Application | Packets | Bytes

Events: 0 ⓘ 0 ! 0 ⚠ 0

Date/Time | Layer | Event | Source A

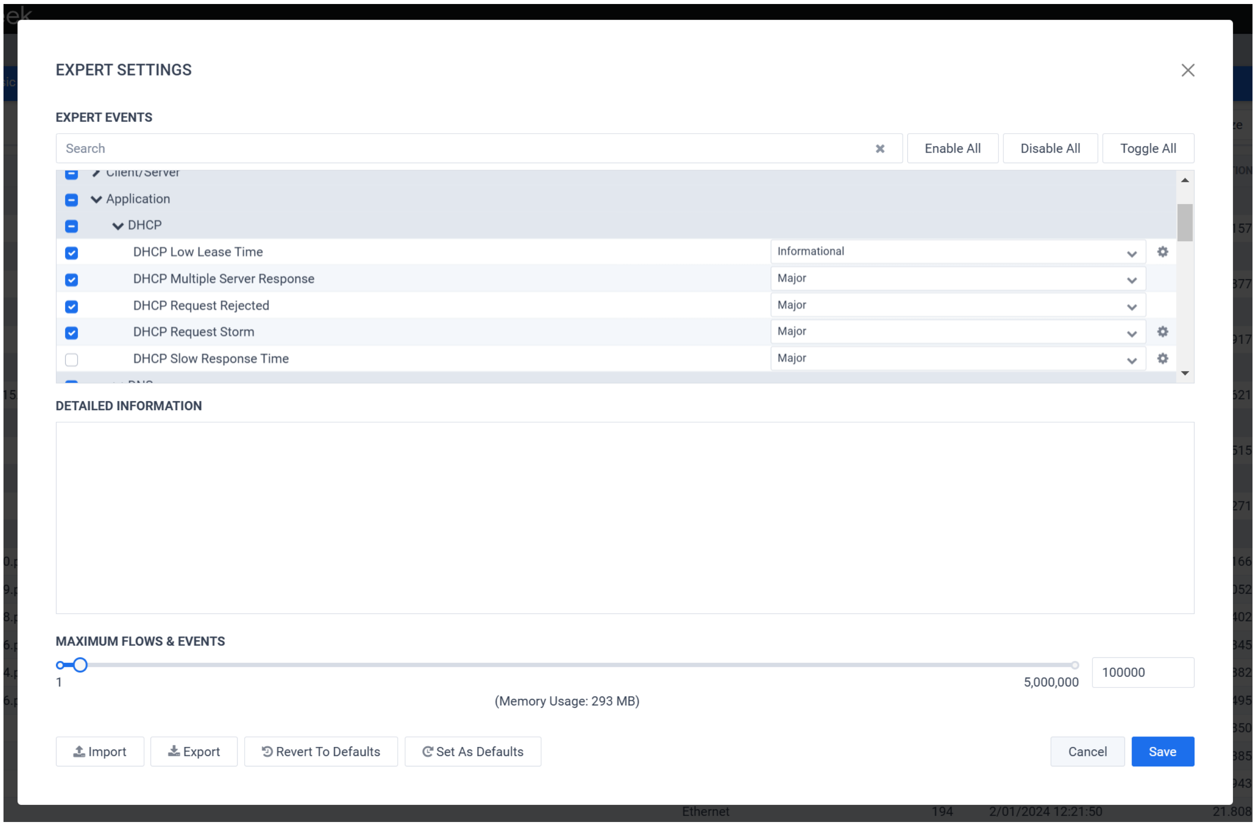
Expert EventFinder Settings

Event	Severity	Enable
› VoIP		■
› Client/Server		■
⌄ Application		■
⌄ DHCP		■
DHCP Low Lease Time	Informational	☑
DHCP Multiple Server Response	Major	☑
DHCP Request Rejected	Major	☑
DHCP Request Storm	Major	☑
DHCP Slow Response Time	Major	☐
⌄ DNS		■
DNS Slow Response Time	Minor	☑
DNS Error	Major	☑
DNS Non-Existent Host or Domain	Informational	☐
DNS Idle Too Long	Informational	☐
DNS Query Format Error	Minor	☐
DNS Server Refused Query	Major	☐
DNS Server Failure	Major	☐
› HTTP		☑
› Oracle		☑

Memory Usage
293 MB

Maximum Flows: 100,000
Maximum Events: 100,000

Note: Settings that are saved take effect the next time you hide packets, read a file, or immediately if you are capturing.



EXPERT SETTINGS

EXPERT EVENTS

- Client/Server
- Application
  - DHCP
    - ☑ DHCP Low Lease Time — Informational
    - ☑ DHCP Multiple Server Response — Major
    - ☑ DHCP Request Rejected — Major
    - ☑ DHCP Request Storm — Major
    - □ DHCP Slow Response Time — Major

DETAILED INFORMATION

MAXIMUM FLOWS & EVENTS

1 — 5,000,000: 100000

(Memory Usage: 293 MB)

Added TACACS+ “groups” to Role Based Access Control (RBAC)

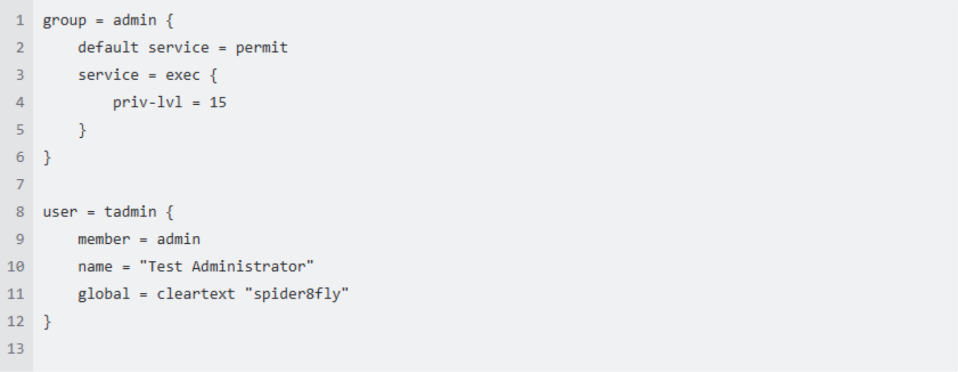
LiveWire RBAC groups now supports TACACS+ “groups”. “groups” is in quotes because the standard group blocks in a TACACS+ configuration file is inaccessible to LiveWire. So, in order to associate TACACS+ users with “groups” in LiveWire RBAC, the user will need to modify their TACACS+ group configuration as detailed in the next section. When the user does this, they will have RBAC group support for TACACS+.

TACACS+ Configuration

In order to support TACACS+ groups in LiveWire RBAC, the user must manually modify their TACACS+ group configuration. For each group block in the TACACS+ configuration file, the user must add a “livewire” service block with a “livewire-group” attribute containing the name of the group as its value.

The TACACS+ configuration file is typically at */etc/tacacs+/tac_plus.conf*.

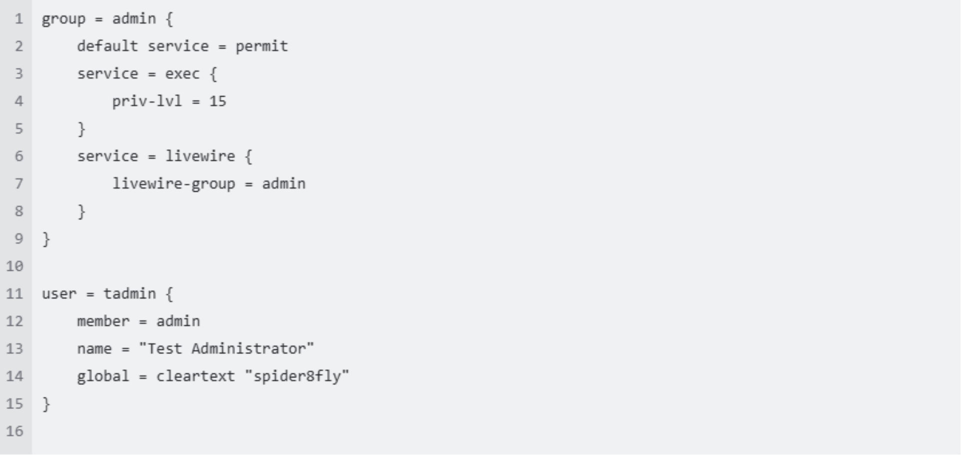
For example, let’s take the following snippet from a TACACS+ configuration file: Add TACACS+ groups to LiveWire RBAC.



```
group = admin {
    default service = permit
    service = exec {
        priv-lvl = 15
    }
}

user = tadmin {
    member = admin
    name = "Test Administrator"
    global = cleartext "spider8fly"
}

```

This snippet has a user named “tadmin” and puts that user in the “admin” group.

In order to make the “admin” group work with LiveWire RBAC, the user will need to add the “livewire” service block with a “livewire-group” attribute containing the name of the group as its value. For example:



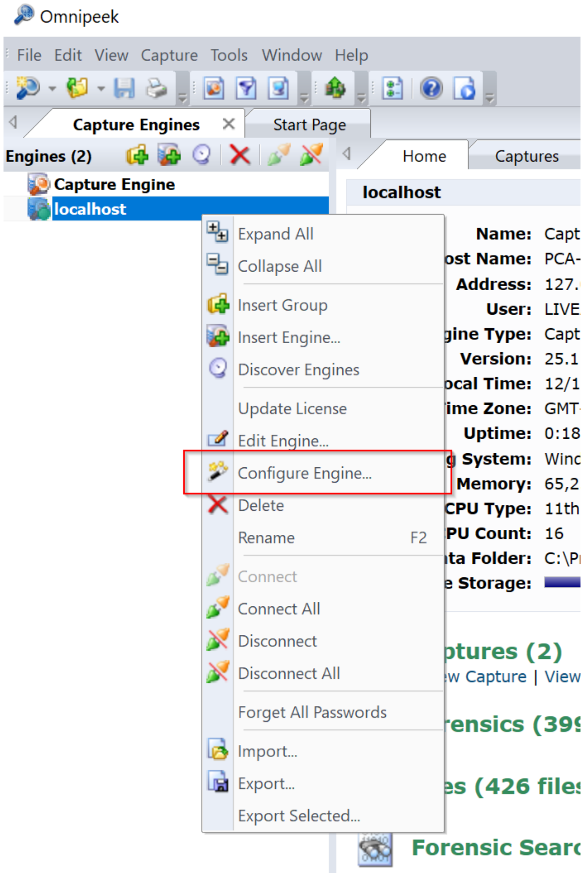
```
group = admin {
    default service = permit
    service = exec {
        priv-lvl = 15
    }
    service = livewire {
        livewire-group = admin
    }
}

user = tadmin {
    member = admin
    name = "Test Administrator"
    global = cleartext "spider8fly"
}

```

A “livewire” service block was added with a “livewire-group” attribute containing the value “admin”, which is the name of the group. Now in LiveWire RBAC, the “tadmin” user is associated with the TACACS+ group “admin”.

Note The TACACS+ service will need to be restarted after this change.

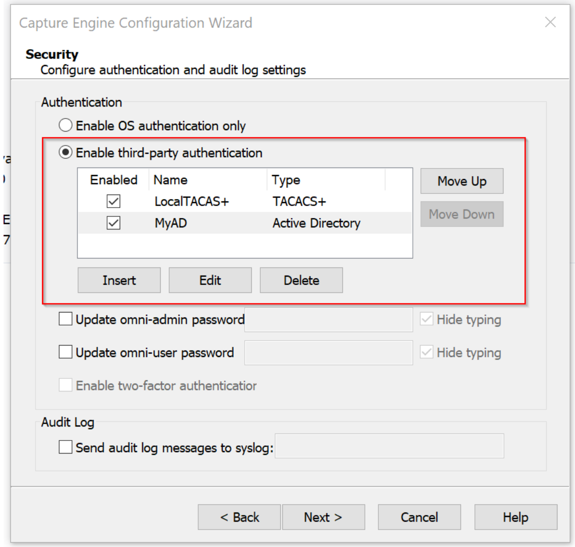
Omnipeek Windows

RBAC can be configured through Omnipeek Windows by right clicking the desired capture engine in the engine list and clicking the "Configure Engine..." menu option.



