

LiveAction



LiveWire

User Guide

LiveAction, Inc.
901 Campisi Way, Ste. 222
Campbell, CA 95008, USA
+1 (888) 881-1116
<https://www.liveaction.com>

Copyright © 2025 LiveAction, Inc.
All rights reserved

20250305_LWU_2510a

On-site Hardware Warranty

WARRANTY COVERAGE

We, LiveAction (the trading name of LiveAction, Inc.), warrant that the hardware product ("Product") you have purchased, shall be free from defects in materials and workmanship for the period of your On-site Hardware Warranty from the date of original purchase. This Hardware Warranty does not cover any software you may have purchased from LiveAction, which would be the subject of a separate license agreement. We will, at our option, either repair, replace or refund the price you have paid for the Product which has failed within the warranty period by reason of faulty design (other than any design made, furnished or specified by you) or faulty workmanship or defective materials.

OBTAINING WARRANTY SERVICE

In the event of Product failure, you must contact us within the warranty period in order to notify us of the failure and obtain a Return Material Authorization number for prompt return of the product for repair or replacement. When the failed component is determined, it will be ordered as soon as possible and support technician will replace the part at the site. This process might take few days depending on the availability of the failed parts. Parts will be shipped from the U.S.

- a. It is your responsibility to back up the contents of any and all hard drives shipped to us for warranty service. We will not be responsible for damage to or loss of any programs, data or other information stored on any media.
- b. If it is determined that the Product cannot be repaired or replaced, LiveAction may, at its sole discretion, refund the price of the Product.
- c. Any replaced parts will be warranted for the remainder of the original warranty period.
- d. If your Product needs to be shipped to LiveAction, the customer is responsible for that shipping. LiveAction will ship repaired or replacement product freight prepaid within the U.S.
- e. If your Product is moved outside of the country purchased, LiveAction must be notified of the move immediately so that there will be no delay in obtaining onsite parts/labor.

EXCLUSIONS AND LIMITATIONS

This warranty covers only the hardware components packaged with the original LiveAction Product. Software, external devices, and accessories or parts added after the Product is shipped from LiveAction are not covered under this warranty. Damage occurring during the original shipment of LiveAction Product to you is not covered under this limited warranty. Damage due to external causes, including accident, abuse, misuse, problems with electrical power, servicing or modifications not authorized in writing by LiveAction, improper installation, usage not in accordance with product instructions and problems caused by use of parts and components not supplied by us is not covered under this limited warranty. No LiveAction agent, employee, or affiliate is authorized to make any modification, extension, or addition to this limited warranty.

IF THIS PRODUCT DOES NOT PERFORM AS DESCRIBED IN THE PRODUCT'S DOCUMENTATION OR IS OTHERWISE DEFECTIVE, WE SHALL NOT BE LIABLE IN ANY EVENT FOR DAMAGES, LOST PROFITS, REVENUE, ANTICIPATED SAVINGS OR ANY OTHER INCIDENTAL, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING FROM THE PURCHASE, USE OR INABILITY TO USE THIS PRODUCT. WE SHALL HAVE NO LIABILITY WHATSOEVER FOR OR AS A RESULT OF THE CONDITION OF THE PRODUCT OR ITS FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE. Some states do not allow exclusions or limitations, so the above may not apply to you. This limited warranty gives you specific legal rights, and you may have other rights, which vary from state to state.

If, upon inspection, it is found that the returned Product is not defective within the terms of this limited warranty, you shall pay our standard repair charges to repair the Product including inspection costs and all transport and shipping costs associated with returning the Product to you. Any product or part supplied under this limited warranty may be new or reassembled or reconditioned from serviceable new and used parts. All defective Product or parts will become our property.

EXCEPT FOR THE EXPRESS WARRANTIES STATE ABOVE, LIVEACTION DISCLAIMS ALL WARRANTIES (EXPRESS, IMPLIED STATUTORY OR OTHERWISE) RELATING TO THE PRODUCT, INCLUDING, BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, AND ANY WARRANTIES THAT MAY ARISE FROM COURSE OF PERFORMANCE OR USAGE OF TRADE. IN ADDITION, THE REMEDIES SET FORTH ABOVE CONSTITUTES THE SOLE REMEDIES FOR YOU AND SOLE OBLIGATION OF US FOR BREACH OF WARRANTY OR OTHER CLAIM WITH RESPECT TO THE PRODUCT. YOU ACKNOWLEDGE THAT LIVEACTION HAS SET ITS PRICES AND ENTERED INTO THESE TERMS IN RELIANCE UPON THE LIMITATION OF LIABILITY AND THE DISCLAIMERS OF WARRANTIES AND DAMAGES SET FORTH HEREIN, AND THAT THE SAME FORM AN ESSENTIAL BASIS OF THE BARGAIN BETWEEN THE PARTIES. YOU AGREE THAT THE LIMITATION AND EXCLUSIONS OF LIABILITY AND DISCLAIMERS SPECIFIED IN THESE TERMS WILL SURVIVE AND APPLY EVEN IF FOUND TO HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

ADDITIONAL INFORMATION

Product Information: www.liveaction.com.

Support Contact Information: <https://www.liveaction.com/support/technical-support/>

LiveAction Global Next Business Day (NBD) Response Warranty Support Statement

Global NBD Response Warranty Includes

Direct telephone and email access to senior-level analysts for expedited troubleshooting of hardware issues. On-Site dispatch of service technician and/or warranty parts to Customer's business location for repairs and resolution necessary due to a defect in materials or workmanship on the Supported System.

Support Procedures

Support Requests: Customer may submit the issue and a service request by contacting LiveAction technical support at <https://www.liveaction.com/support/technical-support/>.

Assist with phone/email-based Troubleshooting

- When request is submitted, please include serial number of unit. Be prepared to identify any error messages received, how and when they occurred, and what activities preceded the error. Also be able to describe what steps have already been taken to solve the problem.
- Analyst will go through a series of additional troubleshooting steps to help diagnose the issue.
- If an on-site dispatch and parts replacement is necessary, the analyst will provide Customer with additional instructions.
- An RMA (Return Merchandise Authorization) will be created and any defective parts will be replaced.

On-Site Support

The On-Site Support includes 24x7 next business day response with repair if parts are available. If parts are not available, the repair will take place the day after the parts arrive at the Customer location.

A service technician will be dispatched to the business location of the affected system. Customer will be contacted in advance to schedule the onsite visit.

On-site Response Time Restrictions/Special Terms

With Next Business Day On-Site Response Service following phone-based/Email troubleshooting, a technician can usually be dispatched to arrive onsite the next business day.

- Available 5 days/week, 8 hours/day - excluding holidays.
- Calls received 5:00 PM local Customer time (Monday - Friday) and/or dispatches made after that time may require an additional business day for service technician to arrive at the Customer's location.

Following completion of remote troubleshooting and problem determination, the analyst will determine if the issue requires an on-site service technician and/or parts to be dispatched or if the issue can be resolved remotely over the phone.

Missed Service Visit: If Customer or Customer's authorized representative is not at the location when the service technician arrives, the service technician cannot service the Supported System. The service technician will leave and customer will be notified and the next appointment will be scheduled. If this occurs, Customer may be charged an additional fee for a follow-up service call.

Software Troubleshooting

Support includes software troubleshooting for select applications and operating systems on Supported Systems over the telephone, or by transmission of software and other information through electronic means, or by shipping software and/or other information to Customer. Covered Software Products include core operating systems, which is installed and Supported by LiveAction.

Software Troubleshooting Does Not Include*

- Any product version not currently supported or provided by the manufacturer.
- Configuration, installation or optimization assistance.
- Any on-site service.
- Remote or on-site training assistance.

*LiveAction software maintenance covers Capture Engine Software maintenance and support.

Global NBD Response Warranty Does Not Include

- LiveWire Edge hardware.
- Accessories, supply items, operating supplies, peripherals or parts such as batteries, frames, and covers.
- Media replacement for software LiveAction no longer ships with new systems.
- Media replacement on non-LiveAction branded / manufactured software.
- Hardware or software support for Customer Factory Integration ("CFI") products.
- Hardware or software support for non-LiveAction peripherals.
- Preventative maintenance.

- Installation, de-installation, or relocation services.
- Direct third party product support.
- Repairs necessitated by software problems, or as a result of alteration, adjustment, or repair by anyone other than LiveAction (or its authorized representatives).
- Support for equipment damaged by misuse, accident, abuse of Supported System or components (such as, but not limited to, use of incorrect line voltages, use of incorrect fuses, use of incompatible devices or accessories, improper or insufficient ventilation, or failure to follow operating instructions), modification, unsuitable physical or operating environment, improper maintenance by Customer (or Customer's agent), moving the Supported System, removal or alteration of equipment or parts identification labels, or failure caused by a product for which LiveAction is not responsible.
- Support for damage resulting from an act of God such as, but not limited to, lightning, flooding, tornado, earthquakes, and hurricanes.
- Any activities or services not expressly described in this Service Description. Please read this Service Description carefully and note that LiveAction reserves the right to change or modify any of the terms and conditions set forth in this Service Description at any time, and to determine whether and when any such changes apply to both existing and future Customers.

Contents

Chapter 1

Introduction	1
About LiveWire	2
LiveWire technical specifications.....	3
LiveWire Edge 1515	3
LiveWire Core I300	3
LiveWire PowerCore 3300.....	6
What's included	7
Front / back panels.....	8
LiveWire Edge 1515 front panel.....	8
LiveWire Edge 1515 back panel.....	10
LiveWire Core I300 front panel	11
LiveWire Core I300 back panel	11
LiveWire PowerCore 3300 front panel.....	12
LiveWire PowerCore 3300 back panel.....	13
Inside the appliance.....	15
LiveWire Core I300 internal components.....	15
LiveWire PowerCore 3300 internal components.....	17
Installing LiveWire Edge 1515	18
Connect to LiveWire Edge 1515 via the Console port	19
LiveNX Integration	20
Starting / shutting down LiveWire Edge 1515.....	20
Using BMC Web UI	20
Installing LiveWire Core I300/PowerCore 3300.....	21
Connecting network cables.....	21
System fans.....	22
Connecting TeraVault to LiveWire PowerCore 3300	22
Connecting multiple TeraVault units	25
Starting / shutting down LiveWire Core I300/PowerCore 3300.....	26
Attaching the front bezel	27
LiveWire Activation.....	27
Activation via Omnipeek Web	27
Activation via Omnipeek	31
Contacting LiveAction support	35

Chapter 2

Configuring LiveWire	36
Logging-in to LiveWire command line	37
Using the LiveAdmin utility.....	37
Login	38
Dashboard.....	39
Authentication	40
Monitor	41
Network	42
Omni.....	44
Support.....	49
Remote Syslog	50
Time	50
TLS	51
Update.....	51
Restart and power off	52
Configuring network settings by command script	52
Using LiveWire with Omnipeek.....	53

	Integrated Remote Access Controller (iDRAC)	54
	iDRAC and network security	54
	Setting the IP address for iDRAC	54
	Access BIOS setting to configure IP address	54
	Connecting to iDRAC on LiveWire	54
	Changing the default password	56
	Accessing a remote console	57
	Reimaging LiveWire with an ISO image	58
	Rebooting LiveWire	61
	Starting / Shutting down LiveWire	61
	Accessing the iDRAC interface over the USB port	62
Chapter 3	Sending LiveFlow Telemetry	63
	About sending telemetry to LiveNX and other platforms	64
	Configuring LiveFlow telemetry	64
	General	65
	Adapter	68
	Hardware Profiles	69
	LiveFlow	74
	Filters	82
	Recommendations for better performance at higher data rates	83
	An example of using LiveWire, LiveNX, and Omnippeek	83
Chapter 4	Creating and Managing API Tokens	87
	About API Tokens	88
	Creating an API Token	88
	Managing API Tokens	90
Chapter 5	Configuring Access Control	92
	About Access Control	93
	Enabling Access Control	93
	About Roles	97
	Configuring Roles	97
	Policy Descriptions	99
	Configuring Filters for Roles	100
	Manage Users for Roles	102
	Manage Groups for Roles	103
	Manage Sessions for Roles	105
	Adding a Role	106
	Enabling Third-Party Authentication	107
	When Upgrading From LiveWire v23.3.1 or Earlier	113
Chapter 6	Capture Adapters for LiveWire	115
	About capture adapters	116
	1G capture adapter	116
	1G capture adapter I/O bracket	116
	LED status	117
	10G capture adapter	117
	10G capture adapter (2-port) I/O bracket	118
	10G capture adapter (4-port) I/O bracket	118
	LED status	118
	40G capture adapter	119
	40G capture adapter I/O bracket	119
	LED status	119
	100G capture adapter	120
	100G capture adapter I/O bracket	120

LED status	121
Enabling PTP support for capture adapters	121
Configuration parameters	122
Synchronizing the capture engine clock	123
Connecting the external time synchronization adapter	124
Troubleshooting the capture adapters	124
Verifying link status	124
Capture adapter technical specifications	126
1G capture adapter specifications	126
10G capture adapter (2-port) specifications	126
10G capture adapter (4-port) specifications	127
40G capture adapter specifications	127
100G capture adapter specifications	128
 Chapter 7	
Network Port Requirements	129
LiveWire/Omnipeek Port Information	130
NetFlow (NetFlow v5, NetFlow v9, and IPFix) (optional)	130
iDRAC (out-of-band LiveWire management) Default Port Requirements ...	130

Introduction

In this chapter:

- About LiveWire. 2
- LiveWire technical specifications. 3
- What’s included. 7
- Front / back panels. 8
- Inside the appliance.15
- Installing LiveWire Edge 151518
- Starting / shutting down LiveWire Edge 1515.20
- Installing LiveWire Core 1300/PowerCore 330021
- Connecting TeraVault to LiveWire PowerCore 3300 22
- Starting / shutting down LiveWire Core 1300/PowerCore 330026
- Attaching the front bezel 27
- LiveWire Activation. 27
- Contacting LiveAction support. 35

About LiveWire

Congratulations on your purchase of LiveWire™! LiveWire appliances uniquely combine flow-based reporting using deep packet inspection (DPI) with high-speed, packet capture and storage. LiveWire is designed to work with LiveAction's LiveNX and various other platforms. Because LiveWire starts with packet data, it is able to provide a unique, and extended, set of flow-based monitoring data called LiveFlow. LiveFlow is extended IPFIX data and is exported to LiveNX and other platforms. See Chapter 3, [Sending LiveFlow Telemetry](#) for the additional tasks you must perform in order to export LiveFlow data from LiveWire. Please also refer to the LiveNX and the other platform documentation for more information on using the LiveFlow data exported to LiveNX and other platforms.

LiveWire is available in the following configurations:

- [LiveWire Edge 1515](#)
- [LiveWire Core 1300](#)
- [LiveWire PowerCore 3300](#)

Note In this guide, references to 'LiveWire' refer to the complete collection of LiveWire appliances described above. When necessary, references to a specific LiveWire appliance are specified to note any differences between appliances.

LiveWire technical specifications

LiveWire Edge 1515

Specification	Description
Base	Lanner NCA-1515A
Base SKU	LWRE-1515-H
Processor	Intel Atom Processor C3758 2.20GHz, 8C/8T
Memory	32G SODIMM DDR4 2400MT/s
Hard Drive	1 x 1 TB 2.5" SSD
Network Adapters	4 x GbE RJ45 Intel® SoC Integrated MAC 2 x GbE RJ45 Intel® i350 2 x GbE SFP Intel® i350
Other Ports	1 x RJ45 Console 1 x RJ45 LOM 2 x USB 2
Fans	1 x Fan
Power Supply	1 x 60W Power Adapter
Power Cords	C13 to NEMA 5-15P, Power Cord, North America
PCIe	2 x Mini-PCIe 1 x M.2 2242 B
Rack Mount Kit	LWRE_1515_RMK

LiveWire Core 1300

Specification	Description
Base	OEM PowerEdge R6615 Server
Chassis	2.5" Chassis with up to 10 Hot Plug Hard Drives
Motherboard	PowerEdge R6615 Motherboard
Processor	AMD 9254 2.9GHz 24C/48T (1)
Memory	32GB RDIMM, 5600MT/s, Dual Rank (4)
RAID/Internal Storage Controllers	PERC H755 SAS, Front
Hard Drive	BOSS-N1 controller card + with 2 M.2 960GB (RAID 1) 2.4TB Hard Drive SAS ISE 12Gbps 10K 512e (10)
Network Adapters	Broadcom 5720 Dual Port 1GbE LOM Broadcom 57416 Dual Port 10GbE BASE-T Adapter, OCP NIC 3.0
Fans	Very High Performance Fan x4
Power Supply	Dual, Hot Plug, Redundant Power Supply (1+1), 1100W
Power Cords	C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America
PCIe Riser	Riser Config 3, 2 x 16 FH

Specification	Description
Embedded Systems Management	iDRAC9, Enterprise
Quick Sync	None
Rack Rails	ReadyRails Sliding Rails Without Cable Management Arm
PSU Specifications:	
PSU	1100W Mixed Mode
Class	Titanium
Heat Dissipation (Maximum)	4100 BTU/hr
Frequency	50/60 Hz
Voltage	100–240 V AC, autoranging
Current	12 - 6.3 A
Temperature Specifications ASHRAE A2:	
Allowable continuous operations	
Temperature range for altitudes <= 900 m (<= 2953 ft)	10 to 35°C (50 to 95°F) with no direct sunlight on the platform
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/300 m (1.8°F/984 Ft) above 900 m (2953 Ft)
Temperature Specifications ASHRAE A3:	
Allowable continuous operations	
Temperature range for altitudes <= 900 m (<= 2953 ft)	5 to 40°C (41 to 104°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 85% RH with 24°C (75.2°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/175 m (1.8°F/574 Ft) above 900 m (2953 Ft)
Temperature Specifications ASHRAE A4:	
Allowable continuous operations	
Temperature range for altitudes <= 900 m (<= 2953 ft)	5 to 45°C (41 to 113°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 90% RH with 24°C (75.2°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/125 m (1.8°F/410 Ft) above 900 m (2953 Ft)
Common Environmental Specifications:	
Maximum temperature gradient (applies to both operation and non-operation)	20°C in an hour* (36°F in an hour) and 5°C in 15 minutes (9°F in 15 minutes), 5°C in an hour* (9°F in an hour) for tape hardware NOTE:* - Per ASHRAE thermal guidelines for tape hardware, these are not instantaneous rates of temperature change.
Non-operational temperature limits	-40 to 65°C (-40 to 149°F)
Non-operational humidity limits	5% to 95% RH with 27°C (80.6°F) maximum dew point
Maximum non-operational altitude	12,000 meters (39,370 feet)
Maximum operational altitude	3,050 meters (10,006 feet)
Maximum Vibration Specifications:	
Operating	0.21 G _{rms} at 5 Hz to 500 Hz for 10 minutes (all operation orientations)
Storage	1.88 G _{rms} at 10 Hz to 500 Hz for 15 minutes (all six sides tested)
Maximum Shock Pulse Specifications:	

Specification	Description
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axis of 6 G for up to 11 ms
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axis (one pulse on each side of the system) of 71 G for up to 2 ms

LiveWire PowerCore 3300

Specification	Description
Base	OEM Dell PowerEdge R7615 Server
Chassis	Chassis with up to 12 x 3.5" HDDs
Motherboard	OEM PowerEdge R7615 Motherboard
Processor	AMD EPYC 9354P 3.25 GHz, 32C/64T
Memory	32GB RDIMM, 4800MT/s, Dual Rank (8)
RAID/Internal Storage Controllers	PERC H755 Adapter, Low Profile
Hard Drive	960 GB BOSS M.2 Drives (2) 20 TB Hard Drive SAS 12 Gbps 7.2 K 512e 3.5 in Hot-Plug (12)
Network Adapters	Broadcom 5720 Dual Port 1GbE LOM Broadcom 57416 Dual Port 10GbE BASE-T Adapter, OCP NIC 3.0
Fans	Performance Fans (6)
Power Supply	Dual, Hot-Plug, Power Supply, 2400W MM (100-240 Vac), Redundant (1+1)
Power Cords	C13, 3 M, 125 V, 15 A (2)
PCIe Riser	Riser Config 3 - 2 x 16 FH (Gen5) - 2 x 8 FH - 2 x 16 LP, Half Length
Embedded Systems Management	iDRAC9, Enterprise
Quick Sync	None
Rack Rails	ReadyRails Sliding Rails Without Cable Management Arm
PSU Specifications:	
PSU	2400 W mixed mode
Class	Platinum
Heat Dissipation (Maximum)	9000
Frequency	50/60
Voltage	2400 W
High Line 200 V 240 V	1400 W
Low Line 100-140 V	N/A
Current	N/A
Temperature Specifications ASHRAE A2:	
Allowable continuous operations	
Temperature range for altitudes <= 900 m (<= 2953 ft)	10–35°C (50–95°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/300 m (1.8°F/984 Ft) above 900 m (2953 Ft)
Temperature Specifications ASHRAE A3:	

Specification	Description
Allowable continuous operations	
Temperature range for altitudes ≤ 900 m (≤ 2953 ft)	5–40°C (41–104°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 85% RH with 24°C (75.2°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/175 m (1.8°F/574 Ft) above 900 m (2953 Ft)
Temperature Specifications ASHRAE A4:	
Allowable continuous operations	
Temperature range for altitudes ≤ 900 m (≤ 2953 ft)	5–45°C (41–113°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 90% RH with 24°C (75.2°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/125 m (1.8°F/410 Ft) above 900 m (2953 Ft)
Relative Humidity Specifications:	
Storage	8% RH with -12°C minimum dew point to 90% RH with 24°C (75.2°F) maximum dew point. Non-condensing at all times.
Operating	10% to 80% relative humidity with 29°C (84.2°F) maximum dew point.
Maximum Vibration Specifications:	
Storage	0.21 Grms at 5 Hz to 500 Hz for 10 minutes (all operation orientations)
Operating	1.88 Grms at 10 Hz to 500 Hz for 15 minutes (all six sides tested)
Maximum Shock Pulse Specifications:	
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axis of 6 G for up to 11 ms.
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axis (one pulse on each side of the system) of 71 G for up to 2 ms.

What's included

Your standard LiveWire package includes:

LiveWire Edge 1515:

- LiveWire Edge packet capture and analysis appliance
- Pre-loaded, tested, and fully integrated LiveWire software for high-speed packet capture, storage, and flow based telemetry generation
- Web-based configuration
- LiveWire Omnipeek
- Omnipeek for Windows License (1)
- AC power adapter and cord
- Rubber feet (4)
- Ethernet cable

LiveWire Core 1300/PowerCore 3300:

- LiveWire packet capture and analysis appliance
- Pre-loaded, tested, and fully integrated LiveWire software for high-speed packet capture, storage, and flow based telemetry generation

- Web-based configuration
- LiveWire Omnipeek
- Omnipeek for Windows License (l)
- Two power cords
- Rack-mount rails
- Chassis bezel

Front / back panels

See the illustrations and descriptions of the front and back panel of LiveWire in the sections below.

LiveWire Edge 1515 front panel



No.	Item	Description
F1	SIM Card Slot	SIM card slot cover (optional)
F2	LED Indicator	Front panel LEDs. See also 'LED Indicators' on page 9.

SFP1 LOM

SPEED 1

LINK/ACT 4

LOM

System Power

System Status

HDD Activity

LAN 3 - 8

SFP2

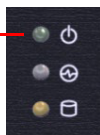
F3	Antenna Port	SMA connector for the Wi-Fi (optional)
----	--------------	--

LED Indicators

The status of the LED indicators on the Front Panel are as follows:

System Power

System Power LED

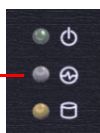


Solid Green	The system is powered on
Off	The system is powered off

System Status

This System Status LED indicator is programmable. You could program it to display the operating status of the behaviors described below:

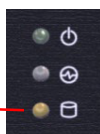
System Status LED



Solid Green	Defined by GPIO
Solid Red	Defined by GPIO
Off	Defined by GPIO

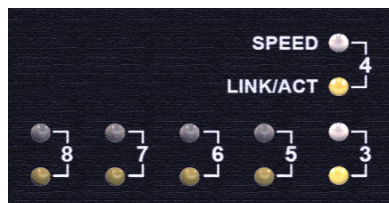
HDD Activity Status

HDD Activity Status LED



Blinking Amber	Data access activities
Off	No data access activities

RJ45 LAN Status



Upper LED (Speed)	Solid Green	Operating as a 100 Mbps connection
	Solid Amber	Operating as a Gigabit connection (1000 Mbps)
	Off	No link has been established

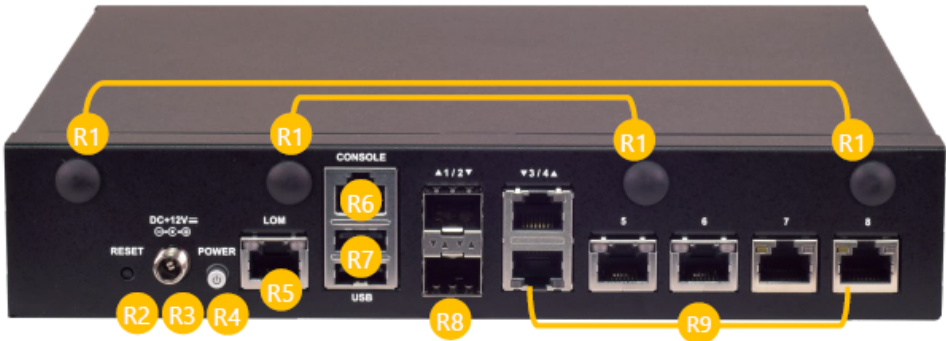
Lower LED (Link Status)	Solid Amber	Link has been established and there is no activity on this port
	Blinking Amber	Link has been established and there is activity on this port
	Off	No link has been established

SFP Port Status



Solid Amber	Link has been established and there is no activity on this port
Blinking Amber	Link has been established and there is activity on this port
Off	No link has been established

LiveWire Edge 1515 back panel



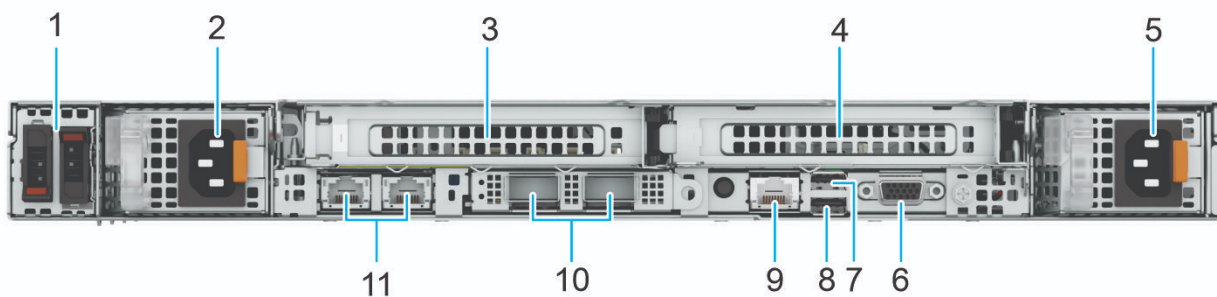
No.	Item	Description
R1	Antenna Port	Port for optional antenna.
R2	Reset Button	Press to perform a reset
R3	DC-Jack	Power supply
R4	Power Button	Press to power on/off the system
R5	LOM Port	1x RJ45 LOM port (optional)
R6	Console Port	1x Gbe RJ45 console port
R7	USB Ports	2x Type A USB 2.0 ports
R8	SFP Ports	2x 1G SFP ports - Port 1 (eth0) - Port 2 (eth1)
R9	GbE Ports	6x GbE RJ45 ports - Port 3 (eth2) - Port 4 (eth3, MGMT) - Port 5 (eth4) - Port 6 (eth5) - Port 7 (eth6, Bridge) - Port 8 (eth7, Bridge)



LiveWire Core 1300 front panel








Item	Ports, Panels, or Slots	Description
1	Left control panel	Contains the system health, system ID, and the status LED indicator.
2	Drives	Enables you to install drives that are supported on your system.
3	Right control panel	Contains the power button with integrated power LED, 1 x VGA port, 1 x 2.0 USB port, iDRAC Direct (Micro-AB USB) port, and the iDRAC Direct status LED.
4	VGA	Enables you to connect a display device to the system.
5	Information tag	The Express Service Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag will also contain the iDRAC secure default password.

LiveWire Core 1300 back panel



Item	Ports, Panels, or Slots	Icon	Description
1	BOSS	N/A	Insert BOSS blank when the BOSS module is not used.
2	Power supply unit (PSU1)	 1	PSU1 is the primary PSU of the system.
3	PCIe expansion card riser 1 (slot 1)	N/A	The expansion card riser enables you to connect PCI Express expansion cards. For more information, see the Expansion card installation guidelines section.
4	PCIe expansion card riser 4 (slot 2)	N/A	The expansion card riser enables you to connect PCI Express expansion cards. For more information, see the Expansion card installation guidelines section.
5	Power supply unit (PSU2)	 2	PSU2 is the secondary PSU of the system.