Security Tab

From there, you can navigate to the "Security" tab and edit the third-party authentication:


Capture Engine Configuration Wizard

Security
Configure authentication and audit log settings

Authentication

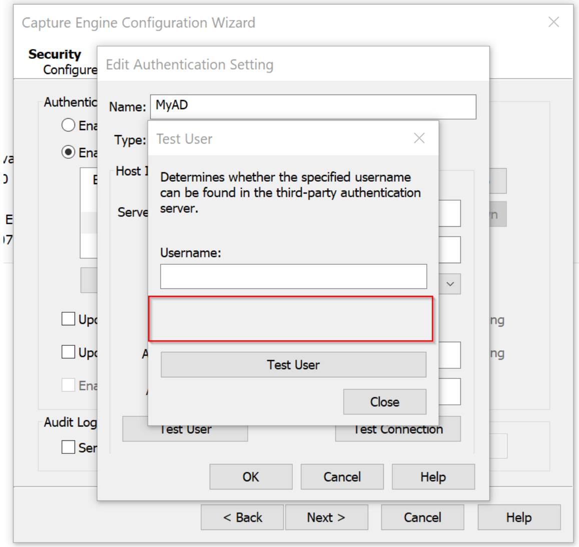
○ Enable OS authentication only
● Enable third-party authentication

Enabled	Name	Type
☑	LocalTACACS+	TACACS+
☑	MyAD	Active Directory

☐ Update omni-admin password ☑ Hide typing
☐ Update omni-user password ☑ Hide typing
☐ Enable two-factor authenticatior

Audit Log
☐ Send audit log messages to syslog:

For Active Directory authentication servers, the edit dialog should work the same as before, and the "Test Connection" button should work the same as before. The only change will be in the dialog that comes up when the user clicks the "Test User" button. The dialog will look a bit more spacious as we need to include a password field for TACACS+, but not for Active Directory so the user will just see some blank space. The user will not need a password to test the user for Active Directory. Note: This "Test User" button will not be visible for TACACS+ for capture engines below v25.1.



Capture Engine Configuration Wizard

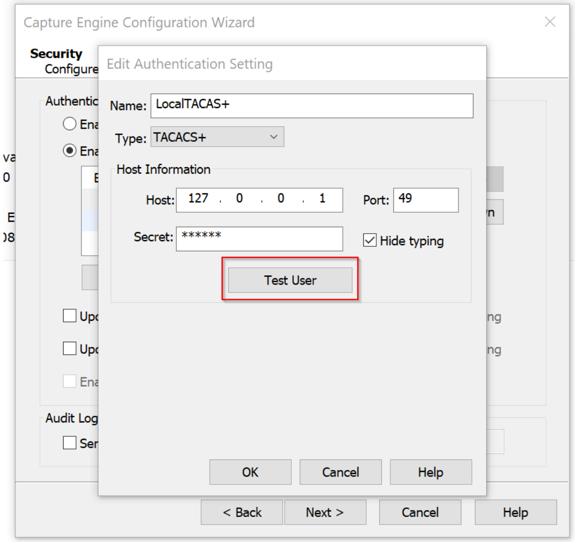
Edit Authentication Setting

Name: MyAD

Test User

Determines whether the specified username can be found in the third-party authentication server.

Username:



Capture Engine Configuration Wizard

Edit Authentication Setting

Name: LocalTACAS+

Type: TACACS+

Host Information

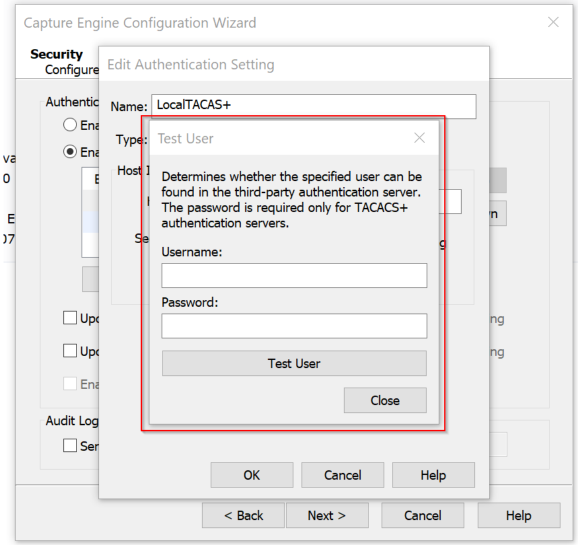
Host: 127 . 0 . 0 . 1

Port: 49

Secret: ******

☑ Hide typing

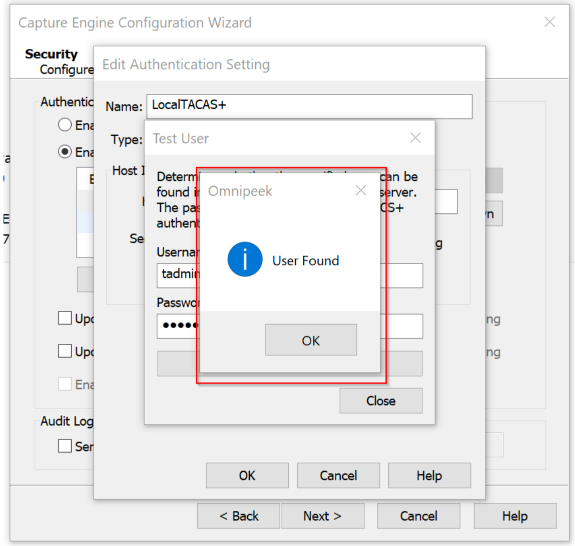
For TACACS+ authentication servers, the edit dialog will now include a "Test User" button. Upon clicking this button, a dialog will appear allowing the user to type in a username and password to test the user existence. No "Test Connection" button will be present as in Active Directory.



Name: LocalTACAS+

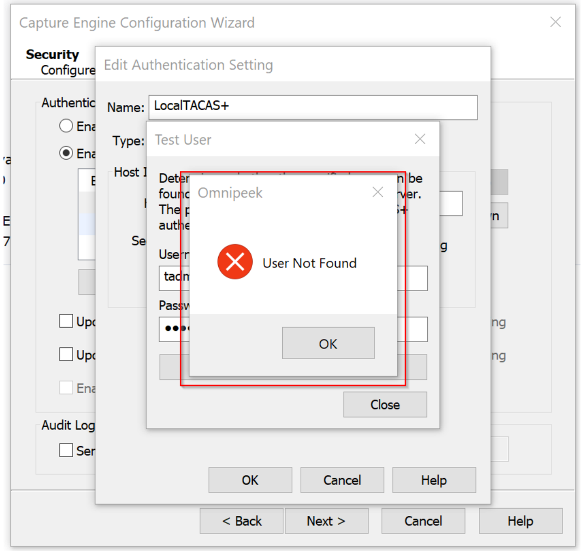
Determines whether the specified user can be found in the third-party authentication server. The password is required only for TACACS+ authentication servers.

The user will see either a success or failure message after clicking the “Test User” button.



Name: LocalTACAS+

User Found

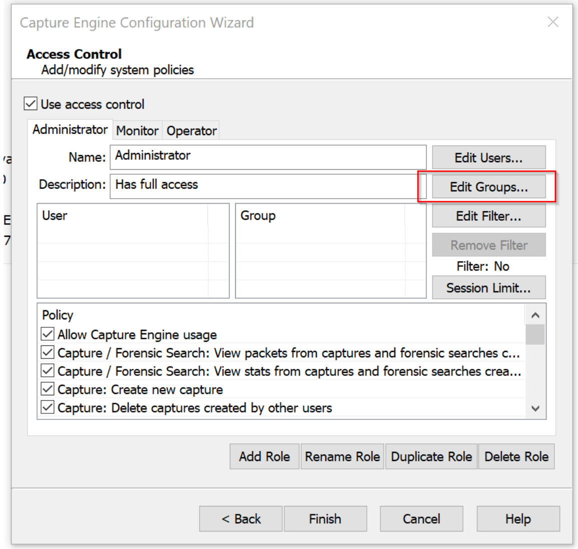


Name: LocalTACAS+

User Not Found

Access Control Tab

In the “Access Control” tab, the only changes are in the dialog that appears from clicking the “Edit Groups…” button.



☑ Use access control

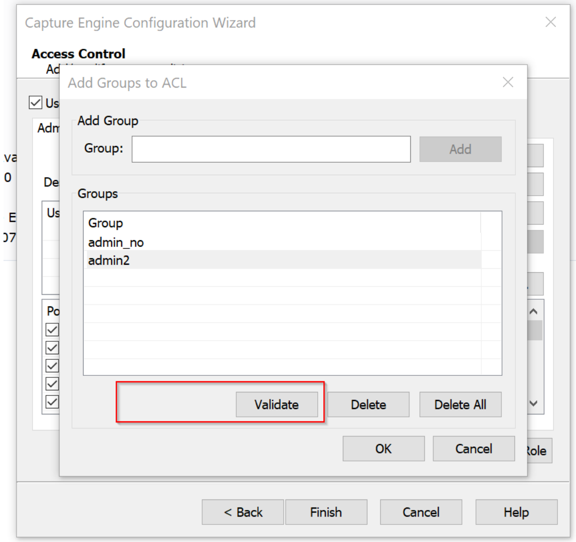
Name: Administrator

Description: Has full access

Filter: No

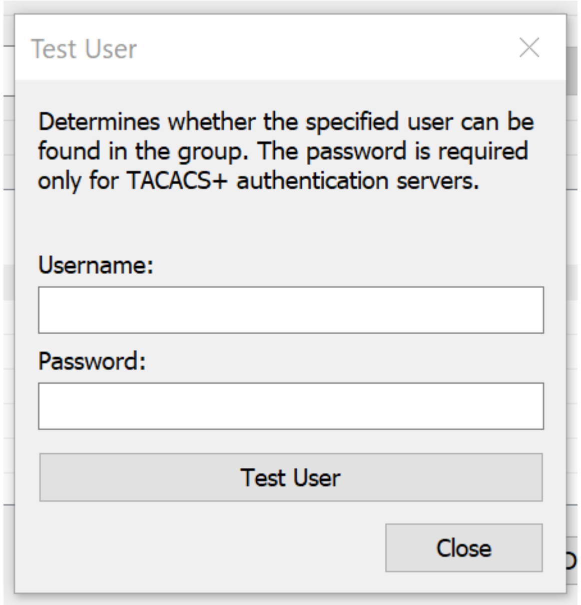
Policy
- ☑ Allow Capture Engine usage
- ☑ Capture / Forensic Search: View packets from captures and forensic searches c...
- ☑ Capture / Forensic Search: View stats from captures and forensic searches crea...
- ☑ Capture: Create new capture
- ☑ Capture: Delete captures created by other users

The “Users” button has been removed from this dialog. The “Validate” button now will only be enabled if there is at least 1 Active Directory or TACACS+ authentication server in use.



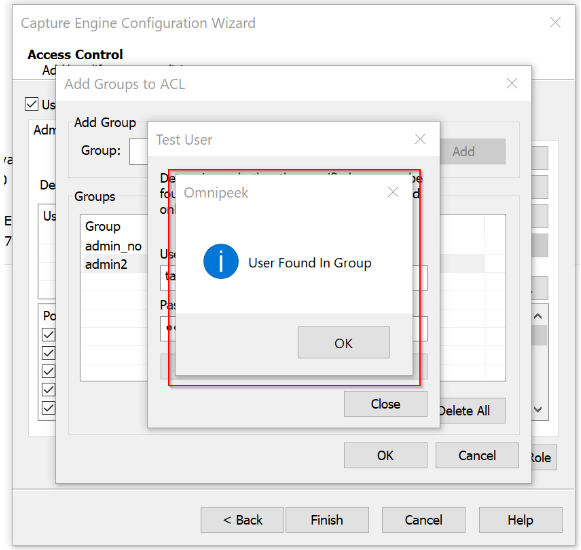
Group
admin_no
admin2

Upon clicking the "Validate" button when a single group is selected in the "Groups" table, a dialog will appear asking the user to type in a username and password, however the password is only necessary if the group in question is a TACACS+ group, as indicated by the dialog prompt.



Determines whether the specified user can be found in the group. The password is required only for TACACS+ authentication servers.