Item	Ports, Panels, or Slots	Icon	Description
6	VGA port		Enables you to connect a display device to the system.
7	USB 2.0 port		The USB port is 4-pin, 2.0-compliant. This port enables you to connect USB devices to the system.
8	USB 3.0 port		The USB ports are 9-pin, 3.0-compliant. These ports enable you to connect USB devices to the system.
9	Dedicated iDRAC9 Ethernet port		Enables you to remotely access iDRAC.
10	OCP NIC card		The OCP NIC card supports OCP 3.0. The NIC ports are integrated on the OCP card which is connected to the system board.
11	NIC ports	N/A	The NIC ports that are integrated on the LOM card provide network connectivity which is connected to the system board. Dell DPU card to be installed in the riser.

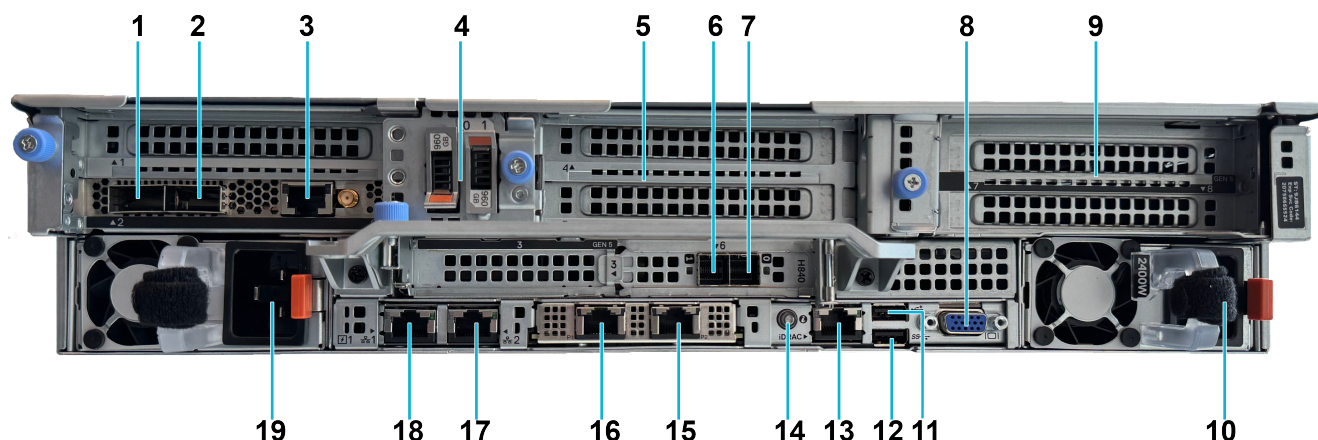
NOTE: The system allows either LOM card or MIC card to be installed in the system.





LiveWire PowerCore 3300 front panel





Item	Ports, Panels, or Slots	Icon	Description
1	Left control panel	N/A	Contains the system health, system ID, and the status LED indicator.
2	Drives	N/A	Enables you to install drives that are supported on your system.
3	Right control panel	N/A	Contains the power button with integrated power LED, 1 x VGA port, 1 x 2.0 USB port, iDRAC Direct (Micro-AB USB) port, and the iDRAC Direct status LED.
4	Information tag	N/A	The Express Service Tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag will also contain the iDRAC secure default password.

LiveWire PowerCore 3300 back panel



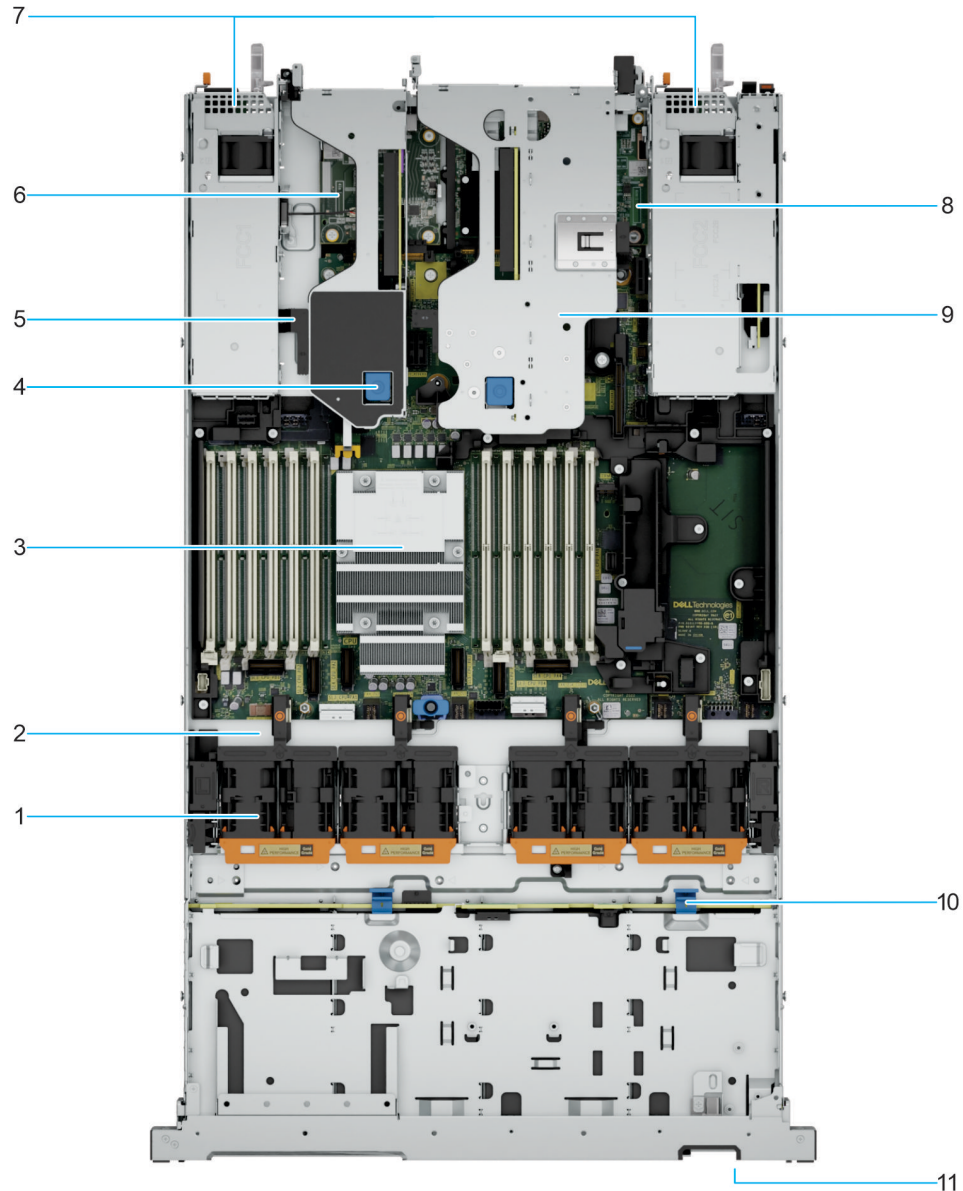
Item	Ports, Panels, or Slots	Icon	Description
1	Port 0	N/A	QSFP28 network port
2	Port 1	N/A	QSFP28 network port
3	RJ45-F 1000BASE-T IEEE1588 PTP	N/A	External RJ45 time synchronization connector
4	BOSS module	N/A	BOSS-N1 module
5	PCIe expansion card riser 3 (slot 5)	N/A	The expansion card riser enables you to connect PCI Express expansion cards. For more information, see the Expansion card installation guidelines section.
6	Port B/1	N/A	Mini-SAS HD external SFF8644 port on the RAID card. The SAS external cascading cable that connects the TeraVault JBOD storage unit to the RAID card on LiveWire PowerCore 3300 is plugged into this port. Make sure the blue pull tab on the cable is on the bottom when plugging into this port.
7	Port A/0	N/A	Mini-SAS HD external SFF8644 port on the RAID card.
8	VGA port	N/A	Enables you to connect a display device to the system.
9	PCIe expansion card riser 4 (slot 7)	N/A	The expansion card riser enables you to connect PCI Express expansion cards. For more information, see the Expansion card installation guidelines section.
10	Power supply unit (PSU2)		PSU2 is the secondary PSU of the system.
11	USB 2.0 port		The USB port is 4-pin, 2.0-compliant. This port enables you to connect USB devices to the system.
12	USB 3.0 port		The USB port is 9-pin and 3.0-compliant. This port enables you to connect USB devices to the system.
13	Dedicated iDRAC9 Ethernet port		Enables you to remotely access iDRAC. For more information, see the Integrated Dell Remote Access Controller User's Guide at PowerEdge Manuals.

Item	Ports, Panels, or Slots	Icon	Description
14	System Identification (ID) button		<p>The System Identification (ID) button is available on the front and back of the system. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode. When pressed, the system ID LED in the back panel blinks until either the front or rear button is pressed again. Press the button to toggle between on or off mode.</p> <p>NOTE: If the server stops responding during POST, press and hold the System ID button for more than five seconds to enter the BIOS progress mode</p> <p>NOTE: To reset the iDRAC (if not disabled on the iDRAC setup page by pressing F2 during system boot), press and hold the System ID button for more than 15 seconds.</p>
15	NIC Port (eth3)	N/A	The NIC port is integrated on the OCP card which is connected to the system board.
16	NIC Port (eth2)	N/A	The NIC port is integrated on the OCP card which is connected to the system board.
17	NIC Port (eth1)	N/A	The NIC port is embedded on the LOM card that is connected to the system board.
18	NIC Port (eth0)	N/A	The NIC port is embedded on the LOM card that is connected to the system board.
19	Power supply unit (PSU1)		PSU1 is the primary PSU of the system.

Inside the appliance

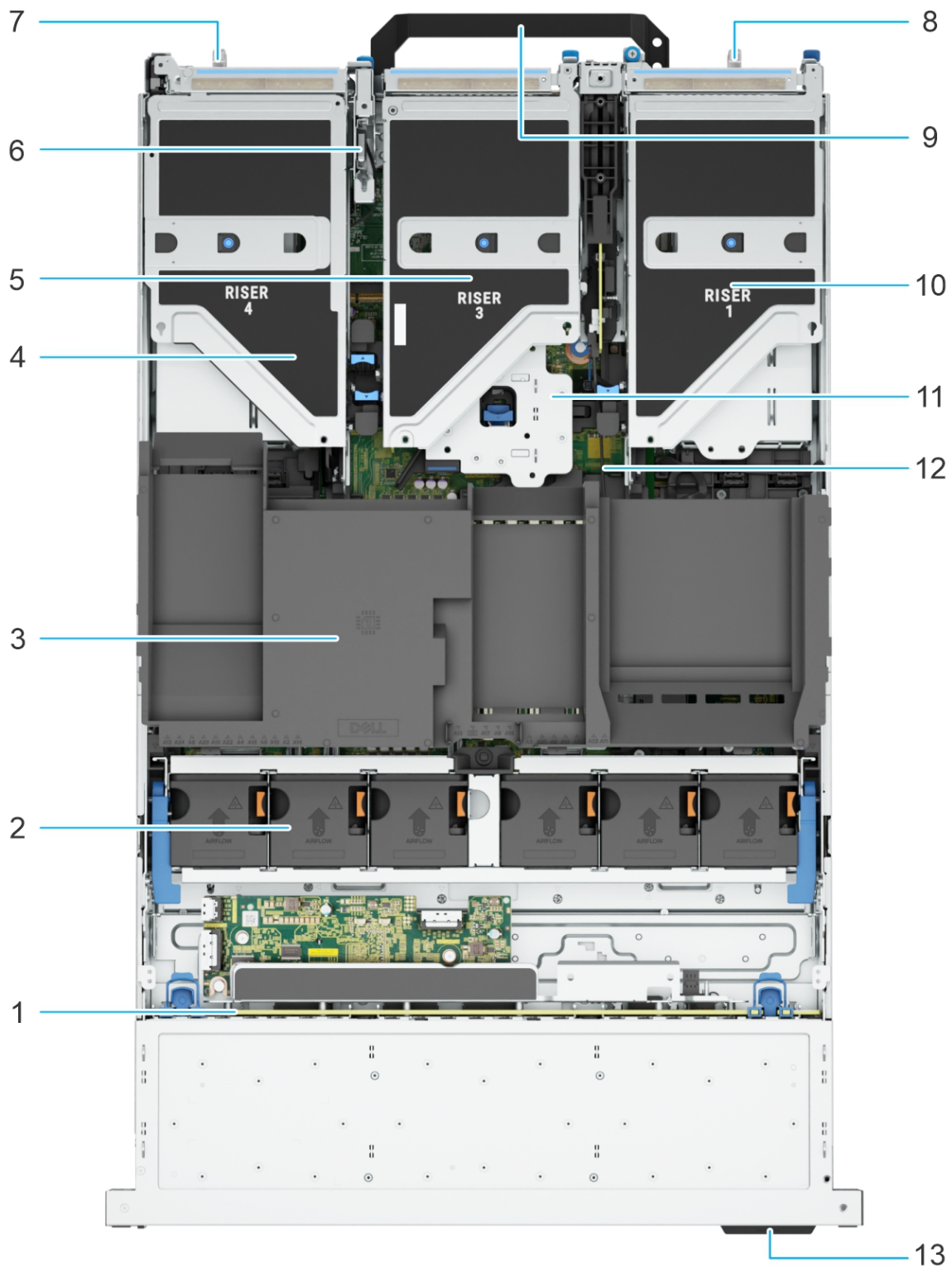
CAUTION! Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as directed by the LiveAction support team. Damage due to servicing that is not authorized by LiveAction is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.

LiveWire Core 1300 internal components



Item	Description
1	Cooling fan cage assembly
2	Fan power connector
3	Processor
4	Latch mechanism to engage Riser module
5	Guiding mechanism to guide Riser module
6	Riser 3
7	Power Supply Units (PSU 1 and 2)
8	System board
9	Riser 2
10	Drive backplane with latch
11	Information Tag

LiveWire PowerCore 3300 internal components



Item	Description
1	Drive backplane
2	Cooling fan cage assembly
3	Air shroud top cover
4	Riser 4
5	Riser 3
6	Intrusion switch
7	Power Supply Unit (PSU 1)
8	Power Supply Unit (PSU 2)
9	Handle
10	Riser 1
11	Riser 2
12	System board
13	Information tag

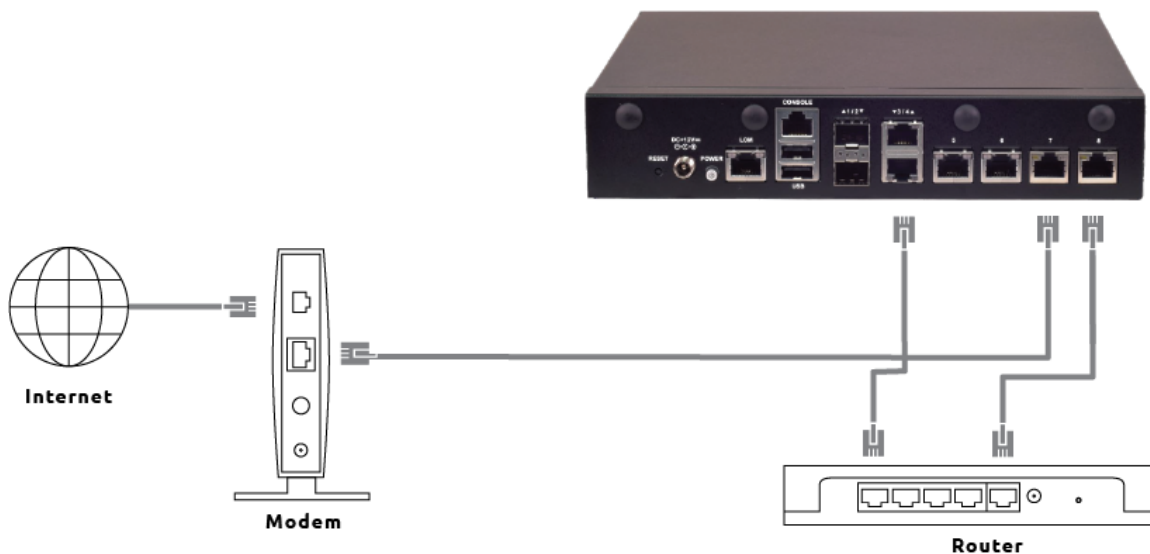
Installing LiveWire Edge 1515

To install LiveWire Edge 1515:

1. Attach the included rubber feet (4) to the bottom of LiveWire Edge 1515 and place LiveWire Edge 1515 on a flat surface.
2. Attach the power adapter by screwing in the connector on the adapter to the power-in socket on the back panel.
3. Plug the other end of the power adapter into a reliable power source.

CAUTION! Do not place anything on top of or directly next to LiveWire Edge 1515. Any obstructions to the heat sink located on top of LiveWire Edge 1515 can cause the unit to overheat.

4. Connect LiveWire Edge 1515 to the network to capture traffic:
 - From the Bridge ports: To use the Bridge ports, connect LiveWire Edge 1515 inline on a network segment. In this mode, connect Port 7 (eth6, Bridge) to the side of the network with the upstream router; and connect Port 8 (eth7, Bridge) to the LAN side of the network.
 - From the remaining RJ45 span ports: To use the span ports, connect LiveWire Edge 1515 directly to a span port from a switch or router.
 - From the SFP ports: To use the SFP ports, install the 1 Gb SFP optic and connect your fiber cable to a fiber port on switch or packet broker.



5. To configure and use the LiveWire Edge 1515, connect Port 4 (eth3, MGMT) to the network.

Connect to LiveWire Edge 1515 via the Console port

The Console port on LiveWire Edge 1515 lets you connect to another computer terminal for advanced diagnostics or recovery access using an USB console cable (USB to RJ45) connected from the USB port on your PC/laptop to the Console port of LiveWire Edge 1515.

Using the Console port on LiveWire Edge 1515, a laptop, and a terminal program of your choice, you can log into LiveWire Edge 1515 and access the LiveWire command prompt (admin@livewire).

To connect to LiveWire Edge 1515:

1. Connect the Console cable from your laptop to the Console port on LiveWire Edge 1515.
2. Navigate to the Windows Device Manager and determine the COM port assigned to the Console port on LiveWire Edge 1515:
 - a. Open the Windows Device Manager.
 - b. In the "Ports (COM & LPT)" category, find the matching COM Port #. For example, "COM4" in "Prolific PL2303GC USB Serial COM Port (COM4)."
3. Using any serial terminal program (e.g., HyperTerminal or Putty), establish a connection to LiveWire Edge 1515 using the COM Port # identified above. Make sure the appropriate terminal settings match the settings below for LiveWire Edge 1515.
 - Connection Type: [Serial]
 - Serial line: [COM#] (see Step 2 above)
 - Terminal Type: [VT100+]
 - Bits per second: [115200]
 - Data Bits: [8]
 - Parity: [None]
 - Stop Bits: [1]
 - Flow Control: [None]
 - VT-UTF8 Combo Key Support: [Enabled]
 - Recorder Mode: [Disabled]

- Resolution 100x31: [Enabled]

4. Once a connection to LiveWire Edge 1515 has been established, the LiveWire Edge 1515 configuration menu appears.

With each configuration change, you are prompted to enter your admin password. The default username and password is:

username: *admin*

password: *admin*

LiveNX Integration

To use LiveWire Edge 1515 to export LiveFlow data to a LiveNX server, go to *Captures > + New LiveFlow Capture* in the Omnipeek Web interface, and adjust any configuration settings as needed. You can also specify router mappings to separate segregated traffic from different segments into separate interfaces in LiveNX.

Additionally, in the LiveNX application, when adding a LiveWire Edge 1515 device to LiveNX from the *Add Device* dialog, configure the 'Enter SNMP connection settings for this device' option as follows:

SNMP Version: **Version 3**

User Name: **admin**

Authentication Protocol: **SHA**

Authentication Password: **Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc**

Privacy Protocol: **AES 128-bit**

Privacy Password: **x3Fmpv9Oplsnk0Qg3rH25BKBd66fxzSK**

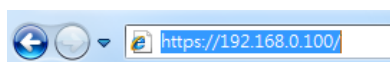
Starting / shutting down LiveWire Edge 1515

To start/shutdown LiveWire Edge 1515:

- Press the power button on the rear panel
- For remote power off or restart, use the BMC via LOM connection. See [Using BMC Web UI](#).

Using BMC Web UI

In the address bar of your Internet browser, input the IP address of the LiveWire Edge 1515 to access the BMC interface.



Initial access of BMC prompts you to enter username and password.

 A screenshot of the BMC Web UI login page. The page has a green header with the text 'Engineering Sample'. Below the header, there are two input fields: 'Username' and 'Password'. At the bottom, there is a green button labeled 'Sign in'.

The default username and password is:

username: *admin*

password: *admin*

When you log in using the default username and password, you will get full administrative rights, and it will ask you to change the default password once you log in.

Note (1) If not specified, the default IP to access BMC is <https://192.168.0.100>. (2) Please use https to access Web UI.

Installing LiveWire Core 1300/PowerCore 3300



LiveWire Core 1200



LiveWire PowerCore 3300

To install LiveWire Core 1300/PowerCore 3300:

1. Place LiveWire Core 1300/PowerCore 3300 on a flat surface, or mount it in a standard 19-inch equipment rack.
2. Connect a power cable to each of the two power outlets at back of the unit.

Note LiveWire Core 1300/PowerCore 3300 has two redundant high-efficiency “hot-swappable” power supplies. If a power module fails, it should be replaced immediately. If your LiveWire Core 1300/PowerCore 3300 is under warranty, please contact Technical Support to arrange for a replacement power supply.

3. Plug the other end of the power cables to an AC outlet.

Important! WARNING: This device has more than one power cord. Disconnect ALL power supply cords before servicing.

AVERTISSEMENT: Cet appareil a plus d’une cordon d’alimentation. Débranchez TOUTES les cordons d’alimentation avant l’entretien.

Connecting network cables

LiveWire Core 1300/PowerCore 3300 includes Gigabit Ethernet ports and Integrated Remote Access Controller (iDRAC) ports used for remotely accessing and troubleshooting LiveWire Core 1300/PowerCore 3300. LiveWire Edge includes Gigabit Ethernet ports, but no iDRAC port. See ‘Front / back panels’ on page 8 for the location of these ports. For information on using iDRAC, see ‘Integrated Remote Access Controller (iDRAC)’ on page 54.

To connect network cables:

- Use a standard Ethernet cable to connect these ports to your network.

Tip To reach LiveWire through an SSH connection, you can use an Ethernet cable connected directly between the Gigabit Ethernet port on LiveWire and your PC or laptop. LiveWire eth0 port is configured at the factory to have a DHCP IP address with a fail over to 192.168.1.21. The PC or laptop must be configured to be on the same IP subnet.

System fans

LiveWire Core 1300/PowerCore 3300 has multiple cooling fans that are used to cool the system chassis. If any one of the fans fail, it should be replaced immediately. If your LiveWire Core 1300/PowerCore 3300 is under warranty, please contact LiveAction Technical Support to arrange for a replacement fan.

Note LiveWire Edge has no fan or any other moving parts.

Important! The chassis top cover must be properly installed in order for the cooling air to circulate correctly through the chassis and cool the components.

Important! WARNING: Slide/rail mounted equipment is not to be used as a shelf or a work space.

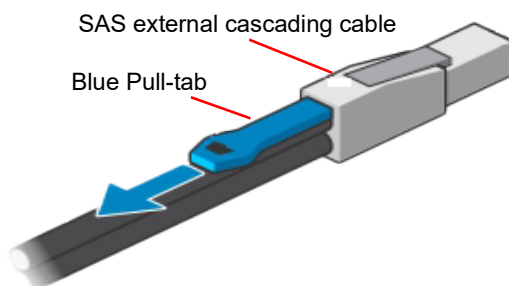
AVERTISSEMENT: Le matériel monté sur rails/coulisseaux ne doit pas être utilisé comme étagère ou espace de travail.

Connecting TeraVault to LiveWire PowerCore 3300

The storage capacity of any LiveWire PowerCore 3300 with 200 TB, RAID 6 (240 TB, optional RAID 0) of total hard disk capacity can be increased through the addition of TeraVault for LiveWire PowerCore. TeraVault is available in a configuration of 200 TB, RAID 6 (240 TB, optional RAID 0). Up to four TeraVault units can be added for a total of up to 1000 TB, RAID 6 (1200 TB, optional RAID 0). If you purchased TeraVault with your LiveWire PowerCore 3300, the instructions to connect it to your LiveWire PowerCore 3300 are provided below.

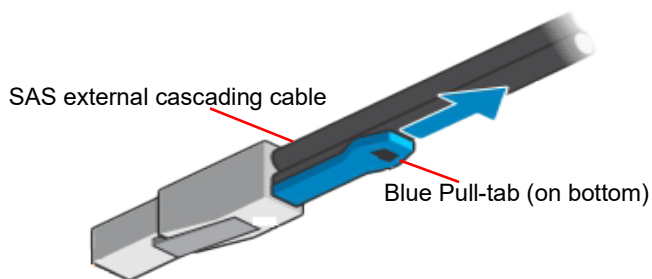
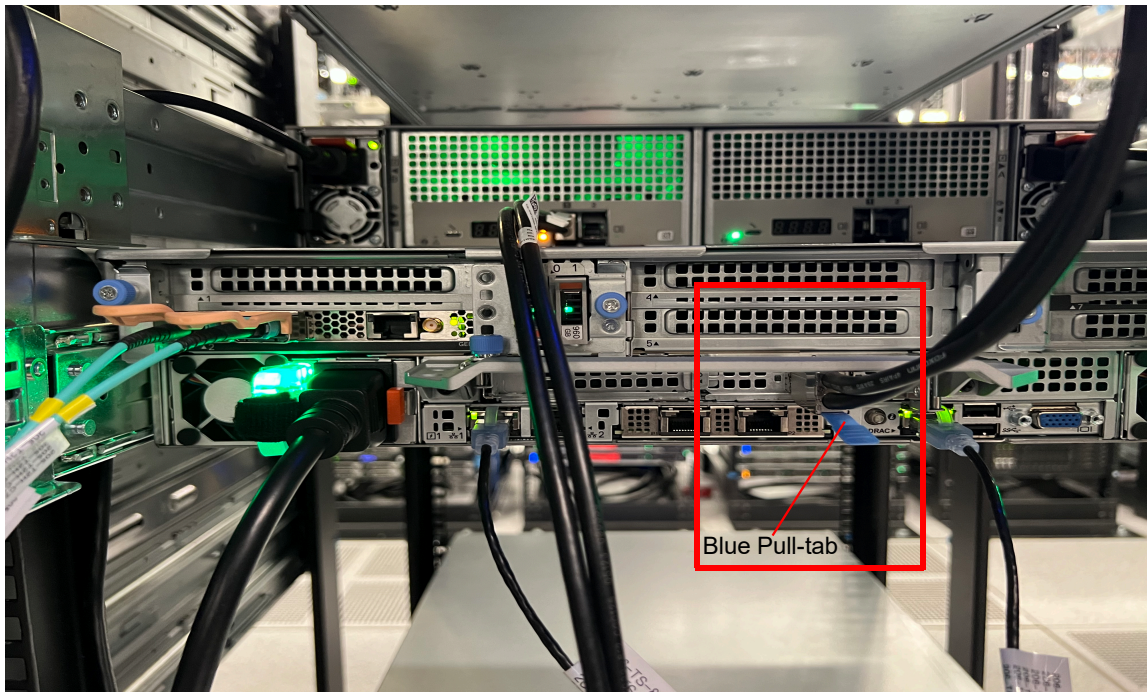
To connect TeraVault to LiveWire PowerCore 3300:

1. Make sure both TeraVault and LiveWire PowerCore 3300 are powered OFF.
2. Select a suitable location for both TeraVault and LiveWire PowerCore 3300. Both units can be installed on a flat surface, or mounted in a standard 19-inch equipment rack.
3. Run the SAS external cascading cable between the units so that the cable is not kinked, bent, or twisted. The SAS external cascading cable is included with TeraVault.



Note If you have multiple TeraVault boxes, and the system is disconnected for any reason, the cabling of the boxes needs to be exactly as it was before, otherwise the RAID won't be seen correctly. To assist you with the cabling, every TeraVault box is labeled with a number, and every TeraVault cable is labeled to the exact port it needs to get plugged into. See 'Connecting multiple TeraVault units' on page 25.

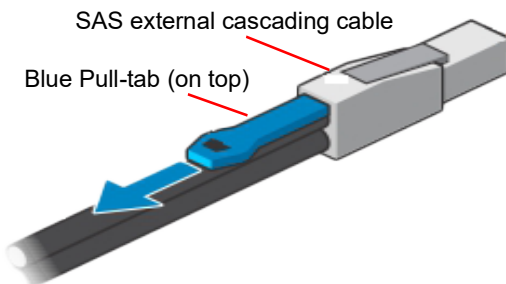
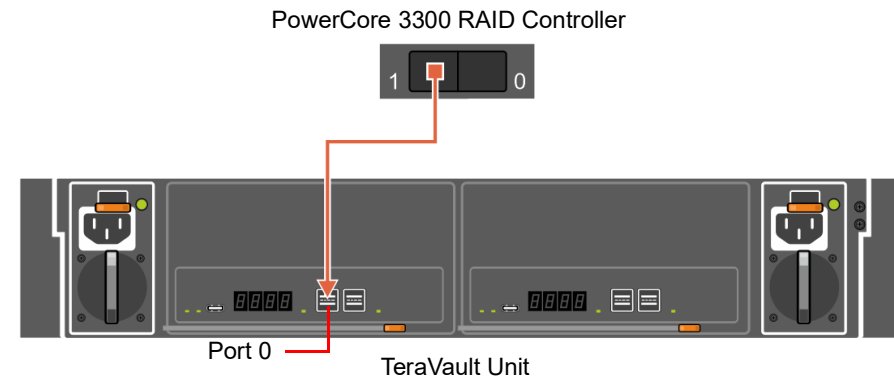
4. Facing the rear of LiveWire PowerCore, insert one connector of the SAS external cascading cable into the left RAID port (Port B/I) of the RAID controller on LiveWire PowerCore 3300 so that the release blue pull-tab is on the bottom as shown below.



Cable orientation when connected to PowerCore 3300 RAID card

Note It may be necessary to remove the handle on the rear of the appliance in order to connect the SAS external cascading cable into the left RAID port (Port B/I) of the RAID controller.

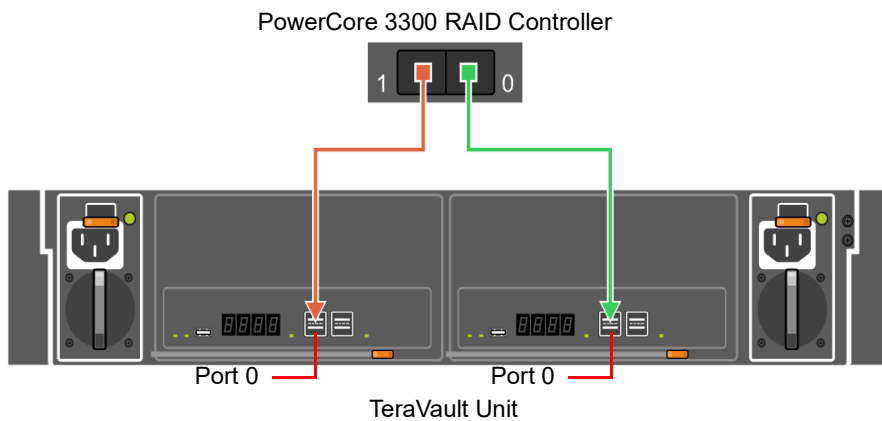
5. Facing the rear of TeraVault, insert the other end of the SAS external cascading cable into Port 0 on the TeraVault so that the release pull-tab is on the top.



Cable orientation when connected to TeraVault

Note Be certain the connectors are installed completely as it can look and feel as if the cable is secured without actually making a connection. Give the connector body a tug, then push it in again to be sure.

6. To set up a configuration with redundant paths, both ports on the LiveWire PowerCore 3300 RAID card must be cabled to the two ports of a single TeraVault unit as shown below. You will essentially repeat steps 1 - 5 above, but this time you will be connecting both ports on the TeraVault unit 'JBOD 1' to both ports on the LiveWire PowerCore 3300 RAID card (H840) as shown below.



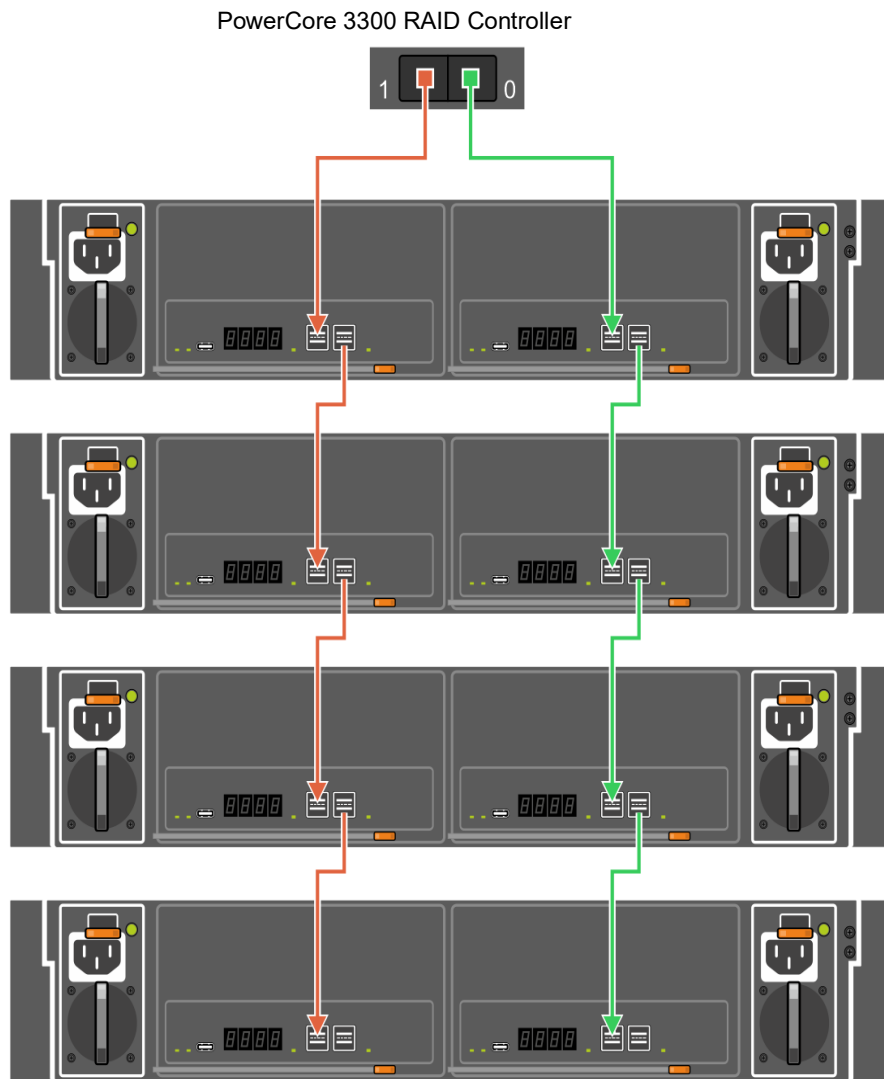
7. Turn on power to TeraVault by simply plugging the power cable into a power supply. The TeraVault must be powered on first (order matters). You may see brief bursts of LED activity as the expander in TeraVault scans the drives.
8. Turn on the power to LiveWire PowerCore. The system is ready for use as soon as the LiveWire PowerCore boot sequence completes.

Connecting multiple TeraVault units

When connecting multiple TeraVault (JBOD) units to LiveWire PowerCore 3300, it is important to note that each LiveWire PowerCore 3300 and TeraVault unit have LiveAction labels with matching serial numbers. Additionally, each TeraVault unit has a label on the front (designating JBOD 1, 2, 3, etc.), which is the order the units are daisy-chained to LiveWire PowerCore 3300 and each of the TeraVault units. Multiple SAS external cascading cables are included and are also labeled to guide you in connecting each of the units.

To connect multiple TeraVault units:

1. Locate the LiveAction label on each LiveWire PowerCore 3300 and TeraVault unit. Make sure the LiveAction serial numbers are the same on LiveWire PowerCore 3300 and each of the storage units.
2. Locate the first TeraVault unit labeled as 'JBOD 1' and also the SAS external cascading cable labeled 'HBA - Port 0.' Use the 'HBA - Port 0' cable and connect the TeraVault unit 'JBOD 1' to LiveWire PowerCore 3300 as described in 'Connecting TeraVault to LiveWire PowerCore 3300' on page 22. **Make sure the blue release pull-tab on the cable connected to the LiveWire PowerCore 3300 RAID card is on the bottom, while the pull-tab connected to the TeraVault JBOD is on the top.**
3. Locate the second TeraVault unit labeled as 'JBOD 2' and also the SAS external cascading cable labeled 'JBOD 1 - Port 1.' Use the 'JBOD 1 - Port 1' cable and connect this TeraVault unit to the previous TeraVault unit (JBOD 1). Make sure the release pull-tab on the cable is on the top.
4. Repeat Step 3 for any additional TeraVault units, making sure each successive 'JBOD' is connected to the previous 'JBOD' using the appropriate SAS external cascading cable.
5. To set up a configuration with redundant paths, both ports on the LiveWire PowerCore 3300 RAID card must be cabled to the ports of a single TeraVault unit as shown below. You will essentially repeat steps 1 - 4 above, but this time you will be connecting both ports on the TeraVault unit 'JBOD 1' to both ports on the LiveWire PowerCore 3300 RAID card.



Starting / shutting down LiveWire Core 1300/PowerCore 3300

To start LiveWire Core 1300/PowerCore 3300:

- Press the power button in the upper right corner on the front of the chassis.

To shutdown LiveWire Core 1300/PowerCore 3300:

- Click the actions link at the top of the configuration utility to display the Actions dialog, and then select Power Off option.
- SSH, or use a console connection to LiveWire and use the 'shutdown' command from the command prompt (*admin@livewire*):

```
shutdown -h now
```

Note You can also use the iDRAC interface to shutdown and start LiveWire Core 1300/PowerCore 3300. See 'Starting / Shutting down LiveWire' on page 61.

Attaching the front bezel

To attach the front bezel (LiveWire Core 1300/PowerCore only 3300):

- Attach the front bezel by inserting the locking hooks into the front chassis of LiveWire Core 1300/PowerCore 3300. The bezel should be centered between the two black tabs on the left and right of the chassis.

LiveWire Activation

Once LiveWire is installed, when you attempt to connect to it for the very first time, you must activate the product before it can be used. You can activate LiveWire either from logging directly into a web-based version of Omnipeek, or from the **Capture Engines Window** in Omnipeek.

Both an automatic and a manual method are available for activation. The automatic method is quick and useful if you have Internet access from the computer from where you are performing the activation. If Internet access is not available, the manual method is available; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

You will need to enter the following information to successfully activate LiveWire, so please have this information readily available:

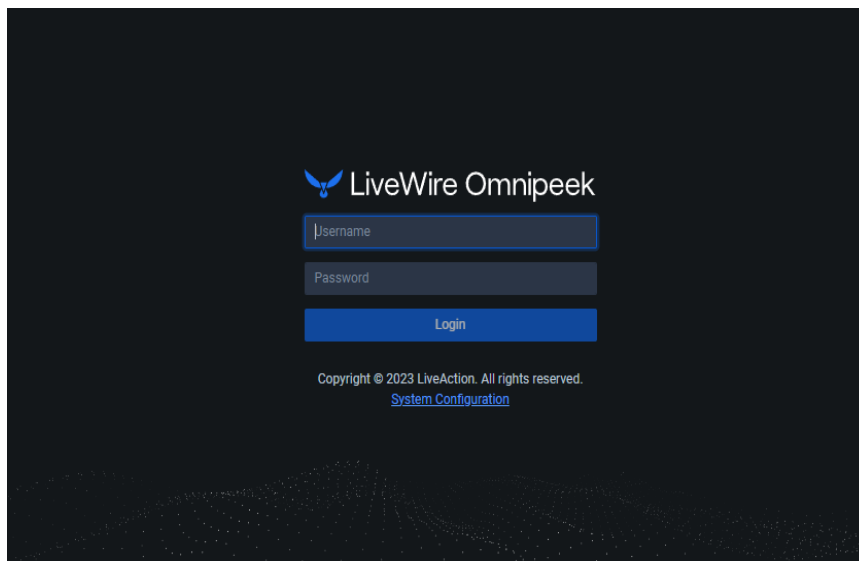
- IP address of LiveWire
- Product key
- User name
- Company name
- Email address
- Version number

Activation via Omnipeek Web

Note Activation via the web-based version of Omnipeek is not supported on an Internet Explorer web browser. Please use any web browser other than Internet Explorer to activate LiveWire via Omnipeek.

To activate LiveWire via Omnipeek:

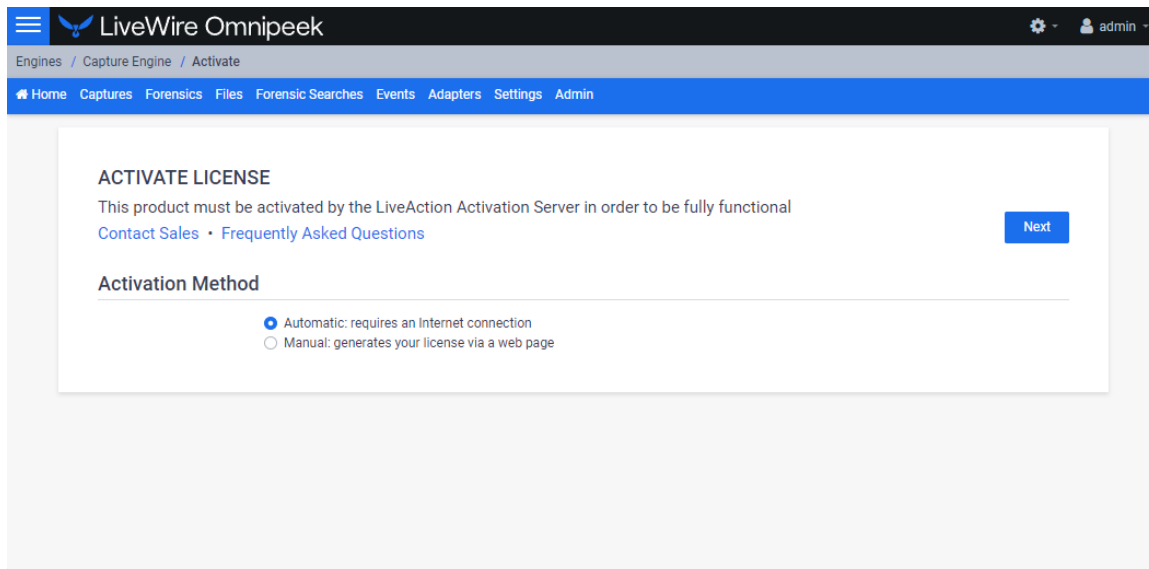
1. From your web browser, type the IP address of LiveWire into the URL field of the browser and press **Enter**. The Omnipeek login screen appears.



- *Username*: Type the username for LiveWire. The default is *admin*.
- *Password*: Type the password for LiveWire. The default is *admin*.

2. Type the *Username* and *Password* and click **Login**. The *Omnipeek Activation License* window appears.

Note You can also access the *Omnipeek Activation License* window by clicking *Update License* from the *Capture Engine Home* screen in Omnipeek.



3. If your client has an active Internet connection, select *Automatic* and click **Next**. The **Customer Information** window appears. Continue with Step 4 below.

ACTIVATE LICENSE

This product must be activated by the LiveAction Activation Server in order to be fully functional
[Contact Sales](#) • [Frequently Asked Questions](#)

Previous Next

Customer Information

NAME

COMPANY

EMAIL

PRODUCT KEY

Device serial number: 785Y422

- *NAME*: Type the user name of the customer.
- *COMPANY*: Type the company name.
- *EMAIL*: Type the email address of the customer.
- *PRODUCT KEY*: Type the product key.

If your client does not have an active Internet connection, or you are prevented from accessing the Internet using personal firewalls, or there are other network restrictions that may block automatic activations, select *Manual* and click **Next**. The **Manual Activation** window appears. Skip to Step 5 below.

Note The manual activation method is available for instances described above; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

ACTIVATE LICENSE

This product must be activated by the LiveAction Activation Server in order to be fully functional
[Contact Sales](#) • [Frequently Asked Questions](#)

Previous Next

Manual Activation

Follow this link to [activate](#) and fill out the form there.

You will need the following information:
 Locking code: *1ZZVZ8W95UM5LD

When you are finished and have a license file, enter the Product Key, click Choose License File below and then click Next.

PRODUCT KEY

Device serial number: 785Y422

LICENSE FILE

Note The **Locking code** displayed in the window above is required in Step 6 below. You can click the small icon next to the code to save it to the clipboard so you can paste it into the Locking Code field in Step 6 below.

4. Complete the Customer Information window and click **Next**. LiveWire is now activated and you can begin using the product. The activation process is complete.

Note If the automatic activation does not complete successfully, go back and select the manual activation process. Personal firewalls or other network restrictions may block automatic activations.

5. Click the *activate* link (https://mypeek.liveaction.com/activate_product.php) in the window. A web browser page opens that allows you to activate your LiveAction product and to obtain and download a license file. The license file is required to complete the manual activation.

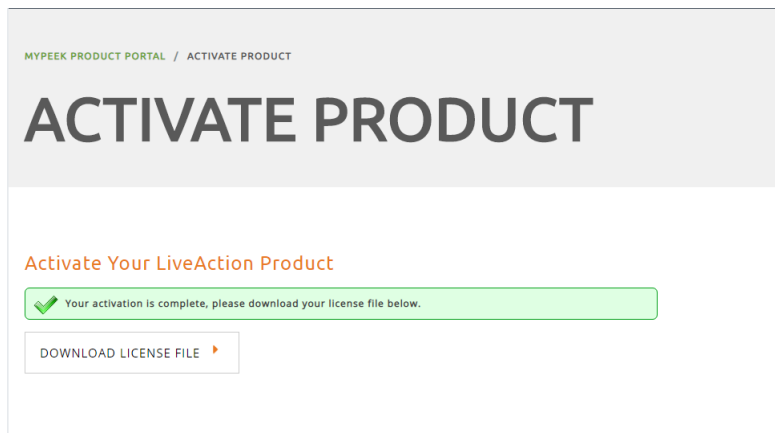
Activate Your LiveAction Product

Use this form to activate LiveAction software in instances where the machine you are installing on doesn't have an internet connection.

PLEASE NOTE: This form is only used to activate version 12.0 and later of our Omnipeek and Capture Engine products. If you have a version previous to 12.0, please go to <https://reg.savvius.com> to manually activate your product.

Version:	<input type="text" value="--"/> <input type="text" value="--"/>	Enter only two numbers, e.g. for 3.0.1, enter 3.0.
Product Key or Serial Number :	<input type="text"/>	
Locking Code:	<input type="text"/>	During installation of your product, this value will be displayed on your screen. Please enter it exactly as shown.
First Name:	<input type="text"/>	
Last Name:	<input type="text"/>	
Email Address:	<input type="text"/>	
Company:	<input type="text"/>	
<input type="button" value="ACTIVATE PRODUCT ▶"/>		

6. Complete the information on the activation page and click **ACTIVATE PRODUCT**. The following page appears once the activation is complete.



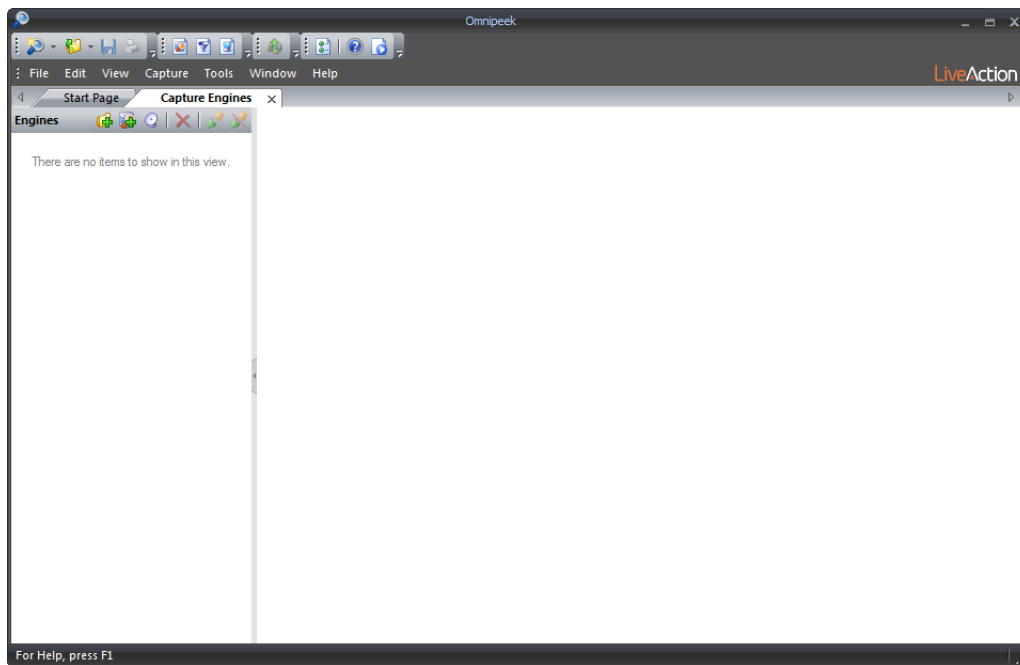
7. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in the following steps.
8. Return back to the **Manual Activation** window, and click **Choose License File**.
9. Navigate to the license file downloaded above and click **Open**.
10. Click **Next** in the **Manual Activation** window. LiveWire is now activated and you can begin using the product. The activation process is complete.

Activation via Omnippeek

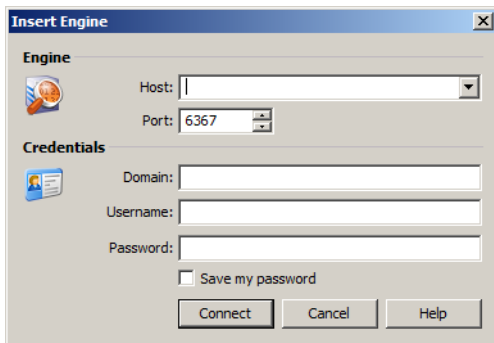
Note Activation of LiveWire via Omnippeek is supported on Omnippeek version 13.1 or higher.

To activate LiveWire via Omnippeek:

1. From the Omnippeek Start Page, click **View Capture Engines** to display the **Capture Engines** window.

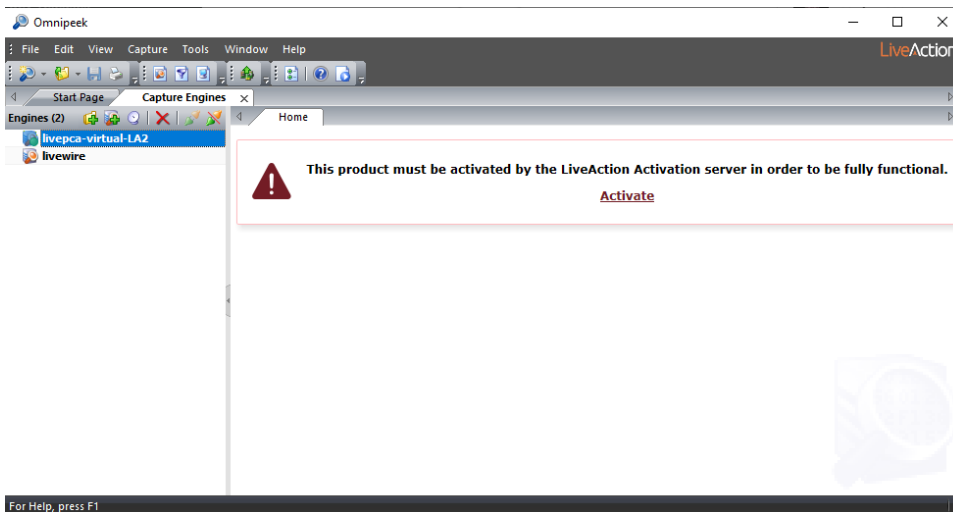


2. Click *Insert Engine* and complete the **Insert Engine** dialog.



- *Host*: Enter the IP address of LiveWire.
- *Port*: Enter the TCP/IP port used for communications. Port 6367 is the default for LiveWire.
- *Domain*: Type the Domain for login to LiveWire. If LiveWire is not a member of any Domain, leave this field blank.
- *Username*: Type the username for LiveWire. The default is *admin*.
- *Password*: Type the password for LiveWire. The default is *admin*.
- *Save my password*: Select this option to remember your password to connect to LiveWire.

3. Click **Connect** to connect to LiveWire. If LiveWire has not yet been activated, the activation message appears in the **Capture Engines** window.



4. Click **Activate LiveWire**. The **Activation Method** dialog appears.

Frequently Asked Questions.' There are two radio button options: 'Automatic: requires an Internet connection' (which is selected) and 'Manual: generates your license via a web page'. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'."/>

5. If your client has an active Internet connection, select *Automatic* and click **Next**. Otherwise, select *Manual* and click **Next**. The **Customer Information** dialog appears.

- *User Name*: Type the user name of the customer.
- *Company Name*: Type the company name.
- *Email*: Type the email address of the customer.
- *Serial Number or Product Key*: Type either the serial number or product key.

6. Complete the **Customer Information** dialog and click **Next**. If you selected the *Automatic* activation, LiveWire is now activated and you can begin using the product. The activation process is complete.

If you selected the *Manual* activation, the **Manual Activation** dialog appears. You will need to continue with the remaining steps.

Note The manual activation method is available for instances when a computer does not have Internet access; however, you will need to go to a computer that does have Internet access in order to download a License file that is required to complete the manual activation.

Note The *Product Key*, and also the *Locking Code* displayed in the **Manual Activation** dialog are required in the next step. You can cut and paste this information from the **Manual Activation** dialog when required in the next step.

- Click the *activate product* link (https://mypeek.liveaction.com/activate_product.php) in the dialog. A web browser page opens that allows you to activate your LiveAction product and to obtain and download a license file. The license file is required to complete the manual activation.

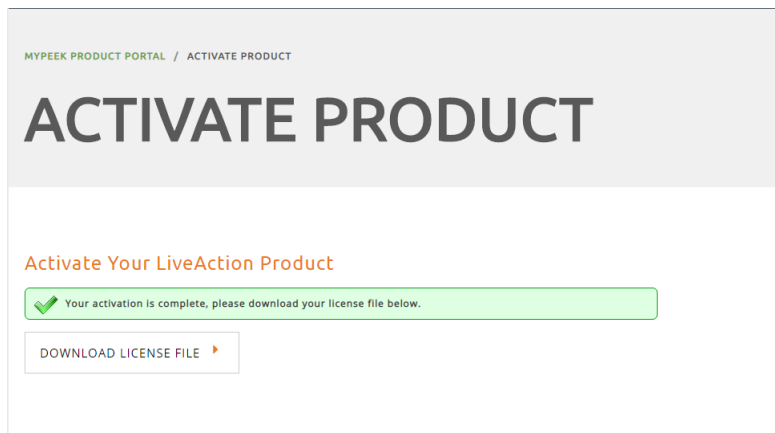
Activate Your LiveAction Product

Use this form to activate LiveAction software in instances where the machine you are installing on doesn't have an internet connection.

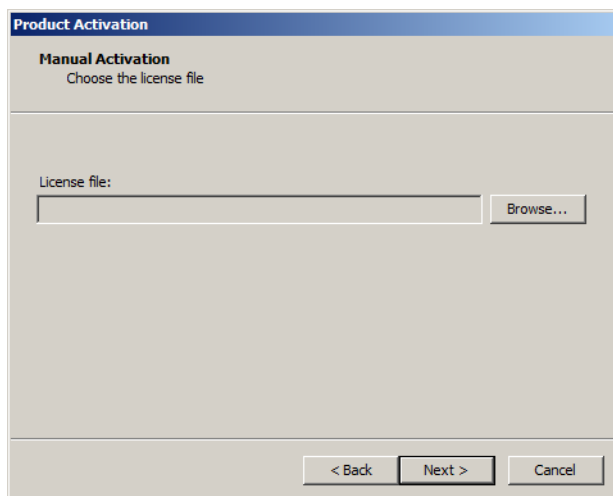
PLEASE NOTE: This form is only used to activate version 12.0 and later of our Omnippeek and Capture Engine products. If you have a version previous to 12.0, please go to <https://reg.savvius.com> to manually activate your product.

Version:	<input type="text" value="--"/> <input type="text" value="--"/>	Enter only two numbers, e.g. for 3.0.1, enter 3.0.
Product Key or Serial Number :	<input type="text"/>	
Locking Code:	<input type="text"/>	During installation of your product, this value will be displayed on your screen. Please enter it exactly as shown.
First Name:	<input type="text"/>	
Last Name:	<input type="text"/>	
Email Address:	<input type="text"/>	
Company:	<input type="text"/>	
<input type="button" value="ACTIVATE PRODUCT"/>		

- Complete the information on the activation page and click **ACTIVATE PRODUCT**. The following page appears once the activation is complete.



9. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in Step 11 below.
10. Return to the **Omnipeek Product Activation** dialog, and click **Next**. The **Manual Activation/Choose the license file** dialog appears.



11. Browse to the license file that was downloaded above and click **Next**. LiveWire is now activated and you can begin using the product. The activation process is complete.

Contacting LiveAction support

Please contact LiveAction support at <https://www.liveaction.com/support/technical-support/> if you have any questions about the installation and use of LiveWire.

An RMA (Return Material Authorization) number must be obtained from LiveAction before returning hardware. Please contact LiveAction technical support at <https://www.liveaction.com/support/technical-support/> for instructions.

Configuring LiveWire

In this chapter:

<i>Logging-in to LiveWire command line</i>	<i>37</i>
<i>Using the LiveAdmin utility.</i>	<i>37</i>
<i>Configuring network settings by command script</i>	<i>52</i>
<i>Using LiveWire with Omnippeek</i>	<i>53</i>
<i>Integrated Remote Access Controller (iDRAC)</i>	<i>54</i>

Logging-in to LiveWire command line

You can log into the LiveWire command line in one of five ways:

- Remotely, using remote SSH software such as *Putty*
- Remotely, using the Integrated Remote Access Controller (iDRAC) firmware and hardware built into LiveWire. See 'Integrated Remote Access Controller (iDRAC)' on page 54. (LiveWire Core/PowerCore only)
- Locally, by connecting a monitor, mouse and keyboard to LiveWire (LiveWire Core/PowerCore only)
- Locally, by using a console cable connected from the USB port on your PC/laptop to the Console Port of LiveWire Edge. See 'Connect to LiveWire Edge 1515 via the Console port' on page 19. (LiveWire Edge only)
- Locally, by using a micro-AB interface cable for iDRAC management (LiveWire Core/PowerCore only). See 'Accessing the iDRAC interface over the USB port' on page 62.

The first time you log into LiveWire, use the following as your username and password:

username: *admin*

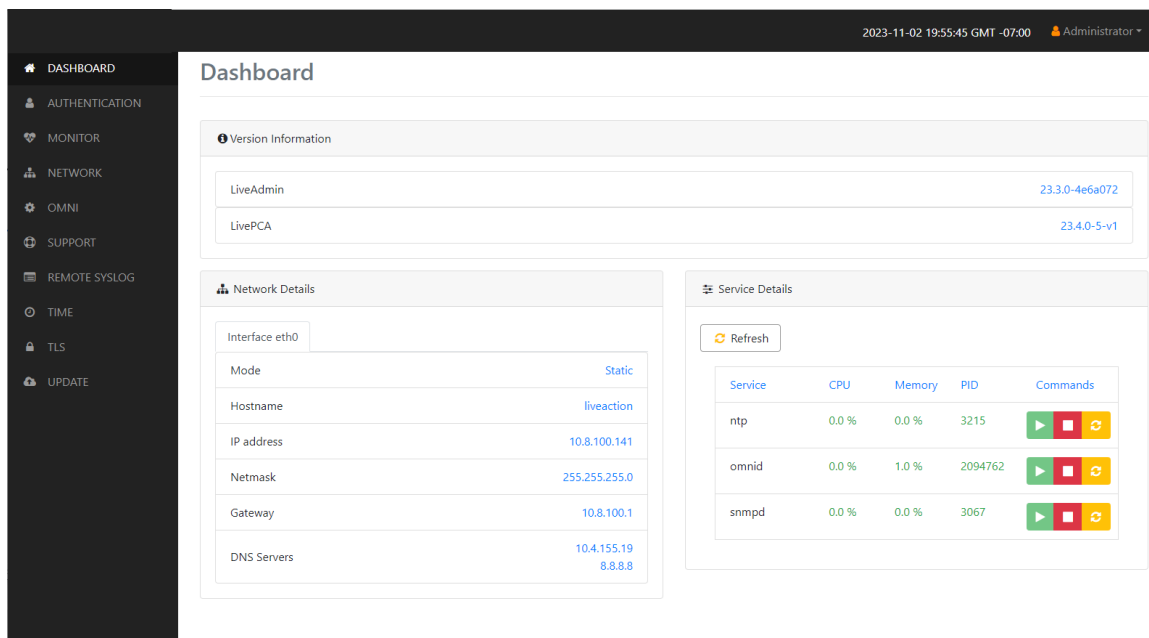
password: *admin*

After you have logged into LiveWire for the first time, you can then change your password and add users and privileges.

Note For security reasons, we strongly recommend changing the default password.

Using the LiveAdmin utility

The LiveAdmin utility on LiveWire lets you view and configure a variety of settings from the LiveAdmin views in the left-hand navigation pane of the utility. To learn more about each of the LiveAdmin views, go to the appropriate section below:



- *Dashboard*: The *Dashboard* view provides you with some very basic information about the system. See 'Dashboard' on page 39.
- *Authentication*: The *Authentication* view lets you change the password for LiveWire. See 'Authentication' on page 40.
- *Monitor*: The *Monitor* view displays the health of the overall system. See 'Monitor' on page 41.

- *Network*: The *Network* view lets you configure the primary network interfaces network settings and the hostname of the system. See 'Network' on page 42.
- *Omni*: The *Omni* view lets you configure *Centralized Management*, *Factory Reset*, *Backup*, *Restore*, *SFTP*, and *SNMP* for the appliance. See 'Omni' on page 44.
- *Support*: The *Support* view lets you download logs from the system that would be helpful in troubleshooting issues. See 'Support' on page 49.
- *Remote Syslog*: The *Remote Syslog* view lets you configure a remote syslog server that receives all system logs. See 'Remote Syslog' on page 50.
- *Time*: The *Time* view lets you configure the system's Timezone and NTP servers. See 'Time' on page 50.
- *TLS*: The *TLS* view lets you change the self-signed certificates that LiveAdmin and Omnippeek use for HTTPS. See 'TLS' on page 51.
- *Update*: The *Update* view lets you update the appliance using a software update package. See 'Update' on page 51.
- *Administrator*: The *Administrator* context menu in the upper right lets you restart LiveWire, power off LiveWire or log out from the LiveAdmin utility. See 'Restart and power off' on page 52.

Important! LiveWire comes pre-configured to obtain its IP address via DHCP. The IP address is required to configure LiveWire, as described below.

Note If an IP address is not assigned to LiveWire by the DHCP server within two minutes of being connected to the network, LiveWire defaults to a static address of 192.168.1.21.

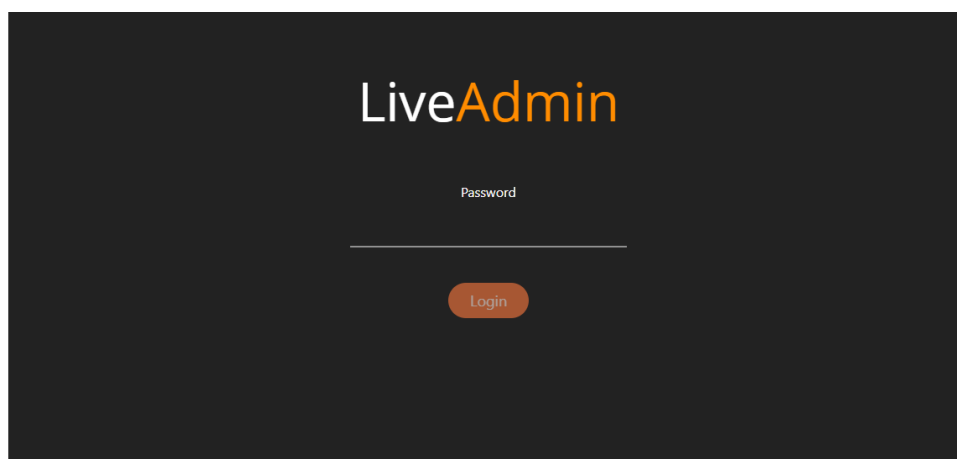
Login

To log into the LiveAdmin utility:

1. **LiveWire Core/PowerCore**: Connect LiveWire Core/PowerCore to your network router or switch with an Ethernet cable.

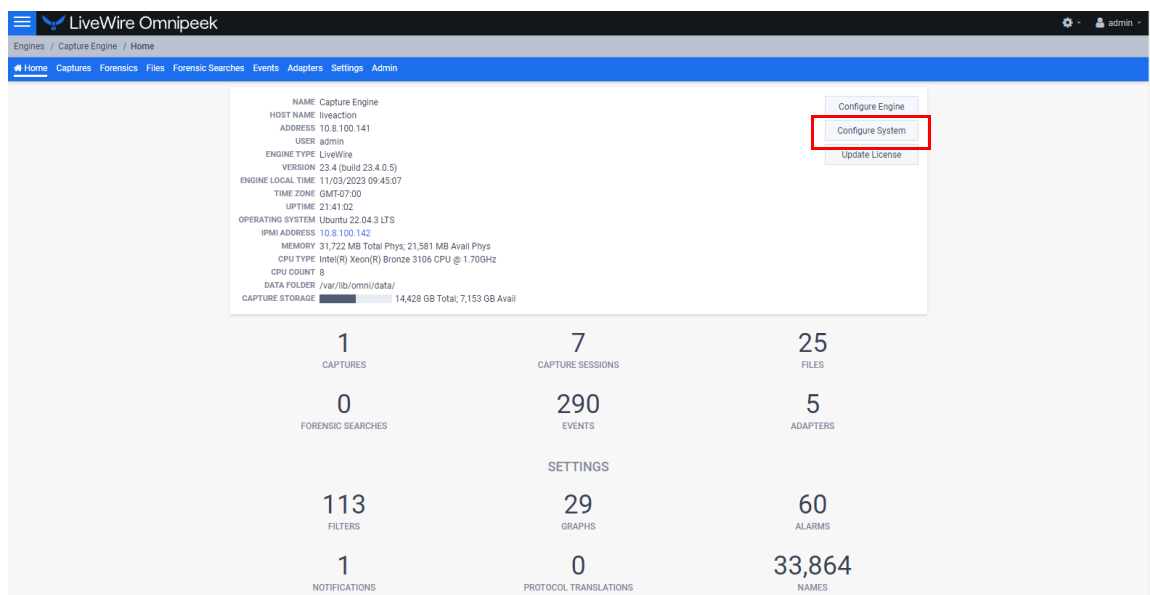
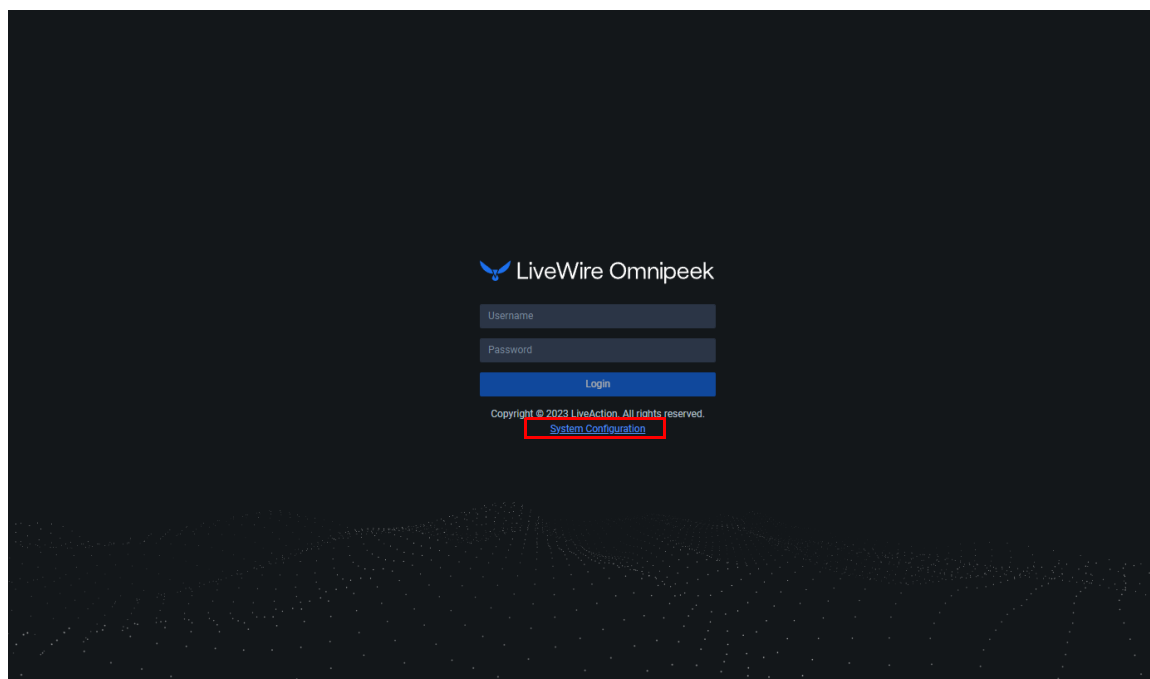
LiveWire Edge: Connect the '0 MGMT' port on LiveWire Edge to your network router or switch with an Ethernet cable.

2. From a browser window on a computer connected to the same network as LiveWire, enter the IP address for LiveWire in the URL box as `<IP address>:8443` (e.g., 192.168.1.21:8443). The LiveAdmin Login screen appears.



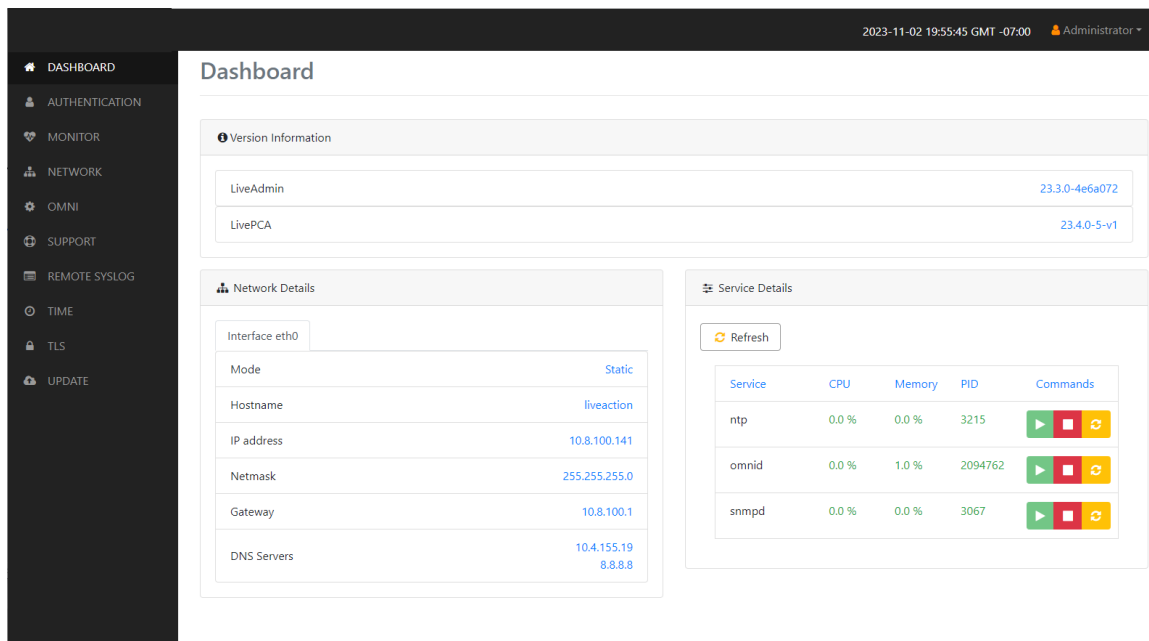
3. Enter the default password 'admin' and click **Login**.

Note If you are using LiveWire Omnippeek, you can also access the LiveAdmin Login screen by clicking *System Configuration* from either the Omnippeek Login screen, or by clicking *Configure System* from within Omnippeek itself.



Dashboard

The *Dashboard* view provides you with some very basic information about the system.



- *Version Information:* This section displays the version numbers of the LiveAdmin utility and the software on the LiveAction appliance.
 - *LiveAdmin:* Displays the version number of the LiveAdmin utility
 - *LivePCA:* Displays the version number of the software installed on the LiveAction appliance.
- *Network Details:* This section displays the management interface details and the system hostname. The management interface is defined from the Network view in LiveAdmin. See 'Network' on page 42.
- *Service Details:* This section lists a set of services you are able to monitor. This has currently been limited to the omnid process only, although additional services could easily be added:
 - *Refresh:* Click to update the view
 - *Service:* Displays the name of the service
 - *CPU:* Displays the amount of CPU the service is using
 - *Memory:* Displays the amount of memory the service is using
 - *PID:* Displays the Process ID of the service
 - *Commands:*
 - Start* - Click to start the service and can only be triggered if the service is stopped.
 - Stop* - Click to stop the service and can only be triggered if the service is running.
 - Restart* - Click to restart the service and can only be triggered if the service is running.

Authentication

The *Authentication* view lets you change the password for LiveWire.

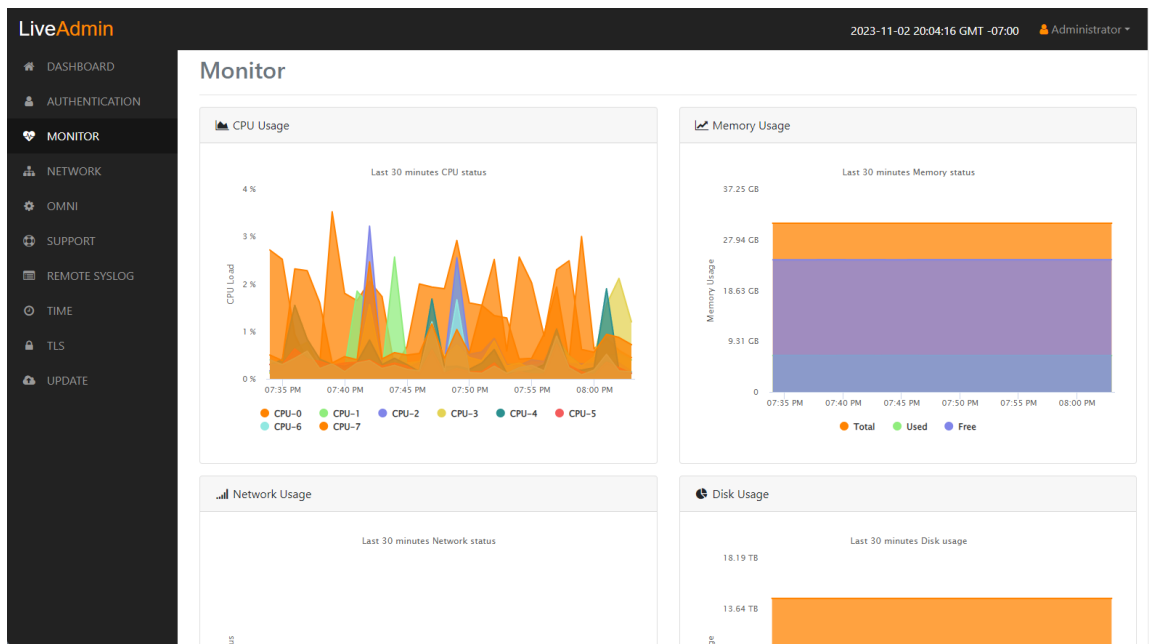
The screenshot shows the LiveAdmin interface with the 'Authentication' section selected in the sidebar. The main content area is titled 'Authentication' and contains a 'Change OS Admin Password' form. The form has a section for 'Password Requirements' with six red error messages: 'Must have 5 different characters than the last password!', 'Must be at least 6 characters!', 'Must contain at least 1 number!', 'Must contain at least 1 uppercase character!', 'Must contain at least 1 lowercase character!', and 'Must contain at least 1 special character!'. Below these are three input fields: 'Current Password*', 'New Password*', and 'Confirm Password*'. Each field has a placeholder text: 'Current Password', 'New Password', and 'Confirm password' respectively. A green 'Update' button is located at the bottom left of the form.

- *Current Password*: Enter the current password for LiveWire. The default is *admin*.
- *New Password*: Enter the new password for LiveWire. The new password must meet the following requirements:
 - Must have 5 different characters than the last password.
 - Must be at least 6 characters.
 - Must contain at least 1 number
 - Must contain at least 1 uppercase character.
 - Must contain at least 1 lowercase character.
 - Must contain at least 1 special character.
- *Confirm Password*: Enter the new password to confirm the password.
- *Update*: Click to change the password.

Note Make sure to note the *Password* that you configure.

Monitor

The *Monitor* view displays the health of the overall system. The view is broken up into four usage charts and one interface statistics table.



- *CPU Usage:* This chart displays the current usage of individual CPUs on the system. Click the CPU label in the legend to enable/disable its data displayed in the chart.
- *Memory Usage:* This chart displays the current amount of memory being consumed on the system. Click the *Total*, *Used*, or *Free* labels in the legend to enable/disable which data to display in the chart.
- *Network Usage:* This chart displays the current throughput of the network interfaces. Click the labels in the legend to enable/disable which data to display in the chart.
- *Disk Usage:* This chart displays the current amount of space being used by the Data and Metadata volumes. Click the *Total*, *Used*, or *Free* labels in the legend to enable/disable which data to display in the chart.
- *Interface Statistics:* This table displays the statistics of the primary management interface. To update the statistics click **Refresh**.

Network

The *Network* view lets you configure the primary network interface network settings and the hostname of the system. You can configure either DHCP or static network settings.

Note Changing the network settings will restart the omni service.

The screenshot shows the 'Network' configuration page in the LiveAdmin interface. The left sidebar contains navigation links: DASHBOARD, AUTHENTICATION, MONITOR, NETWORK (selected), OMNI, SUPPORT, REMOTE SYSLOG, TIME, TLS, and UPDATE. The top right shows the date and time '2023-11-02 20:07:30 GMT -07:00' and the user 'Administrator'. The main content area is titled 'Network' and contains the following fields:

- Hostname***: A text input field containing 'liveaction'.
- Network Mode***: A dropdown menu set to 'Static'.
- IP Address***: A text input field containing '10.8.100.141'.
- Netmask***: A text input field containing '255.255.255.0'.
- Gateway***: A text input field containing '10.8.100.1'.
- DNS**: A section with an 'Add DNS server' button (plus icon) and two existing entries: '10.4.155.19' and '8.8.8.8', each with a red 'x' icon for deletion.
- Submit**: A green button at the bottom.

- **Hostname**: Enter a name for LiveWire. A unique device name allows for easy identification of data sources. The hostname can only contain alphanumeric characters and hyphens, and cannot be longer than 255 characters.
- **Network Mode**: This setting lets you to specify whether LiveWire uses a DHCP or static setting for its IP address. If *Static* is selected, then *IP Address*, *Netmask*, *Gateway*, and *DNS* settings can be configured for LiveWire. If *DHCP* is selected, then LiveWire is configured by a DHCP server.

Important! LiveWire is pre-configured to obtain an IP address automatically from a DHCP server; however, we strongly recommend the use of a static IP address for LiveWire. If DHCP is selected as the *IP Assignment*, and if the address should change on a new DHCP lease, then the user must look up the new IP address assigned to LiveWire. To help you look up the IP address, the MAC Address of LiveWire is displayed as the *Ethernet Address*.

Note If *DHCP* is selected, you have approximately two minutes to connect LiveWire to your network in order for the DHCP server to assign an IP address. If an IP address is not assigned to LiveWire by the DHCP server within two minutes of being connected to the network, LiveWire defaults to a static address of 192.168.1.21. Please make sure LiveWire is connected to your network within the two minute time period from the time you click **Apply**. If you reboot LiveWire, the two minute clock is also reset.

- **IP Address**: This setting lets you specify the IP address that you are assigning to LiveWire.
- **Netmask**: A Netmask, combined with the IP address, defines the network associated with LiveWire.
- **Gateway**: Also known as 'Default Gateway.' When LiveWire does not have an IP route for the destination, the IP packet is sent to this address as it does not know how to direct it locally. Only a single default gateway can be defined.
- **DNS**: This is the domain name server. A Domain Name Server translates domain names (e.g., www.liveaction.com) into an IP address. To add a DNS server, enter the address of the server, and click the plus (+) icon. Multiple DNS name servers can be defined. You can also edit or delete any defined DNS servers.

Configure DHCP

To configure a DHCP IP address:

1. Enter a hostname in the *Hostname* field.
2. From the *Network Mode* list, select *DHCP*.
3. Click **Submit**.

Configure Static

To configure a static IP address:

1. Enter a hostname in the *Hostname* field.
2. From the *Network Mode* list, select *Static*.
3. Enter a valid IP address in the *IP Address* field.
4. Enter a valid netmask in the *Netmask* field.
5. Enter a valid default gateway in the *Gateway* field.
6. (Optional) Enter a valid DNS server in the *Add DNS server* field and click the plus (+) button.
7. Click **Submit**.

Note You will lose connection to LiveWire if you configured a new static address in *IP Address* above.

Omni

The *Omni* view lets you configure *Centralized Management*, *Factory Reset*, *Backup*, *Restore*, *SFTP*, and *SNMP* for the appliance.

LiveAdmin Administrator

- DASHBOARD
- AUTHENTICATION
- MONITOR
- NETWORK
- OMNI**
- SUPPORT
- REMOTE SYSLOG
- TIME
- TLS
- UPDATE

Omni

- Centralized Management**
- Factory Reset
- Backup
- Restore
- SFTP
- SNMP

Centralized Management Settings

Centralized Management is the preferred way to manage and configure multiple LiveAction appliances. In order to enable centralized management select the checkbox below. Once enabled, changes can still be made locally but configuration changes made in the centralized management console will supersede local changes. For instructions on how to register and manage devices from the centralized console please visit [MyPeek](#).

☒ Enable Centralized Management

HTTP Proxy Configuration

Hostname

Port

Username

Password

Confirm Password

Centralized Management

Centralized management is the preferred way to manage and configure multiple LiveAction appliances. In order to enable centralized management select the *Centralized Management* check box and configure the *HTTP Proxy Configuration* settings. Once enabled, changes can still be made locally but configuration changes made in the centralized management console supersedes local changes. For instructions on how to register and manage devices from the centralized console please visit [MyPeek](#).

The screenshot shows the LiveAdmin interface with the 'Omni' section selected. Under 'Centralized Management', the 'Enable Centralized Management' checkbox is checked and highlighted with a red box. Below this, the 'HTTP Proxy Configuration' section contains several input fields: 'Hostname' (with a dropdown set to 'https' and a text field containing 'hostname'), 'Port' (with a text field containing '443'), 'Username', 'Password', and 'Confirm Password'. Each of these fields has a corresponding input box. At the bottom of the configuration section is a green 'Apply' button.

- *Enable Centralized Management.* Select this check box to enable LiveWire Grid to manage and configure LiveWire from the cloud. Refer to the [LiveWire Grid Quick Guide](#) for instructions on using LiveWire Grid to manage and configure LiveAction appliances.

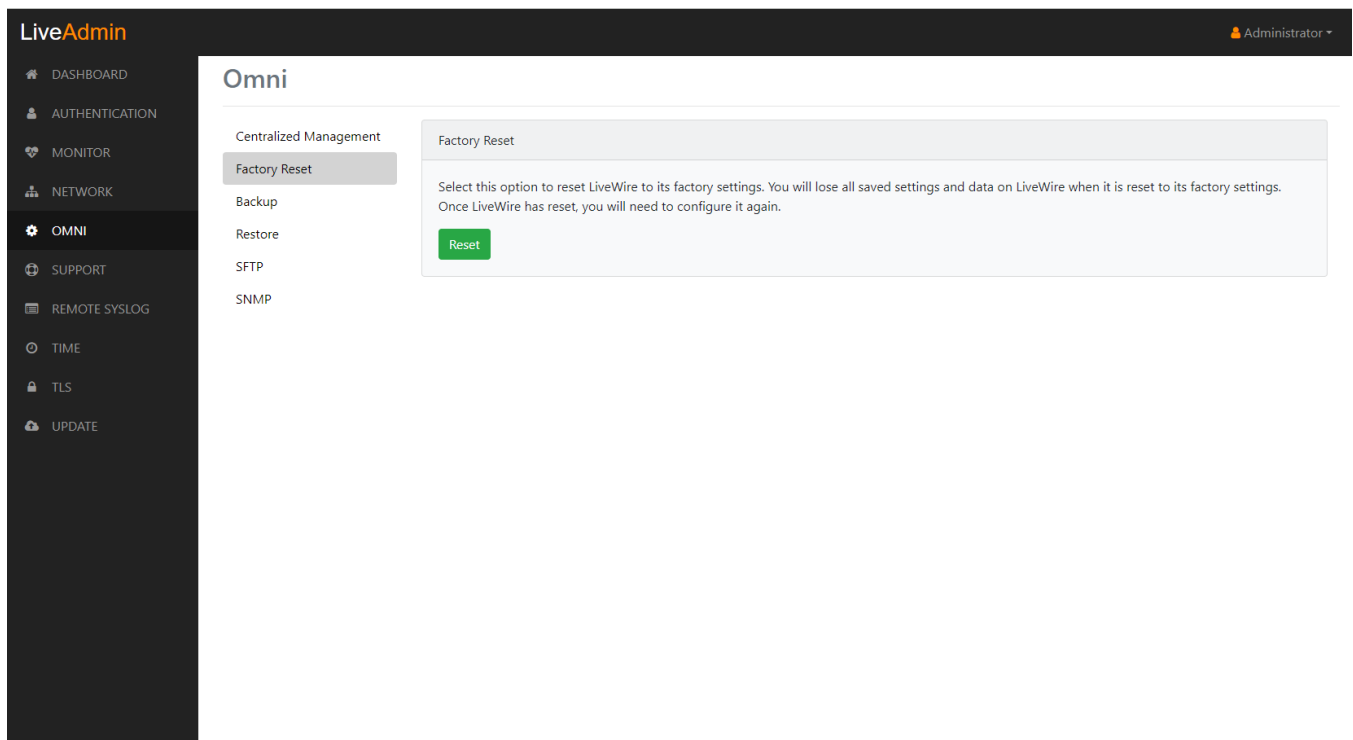
Note When Centralized Management is enabled, you can make local changes to LiveWire using the LiveAdmin utility; however, changes made with Grid will overwrite any local changes made with the LiveAdmin utility.