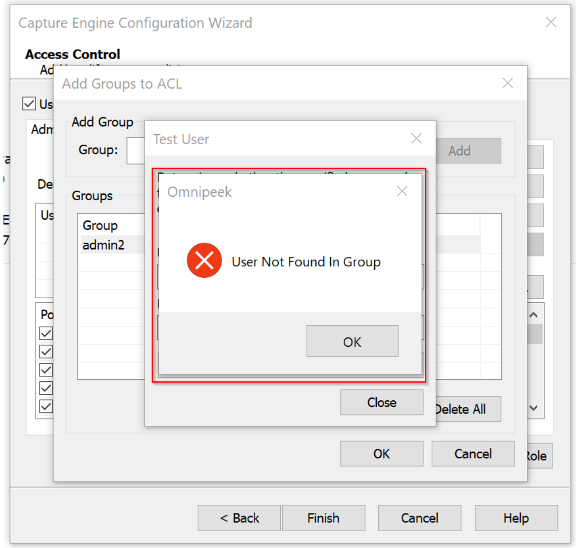
The user will see either a success or failure message after clicking the “Test User” button.



Omnipeek

User Found In Group

OK

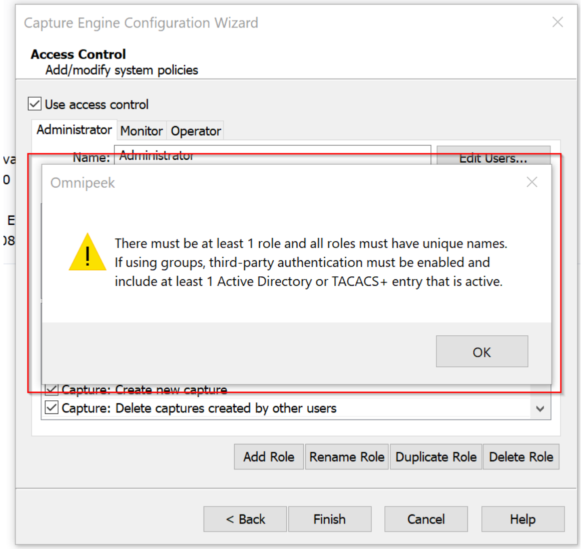


Omnipeek

User Not Found In Group

OK

If there is at least one group specified, the user will be unable to apply changes to the role-based ACL unless third-party authentication is enabled and at least 1 Active Directory or TACACS+ authentication server is provided and in use.



Capture Engine Configuration Wizard

Access Control
Add/modify system policies

☑ Use access control

Administrator | Monitor | Operator

Name: Administrator Edit Users...

Omnipeek

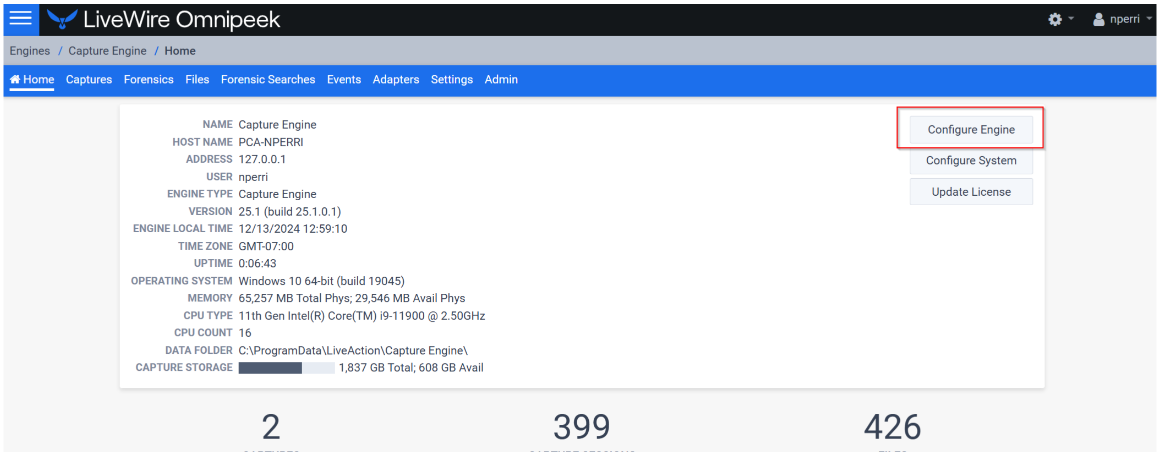
There must be at least 1 role and all roles must have unique names.
If using groups, third-party authentication must be enabled and include at least 1 Active Directory or TACACS+ entry that is active.

OK

☑ Capture: Create new capture
☑ Capture: Delete captures created by other users

LiveWire Omnipeek

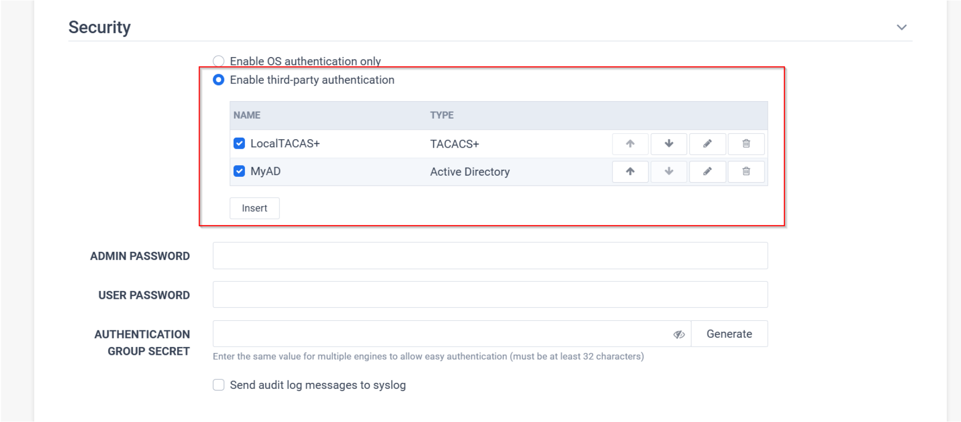
RBAC can be configured through Omnipeek Web by clicking the “Configure Engine” button in the Home view.



NAME	Capture Engine
HOST NAME	PCA-NPERRI
ADDRESS	127.0.0.1
USER	nperri
ENGINE TYPE	Capture Engine
VERSION	25.1 (build 25.1.0.1)
ENGINE LOCAL TIME	12/13/2024 12:59:10
TIME ZONE	GMT-07:00
UPTIME	0:06:43
OPERATING SYSTEM	Windows 10 64-bit (build 19045)
MEMORY	65,257 MB Total Phys; 29,546 MB Avail Phys
CPU TYPE	11th Gen Intel(R) Core(TM) i9-11900 @ 2.50GHz
CPU COUNT	16
DATA FOLDER	C:\ProgramData\LiveAction\Capture Engine\
CAPTURE STORAGE	1,837 GB Total; 608 GB Avail

Security Section

From there, you can navigate to the “Security” section and edit the third-party authentication:



Security

○ Enable OS authentication only
● Enable third-party authentication

NAME	TYPE
☑ LocalTACAS+	TACACS+
☑ MyAD	Active Directory

ADMIN PASSWORD

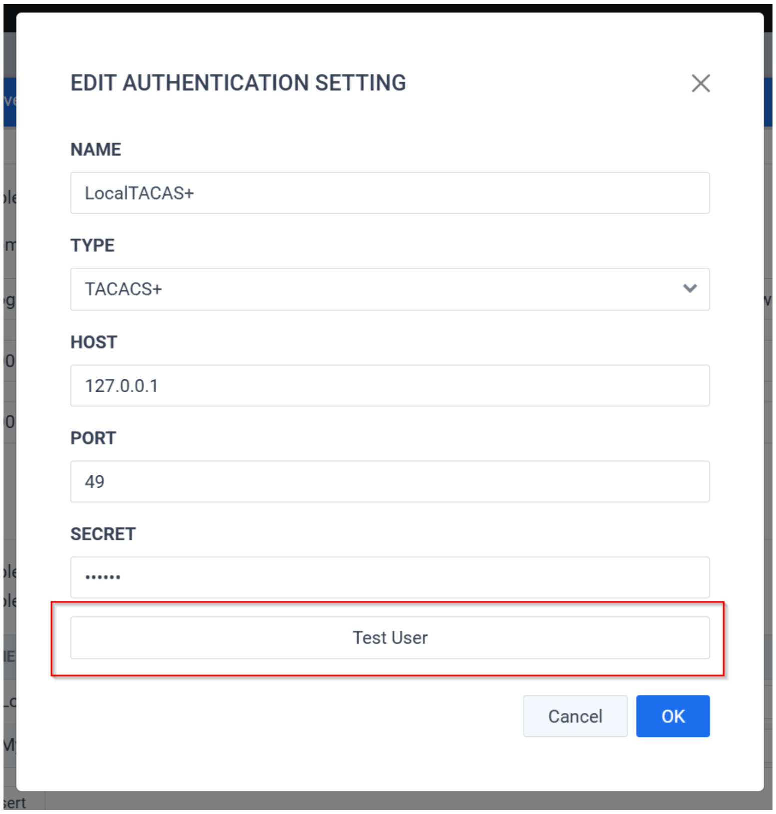
USER PASSWORD

AUTHENTICATION GROUP SECRET Generate
Enter the same value for multiple engines to allow easy authentication (must be at least 32 characters)

□ Send audit log messages to syslog

For Active Directory authentication servers, the edit dialog should work the same as before.

For TACACS+ authentication servers, the edit dialog will now include a “Test User” button. Upon clicking this button, a dialog will appear allowing the user to type in a username and password to test the user existence. No “Test Connection” button will be present as in Active Directory. Note: This “Test User” button will not be visible for capture engines below v25.1.



EDIT AUTHENTICATION SETTING

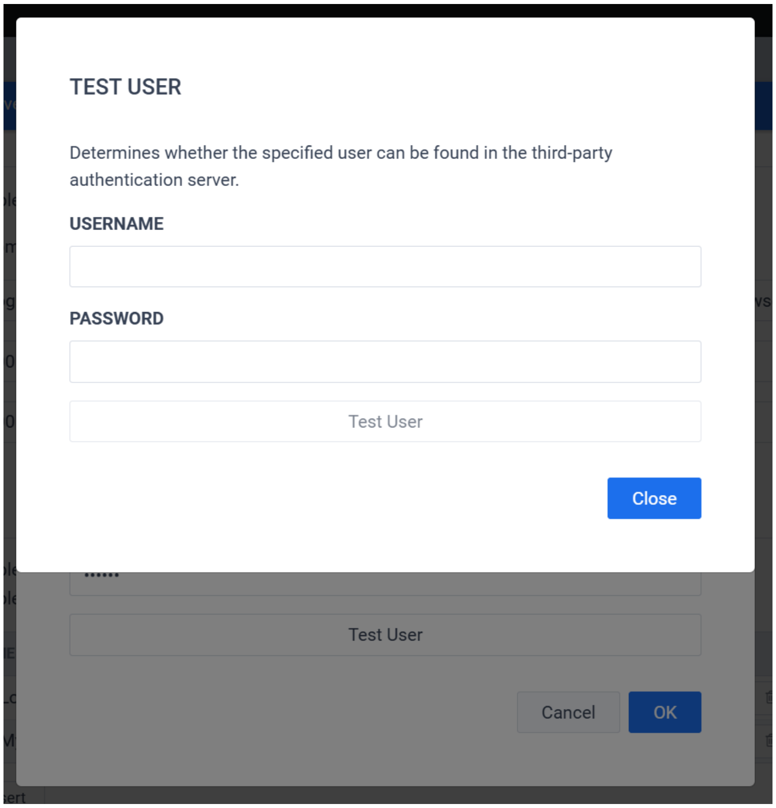
NAME: LocalTACAS+

TYPE: TACACS+

HOST: 127.0.0.1

PORT: 49

SECRET: ••••••



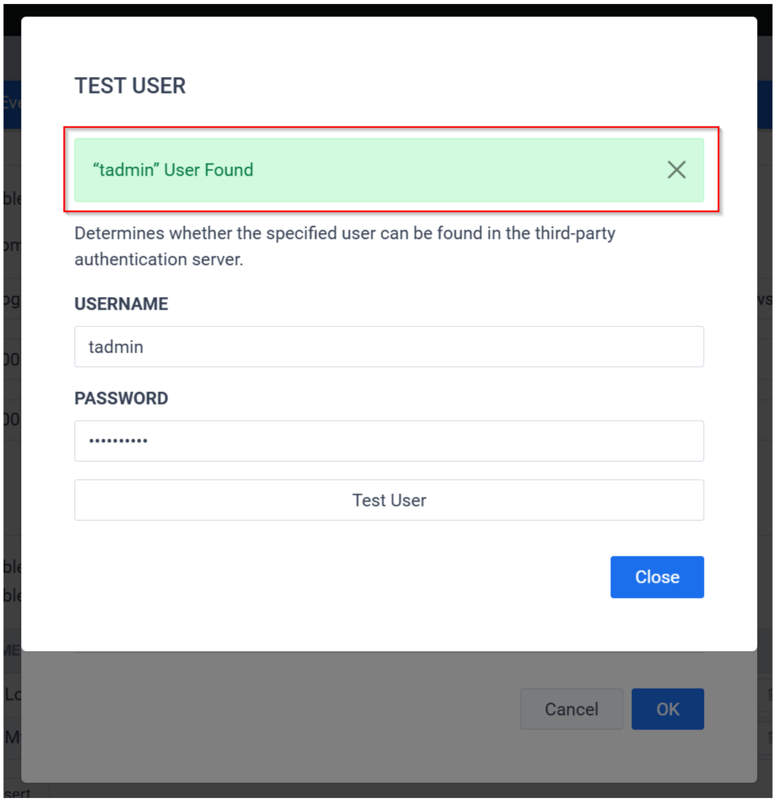
TEST USER

Determines whether the specified user can be found in the third-party authentication server.

USERNAME

PASSWORD

The user will see either a success or failure message after clicking the “Test User” button.


TEST USER

“tadmin” User Found

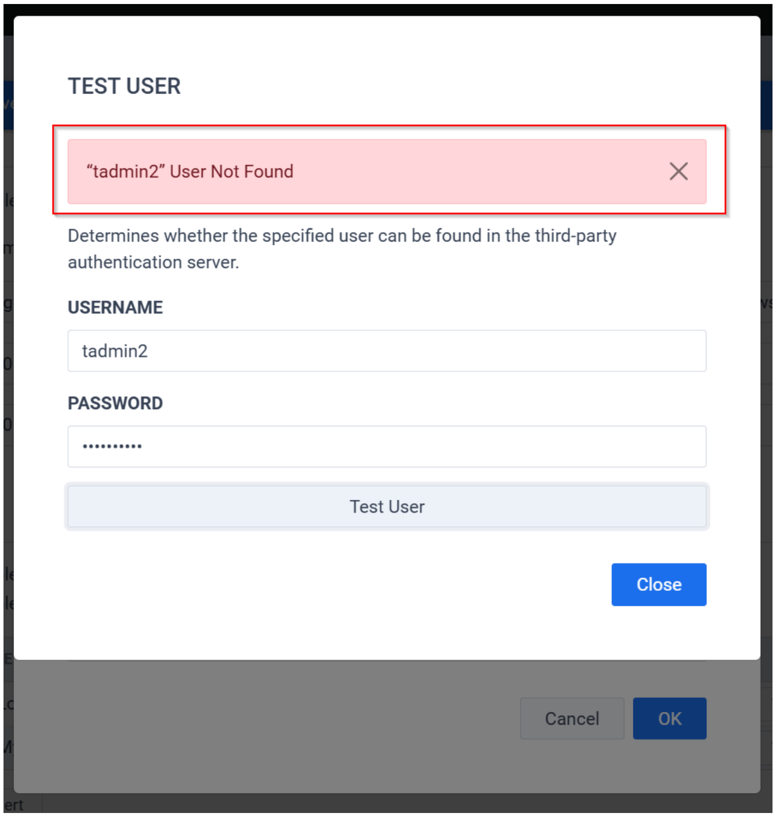
Determines whether the specified user can be found in the third-party authentication server.

USERNAME

tadmin

PASSWORD

••••••••••


TEST USER

“tadmin2” User Not Found

Determines whether the specified user can be found in the third-party authentication server.

USERNAME

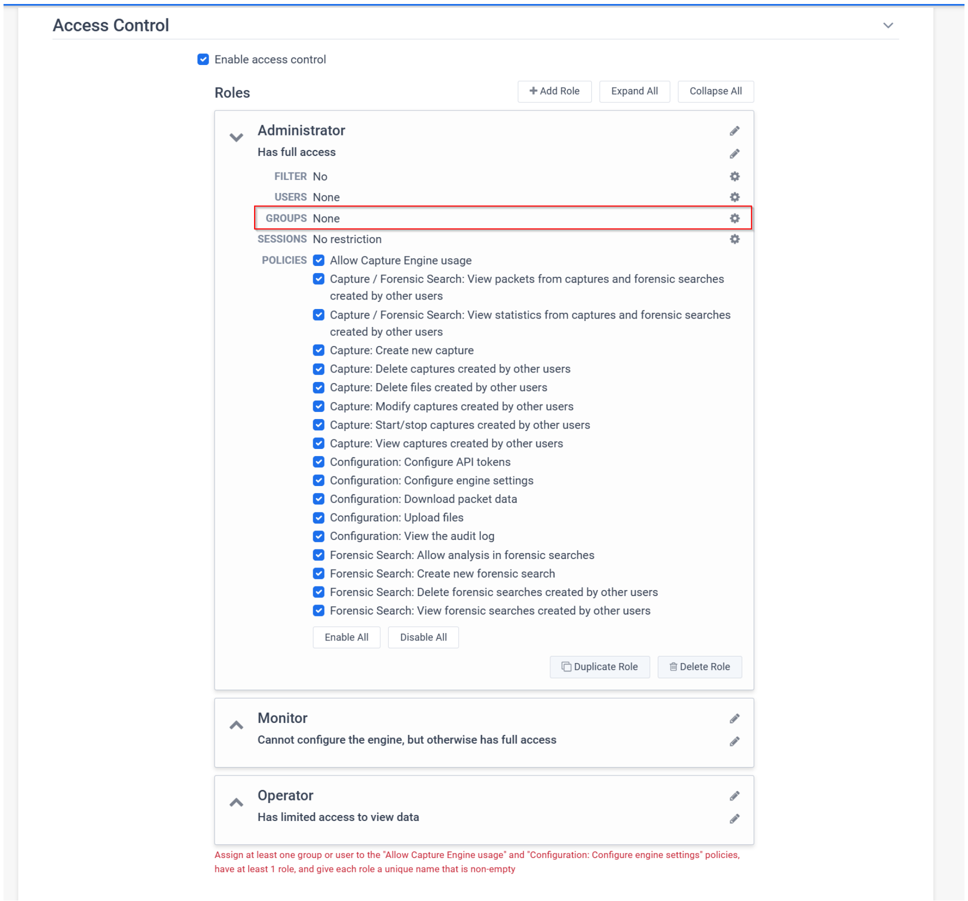
tadmin2

PASSWORD

••••••••••

Access Control Section

In the "Access Control" section, the only changes are in the dialog that appears from clicking the gear icon in the "Groups" row.



Access Control

☑ Enable access control

Roles

Administrator
Has full access

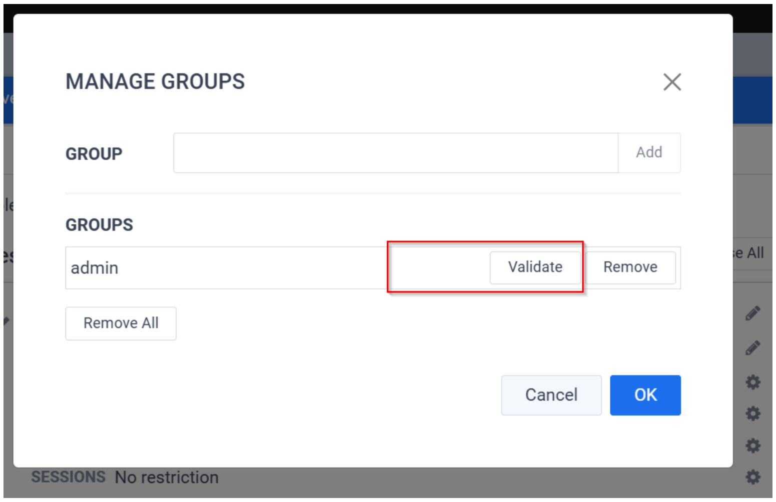
FILTER No
USERS None
GROUPS None
SESSIONS No restriction
POLICIES
☑ Allow Capture Engine usage
☑ Capture / Forensic Search: View packets from captures and forensic searches created by other users
☑ Capture / Forensic Search: View statistics from captures and forensic searches created by other users
☑ Capture: Create new capture
☑ Capture: Delete captures created by other users
☑ Capture: Delete files created by other users
☑ Capture: Modify captures created by other users
☑ Capture: Start/stop captures created by other users
☑ Capture: View captures created by other users
☑ Configuration: Configure API tokens
☑ Configuration: Configure engine settings
☑ Configuration: Download packet data
☑ Configuration: Upload files
☑ Configuration: View the audit log
☑ Forensic Search: Allow analysis in forensic searches
☑ Forensic Search: Create new forensic search
☑ Forensic Search: Delete forensic searches created by other users
☑ Forensic Search: View forensic searches created by other users

Monitor
Cannot configure the engine, but otherwise has full access

Operator
Has limited access to view data

Assign at least one group or user to the "Allow Capture Engine usage" and "Configuration: Configure engine settings" policies, have at least 1 role, and give each role a unique name that is non-empty

The "Users" button has been removed from the group rows in the "Groups" table. The "Validate" button now will only be enabled if there is at least 1 Active Directory or TACACS+ authentication server in use.

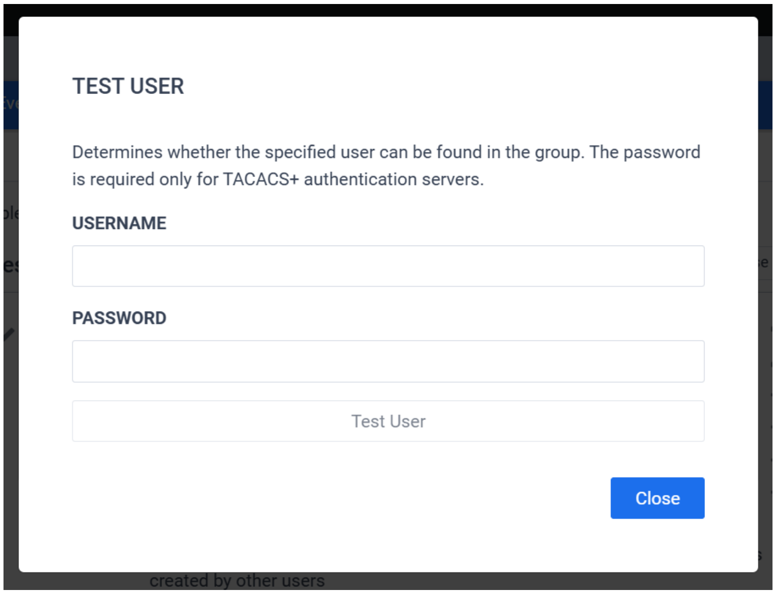


MANAGE GROUPS

GROUP

GROUPS
admin

Upon clicking the "Validate" button for a group in the "Groups" table, a dialog will appear asking the user to type in a username and password, however the password is only necessary if the group in question is a TACACS+ group, as indicated by the dialog prompt. If the group is an Active Directory group, the user can ignore the password field as it is not mandatory.