Factory reset

Factory reset allows you to reset the LiveAction software to factory defaults on LiveWire.

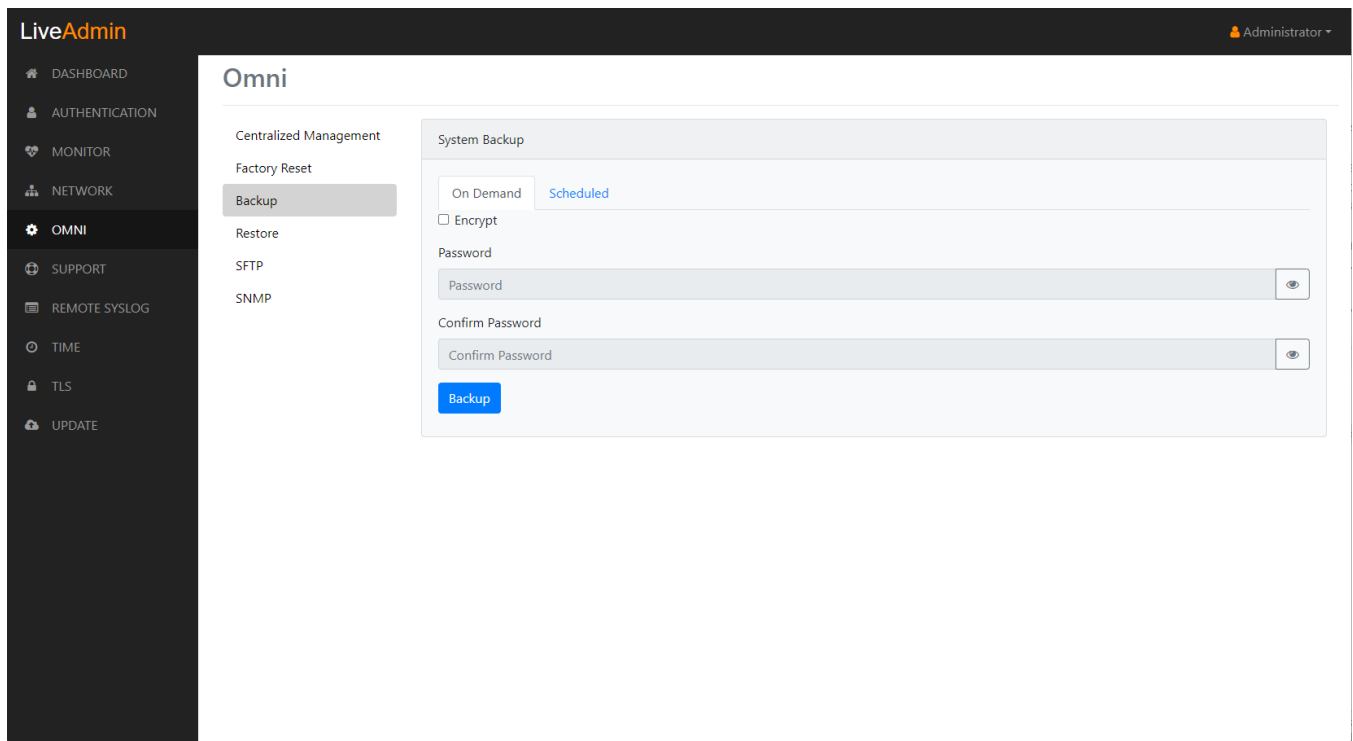
- *Factory Reset.* Click **Reset** to reset the LiveAction software.

CAUTION! All data captured by the LiveAction software will be deleted. All configuration settings will revert to their factory defaults, including the IP address of the management port.



Backup

Backup allows you to back up all the system data on LiveWire to a back up file that you can restore at a later time.



On Demand

- *Encrypt*: Select this data to encrypt the system backup. You will need to enter a password that is required to restore the backup to LiveWire.
- *Password*: Type a password for the backup.

- *Confirm Password:* Type the password again to confirm the password.
- *Backup:* Click to start the backup.

Scheduled

- *Backup Type:* Select either an *SFTP* or *Cloud* backup type.
- *History:* Displays the history for previous SFTP backups.

Restore

Restore allows you to restore to LiveWire a backup that was previously performed on LiveWire. To perform a restore, you will need the backup file you want to restore from and any password associated with the backup.

- *Application settings:* Select this option to restore the appliance application settings and customizations.
- *Application and system settings:* Select this option to restore the appliance, application settings, and customizations.
- *Backup File:* Click **Browse** to select the backup file from which you are restoring.
- *Encryption Password:* Enter the password for the backup from which you are restoring.
- *Restore:* Click to start the restore.

SFTP

SFTP allows you to configure an SFTP (Secure FTP) server for backing up the application and system settings on LiveWire.

LiveAdmin Administrator ▾

Omni

Centralized Management
Factory Reset
Backup
Restore
SFTP
SNMP

SFTP Settings

SFTP Server*
127.0.0.1

Port*
22

Username*
Username

Password*
Password

Directory*
/data/backup

Save Test

- *SFTP Server*: Type the IP address of the SFTP server.
- *Port*: Type the port used for the SFTP Server.
- *Username*: Type a username.
- *Password*: Type a password for the SFTP server.
- *Directory*: Type the directory where backups are saved on the SFTP server.

SNMP

SNMP settings allow you to configure the SNMP Credentials *Authentication Key* and *Privacy Key* for LiveWire.

- *Authorization Key*: Type a new *Authorization Key* to change it from the default *Authorization Key* displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 74.
- *Privacy Key*: Type a new *Privacy Key* to change it from the default *Privacy Key* displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 74.
- *Save*: Click to apply the SNMP credentials to the device.

Support

The *Support* view lets you generate a diagnostic and support data report from LiveWire that would be helpful in troubleshooting issues.

- *Generate Report*: Click to generate a diagnostic and support data report.

Remote Syslog

The *Remote Syslog* view lets you configure a remote syslog server that receives all system logs.

- *Server*: Enter the IP address of the remote syslog server.
- *Port*: Enter the Port address of the remote syslog server.
- *Protocol*: Select either TCP or UDP for the protocol.
- *Save*: Click to save the *Remote Syslog* settings.

Time

The *Time Configuration* view lets you configure the system's Timezone and NTP servers.

- *Timezone*: The Timezone setting lets you specify the physical location of LiveWire. Select from the list the location closest to your LiveWire.

- **NTP Servers:** The NTP (Network Time Protocol) server setting displays the NTP servers used to synchronize the clocks of computers over a network. Many features of LiveWire require accurate timestamps to properly analyze data.

To synchronize the LiveWire clock, you can specify the IP address of an NTP server located on either the local network or Internet. Once an NTP server is added to LiveWire, you can update (edit) or delete a server displayed in the list.

- **Add Server:** Click to add a new NTP server to the list. Enter the IP address of the Server, and optional Key Type (MD5, SHA1) and Key, and click **Save** (green check) to save the server to the list. Multiple NTP servers can be defined.
- **Submit:** Click to save your changes to LiveWire.

TLS

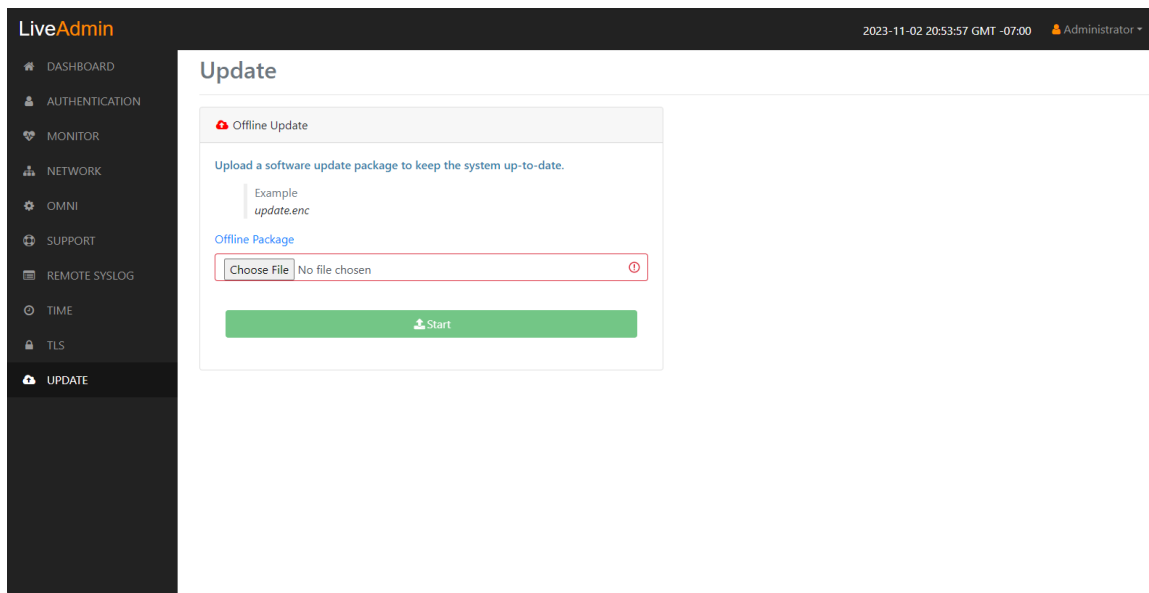
The *TLS Certificates* view lets you change the self-signed certificates that Omnippeek and LiveAdmin use for HTTPS.

- **Public Certificate* (PEM):** Click **Choose File** to browse and select your Public Certificate file. Click the information icon to display an example of the file.
- **Private Key* (RSA unencrypted):** Click **Choose File** to browse and select your Private Key file. Click the information icon to display an example of the file.
- **CA Certificate (PEM optional):** Click **Choose File** to browse and select your CA Certificate file. Click the information icon to display an example of the file.
- **Upload:** Click to upload the selected files to LiveWire.

Update

The Update view lets you update the appliance using the software update package.

Note Updating the software will cause the system to reboot.



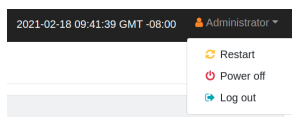
To update the software:

1. Download the latest software update package to your system.
2. Click **Choose File** and select the software update package.
3. Click **Start** to upload the package and begin the update process.

Once the update process is complete, the system restarts. A restart message is broadcast to all users connected to the appliance.

Restart and power off

The *Administrator* context menu at the top of the LiveAdmin utility has options that let you restart and power off LiveWire and log out from the utility.



To restart LiveWire:

1. Click the *Administrator* context menu and select **Restart**.
2. Click **Yes, restart now!** to confirm the restart.

To power off LiveWire:

1. Click the *Administrator* context menu and select **Power off**.
2. Click **Power Off** to confirm you want to power off.

To log out of the LiveAdmin utility:

- Click the *Administrator* context menu and select **Log out**.

Configuring network settings by command script

You can configure LiveWire network settings by using the 'omni-interface' command script from the 'root' user command prompt (*root@LiveWire*). To get to the 'root' user command prompt, enter the following command from the command prompt and enter '**admin**' as the password when prompted:

```
#sudo su
```

Note There are numerous ways to log into the LiveWire command prompt for LiveWire. See 'Logging-in to LiveWire command line' on page 37.

Here are the commands to configure the network settings from the command prompt:

Usage: *omni-interface [options]*

Example (IP configuration): *omni-interface -a eth0 -s -r x.x.x.x -m x.x.x.x -g x.x.x.x -d x.x.x.x*

options:

<i>-a, --adapter</i>	adapter to modify
<i>-f, --wifi</i>	enable or disable Remote AP Capture capability [on off]
<i>-c, --dhcp</i>	configure dhcp
<i>-s, --static</i>	configure static
<i>-l, --manual</i>	configure manual
<i>-r, --address</i>	static adapter address
<i>-m, --netmask</i>	static adapter netmask
<i>-b, --broadcast</i>	static adapter broadcast address
<i>-w, --network</i>	static adapter network address
<i>-g, --gateway</i>	static adapter gateway address
<i>-h, --hwaddress</i>	static adapter mac address
<i>-d, --dns</i>	static dns servers (comma separated)

Important! The Ethernet ports can be configured to obtain an IP address automatically from a DHCP server by specifying 'dhcp' instead of 'static' settings; however, we strongly recommend the use of static IP addresses for the Ethernet ports. If DHCP is used, and if the address should change on a new DHCP lease, then the user must restart the Capture Engine service to see the new IP addresses in the 'Adapters' capture options in Omnippeek.

Additionally, if you specify 'dhcp' instead of 'static' settings, and there is no DHCP server available, you must allow the command to time-out.

Using LiveWire with Omnippeek

Any computer on the network with the Omnippeek Windows software installed can now access the Capture Engine running on LiveWire. From the **Capture Engine** window in Omnippeek, you can configure, control, and view the results of the Capture Engine remote captures.

For more information on how to view and analyze remote captures from within the Omnippeek console, please see 'Using Capture Engines with Omnippeek' on page 115, and also the *Omnipeek User Guide* or Omnippeek online help.

Integrated Remote Access Controller (iDRAC)

The Integrated Remote Access Controller (iDRAC) firmware and hardware built into LiveWire (LiveWire Core/PowerCore only) lets you remotely access LiveWire as if you were in the same room as the LiveWire. Using an Internet browser, you can easily perform tasks such as accessing a remote console, reimaging LiveWire, rebooting, shutting down, and starting LiveWire (even if LiveWire is off). See also XXX for LiveWire StorageCore.

iDRAC and network security

iDRAC is a powerful tool for performing various tasks remotely on LiveWire; however, there are potential network security vulnerabilities when using iDRAC.

Below are some suggestions to ensure that vulnerabilities through iDRAC are minimized:

- **Restrict iDRAC to Internal Networks:** Restrict iDRAC traffic to trusted internal networks. Traffic from iDRAC (usually UDP port 623) should be restricted to a management VLAN segment with strong network controls. Scan for iDRAC usage outside of the trusted network, and monitor the trusted network for abnormal activity.
- **Utilize Strong Passwords:** Make sure the iDRAC password on LiveWire is set to a strong, unique password. See 'Changing the default password' on page 56.
- **Encrypt Traffic:** Enable encryption on iDRAC, if possible. For example, use HTTPS in your web browser's URL location field when connecting to iDRAC (e.g., 'https://xxx.xxx.xxx.xxx').

Setting the IP address for iDRAC

iDRAC on LiveWire requires its own IP address for communication. You can set this in one of two ways:

- Access the BIOS settings for LiveWire and configure the IP address
- Use CLI commands from the command prompt and configure the IP address

Access BIOS setting to configure IP address

You must be physically present at LiveWire to initially set the iDRAC IP address. Once set, you can use iDRAC to view or change the setting.

To initially set the iDRAC IP address:

1. Locate the iDRAC port on the front or back of LiveWire, and connect an Ethernet cable from your network to the iDRAC port.
2. Reboot or restart LiveWire.
3. Press the [F2] key multiple times during system boot to enter the BIOS settings.
4. Select *iDRAC Settings* from the Advanced menu.
5. Select *Network* from the iDRAC submenu.
6. iDRAC is set to 192.168.1.21 by default. You can change the static address as well. You will need this IP address in order to remotely access LiveWire.
7. Press [Esc] to back out of each menu, then press **Enter** to confirm exit.

Connecting to iDRAC on LiveWire

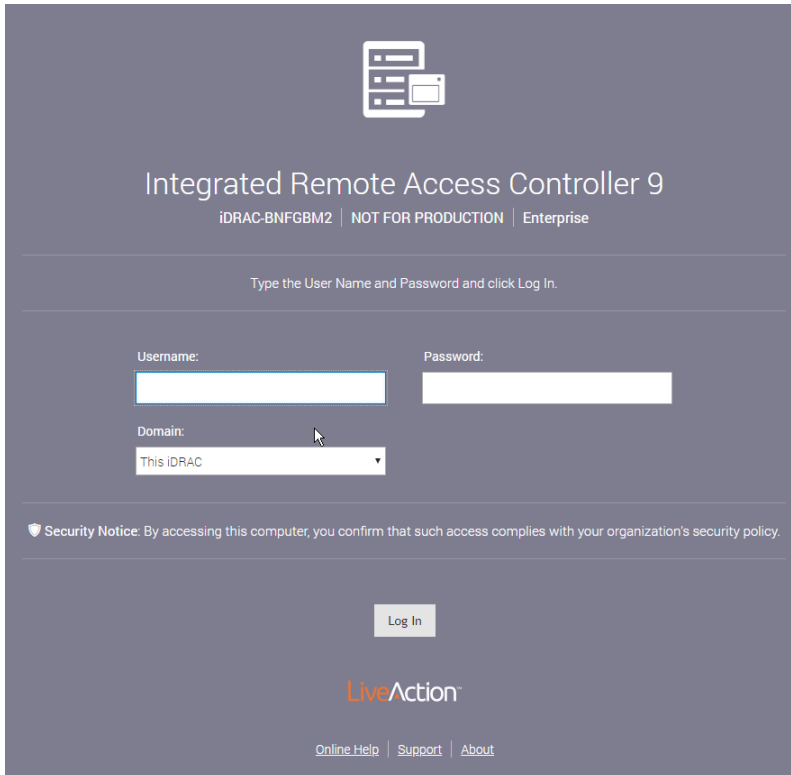
You can use an Internet browser window to connect to iDRAC on LiveWire. Additionally, you must make sure the following ports are accessible through any firewall:

- Port 80 (TCP)
- Port 443 (Web HTTP SSL)

- Port 623 (UDP)
- Port 5901 (Video)
- Port 5900 (Keyboard/Mouse)
- Port 5120 (Media Redirection)

To connect to iDRAC on LiveWire using your browser:

1. From a computer connected to the network, open an Internet browser window.
2. Enter the iDRAC IP address of LiveWire in the address bar of your browser.
3. Once the connection is made, the Login screen appears.



4. Enter the *Username* and *Password*, and then click **Login** (the default username is **root**, and the default password is **liveaction**). The iDRAC dashboard appears.

Note For security reasons, we strongly recommend changing both the default iDRAC username and password on LiveWire.

Integrated Remote Access Controller 9 | Enterprise

Dashboard

Graceful Shutdown Identify System More Actions

System Health

- Batteries
- CPUs
- Cooling
- Intrusion
- Memory
- Power Supplies
- Voltages
- Miscellaneous

System Information

Power State	ON
Model	NOT FOR PRODUCTION
Host Name	localhost.localdomain
Operating System	Ubuntu
Operating System Version	14.04, Trusty Tahr Kernel 3.13.0-143-generic (x86_64)
Service Tag	BNFGBM2
BIOS Version	1.3.7
iDRAC Firmware Version	3.15.17.15
iDRAC MAC Address	d0:94:66:25:8b:83

Virtual Console

Launch Virtual Console

Settings

Recent Logs

Severity	Description	Date and Time
✓	The chassis is closed while the power is off.	Tue 06 Feb 2018 17:42:44
✗	The chassis is open while the power is off.	Tue 06 Feb 2018 17:42:39
✓	The chassis is closed while the power is off.	Fri 02 Feb 2018 22:17:49

Notes

+ add note
view all

Date and Time	Description
There are no work notes to be displayed.	

- View the remaining instructions in this section for instructions on using iDRAC to perform tasks such as changing the default password, accessing a remote console, reimaging, rebooting, starting, and shutting down LiveWire.

Changing the default password

For security reasons, we strongly recommend changing both the default username and password to iDRAC.

To change the default password:

- In the iDRAC Settings, click *Users*. The list of *Local Users* appears.

Integrated Remote Access Controller 9 | Enterprise

iDRAC Settings

Overview Connectivity Services **Users** Settings Refresh

Local Users

Details + Add Edit Disable Delete

ID	User Name	State	User Role	IPMI LAN Privilege	IPMI Serial Privilege	Serial Over LAN	SNMP v3
2	root	Enabled	Administrator	Administrator	Administrator	Enabled	Disabled
3	ADMIN	Enabled	Administrator	Administrator	Administrator	Enabled	Disabled

Directory Services

Smart Card

Default Password Warning

Sessions

2. Select the *User ID* of the user you are configuring (in this case, user ID 2), and click **Edit**. The **User Account Settings** dialog for the selected user ID appears.

Edit User

User Configuration SSH Key Configurations Smart Card Configuration

User Account Settings

ID: 2

User Name*: root

Password*: [masked]

Confirm Password*: [masked]

User Privileges

User Role: Administrator

<input checked="" type="checkbox"/> Login	<input checked="" type="checkbox"/> Configure	<input checked="" type="checkbox"/> Configure Users
<input checked="" type="checkbox"/> Logs	<input checked="" type="checkbox"/> System Control	<input checked="" type="checkbox"/> Access Virtual Console
<input checked="" type="checkbox"/> Access Virtual Media	<input checked="" type="checkbox"/> System Operations	<input checked="" type="checkbox"/> Debug

Close Save

3. Make your edits to the *User Name* and *Password* settings, and then click **Save**.

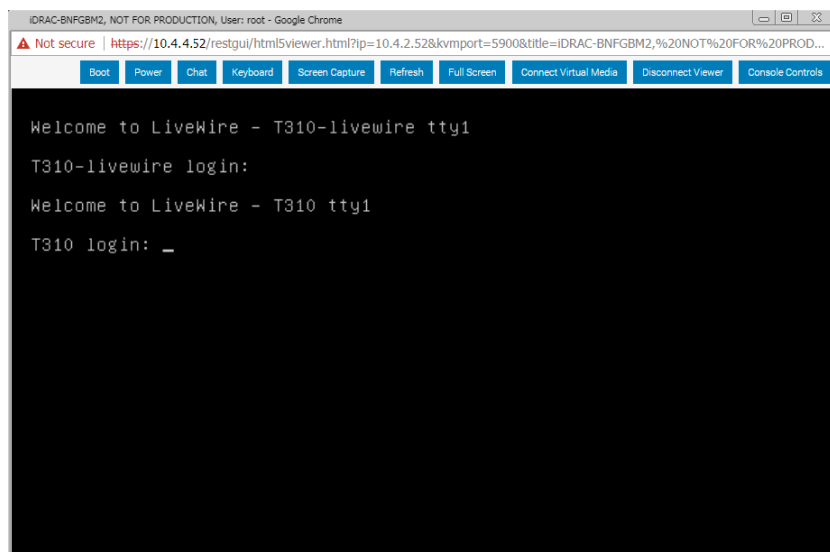
Accessing a remote console

A powerful feature when using iDRAC is the ability to open a remote console from which you can enter commands to LiveWire.

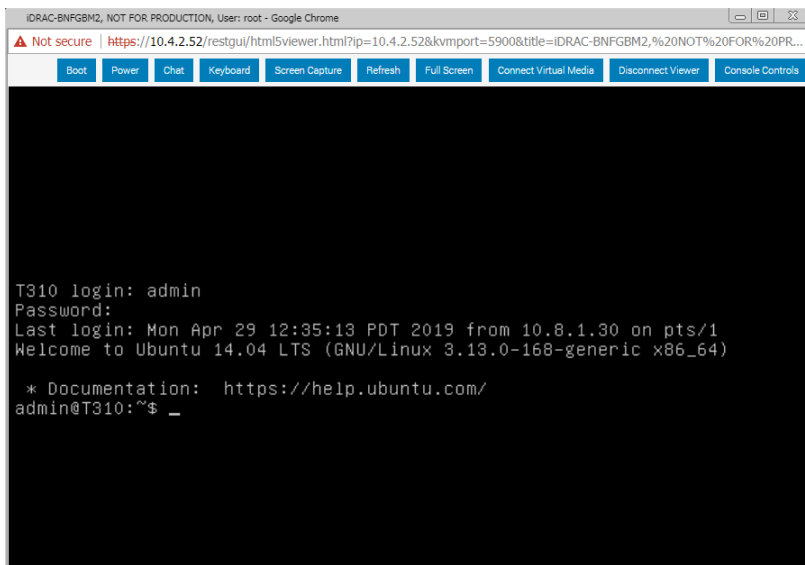
To open a remote console:

Note The *Plug-in Type* was changed to 'HTML5' from the default of 'Native' for the instructions in this section. To change the *Plug-in Type*, click *Settings* in the *Virtual Console Preview*.

1. From the iDRAC dashboard, click *Launch Virtual Console*. The LiveWire login window appears.



2. Log into LiveWire using LiveWire login user name and password. The `admin@livewire:~#` command prompt appears once you are logged into LiveWire.

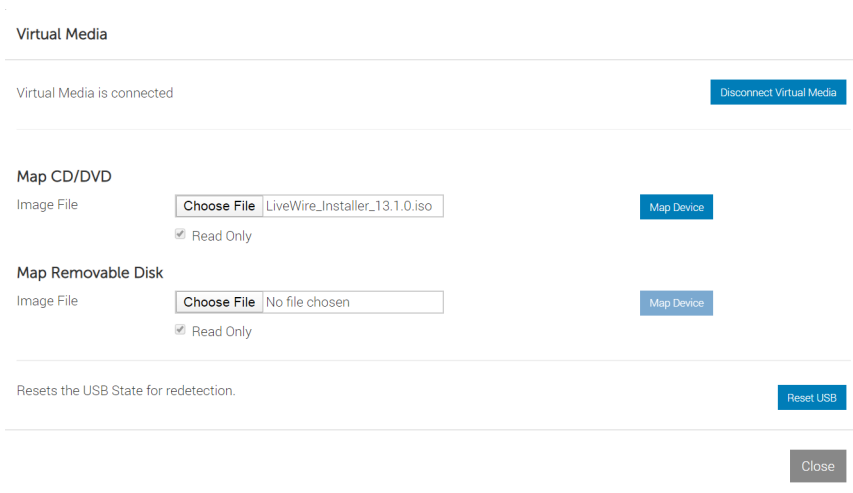


Reimaging LiveWire with an ISO image

You can reimage LiveWire remotely using iDRAC and an ISO image available from LiveAction technical support. See 'Contacting LiveAction support' on page 35.

To reimage LiveWire:

1. From the remote console, click **Connect Virtual Media**. The **Virtual Media** dialog appears.



2. Click **Choose File** under *Map CD/DVD* to select the ISO file (e.g., *omni-20.1.0-x.iso*), and then click **Map Device**. The ISO image is mapped to the CD/DVD drive.

Virtual Media is connected Disconnect Virtual Media

Map CD/DVD

Image File

LiveWire_Installer_T3.1.0.iso is mapped to CD/DVD drive.(Read Only)

Un-Map Device

Map Removable Disk

Image File

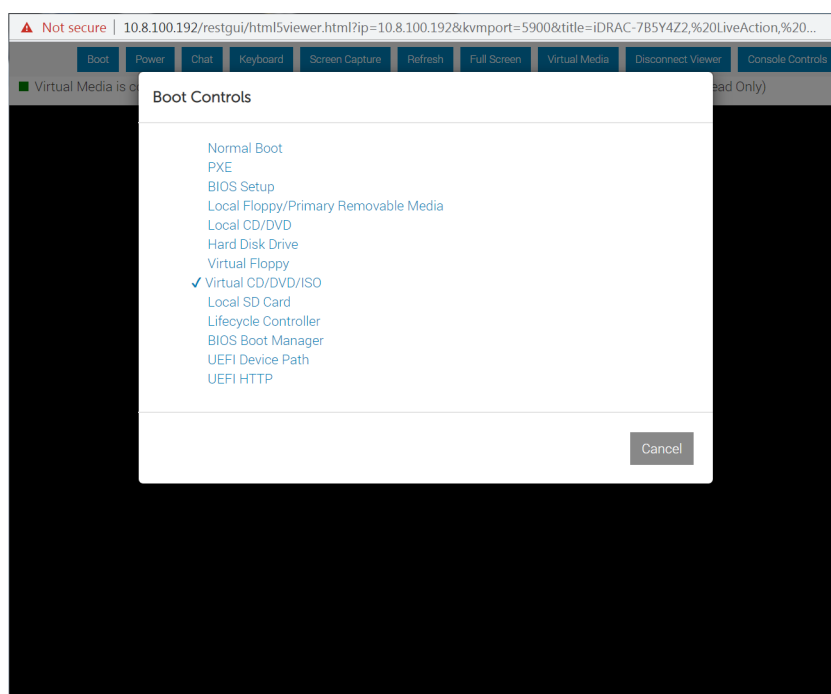
Choose File No file chosen

Map Device

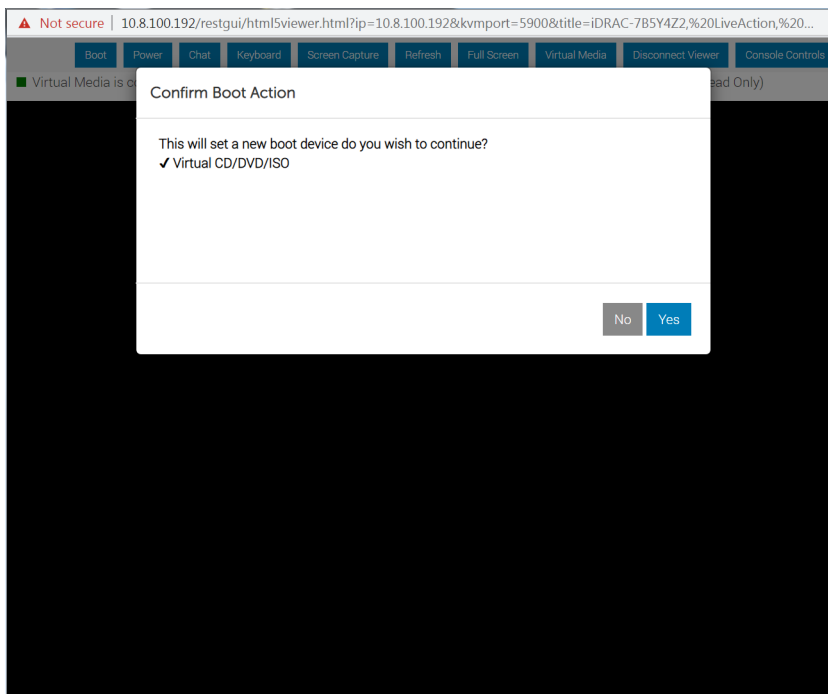
☒ Read Only

Resets the USB State for redetection. Reset USB

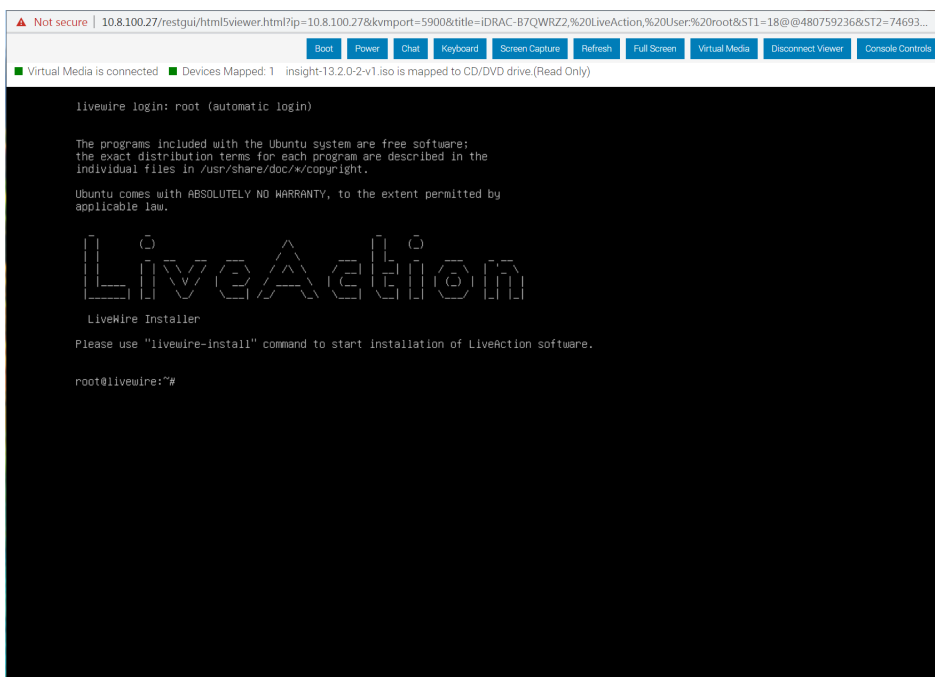
3. Click **Close** to close the dialog.
4. From the remote console, click **Boot** and select *Virtual CD/DVD/ISO* from the boot controls. The **Confirm Boot Action** dialog appears.



5. Click **Yes** to set the *Virtual CD/DVD/ISO* as the new boot device.



6. From the remote console, click **Power** and select *Power Cycle System (cold boot)*. The **Confirm Power Action** dialog appears.
7. Click **Yes** to execute the *Power Cycle System (cold boot)*.
8. Click **OK** to confirm, and the system will start to load the ISO image. Allow the system to fully boot from the ISO image.
9. Once the ISO image is fully loaded, you are prompted to log into the boot ISO image. Log in using the username ('root') and password ('liveaction').
10. At the command prompt, type *livewire-install* and press **Enter**. You will receive a warning message that all data will be lost.



11. Type **Yes** and press **Enter**. The install process takes up to 20 minutes.

Note When running the *livewire-install* script through the remote console, do not close the console until the script completes. Closing the console prematurely causes the reimaging process to fail.

12. When the install process is finished, type *reboot* and press **Enter**. You will receive instructions to eject any disc.
13. Click the Power button again and select **Reset System (warm boot)**.
14. Once LiveWire has rebooted, you can proceed to configuring the management IP, time zone, NTP, and other settings for LiveWire as you normally would. See those sections in this guide for instructions.

Rebooting LiveWire

To reboot LiveWire:

- From the remote console, click **Boot** and select *Normal Boot* from the boot controls and follow the prompts to reboot.
- From the remote console, enter the *reboot* command.

```

usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
root@livewire:~# sudo su
root@livewire:~# livewire-install
LiveWire 13.2.0-2-v1 installation script
This will erase all data on the hard drive
Would you like to continue? (Yes/No) [No]: yes
Turning off swaps... OK
Configuring hardware raid... OK
Probing drives... OK
Selecting boot drive: sda - 3814912 MB
Selecting var drive: sdb - 3814912 MB
Selecting data drive(s):
Data drive: sda - 3814912 MB
Data drive: sdb - 3814912 MB
Data drive: sdc - 3814912 MB
Data drive: sdd - 3814912 MB
Unmounting all partitions of sda
Unmounting all partitions of sdb
Unmounting all partitions of sdc
Unmounting all partitions of sdd
Deleting all existing partitions on boot drive
Clear all existing partitions
Creating a new partition table on sda
Deleting all existing partitions on data drive - sdb
Clear all existing partitions
Creating a new partition table on sdb
Deleting all existing partitions on data drive - sdc
Clear all existing partitions
Creating a new partition table on sdc
Deleting all existing partitions on data drive - sdd
Clear all existing partitions
Creating a new partition table on sdd
Creating new partitions...
parted -s /dev/sda set 1 esp off
parted -s /dev/sda set 1 bios_grub on
Creating live on data partitions...
Creating filesystem on /dev/sda2... OK
Creating swap volume on /dev/sdb2... OK
Creating filesystem on /dev/sdb1... OK
Creating filesystem on /dev/data/raid0... OK
Mounting /dev/sda2
Setting up grub... OK
Copying system image files to /dev/sda2... OK
Unpacking system image files: OK
Updating boot menu: OK
Configuring DELL iDRAC... OK
Done!
root@livewire:~# reboot

```

Starting / Shutting down LiveWire

If your power cables and Ethernet cable are connected to LiveWire, you can access iDRAC even if LiveWire is off. Once iDRAC is accessed, you can use iDRAC to start LiveWire.

To start or shut down LiveWire:

- From the iDRAC dashboard, if LiveWire is off click *Power On System*, or *Graceful Shutdown* if it is on.

Note If you have a remote console open, you can also select the start or power off commands from the **Power** menu of the remote console.

You can also issue the *#poweroff* command (recommended) from the remote console to shut down LiveWire.

Accessing the iDRAC interface over the USB port

The iDRAC direct feature allows you to directly connect your laptop to the iDRAC micro-USB port on LiveWire using a USB to micro-USB cable. The location of the iDRAC micro-USB port is found in the right control panel on the front of LiveWire.

To access the iDRAC interface:

1. Turn off any wireless networks and disconnect from any other hard wired network.
2. Ensure that the USB port is enabled in your system BIOS settings (*System BIOS > Integrated Devices*).
3. Use a USB to micro-USB cable and connect your laptop to the iDRAC micro-USB port on LiveWire.
4. After you connect the micro-USB cable to the laptop, the laptop will download the "iDRAC Virtual NIC USB Device" driver automatically.

You will see Remote NDIS Compatible Device #2 appearing in Network adapters in Device Manager.

5. Wait for the laptop to obtain the IP address 169.254.0.4. It is always the same IP address. It may take several seconds for the IP addresses to be acquired. iDRAC acquires the IP address 169.254.0.3.

To check if the iDRAC is responding, issue the ping command.

6. You can now start using the iDRAC network interfaces. For example, to access the iDRAC web interface, open a supported browser, and type the address 169.254.0.3 and press **Enter**. The iDRAC login screen appears.
7. When iDRAC is using the USB port, the LED on LiveWire blinks indicating activity. The blink frequency is 4 per second. After completing the desired actions, disconnect the micro-USB cable from LiveWire. The LED turns off.
8. If the micro-USB cable can't be recognized, please navigate to *iDRAC Settings > Media and USB Port Settings > iDRAC Direct Only*.

Sending LiveFlow Telemetry

In this chapter:

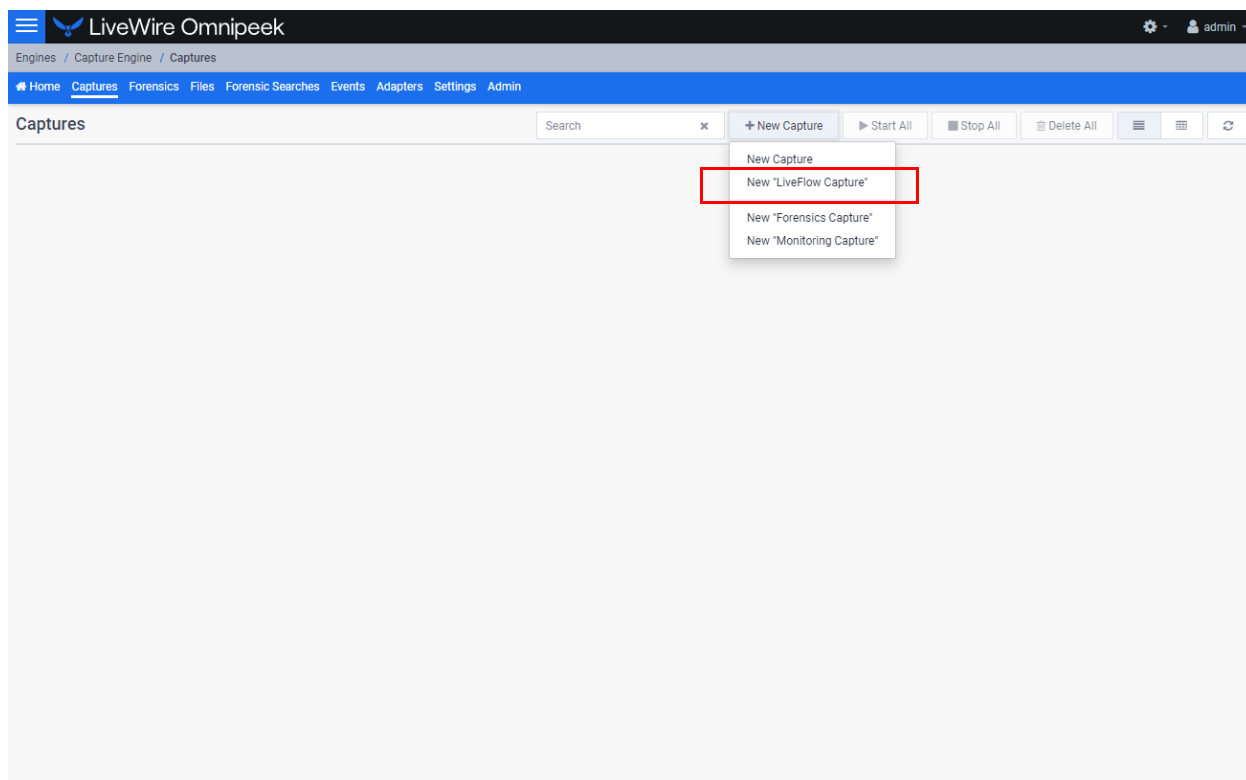
<i>About sending telemetry to LiveNX and other platforms</i>	<i>64</i>
<i>Configuring LiveFlow telemetry</i>	<i>64</i>
<i>An example of using LiveWire, LiveNX, and Omnipeek</i>	<i>83</i>

About sending telemetry to LiveNX and other platforms

LiveWire is designed to send LiveFlow telemetry data to LiveAction's LiveNX and various other platforms. LiveNX is a network and application performance monitoring platform with patented end-to-end visualization for a global view of the network and the ability to drill-down to individual devices. In addition to sending LiveFlow telemetry to LiveNX, LiveFlow telemetry can also be sent other platforms including Cisco SNA and Splunk. This chapter describes the tasks you must perform in order to properly send LiveFlow telemetry data from LiveWire to LiveNX and various other platforms.

Configuring LiveFlow telemetry

To send the LiveFlow telemetry data used in LiveNX and other platforms, you must use Omnippeek to first create a new LiveFlow capture and then configure the settings for that capture to send LiveFlow telemetry to the desired platforms.



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) 4096

DISK SPACE FOR THIS CAPTURE 4 GB Disk Space: 132,140 GB
Files: 33,035

☐ Retention time 1 Days

☐ New file every 6 Hours

CAPTURE STATISTICS

☒ Timeline statistics

☐ Top statistics

☒ Application statistics

☐ VoIP statistics

PACKET FILE INDEXING

☐ Application ☐ Physical Address

☐ Country ☐ Port

☐ IP Address ☐ Protocol

☐ IPv6 Address ☐ VLAN

☐ MPLS

BUFFER SIZE (MB) 256

☒ Start capture immediately

Cancel OK

Note Scroll down in the capture options to see LiveFlow settings for *IPFIX Template Refresh Interval* and *IPFIX Options Template Refresh Interval*. These settings let you configure the amount of time (in seconds) LiveWire sends template information to the desired platforms. The templates provide the instructions to the desired platforms on how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). If you make any changes to your template settings, it will take the specified number of seconds for the changes to take effect. If you recently connected LiveWire to the network, it may take up to 600 seconds for the desired platforms to see the LiveFlow data from LiveWire. You may want to adjust the settings to the desired intervals.

General

The *General* settings let you set up and configure the LiveFlow capture.

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) 4096

DISK SPACE FOR THIS CAPTURE 4 GB Disk Space: 132,140 GB
Files: 33,035

☐ Retention time 1 Days

☐ New file every 6 Hours

CAPTURE STATISTICS

☒ Timeline statistics

☐ Top statistics

☒ Application statistics

☐ VoIP statistics

PACKET FILE INDEXING

☐ Application ☐ Physical Address

☐ Country ☐ Port

☐ IP Address ☐ Protocol

☐ IPv6 Address ☐ VLAN

☐ MPLS

BUFFER SIZE (MB) 256

☒ Start capture immediately

Cancel OK

- **Name:** Type a descriptive name for the capture. Unique names can help you to identify and organize your captures. Users cannot change the name of the LiveFlow capture.
- **Capture to disk:** Select this option to save packet files on your disk. Packet files saved to your hard disk (and the individual packets/packet decodes in each of the files) can be opened and analyzed at a later time with Omnipeek. If you are more interested in speeding up analysis of the data and conserving hard disk space, you may want to disable *Capture to disk*.
 - **Priority to CTD:** Select this option so that real-time analysis doesn't impact the capture-to-disk (CTD) performance. When this option is enabled, it is less likely that packets are dropped when they are captured to disk. If capturing all the packets to disk is desirable, enable *Priority to CTD*. If analysis is more important, disable *Priority to CTD*.
 - **Intelligent CTD:** Select this option to reduce the amount of data stored to disk and increase your retention time by intelligently slicing off encrypted payloads. It does this by tracking flows—if a flow is encrypted, the full data for the first 20 packets is kept and the payload from the rest of the packets is sliced. It keeps the first 20 without slicing so the certificate exchange is always included.

Intelligent CTD is an advanced feature that provides significant benefits to network security and data retention. It reduces the amount of data stored on disk and increases retention time by intelligently slicing off encrypted payloads, which helps to conserve storage space and improve system performance.

The way *Intelligent CTD* works is by tracking flows on the network. When a flow is detected as encrypted, *Intelligent CTD* keeps the full data for the first 20 packets and slices the payload from

the rest of the packets. This ensures that the certificate exchange is always included in the data, which is critical for identifying encrypted traffic and providing context for analysis.

The benefits of *Intelligent CTD* are numerous. Firstly, it helps to optimize storage usage, as the system doesn't store unnecessary data. This helps to reduce the cost of storage and improve system performance by reducing the amount of data that needs to be processed.

Secondly, *Intelligent CTD* helps to improve retention time. By conserving storage space, it enables organizations to retain data for longer periods, which can be critical for compliance and regulatory requirements. This also enables organizations to perform more in-depth analysis of data, which can provide valuable insights into network activity and help to identify potential threats.

Thirdly, *Intelligent CTD* helps to maintain privacy and compliance. By keeping the certificate exchange in the data, it ensures that the system can identify encrypted traffic and provide context for analysis, without compromising the privacy of users. This helps organizations to comply with privacy regulations and maintain the trust of their users.

Overall, *Intelligent CTD* is a powerful feature that provides numerous benefits to network security and data retention. By intelligently slicing off encrypted payloads, it helps to optimize storage usage, improve retention time, and maintain privacy and compliance.

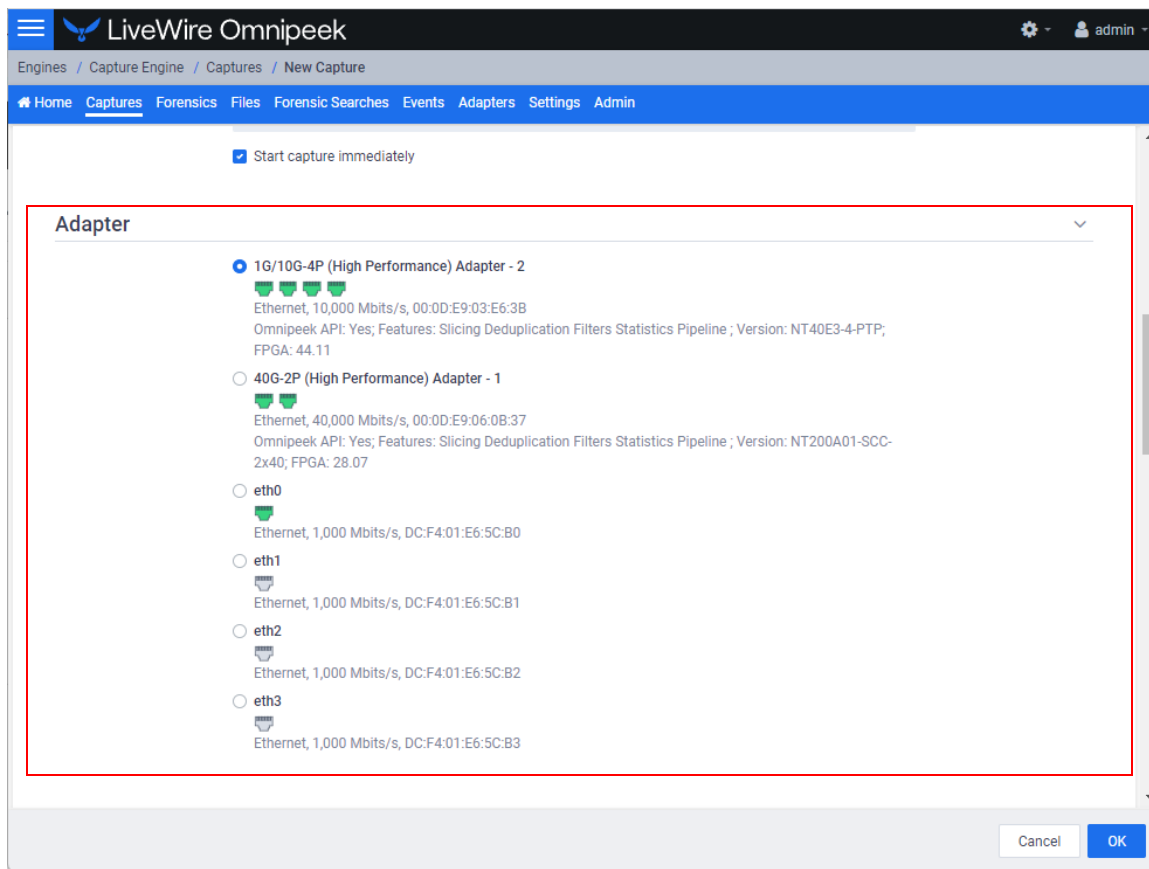
- *Compression*: Select this option to compress blocks of packets before writing them to the file. This setting is only available when you are capturing from a capture card that supports this feature, and only when you are saving files to the *.npkt* file format.
- *File Name*: Type the name used as a base file name prefix for each capture file that is created using the *Capture to disk* option. Additionally, each capture file is appended with a timestamp indicating the date and time the file was saved. The format of the timestamp is *YYYY-MM-DD-HH.MM.SS.mmm*.
- *File Size (MB)*: Enter or select the maximum file size before a new file is created.
- *Disk Space For This Capture*: Move the slider control to set the amount of hard disk space allocated for the capture. The minimum value of the slider is the minimum size of disk space a capture can occupy.
 - *Retention time*: Select this option to configure how long CTD files can remain on disk. You will need to configure the amount of minutes, hours, or days. For example, if you specify 3 days as the retention time, you'll only see the CTD files written within the past 3 days regardless of how much disk space you reserve for the capture.
 - *New file every*: Select this option to create a new CTD file at a specific time interval rather than when the CTD file size specified is reached. You will need to configure the amount of minutes, hours, or days. For example, if you specify that you want a new file every 1 minute with a 4 GB CTD file size, there will be a new CTD file every 1 minute even if the CTD file is only 1 GB in size. If the 4 GB size limit is reached before the 1 minute mark, then the *New file every* option doesn't come into effect.
- *Capture Statistics*: Select the type of statistics desired for the capture:
 - *Timeline Statistics*: Select this option to populate the capture engine database with capture data and basic network statistics such as utilization, size, distribution, etc. These statistics are then made available through the *Capture Engine Forensics* tab.
 - *Top Statistics*: Select this option to populate the capture engine database with top nodes and top protocols statistics. These statistics are then made available through the *Capture Engine Forensics* tab.
 - *Application Statistics*: Select this option to populate the capture engine database with applications statistics which are made available through the various 'application' displays.
 - *VoIP Statistics*: Select this option to populate the capture engine database with VoIP call quality and call volume statistics. These statistics are then made available through the *Capture Engine Forensics* tab.

Note Selecting the *VoIP Statistics* option may affect capture performance, especially when there are more than 2000 simultaneous calls on the network. Selecting the *Top Statistics* option may affect capture performance, especially when there are more than 10,000 active nodes captured on the network.

- *Packet File Indexing*: Under certain conditions, *Packet File Indexing* increases performance for forensic searches that use software filters. 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. Enable the packet characteristics below you are most likely to use in a forensic search software filter.
 - *Application*
 - *Country*
 - *IP Address*
 - *IPv6 Address*
 - *MPLS*
 - *Physical Address*
 - *Port*
 - *Protocol*
 - *VLAN*
- *Buffer Size (MB)*: Enter a buffer size, in megabytes, for the amount of memory dedicated for the capture buffer. The capture buffer is where packets are placed for analysis. The default is 256 megabytes. A larger buffer can reduce or eliminate packet loss due to spikes in traffic. When *Capture to disk* is enabled, the *Buffer Size* option is unavailable.
- *Start Capture Immediately*: Select this option to immediately begin capturing packets once you click **OK**.

Adapter

The *Adapter* settings display the capture adapters available on LiveWire. Select the desired adapter for the LiveFlow capture.



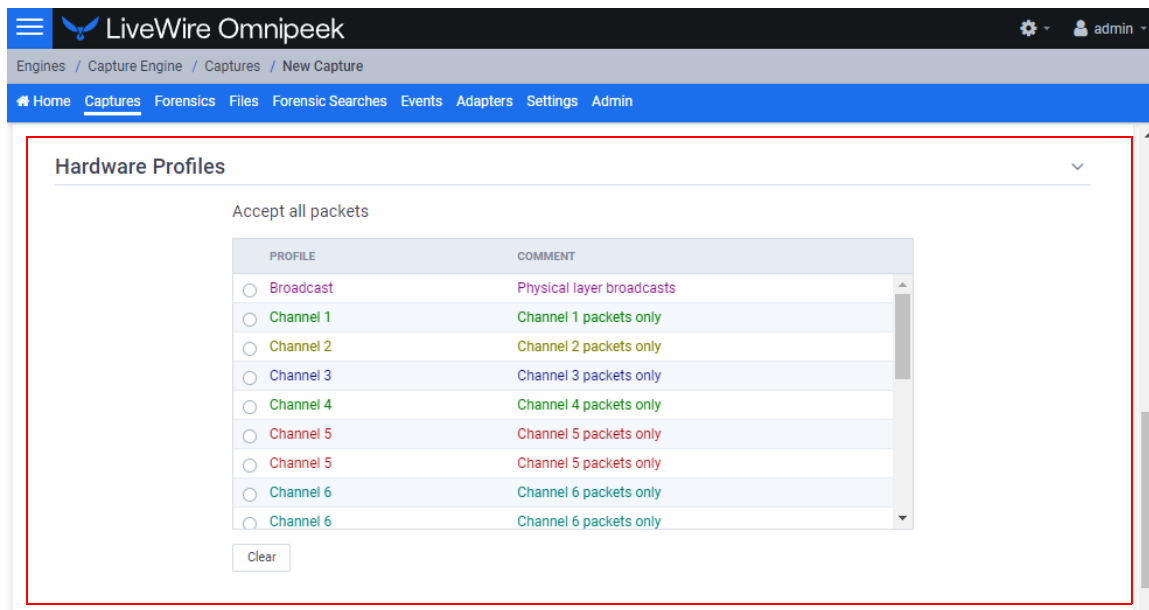
Hardware Profiles

If the selected adapter supports hardware profiles, then Hardware Profiles settings are available and can be selected and configured for the LiveFlow telemetry.

Hardware profiles tell a capture adapter the type of traffic to capture and how to manage that traffic. Hardware profiles can slice the packets, discard error or duplicate packets, and apply an address, port, mpls, vlan, or value filter. Different settings can be applied per capture adapter channel as well.

Important! All of the hardware profile settings are applied in hardware, and allow for better performance than performing these operations in software.