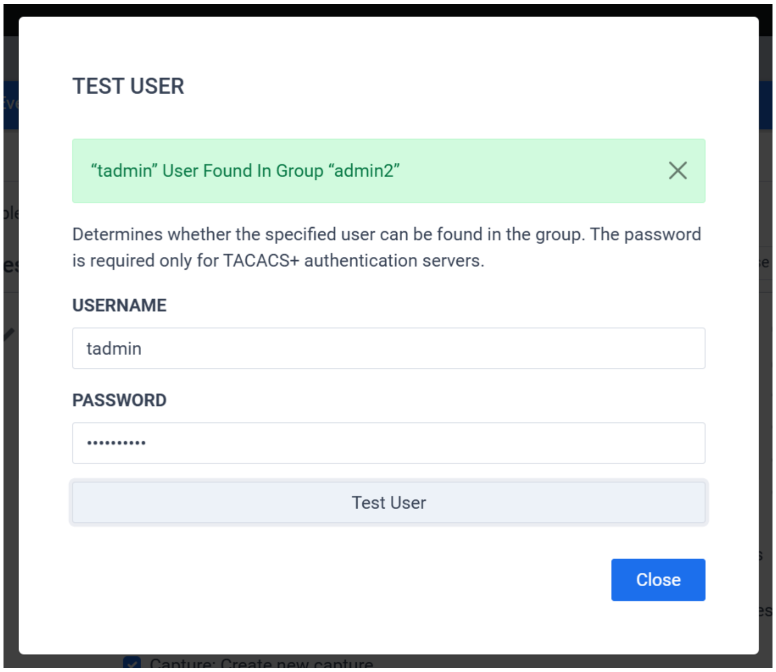
TEST USER

Determines whether the specified user can be found in the group. The password is required only for TACACS+ authentication servers.

USERNAME

PASSWORD

The user will see either a success or failure message after clicking the "Test User" button.



TEST USER

"tadmin" User Found In Group "admin2"

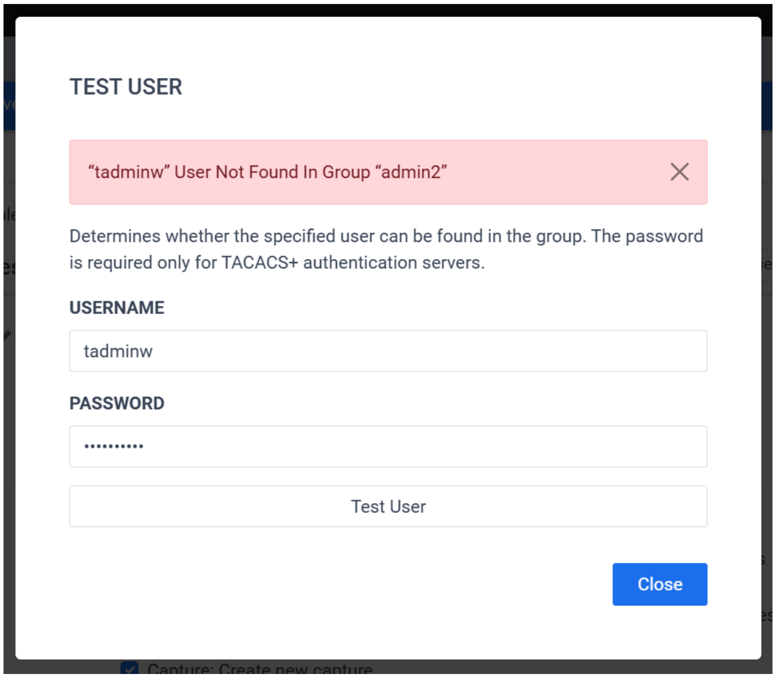
Determines whether the specified user can be found in the group. The password is required only for TACACS+ authentication servers.

USERNAME

tadmin

PASSWORD

••••••••••



TEST USER

"tadminw" User Not Found In Group "admin2"

Determines whether the specified user can be found in the group. The password is required only for TACACS+ authentication servers.

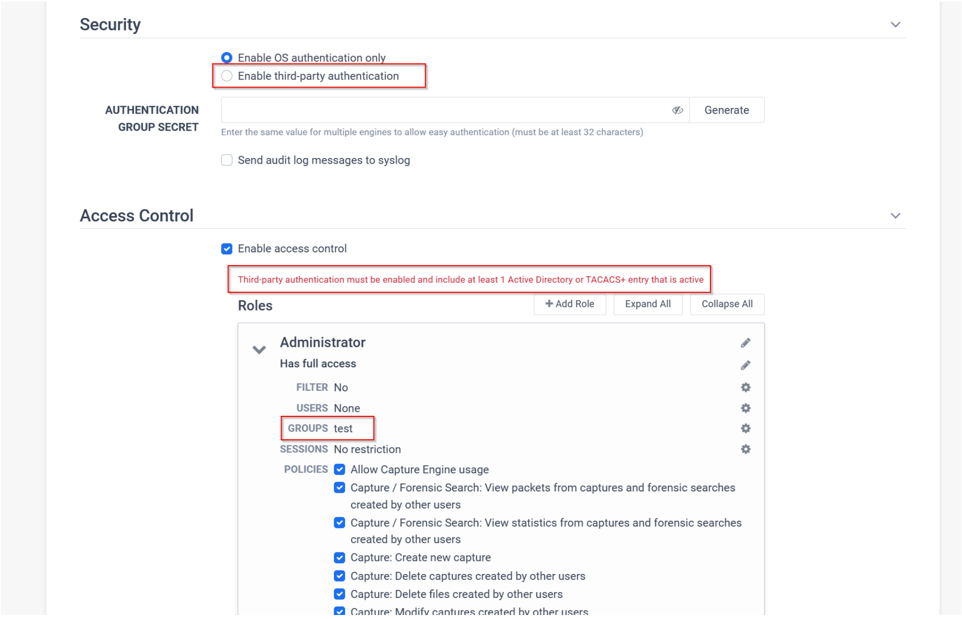
USERNAME

tadminw

PASSWORD

••••••••••

If there is at least 1 group specified, the user will be unable to apply changes to the role-based ACL unless third-party authentication is enabled and at least 1 Active Directory or TACACS+ authentication server is provided and in use.



Security

● Enable OS authentication only
○ Enable third-party authentication

AUTHENTICATION GROUP SECRET: Generate
Enter the same value for multiple engines to allow easy authentication (must be at least 32 characters)

□ Send audit log messages to syslog

Access Control

☑ Enable access control

Third-party authentication must be enabled and include at least 1 Active Directory or TACACS+ entry that is active

Roles

Administrator
Has full access

FILTER No
USERS None
GROUPS test
SESSIONS No restriction
POLICIES
☑ Allow Capture Engine usage
☑ Capture / Forensic Search: View packets from captures and forensic searches created by other users
☑ Capture / Forensic Search: View statistics from captures and forensic searches created by other users
☑ Capture: Create new capture
☑ Capture: Delete captures created by other users
☑ Capture: Delete files created by other users
☑ Capture: Modify captures created by other users

Improved Hardware Deduplication

The Napatech hardware deduplication process has been improved and now defaults to using the beginning of the Inner Layer 3 Header to the end of the packet (minus the frame check sequence) to determine if packets are the same. The user may change the Napatech hardware deduplication mode by changing the "hwdeduplicationmode" property in *omni.conf*. The value must be one of the following:

0 = The entire packet contents (minus the frame check sequence) is used for deduplication - this is the old way

1 = The beginning of the Layer 3 Header to the end of the packet (minus the frame check sequence) is used for deduplication

2 = The beginning of the Inner Layer 3 Header to the end of the packet (minus the frame check sequence) is used for deduplication

Note If a packet has only a single layer 3 header, it will be considered the layer 3 header and the inner layer 3 header. So, in this case methods 1 & 2 will result in the same outcome. Methods 1 & 2 may differ if a packet has multiple Layer 3 headers. Method 0 & 1 will include the MPLS/VLAN/VXLAN tags in determining duplicate packets.

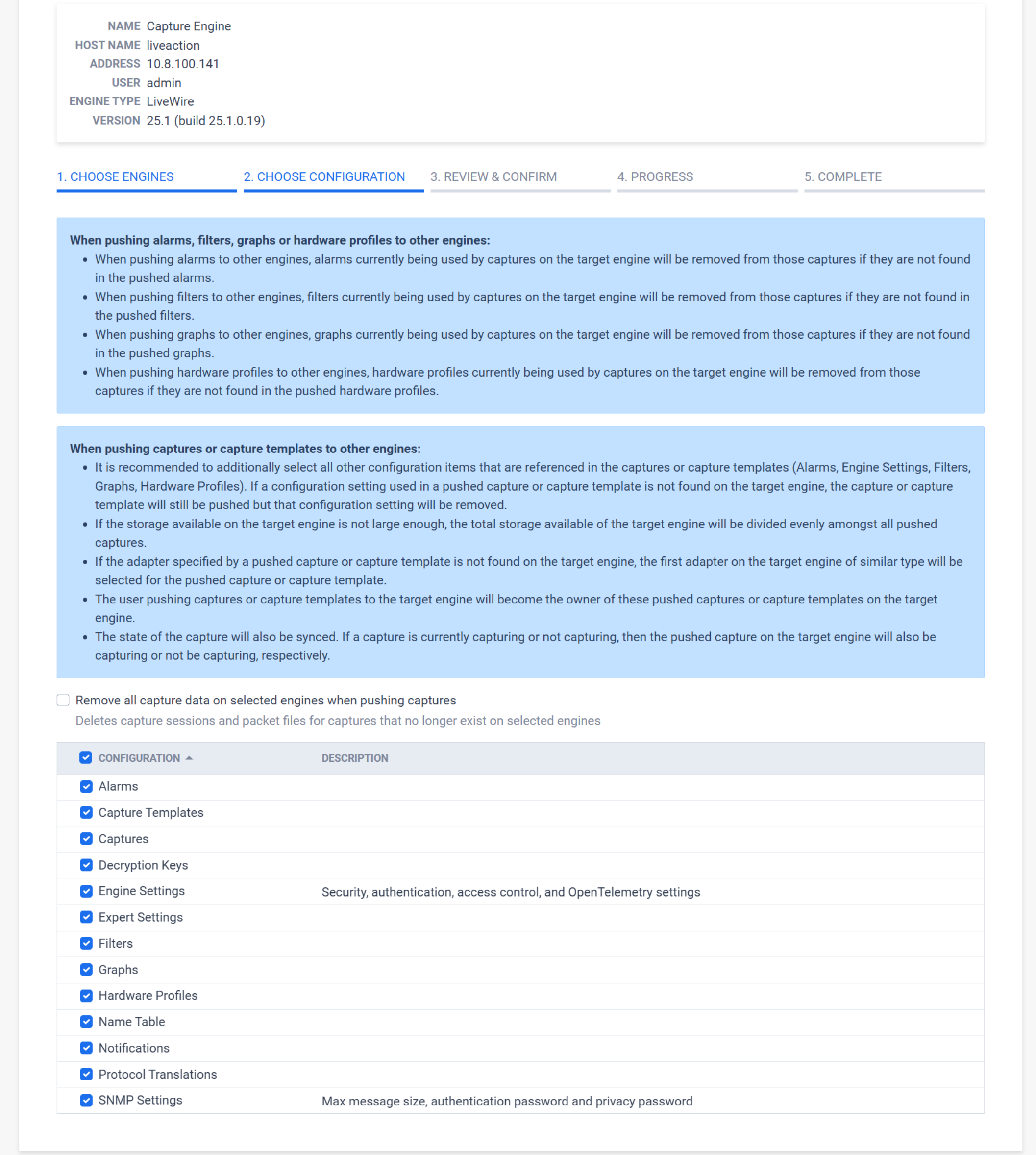
Added More Items to Engine Configuration Sync

The following items have been added to Engine Configuration Sync:

Item	LiveWire Omnipeek	Grid
Capture Templates	Yes	Yes
Decryption Keys	Yes	Yes
Expert Settings	Yes	Yes
Name Table	Yes	No
Notifications	Yes	Yes
Protocol Translations	Yes	Yes
SNMP Settings	Yes	Yes

LiveWire Omnipeek UI

The LiveWire Omnipeek UI has not changed, but these new items are now available in the list of items to sync:



NAME	Capture Engine
HOST NAME	liveaction
ADDRESS	10.8.100.141
USER	admin
ENGINE TYPE	LiveWire
VERSION	25.1 (build 25.1.0.19)

When pushing alarms, filters, graphs or hardware profiles to other engines:

- When pushing alarms to other engines, alarms currently being used by captures on the target engine will be removed from those captures if they are not found in the pushed alarms.
- When pushing filters to other engines, filters currently being used by captures on the target engine will be removed from those captures if they are not found in the pushed filters.
- When pushing graphs to other engines, graphs currently being used by captures on the target engine will be removed from those captures if they are not found in the pushed graphs.
- When pushing hardware profiles to other engines, hardware profiles currently being used by captures on the target engine will be removed from those captures if they are not found in the pushed hardware profiles.