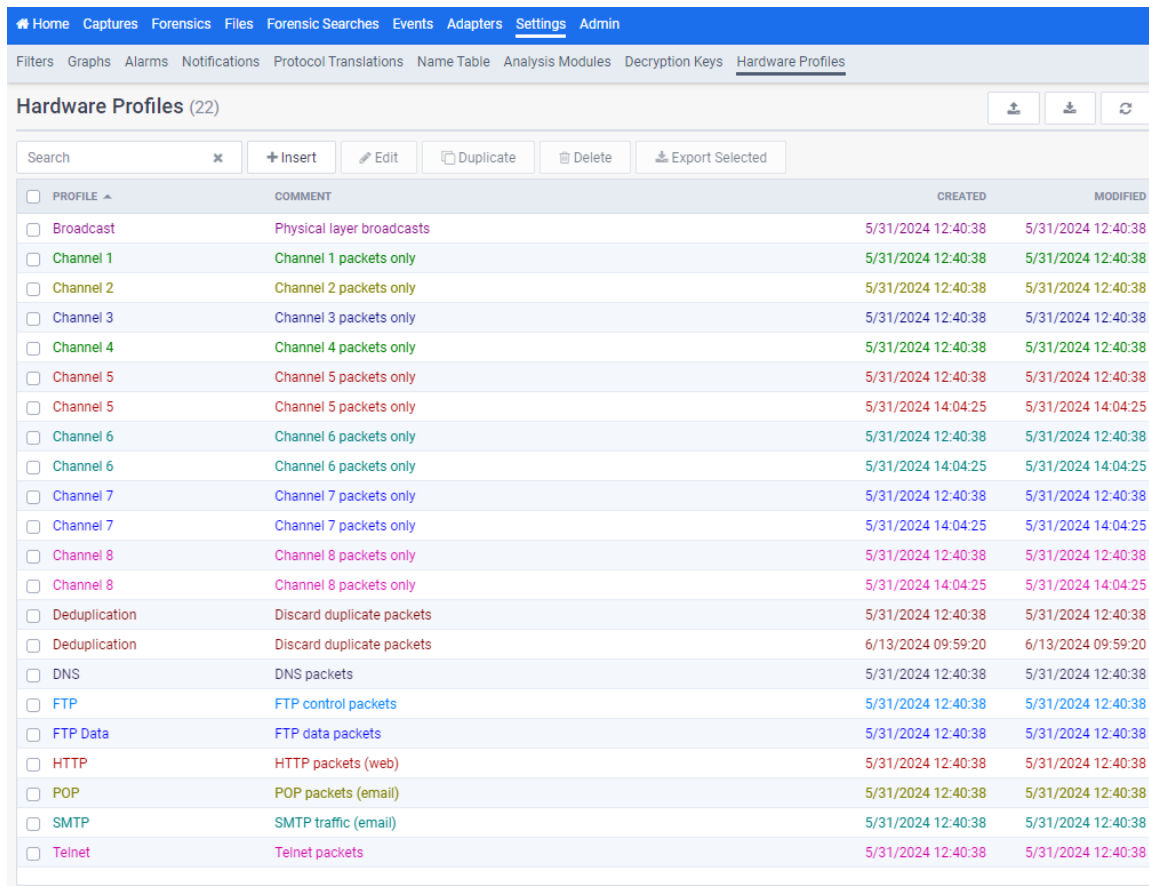
Note Only one hardware profile per capture can be implemented at a time.



The **Hardware Profiles** view in the **Settings** view allows you to define and manage your hardware profiles.

To create a new hardware profile:

1. Display the **Hardware Profiles** view from the **Settings** view.



2. Click *Insert*. The **Insert Profile** view appears.

3. Configure the settings:

Important! Hardware profiles containing an overly complex configuration using the options specified below may result in an error dialog indicating that the hardware profile is too complex. When starting a capture, you may also get the error dialog when multiple captures use hardware profiles that are collectively too complex when used together. If you receive this error dialog, try reducing the complexity of the hardware profile. For example, try limiting the number of filters, reduce the number of channels, limit the number of VLAN IDs or MPLS labels, or limit the number of layers used in the hardware profile.

Additionally, when using multiple hardware profiles on the same capture adapter, these hardware profiles should be exclusive with each other (capturing a unique set of packets) or else you may find that some of the captures are missing packets since a packet can only be sent to one capture. When a packet matches more than one hardware profile in use, the most recent captures have precedence over less recent captures.

- *Profile:* Type a name for the profile.
- *Color:* Select a color for the profile.
- *Comment:* Type a comment to provide a more complete description of the hardware profile's properties.
- *Slice packets (all channels):* Select this option and specify how to slice the packets.

Important! If you have two captures on the same capture adapter, and one has a hardware profile that has *Slice packets (all channels)* enabled, while the other has *Slice packets (all channels)* disabled, only the last capture started receives packets while the other capture stops receiving packets.

- *Discard duplicate packets:* If your capture adapter supports this feature, this option is available and can be selected to discard duplicate packets.

Important! If you have two captures on the same capture adapter, and one has a hardware profile that has *Discard duplicate packets* enabled, while the other has *Discard duplicate packets* disabled, only the last capture started receives packets while the other capture stops receiving packets.

- *Apply Channel 1 settings to all channels:* Select this option to assign the same properties defined for Channel 1 to all channels. Clear the check box if you want to define properties separately for each channel.
- *Discard error packets:* Select this option to discard error packets.
- *Reject packets matching this filter:* Select this option to pass packets to Omnipeek that do not match this filter.
- *Address filter:* Select this check box to specify a filter parameter based on address.

Note Wildcard addresses (or range of addresses) and CIDR range filtering are supported for *Address filter*.

- *Type:* Select the type of addresses you want to enter. Both Address 1 and Address 2 must be of the same type and must be entered in the correct format.
Click Direction below to select the send/receive relationship between Address 1 and Address 2.
- *Address 1:* Type or select the first address for the filter.
- *Direction:* Select the direction for the filter.
- *Address 2:* Type or select the second address for the filter.
- *Any address:* Select this option to specify any address for Address 2.
- *Port filter:* Select this check box to specify a filter parameter based on port.
 - *Type:* Select the type of port you want to enter. Both Port 1 and Port 2 must be of the same type and must be entered in the correct format.
Click Direction below to select the send/receive relationship between Port 1 and Port 2.
 - *Port 1:* Type or select the first port for the filter.
 - *Direction:* Select the send/receive relationship between Port 1 and Port 2.
 - *Port 2:* Type or select the second port for the filter.
 - *Any port:* Select this option to specify any port for Port 2.
- *VLAN filter:* Select this option to enable VLAN filtering. This allows you to enter a comma separated list of VLAN IDs to match against.
 - *IDs:* Type the list of VLAN IDs, separated by a comma. The list cannot exceed 32 entries and must be within the valid VLAN ID range of 0 to 0xFFFF.
 - *Layers:* Select how deep of a VLAN stack to match against, with 1 being the minimum and 2 being the maximum.
- *MPLS filter:* Select this option to enable MPLS filtering. This allows you to enter a comma separated list of MPLS labels to match against.

- *Labels*: Type the list of MPLS labels, separated by a comma. The list cannot exceed 32 entries and must be within the valid MPLS Label range of 0 to 0xFFFFF.
- *Layers*: Select how deep of an MPLS stack to match against, with 1 being the minimum and 3 being the maximum.
- *Value filter*: Select this option to enable Value filtering. This allows to add a combination of Value filters, which are connected to each other through AND/OR conjunctions. You can add up to four Value filters due to hardware limitations on the capture adapter.
 - *And*: Select to add an 'And' to the filter.
 - *Or*: Select to add an 'Or' to the filter.
 - *Delete All*: Click to delete the parameters of the filter.
 - *Offset*: Type or select a signed number between -1024 and 1024, inclusive.
 - *Offset Relative To*: Select the offset relative to the beginning of each packet.
 - *Length*: Select the length of the filter.
 - *Mask*: Type a mask for the *Value* of the filter. This mask must represent a single continuous range of bits. This field is ignored if *Length* is an address (MAC, IPv4, or IPv6).
 - *Operator*: Select an operator for the filter.
 - *Value*: If *Length* is 1 Byte, 2 Bytes or 4 Bytes, the *Value* must be an unsigned number that does not exceed the number of bytes specified.

If *Length* is an address (MAC, IPv4 or IPv6), the *Value* must be a valid address of that type, which can include wildcards and CIDR ranges.

4. Configure other channels if you are not applying Channel 1 settings to all channels, or if you want to define properties separately for each channel.
5. Click **OK** to add the new hardware profile to the list of profiles.

LiveFlow

The *LiveFlow* settings lets you further configure the LiveFlow data of the capture.

IPFIX Max Payload

- *IPFIX Max Payload (Bytes)*: Enter the number of bytes indicating the maximum payload size (in bytes) for generated IPFIX packets. You can configure a value between 256 and 65535.

IPFIX Template Refresh Interval

- *IPFIX Template Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire generates and sends IPFIX template records to the desired platforms. The templates provide the instructions to the desired platforms on how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.

Note If you recently connected LiveWire to the network, it may take up to 600 seconds for the desired platforms to see the LiveFlow data from LiveWire. You may want to adjust this setting to the desired intervals.

IPFIX Options Template Refresh Interval

- *IPFIX Options Template Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire generates and sends IPFIX option template records. The templates provide the instructions on

how to interpret the template data records in the exported LiveFlow data. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.

Note If you recently connected LiveWire to the network, it may take up to 600 seconds the desired platforms to see the LiveFlow data from LiveWire. You may want to adjust this setting to the desired intervals.

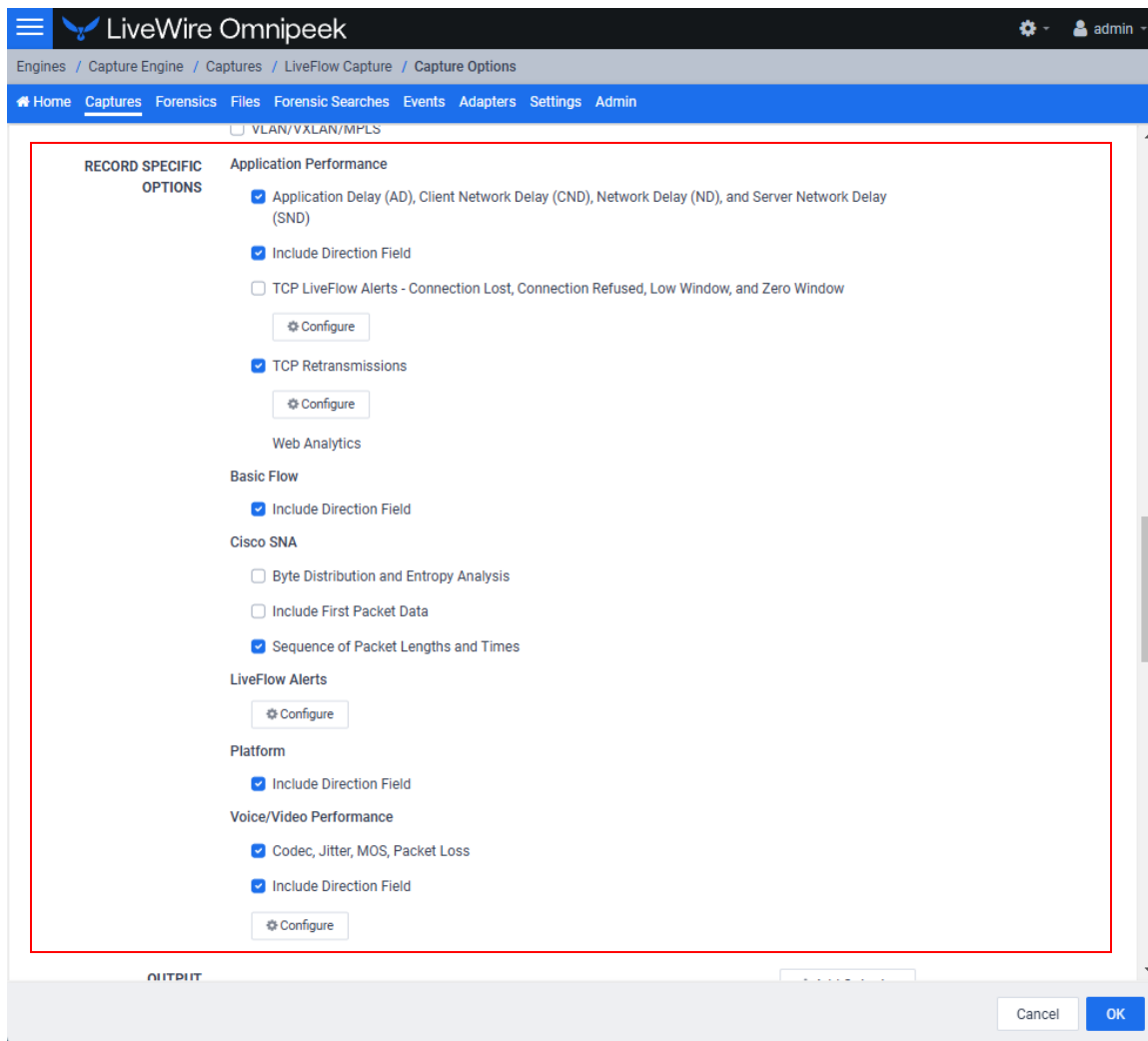
Flow Refresh Interval

- *Flow Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire generates and sends IPFIX data records. The default is set to 600 seconds (10 minutes). You can configure anywhere from 1 to 1800 seconds. If you make any changes to your template settings, it will take the specified number of seconds for the changes to take place.

General Analysis

- *Enforce 3-Way Handshake*: Select this option to require a 3-way handshake (SYN, SYN-ACK, ACK) for a TCP flow in order for it to be included in processing and analyzing the LiveFlow telemetry. The *Enforce 3-Way Handshake* option becomes disabled and cannot be selected whenever 'Platform' records are enabled.
- *VLAN/VXLAN/MPLS*: Select this option to perform VLAN, VXLAN, and MPLS analysis in the LiveFlow telemetry.

Record Specific Options



- *Application Performance*
 - *Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)*: Select this option to perform latency and delay analysis in the LiveFlow telemetry.
 - *Include Direction Field*: Select this option to include flow direction (0 for ingress, 1 for egress) analysis in the Application Performance flow records.
 - *TCP LiveFlow Alerts - Connection Lost, Connection Refused, Low Window, and Zero Window*: Select this option to perform TCP quality analysis in the LiveFlow telemetry.
 - *Configure*: Click to view TCP LiveFlow alerts. Click an individual alert to display a description, cause, and remedy in the Detailed Information window. For various alerts, a threshold value can also be configured.
 - *TCP Retransmissions*: Select this option to perform TCP retransmission analysis (Expert) in the LiveFlow telemetry.
 - *Configure*: Click to select the TCP LiveFlow alerts to include in the TCP Retransmissions Configurations. Click an individual alert to display a description, cause, and remedy in the Detailed Information window. For numerous LiveFlow alerts, you can configure the threshold values for those events.
 - *Web Analytics*: Select this option to perform web analytics in the LiveFlow telemetry.

Note The *Web Analytics* option becomes disabled and cannot be selected whenever 'Platform' records are enabled.

- *Decrypt Packets*: If *Web Analytics* is enabled, the *Decrypt Packets* option is made available. Select this option to perform decryption analysis on HTTPS packets in the LiveFlow telemetry. You will need to also click *Manage* to configure the Decryption Keys that allow you to decrypt packets.
- *Basic Flow*
 - *Include Direction Field*: Select this option to include flow direction (0 for ingress, 1 for egress) analysis in the Basic Flow records.
- *Cisco SNA*
 - *Byte Distribution and Entropy Analysis*: Select this option to perform Entropy and Byte Distribution analysis in the Cisco SNA flow records.
 - *Include First Packet Data*: Select this option to include the payload of the first packet of a flow in the Cisco SNA flow records.
 - *Sequence of Packet Lengths and Times*: Select this option to perform SPLT analysis in the Cisco SNA flow records.
- *LiveFlow Alerts*
 - *Configure*: Click to select the LiveFlow alerts to include in the LiveFlow telemetry. For numerous LiveFlow alerts, you can enable/disable LiveFlow alerts, and also configure the threshold values for those alerts.
- *Platform*
 - *Include Direction Field*: Select this option to include flow direction (0 for ingress, 1 for egress) analysis in the Platform flow records.
- *Voice/Video Performance*
 - *Codec, Jitter, MOS, Packet Loss*: Select this option to perform RTP analysis when MediaNet IPFIX flow records are generated.
 - *Include Direction Field*: Select this option to include flow direction (0 for ingress, 1 for egress) analysis in the Voice/Video Performance flow records.
 - *Configure*: Click to configure which flows are excluded from Voice/Video Performance analysis.

Output

Important! The *Server Address* and *Server Port* combination must be unique between all outputs. There can only be three output targets.

- *+Add Output*: Click to select an output target. You can select from and display the following output targets:
 - *Cisco SNA Telemetry*
 - *IPFIX Telemetry*
 - *LiveNX Telemetry*
 - *OpenTelemetry (LiveFlow Alerts)*
- *Cisco SNA Telemetry*: Enable this option to send LiveFlow telemetry optimized for Cisco SNA.
 - *Server Address*: Enter the IP address of the server which receives the telemetry optimized for Cisco SNA.
 - *Server Port*: Enter the IP port of the server which receives the telemetry optimized for Cisco SNA.
 - *IPFIX Records*: Select the check box of the types of IPFIX records to include in the LiveFlow telemetry for Cisco SNA (click the small information icon next to the IPFIX records to view a tool tip indicating what will be in the records):
 - *Application Performance*
 - *Basic Flow*
 - *Cisco SNA* (enabled by default)
 - *Platform*
 - *Signaling DN*

- *Voice/Video Performance*
- *IPFIX Telemetry*: Enable this option to send LiveFlow telemetry optimized for IPFIX.
 - *Server Address*: Enter the IP address of the server which receives the telemetry optimized for IPFIX.
 - *Server Port*: Enter the IP port of the server which receives the telemetry optimized for IPFIX.
 - *IPFIX Records*: Select the check box of the types of IPFIX records to include in the LiveFlow telemetry for IPFIX (click the small information icon next to the IPFIX records to view a tool tip indicating what will be in the records):
 - *Application Performance* (enabled by default)
 - *Basic Flow* (enabled by default)
 - *Cisco SNA* (enabled by default)
 - *Platform* (enabled by default)
 - *Signaling DN* (enabled by default)
 - *Voice/Video Performance* (enabled by default)
- *LiveNX Telemetry*: Enable this option to send LiveFlow telemetry optimized for LiveNX.
 - *Server Address*: Enter the IP address of the server which receives the telemetry optimized for LiveNX.
 - *Server Port*: Enter the IP port of the server which receives the telemetry optimized for LiveNX.
 - *IPFIX Records*: Select the check box of the types of IPFIX records to include in the LiveFlow telemetry for LiveNX (click the small information icon next to the IPFIX records to view a tool tip indicating what will be in the records):
 - *Application Performance* (enabled by default)
 - *Basic Flow* (enabled by default)
 - *Cisco SNA*
 - *Platform*
 - *Signaling DN*
 - *Voice/Video Performance* (enabled by default)
- *OpenTelemetry (LiveFlow Alerts)*: Enable this option to send LiveFlow alerts to the configured location in the *Configure OpenTelemetry* settings.
 - *Records*: Select the check box of the types of records to include in the LiveFlow telemetry for OpenTelemetry (click the small information icon next to the records to view a tool tip indicating what will be in the records).
 - *OpenTelemetry Status*: Displays the OpenTelemetry Status selected in *Configure OpenTelemetry*.

OpenTelemetry

☐ Disable OpenTelemetry
☒ Enable OpenTelemetry

CUSTOMER ID

CustomerID

ENDPOINT

https://telemetry.0000000000000000007-test.platform.io/

TOKEN

8a25f6ef-4099-1b37-522e-6cee61eb5c95

SEND

☒ LiveFlow Alerts
☐ Use TLS

Router Mappings

- *Router Mappings*: Router mappings are used exclusively when you are exporting LiveFlow data to LiveNX, and are used by LiveNX to display aggregated traffic from different segments as separate interfaces per the router map entries you enter in the *Router Mappings* settings.

ROUTER MAPPINGS LiveFlow will search the Router Mappings from top to bottom and select the first router that matches.

INTERFACE NAME	MAC	MPLS LABEL	VLAN ID	VXLAN VNI

+ Insert Edit Delete

LIVENX SNMP CONFIGURATION When adding a LiveFlow device to LiveNX from the LiveNX Add Device dialog, configure the 'Enter SNMP connection settings for this device' option as follows:

SNMP VERSION Version 3
 USER NAME admin
 AUTHENTICATION PROTOCOL SHA
 AUTHENTICATION PASSWORD Ys2Q5Xxu7g3gUoHxfUFifqIXSXd2tkc
 PRIVACY PROTOCOL AES 128-bit
 PRIVACY PASSWORD x3Fmpv90plsnk0Qg3rH25BKbD66fxzSK

Cancel OK

To add a router map entry for any adapter other than the Bridge adapter on LiveWire Edge, you will need to specify an interface name (ifname) and a MAC address of the gateway or router. The interface name can be up to 15 characters, and can include letters, numbers, and underscores. This will tell LiveNX to display aggregated traffic from different segments as separate interfaces per the router map entries.

To find the MAC address of the gateway or router, the CLI can be used; otherwise, capture some traffic, or do a Forensics search and look at the *Nodes* view in hierarchical mode. The top level addresses should be the MAC addresses of the gateways and routers for each segment being captured.

Note Although the CLI may display the MAC address using the abbreviated dot notation, the address must be formatted in full colon notation in the LiveWire *Router Mapping* entry dialog.

- *Interface Name*: Displays the interface name of the router. All interface names must be unique, must not be empty, must not be more than 15 characters long, and may only include the following characters: numbers, letters and an underscore (_).
- *MAC*: Displays the MAC address of the router. All MAC addresses must be a valid MAC address.
- *MPLS Label*: Displays the MPLS label (optional).
- *VLAN ID*: Displays the VLAN ID (optional).
- *VXLAN VNI*: Displays the VXLAN Network Identifier (optional).

- *Insert*: Click to add a new router mapping. You can add an unlimited number of router mappings.
- *Edit*: Click to edit the selected router mapping.
- *Delete*: Click to delete the selected router mappings from the list of router mappings.

Note The combination of *MAC address*, *MPLS Label*, *VLAN ID* and *VXLAN VNI* must be unique within the router mappings.

The router mappings are checked from top to bottom so you should be mindful to specify them in their desired order. Up and down arrows are provided for each row in the table to allow you to reorder them.

LiveNX SNMP Configuration

- *LiveNX SNMP Configuration*: For each LiveWire device that you want to use with LiveNX, you must use the Web client in LiveNX to add the device to LiveNX (see the LiveNX documentation). Since you are most likely adding LiveWire as an SNMP device to LiveNX, you will need the information provided below when adding the LiveWire device.

The screenshot shows the LiveWire Omnipeek web interface. The top navigation bar includes links for Home, Captures, Forensics, Files, Forensic Searches, Events, Adapters, Settings, and Admin. The main content area is titled 'LIVENX SNMP CONFIGURATION' and contains the following text: 'When adding a LiveFlow device to LiveNX from the LiveNX Add Device dialog, configure the 'Enter SNMP connection settings for this device' option as follows:'. Below this text is a form with the following fields:

SNMP VERSION	Version 3
USER NAME	admin
AUTHENTICATION PROTOCOL	SHA
AUTHENTICATION PASSWORD	Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc
PRIVACY PROTOCOL	AES 128-bit
PRIVACY PASSWORD	x3Fmpv9Oplsnk0Qg3rH25BKbd66fzxSK

At the bottom of the dialog, there are 'Cancel' and 'OK' buttons.

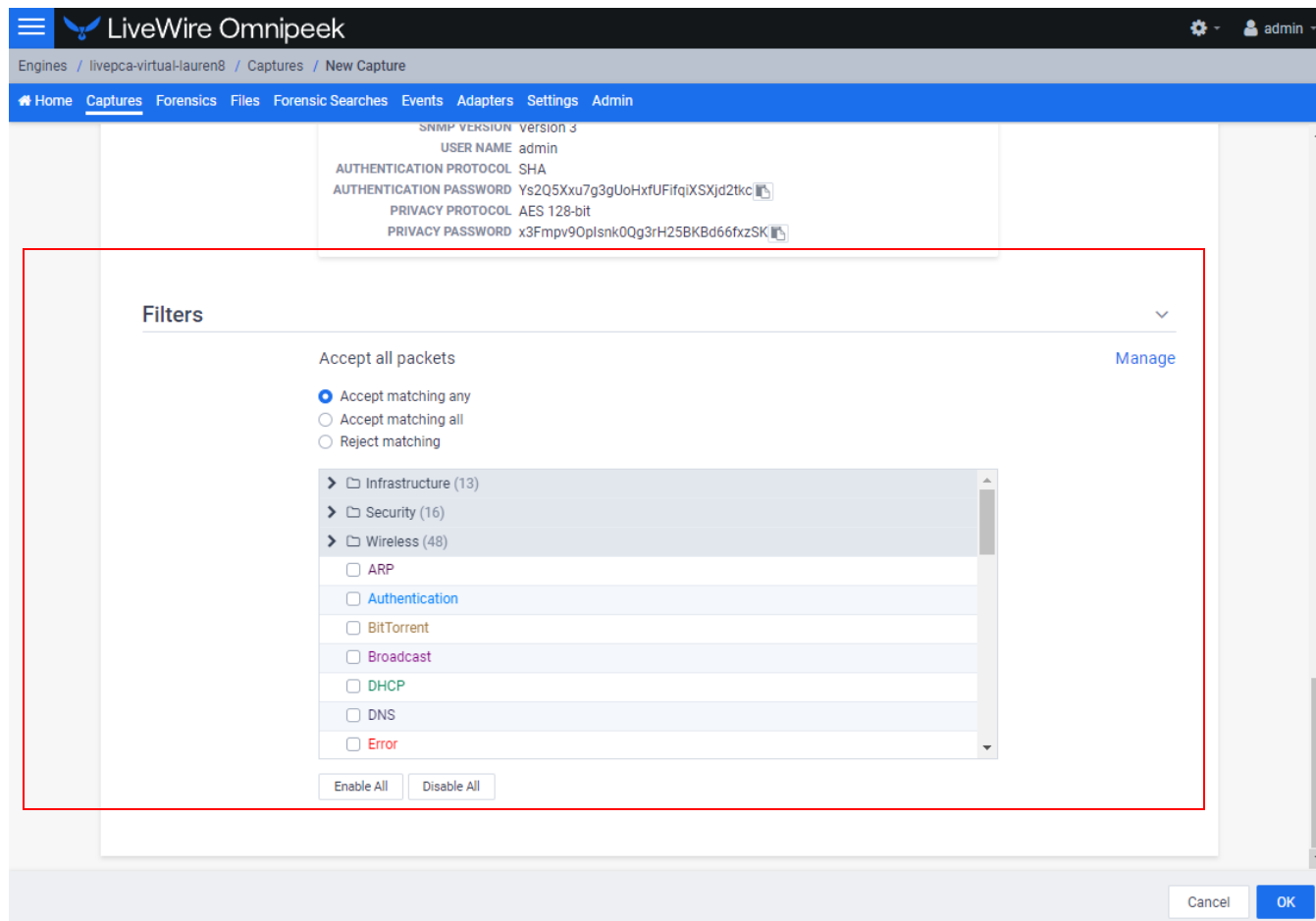
When configuring the 'Enter SNMP connection settings for this device' option from the **Add Device** dialog in LiveNX client, configure the option as follows:

SNMP Version: **Version 3**
 User Name: **admin**
 Authentication Protocol: **SHA**
 Authentication Password: **Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc**
 Privacy Protocol: **AES 128-bit**
 Privacy Password: **x3Fmpv9Oplsnk0Qg3rH25BKbd66fzxSK**

Note You can configure and change the *Authentication Password* and *Privacy Password*. See 'SNMP Credentials' in 'SNMP' on page 48.

Filters

The *Filters* settings let you enable or disable filters used when capturing packets or opening packet files. Select the filters you want to enable and then click *Accept Matching Any*, *Accept Matching All*, or *Reject Matching*.



- *Accept Matching Any*: When you choose *Accept Matching Any*, only those packets which match the parameters of at least one of the enabled filters are placed into the capture buffer.
- *Accept Matching All*: When you choose *Accept Matching All*, only those packets which match the parameters of all the enabled filters are placed into the capture buffer.
- *Reject Matching*: When you choose *Reject Matching*, only those packets which do not match any of the enabled filters are placed into the capture buffer.
- *Enable All*: Click to enable all filters.
- *Disable All*: Click to disable all filters.

Recommendations for better performance at higher data rates

- At high data rates the capture file can roll over multiple times every second. For higher data rates, the File Size should be increased. This will decrease how often the capture file has to be rolled over, and indirectly increase the performance.
- Forensic Searches use the same partition as the capture files, so leave some disk space available for the Forensic Search. Typically, 10-20 GB is sufficient, but the right setting will depend on the size of the forensic searches, and how many there are.
- Packet File Indexing is used to potentially increase Forensic Search performance when relevant filters are used. However, packet file indexing also decreases capture performance and can take a considerable amount of disk space.
- The file size and file indexes are related in that the smaller the file size the more packet indexes there will be. When there are more addresses, this can lead to large index files. A larger file size will generate fewer indexes.