When pushing captures or capture templates to other engines:

- It is recommended to additionally select all other configuration items that are referenced in the captures or capture templates (Alarms, Engine Settings, Filters, Graphs, Hardware Profiles). If a configuration setting used in a pushed capture or capture template is not found on the target engine, the capture or capture template will still be pushed but that configuration setting will be removed.
- If the storage available on the target engine is not large enough, the total storage available of the target engine will be divided evenly amongst all pushed captures.
- If the adapter specified by a pushed capture or capture template is not found on the target engine, the first adapter on the target engine of similar type will be selected for the pushed capture or capture template.
- The user pushing captures or capture templates to the target engine will become the owner of these pushed captures or capture templates on the target engine.
- The state of the capture will also be synced. If a capture is currently capturing or not capturing, then the pushed capture on the target engine will also be capturing or not be capturing, respectively.

□ Remove all capture data on selected engines when pushing captures

Deletes capture sessions and packet files for captures that no longer exist on selected engines

☑ CONFIGURATION ▲	DESCRIPTION
☑ Alarms	
☑ Capture Templates	
☑ Captures	
☑ Decryption Keys	
☑ Engine Settings	Security, authentication, access control, and OpenTelemetry settings
☑ Expert Settings	
☑ Filters	
☑ Graphs	
☑ Hardware Profiles	
☑ Name Table	
☑ Notifications	
☑ Protocol Translations	
☑ SNMP Settings	Max message size, authentication password and privacy password

Added Support NPKT Format Including Compression

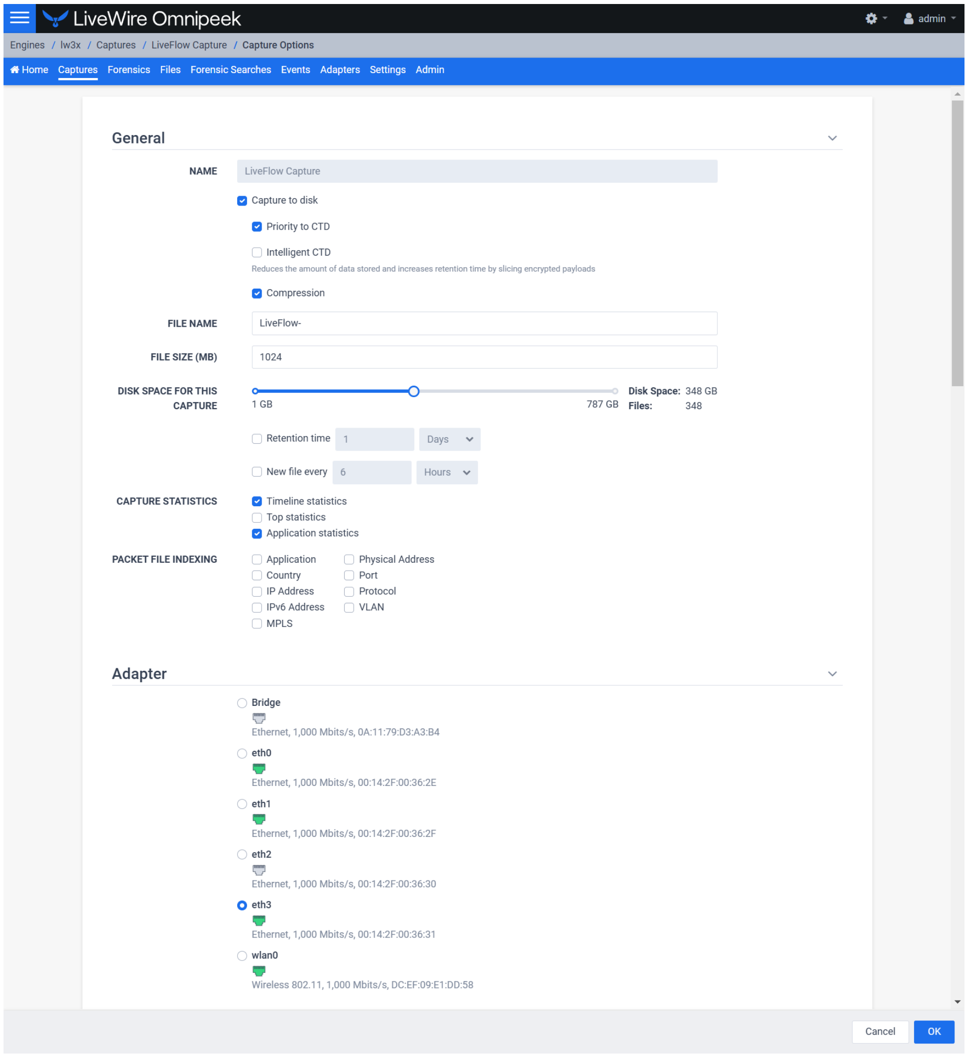
The option to enable compression in capture options is now present and is the default when non-Napatech adapters are selected.

Enabling compression switches the file format to *.npkt* since it is the only format that supports it. It's also possible to save in *.npkt* format without compression enabled by adding the *.npkt* extension to the packet file name. Changing to other formats that don't support compression (*.pkt*, *.pcap*, or *.pcapng*) is disallowed when the check box is selected.

Compression is fully supported for LiveFlow captures which save to multiple files simultaneously.

Workflow

User interface changes are minimal, adding only a Compression check box when a non-Napatech adapter is selected.


LiveWire Omnipeek
admin
Engines / lw3x / Captures / LiveFlow Capture / Capture Options
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin

General

NAME: LiveFlow Capture

☑ Capture to disk

☑ Priority to CTD

☐ Intelligent CTD
Reduces the amount of data stored and increases retention time by slicing encrypted payloads

☑ Compression

FILE NAME: LiveFlow-

FILE SIZE (MB): 1024

DISK SPACE FOR THIS CAPTURE: 1 GB – 787 GB
Disk Space: 348 GB
Files: 348

☐ Retention time 1 Days

☐ New file every 6 Hours

CAPTURE STATISTICS
☑ Timeline statistics
☐ Top statistics
☑ Application statistics

PACKET FILE INDEXING
☐ Application ☐ Physical Address
☐ Country ☐ Port
☐ IP Address ☐ Protocol
☐ IPv6 Address ☐ VLAN
☐ MPLS

Adapter

○ Bridge
Ethernet, 1,000 Mbits/s, 0A:11:79:D3:A3:B4

○ eth0
Ethernet, 1,000 Mbits/s, 00:14:2F:00:36:2E

○ eth1
Ethernet, 1,000 Mbits/s, 00:14:2F:00:36:2F

○ eth2
Ethernet, 1,000 Mbits/s, 00:14:2F:00:36:30

● eth3
Ethernet, 1,000 Mbits/s, 00:14:2F:00:36:31

○ wlan0
Wireless 802.11, 1,000 Mbits/s, DC:EF:09:E1:DD:58

Added Support for the TCPDump Adapter to LiveWire Omnipeek

Support for the TCPDump Adapter has been added the LiveWire Omnipeek UI. The TCPDump Adapter is a plugin which allows the user to capture packets on a remote system, sending the packet data back to the LiveWire via an SSH connection.

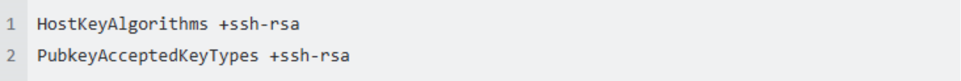
Note The target box must be running Linux.

Required SSH Configuration

Usage of this plugin will likely require changes to the LiveWire and the target box. Both endpoints must be able to agree on a ciphersuite which is also supported by Ubuntu's libssh1.10.

LiveWire config:

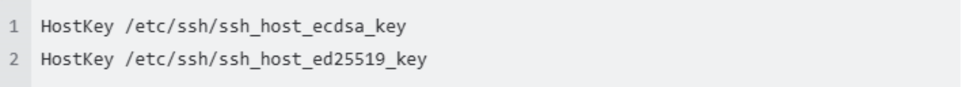
- Add the following lines to */root/.ssh/config*



```
HostKeyAlgorithms +ssh-rsa
PubkeyAcceptedKeyTypes +ssh-rsa
```

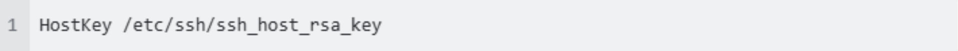
Target config:

- Make the following changes to */etc/ssh/sshd_config*
  - Delete the following lines if they exist:



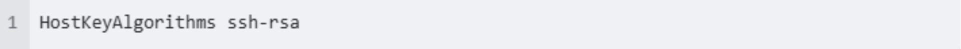
```
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
```

- Add the following line if it does not exist:



```
HostKey /etc/ssh/ssh_host_rsa_key
```

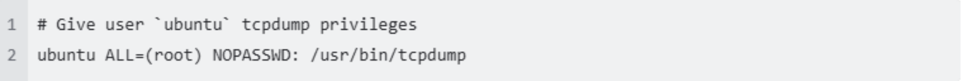
- Add `ssh-rsa` to the list of HostKeyAlgorithms.



```
HostKeyAlgorithms ssh-rsa
```

Be sure to restart sshd on both endpoints and omnid on the LiveWire. Currently, only RSA and DSS keys are supported.

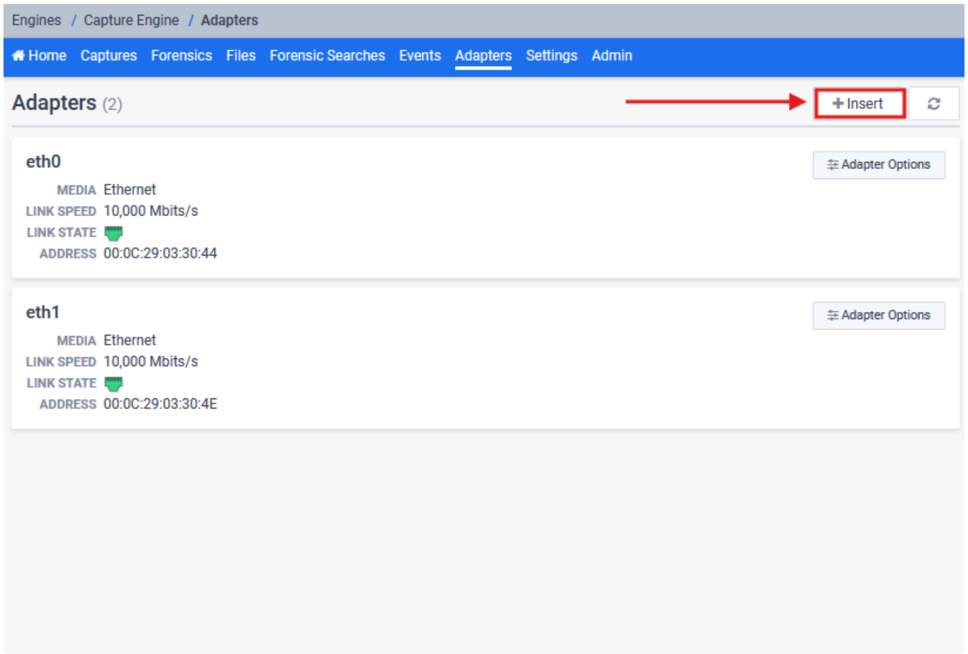
The user also needs to modify the */etc/sudoers* file on the target host to allow tcpdump to run with elevated privilege.



```
# Give user `ubuntu` tcpdump privileges
ubuntu ALL=(root) NOPASSWD: /usr/bin/tcpdump
```

Workflow

Create a new adapter:



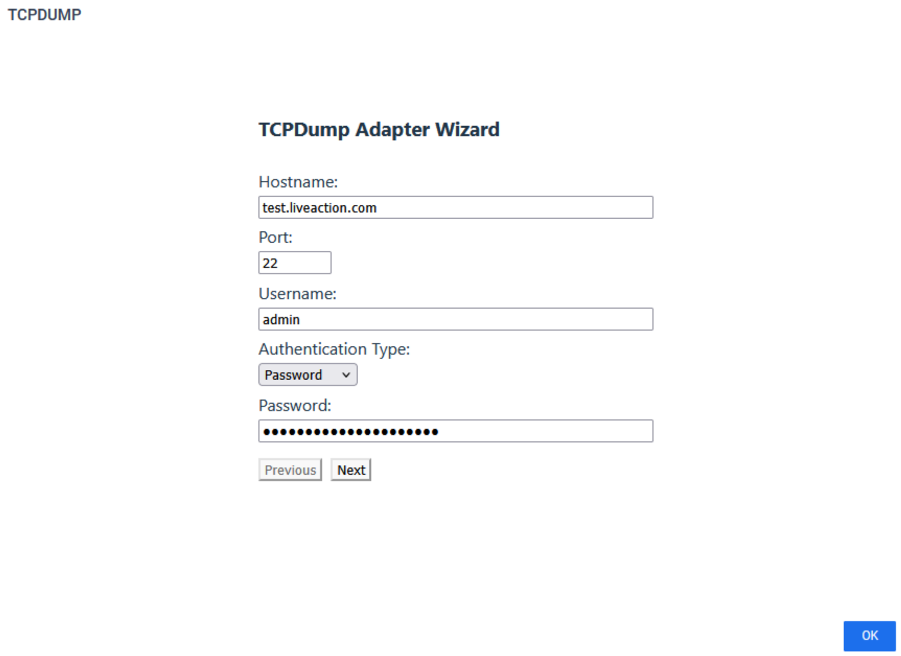
Engines / Capture Engine / Adapters
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
+ Insert
Adapter Options

Adapters (2)

eth0
MEDIA Ethernet
LINK SPEED 10,000 Mbits/s
LINK STATE 🟩
ADDRESS 00:0C:29:03:30:44

eth1
MEDIA Ethernet
LINK SPEED 10,000 Mbits/s
LINK STATE 🟩
ADDRESS 00:0C:29:03:30:4E

Enter address and credentials, then click Next:



TCPDump Adapter Wizard

Hostname: test.liveaction.com

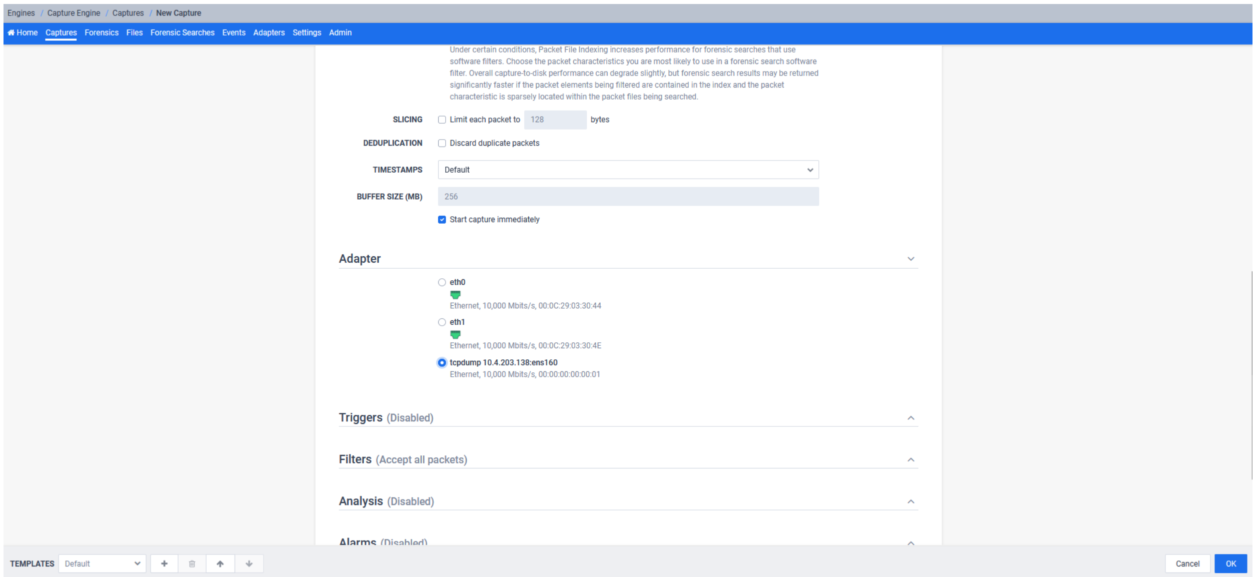
Port: 22

Username: admin

Authentication Type: Password

Password: ••••••••••••••••••••••

Create a capture with the new adapter:



Under certain conditions, Packet File Indexing increases performance for forensic searches that use software filters. Choose the packet characteristics you are most likely to use in a forensic search software filter. Overall capture-to-disk performance can degrade slightly, but forensic search results may be returned significantly faster if the packet elements being filtered are contained in the index and the packet characteristic is sparsely located within the packet files being searched.

SLICING	□ Limit each packet to 128 bytes
DEDUPLICATION	□ Discard duplicate packets
TIMESTAMPS	Default
BUFFER SIZE (MB)	256
	☑ Start capture immediately

Adapter

○ eth0
Ethernet, 10,000 Mbits/s, 00:0C:29:03:30:44

○ eth1
Ethernet, 10,000 Mbits/s, 00:0C:29:03:30:4E

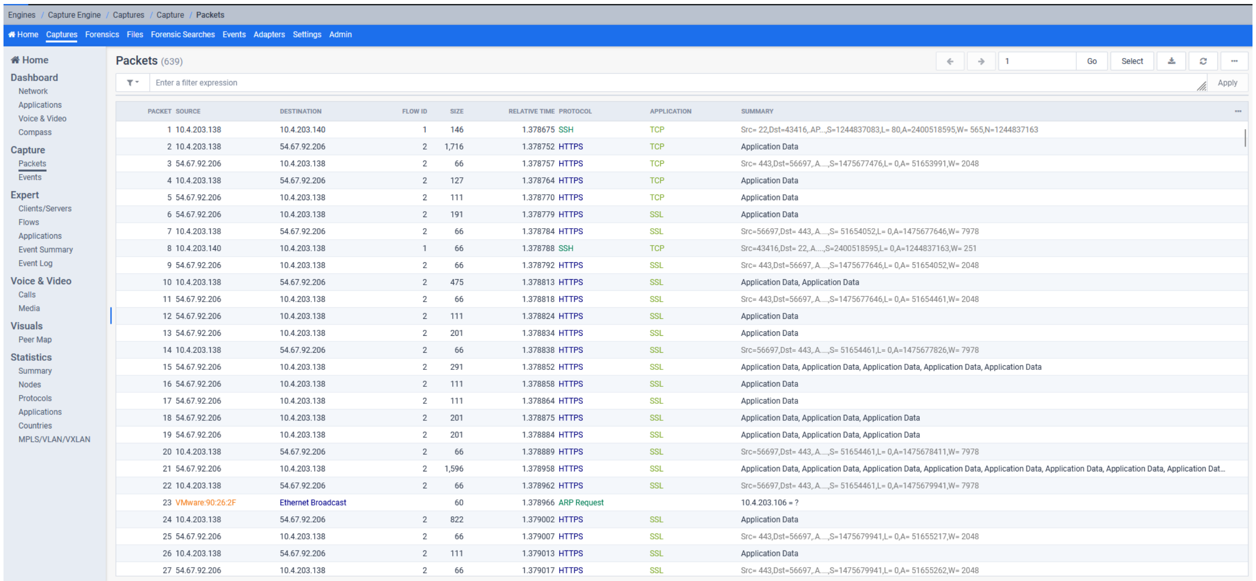
● tcpdump 10.4.203.138:ens160
Ethernet, 10,000 Mbits/s, 00:00:00:00:00:01

Triggers (Disabled)

Filters (Accept all packets)

Analysis (Disabled)

Alarms (Disabled)



Packets (639)

PACKET	SOURCE	DESTINATION	FLOW ID	SIZE	RELATIVE TIME	PROTOCOL	APPLICATION	SUMMARY
1	10.4.203.138	10.4.203.140	1	146	1.378675	SSH	TCP	Src= 22,Dst=43416,.AP...,S=1244837083,L= 80,A=2400518595,W= 565,N=1244837163
2	10.4.203.138	54.67.92.206	2	1,716	1.378752	HTTPS	TCP	Application Data
3	54.67.92.206	10.4.203.138	2	66	1.378757	HTTPS	TCP	Src= 443,Dst=56697,.A....,S=1475677476,L= 0,A= 51653991,W= 2048
4	10.4.203.138	54.67.92.206	2	127	1.378764	HTTPS	TCP	Application Data
5	54.67.92.206	10.4.203.138	2	111	1.378770	HTTPS	TCP	Application Data
6	54.67.92.206	10.4.203.138	2	191	1.378779	HTTPS	SSL	Application Data
7	10.4.203.138	54.67.92.206	2	66	1.378784	HTTPS	SSL	Src=56697,Dst= 443,.A....,S= 51654052,L= 0,A=1475677646,W= 7978
8	10.4.203.140	10.4.203.138	1	66	1.378788	SSH	TCP	Src=43416,Dst= 22,.A....,S=2400518595,L= 0,A=1244837163,W= 251
9	54.67.92.206	10.4.203.138	2	66	1.378792	HTTPS	SSL	Src= 443,Dst=56697,.A....,S=1475677646,L= 0,A= 51654052,W= 2048
10	10.4.203.138	54.67.92.206	2	475	1.378813	HTTPS	SSL	Application Data, Application Data
11	54.67.92.206	10.4.203.138	2	66	1.378818	HTTPS	SSL	Src= 443,Dst=56697,.A....,S=1475677646,L= 0,A= 51654461,W= 2048
12	54.67.92.206	10.4.203.138	2	111	1.378824	HTTPS	SSL	Application Data
13	54.67.92.206	10.4.203.138	2	201	1.378834	HTTPS	SSL	Application Data
14	10.4.203.138	54.67.92.206	2	66	1.378838	HTTPS	SSL	Src=56697,Dst= 443,.A....,S= 51654461,L= 0,A=1475677826,W= 7978
15	54.67.92.206	10.4.203.138	2	291	1.378852	HTTPS	SSL	Application Data, Application Data, Application Data, Application Data, Application Data
16	54.67.92.206	10.4.203.138	2	111	1.378858	HTTPS	SSL	Application Data
17	54.67.92.206	10.4.203.138	2	111	1.378864	HTTPS	SSL	Application Data
18	54.67.92.206	10.4.203.138	2	201	1.378875	HTTPS	SSL	Application Data, Application Data, Application Data
19	54.67.92.206	10.4.203.138	2	201	1.378884	HTTPS	SSL	Application Data, Application Data, Application Data
20	10.4.203.138	54.67.92.206	2	66	1.378889	HTTPS	SSL	Src=56697,Dst= 443,.A....,S= 51654461,L= 0,A=1475678411,W= 7978
21	54.67.92.206	10.4.203.138	2	1,596	1.378958	HTTPS	SSL	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Dat...
22	10.4.203.138	54.67.92.206	2	66	1.378962	HTTPS	SSL	Src=56697,Dst= 443,.A....,S= 51654461,L= 0,A=1475679941,W= 7978
23	VMware:90:26:2F	Ethernet Broadcast		60	1.378966	ARP Request		10.4.203.106 = ?
24	10.4.203.138	54.67.92.206	2	822	1.379002	HTTPS	SSL	Application Data
25	54.67.92.206	10.4.203.138	2	66	1.379007	HTTPS	SSL	Src= 443,Dst=56697,.A....,S=1475679941,L= 0,A= 51655217,W= 2048
26	10.4.203.138	54.67.92.206	2	111	1.379013	HTTPS	SSL	Application Data
27	54.67.92.206	10.4.203.138	2	66	1.379017	HTTPS	SSL	Src= 443,Dst=56697,.A....,S=1475679941,L= 0,A= 51655262,W= 2048

Added New TCP Handshake Expert and LiveFlow AVC field

A new Expert Event has been added to track the full length of a TCP Handshake from the first SYN sent from the client to the ACK that closes off the three-way handshake. This Expert Events provides a value that better represents the network latency from a user's perspective.

LiveWire::

	Expert Event	Notes
1	TCP Slow Connection Setup	**Description**: The TCP handshake appears to be slow based on the configured threshold. This expert measures from the first SYN packet that the client sends, rather than the last SYN packet. This gives a more realistic value from the perspective of the client attempting a connection. **Cause**: There is network latency or the endpoints are slow to process the handshake. **Remedy**: Check round-trip packet delay (latency). Check the CPU utilization of the receiver. Check the responsiveness of the receiver by capturing at the receiving end of the data.

A new expert called *TCP Slow Connection Setup* has been added to LiveWire, as well as a new engine expert column called *TCP Connection Setup (sec).*

LiveFlow:

On the LiveFlow side: There is a new AVC field called *artConnectionSetupTimeSum.*

LiveFlow Configuration

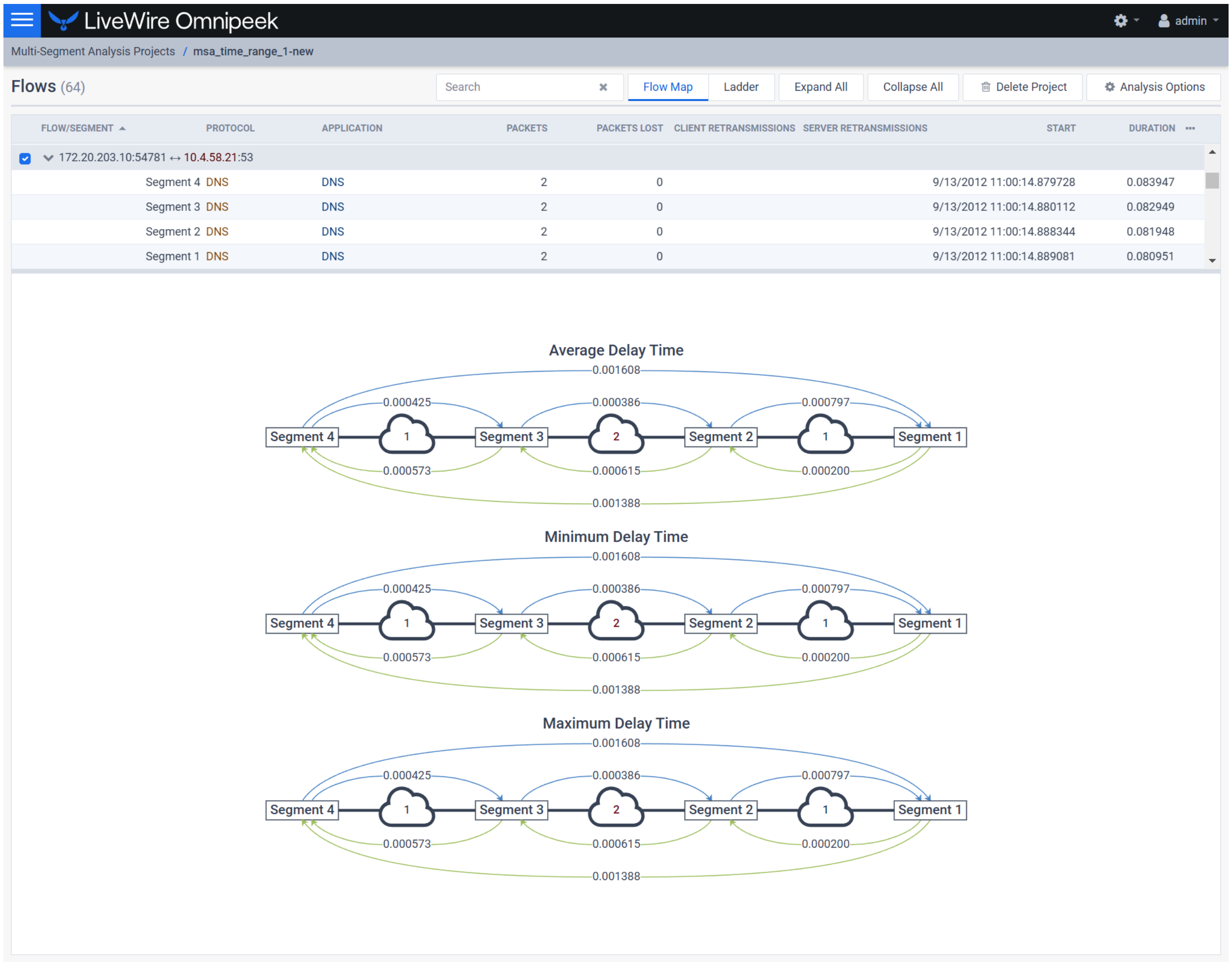
LiveFlow has two flow timeout values set in liveflow.json that affect this field. By default, the `tcp_handshake_timeout` is 2 seconds, and the `tcp_wait_timeout` is 3 seconds - these values are set for optimization purposes. The customer may configure the values to a maximum of 30 seconds to suit their needs, otherwise the long tcp handshake will be split into multiple flows.

Added Support for UDP in Multi-Segment Analysis

Multi-segment analysis currently works with TCP flows only. Support for UDP has been added so customers can also view the inter-segment delays for UDP flows.

Workflow

UDP support in multi-segment analysis is enabled by default with no additional settings in both the LiveWire Omnipeek UI and Omnipeek Windows UI.

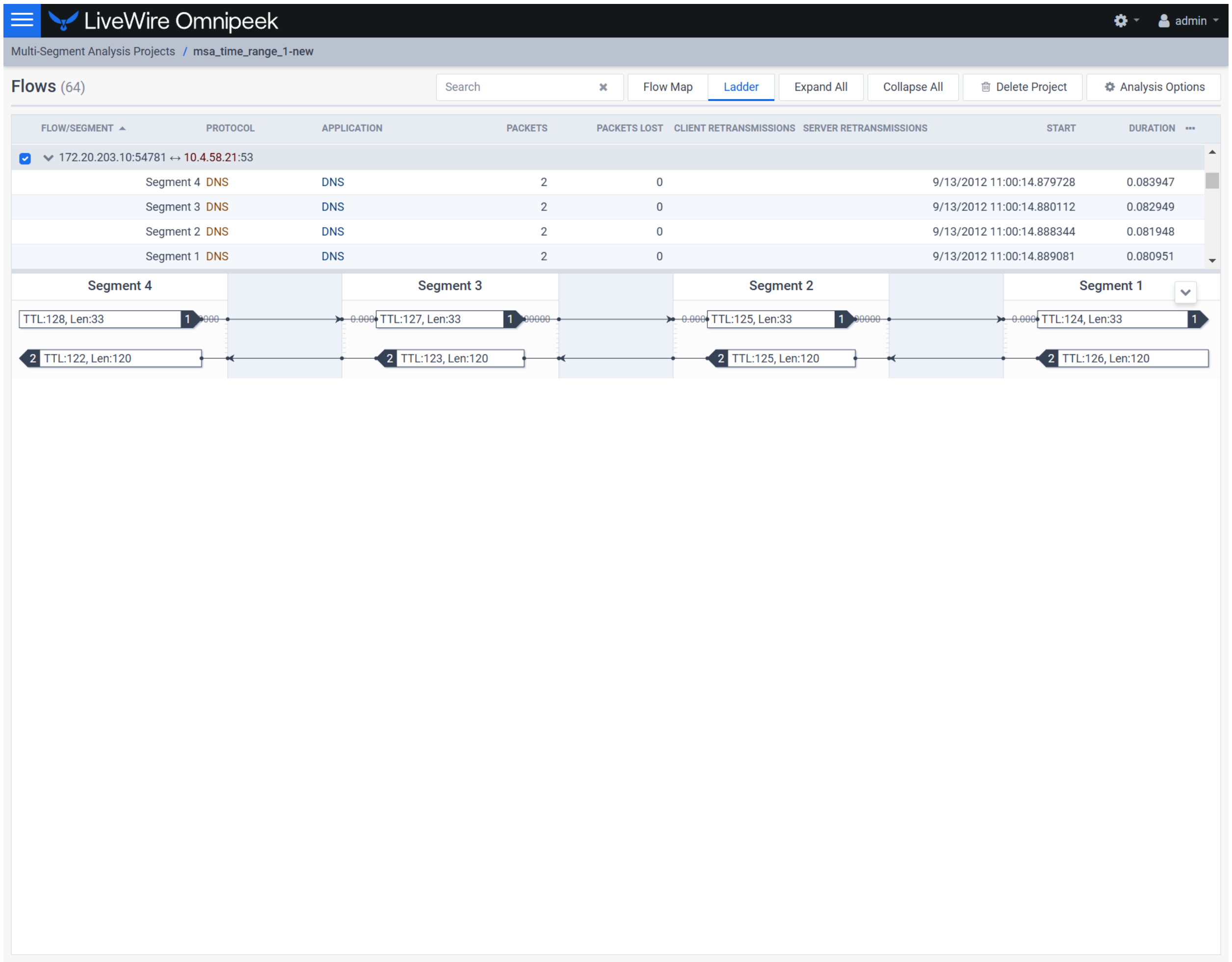


Multi-Segment Analysis Projects / msa_time_range_1-new

Flows (64)

FLOW/SEGMENT	PROTOCOL	APPLICATION	PACKETS	PACKETS LOST	CLIENT RETRANSMISSIONS	SERVER RETRANSMISSIONS	START	DURATION
☑ 172.20.203.10:54781 ↔ 10.4.58.21:53								
Segment 4	DNS	DNS	2	0			9/13/2012 11:00:14.879728	0.083947
Segment 3	DNS	DNS	2	0			9/13/2012 11:00:14.880112	0.082949
Segment 2	DNS	DNS	2	0			9/13/2012 11:00:14.888344	0.081948
Segment 1	DNS	DNS	2	0			9/13/2012 11:00:14.889081	0.080951

MSA Flow Map with a DNS Flow



FLOW/SEGMENT	PROTOCOL	APPLICATION	PACKETS	PACKETS LOST	CLIENT RETRANSMISSIONS	SERVER RETRANSMISSIONS	START	DURATION
☑ 172.20.203.10:54781 ↔ 10.4.58.21:53								
Segment 4	DNS	DNS	2	0			9/13/2012 11:00:14.879728	0.083947
Segment 3	DNS	DNS	2	0			9/13/2012 11:00:14.880112	0.082949
Segment 2	DNS	DNS	2	0			9/13/2012 11:00:14.888344	0.081948
Segment 1	DNS	DNS	2	0			9/13/2012 11:00:14.889081	0.080951

Improved Network Utilization Calculations

A standard interpacket gap value has been added to better represent on-the-wire utilization.

Workflow

Version 25.1 now calculates network utilization using 20 bytes per packet of “overhead” that includes 8 bytes of preamble/SFD plus 12 bytes of interframe gap in both the LiveWire web UI (REST API) and Omnipeek Windows.

The per-packet overhead value can be configured with a *.conf* file setting (or Windows Registry for Omnipeek) if necessary.

Auto-renew Added to Omnipeek Subscription Licenses

Automatic auto-renewal is now attempted at startup if the license is expired or will expire in the next 30 days. If auto-renew succeeds, the application continues without any disruption for the user. If auto-renew fails, the expiration notice is displayed with the option of performing the traditional renewal workflow.

Added Additional VoIP Support

RTP identification has been modified to include RTP/RTCP over STUN/TURN (a type of NAT tunneling) and RTP Payload Types in the reserved range 35-63 frequently used by WebRTC.

Identifying these packets as RTP allows VoIP analysis, filtering, etc., in LiveWire captures and forensic searches. LiveFlow already includes support.

Removed Capture-To-Disk VoIP Statistics

The CTD VoIP statistics capture options have been removed along with the VoIP Call Quality and Call Utilization graphs in the Forensic view. We recommend now using LiveFlow VoIP analysis for more accurate results.

Include and Configure Prometheus Metrics

Previous releases included some support for Prometheus metric in LiveWire, but it was disabled by default, and was necessary to add the packages and configure them manually.

In this release, the packages have been added and configure and LiveWire metrics are now default enabled.

Metrics are collected automatically and retained for 15 days.

It is still necessary to open a port in the firewall to access metrics externally through the built-in Prometheus interface or with Grafana.

Allow Users to Stop a Distributed Forensic Search

While running a distributed forensic search you may get more packets than you intended, or one search is returning far more packets than the others, or the search is simply taking too long. You might want to get results up to that point. Previously you'd have to wait for the search to complete. This release adds a "Stop" button to stop searching and receive results at that point.