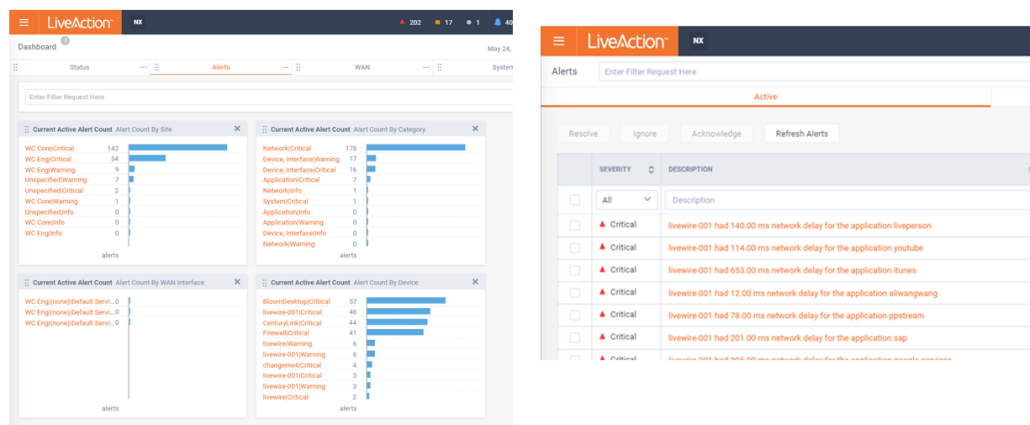
An example of using LiveWire, LiveNX, and Omnippeek

A web-based version of LiveAction's Omnippeek Network Analysis Software is available from LiveNX. You can easily start and use Omnippeek whenever you identify an interesting alert or flow in LiveNX that needs further investigation and you want to analyze the packet level details more closely in Omnippeek.

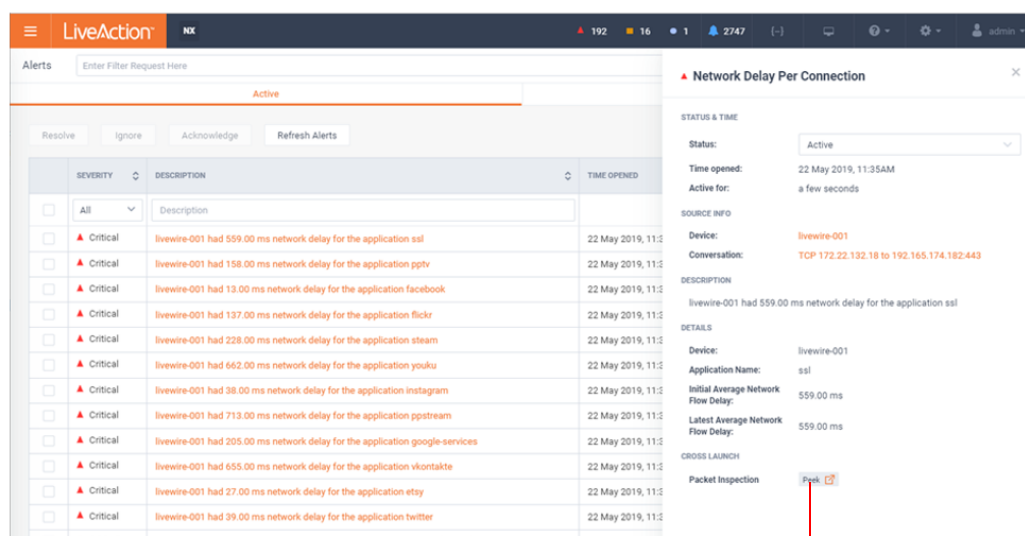
Note Omnippeek can be used independently of LiveNX, directly from the LiveWire appliance by entering the IP address of the LiveWire appliance into a web browser.

For example, a user on your network experiences poor call quality during a portion of their teleconference meeting. Since you have LiveNX and are populating it with both NetFlow from infrastructure routers as well as LiveFlow from LiveWire appliance, you can visualize any flow, including this teleconference call, from end to end.

Since the user did not want to disrupt their meeting to report the issue, you find out after the call has ended that the user experienced problems. Based on the user's information, you can quickly find the flow in LiveNX and see critical metrics regarding the call, including jitter and latency. The screen below shows alerts generated by LiveFlow sent from LiveWire.

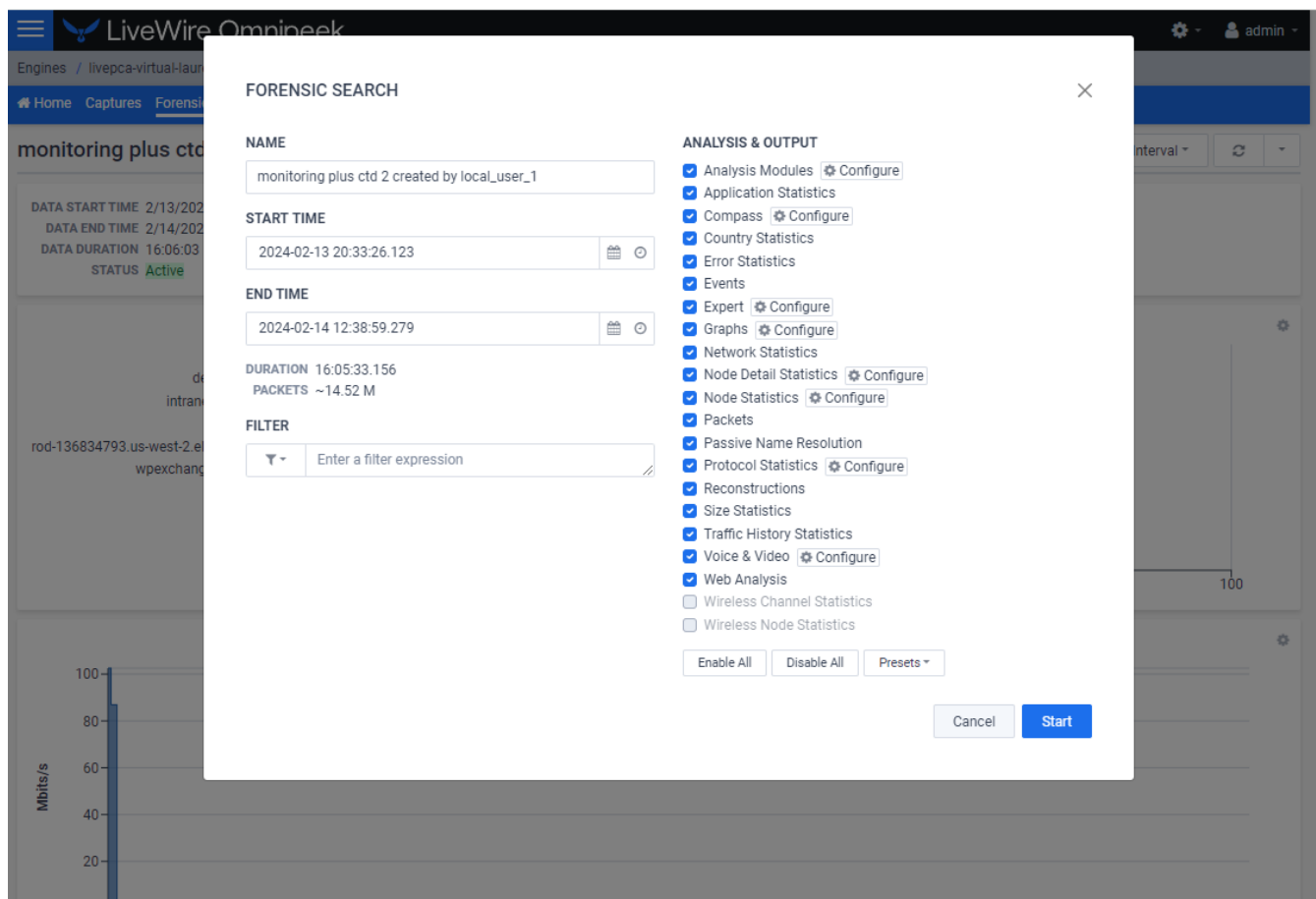


You also notice that an alert was triggered for excessive delay. This alert confirms the user's report, but you'd like to dig in even deeper to perform a root cause analysis of the issue. The best way to do this is with the network packets themselves, and since this call was captured by a LiveWire appliance you can simply click the 'Peek' button with the alert and immediately see all of the network packets for that teleconference session.



'Peek' button

When the Peek button is clicked to cross-launch to packets, a new tab will open in the browser, and a Forensic Search dialog will appear with various options. This allows you to perform detailed analysis on the call in Omnippeek and determine exactly when the jitter was bad, and correlate that with other activity on the network, to determine the root cause.

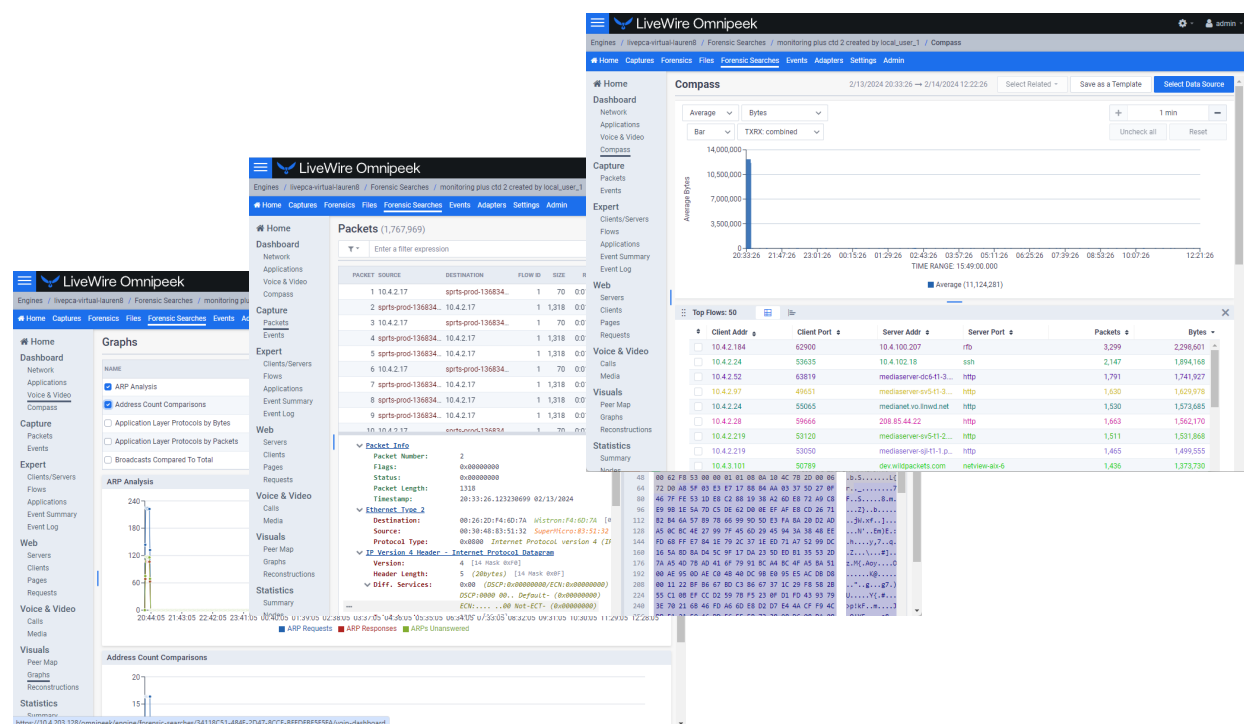


The default filter in the Forensic Search dialog includes the source and destination IP addresses of the flow. The filter can be changed to include more packets in the result, providing insight into what other traffic may be related or affecting the quality of the flow in question.

The time range can be adjusted to include more (or less) packets. This can work in conjunction with the filter, which when widened, will include more packets from the other flows between the source and destination IP.

The *Analysis & Output* options are used to include more or less analysis. The less analysis, the faster the forensic search will be. For example, if all you want are the packets, to load into Omnippeek, then just enable the packets option. Multiple forensic searches can be performed at the same time, and left running for others to use collaboratively. Keep in mind that a forensic search exists on the appliance, using memory and hard disk. When you are done using a forensic search it should be deleted.

The screen below shows various analysis views in Omnippeek which are good places to start understanding the problem as well as drill-down to the packets view.



The screen below shows the *Packets* view in Omnippeek which displays the list of packets and various other details about them, including the Experts, decode, and Hex view for each one.

LiveWire Omnipeek admin

Engines / livepca-virtuaLauren8 / Forensic Searches / monitoring plus ctd 2 created by local_user_1 / Packets

Home Captures Forensics Files **Forensic Searches** Events Adapters Settings Admin

Packets (1,767,969)

Enter a filter expression Apply

PACKET	SOURCE	DESTINATION	FLOW ID	SIZE	RELATIVE TIME	PROTOCOL	APPLICATION	SUMMARY	EXPERT	...
1	10.4.2.17	sprts-prod-136834...	1	70	0:01:20.190989	HTTPS	TCP	Src=53459,Dst= 4...		
2	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.190989	HTTPS	TCP	Src= 443,Dst=534...		
3	10.4.2.17	sprts-prod-136834...	1	70	0:01:20.190989	HTTPS	TCP	Src=53459,Dst= 4...		
4	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.191559	HTTPS	TCP	Src= 443,Dst=534...		
5	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.191559	HTTPS	TCP	Src= 443,Dst=534...		
6	10.4.2.17	sprts-prod-136834...	1	70	0:01:20.191559	HTTPS	TCP	Src=53459,Dst= 4...		
7	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.191559	HTTPS	TCP	Src= 443,Dst=534...		
8	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.191559	HTTPS	TCP	Src= 443,Dst=534...		
9	sprts-prod-136834...	10.4.2.17	1	1,318	0:01:20.191560	HTTPS	TCP	Src= 443,Dst=534...		
10	10.4.2.17	sprts-prod-136834...	1	70	0:01:20.191560	HTTPS	TCP	Src=53459,Dst= 4...		

Packet Info

Packet Number: 2

Flags: 0x00000000

Status: 0x00000000

Packet Length: 1318

Timestamp: 20:33:26.123230699 02/13/2024

Ethernet Type 2

Destination: 00:26:2D:F4:6D:7A *Wistron:F4:6D:7A* [0

Source: 00:30:48:83:51:32 *SuperMicro:83:51:32*

Protocol Type: 0x0800 *Internet Protocol version 4 (IP)*

IP Version 4 Header - Internet Protocol Datagram

Version: 4 [14 Mask 0xF0]

Header Length: 5 (20bytes) [14 Mask 0xF0]

Diff. Services: 0x00 (DSCP:0x00000000/ECN:0x00000000)

DSCP:0000 00.. Default- (0x00000000)

ECN:.... ..00 Not-ECT- (0x00000000)

00 26 2D F4 6D 7A 00 30 48 83 51 32 08 00 45 00 .&-..mz.00

05 14 25 57 40 00 33 06 E3 23 36 F5 F7 5F 0A 04 ..%0.3..#6..

02 11 01 8B D0 D3 31 0E EB 11 30 45 1F 08 80 101...0E.

00 62 F8 53 00 00 01 01 08 0A 10 4C 7B 2D 00 06 .b.S.....L{

72 D0 A8 5F 03 E3 E7 17 88 84 AA 03 37 5D 27 0F F.....7

46 7F FE 53 1D E8 C2 88 19 38 A2 60 E8 72 A9 C8 F..S.....m.

E9 98 1E 5A 7D C5 DE 62 D0 0E EF AF E8 CD 26 71 ...Z}.b.....

B2 B4 6A 57 89 78 66 99 9D 5D E3 FA 8A 20 D2 AD ..jW.xf...]

A5 0C BC 4E 27 99 7F 45 6D 29 45 94 3A 38 48 EE ...N'...Em)E.:.

FD 68 FF E7 84 1E 79 2C 37 1E ED 71 A7 52 99 DC .h....y7..q.

16 5A 8D 8A D4 5C 9F 17 DA 23 5D ED B1 35 53 2D 16 5A 8D 8A D4 5C 9F 17 DA 23 5D ED B1 35 53 2D

7A A5 4D 7B AD 41 6F 79 91 BC A4 BC 4F A5 BA 51 z.M{.Aoy....0

00 AE 95 0D AE C0 48 40 DC 9B E0 95 E5 AC D8 D8K@.....

00 11 22 BF B6 67 BD C3 86 67 37 1C 29 F8 58 28 ..".g...g7.)

55 C1 08 EF CC D2 59 78 F5 23 0F D1 FD 43 93 79 U.....Y{.#...

3E 70 21 68 46 FD A6 6D E8 D2 D7 E4 4A CF F9 4C >p1kF..m...J

Creating and Managing API Tokens

In this chapter:

About API Tokens 88

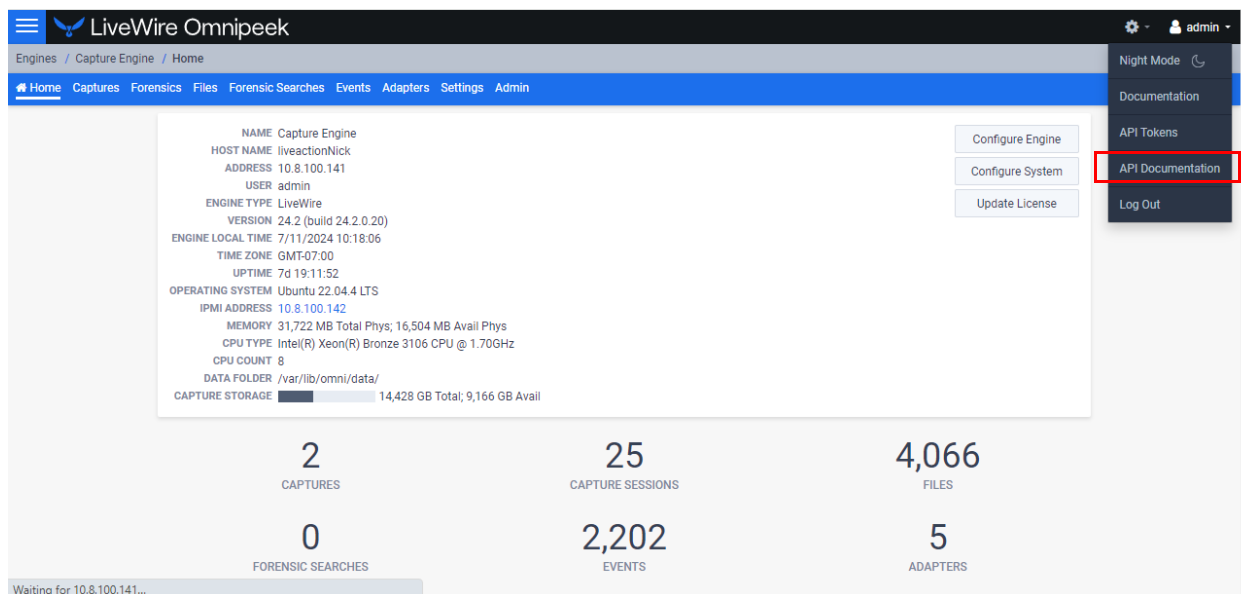
Creating an API Token 88

Managing API Tokens 90

About API Tokens

API tokens are used for authentication when using the Capture Engine REST-API. You can create and manage API tokens from Omnippeek. Once a token is created in Omnippeek, you can use the token in the REST-API calls.

The instructions to create and manage API tokens for the REST-API are provided below. For instructions on how to use the Capture Engine REST-API, refer to the *API Documentation* available from the *admin/user* menu in Omnippeek.



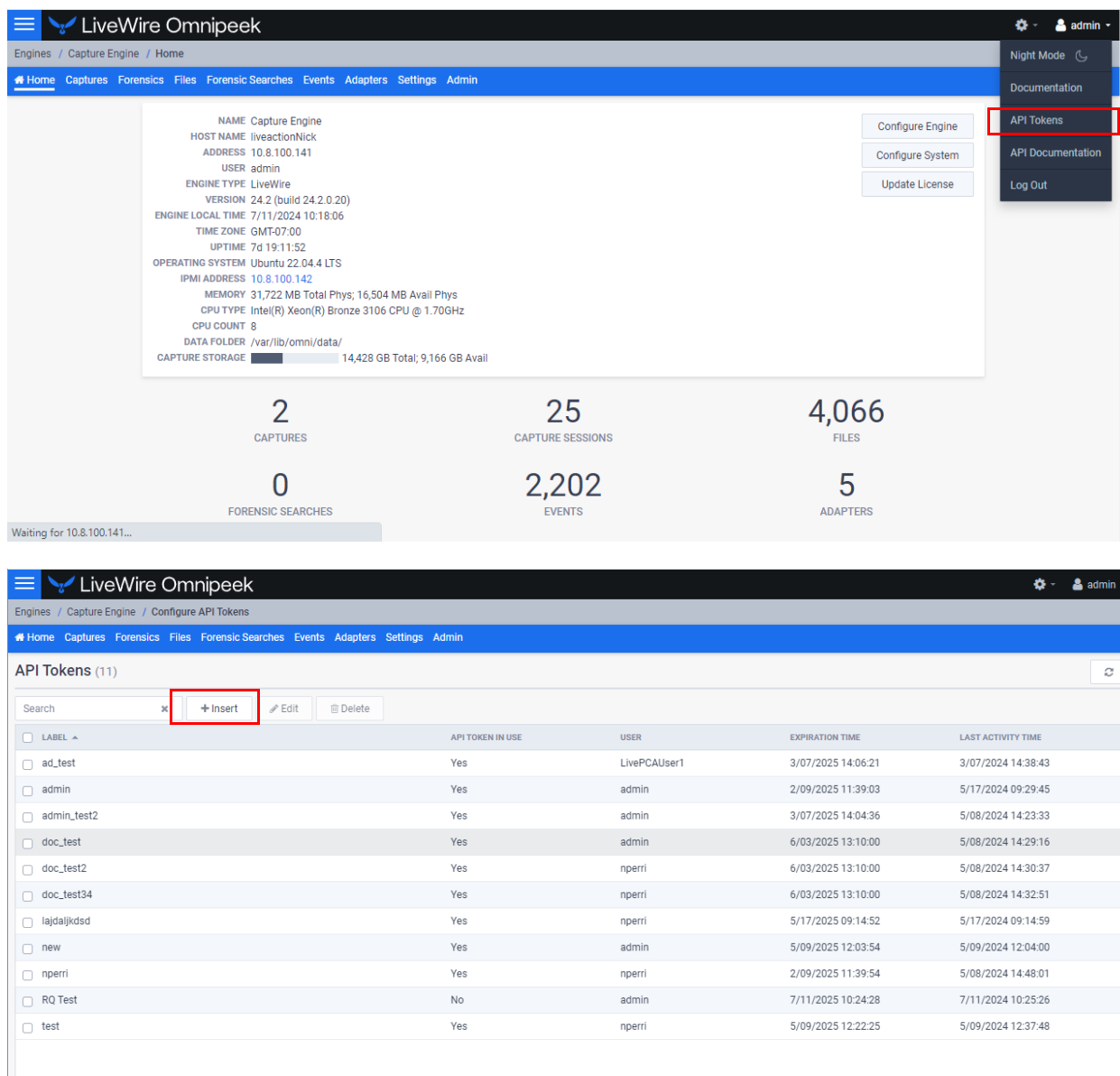
Creating an API Token

Note An API token has all of the permissions/policies as the user that created the API token.

To create an API token:

1. In Omnippeek, click **API Tokens** from the *admin* menu. The *API Tokens* page appears.

Note The **API Tokens** menu item is only available if ACL is disabled or if the *Configuration: Configure API Tokens* ACL policy is enabled. See 'Enabling Access Control' on page 93.



NAME Capture Engine
 HOST NAME liveactionNick
 ADDRESS 10.8.100.141
 USER admin
 ENGINE TYPE LiveWire
 VERSION 24.2 (build 24.2.0.20)
 ENGINE LOCAL TIME 7/11/2024 10:18:06
 TIME ZONE GMT-07:00
 UPTIME 7d 19:11:52
 OPERATING SYSTEM Ubuntu 22.04.4 LTS
 IPMI ADDRESS 10.8.100.142
 MEMORY 31,722 MB Total Phys; 16,504 MB Avail Phys
 CPU TYPE Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz
 CPU COUNT 8
 DATA FOLDER /var/lib/omni/data/
 CAPTURE STORAGE 14,428 GB Total; 9,166 GB Avail

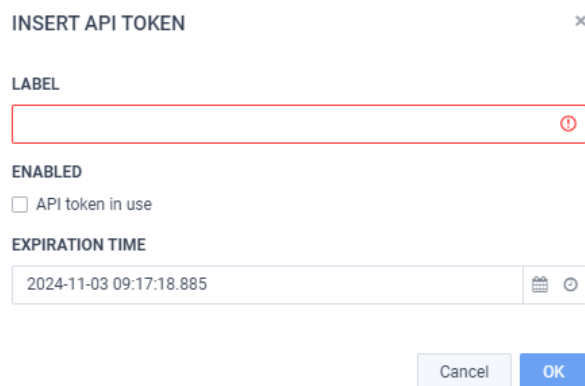
2 CAPTURES
 25 CAPTURE SESSIONS
 4,066 FILES
 0 FORENSIC SEARCHES
 2,202 EVENTS
 5 ADAPTERS

Waiting for 10.8.100.141...

API Tokens (11)

LABEL	API TOKEN IN USE	USER	EXPIRATION TIME	LAST ACTIVITY TIME
ad_test	Yes	LivePCAUser1	3/07/2025 14:06:21	3/07/2024 14:38:43
admin	Yes	admin	2/09/2025 11:39:03	5/17/2024 09:29:45
admin_test2	Yes	admin	3/07/2025 14:04:36	5/08/2024 14:23:33
doc_test	Yes	admin	6/03/2025 13:10:00	5/08/2024 14:29:16
doc_test2	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:30:37
doc_test34	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:32:51
lajdaljkdsd	Yes	nperrri	5/17/2025 09:14:52	5/17/2024 09:14:59
new	Yes	admin	5/09/2025 12:03:54	5/09/2024 12:04:00
nperrri	Yes	nperrri	2/09/2025 11:39:54	5/08/2024 14:48:01
RQ Test	No	admin	7/11/2025 10:24:28	7/11/2024 10:25:26
test	Yes	nperrri	5/09/2025 12:22:25	5/09/2024 12:37:48

2. Click **Insert**. The *Insert API Token* dialog appears.



INSERT API TOKEN

LABEL

ENABLED

☐ API token in use

EXPIRATION TIME

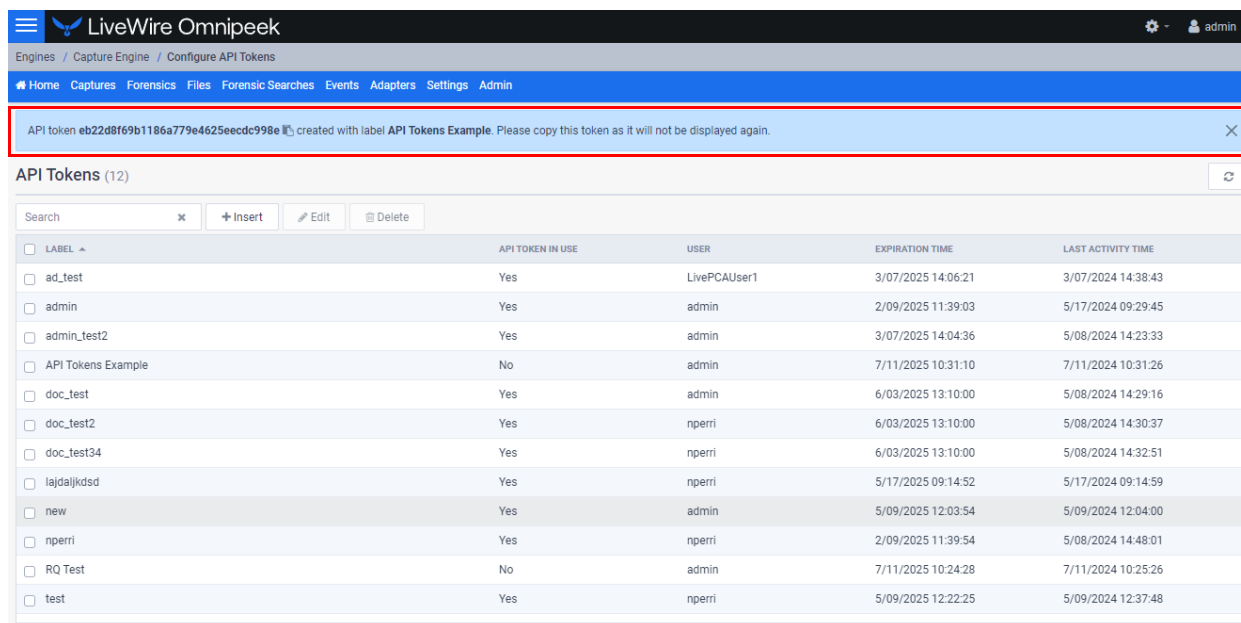
2024-11-03 09:17:18.885

Cancel OK

3. Configure the dialog:

- **Label:** Enter a descriptive label for the API token. A descriptive label helps you to identify the API token.
- **Enabled:** Select the check box to enable the API token.
- **Expiration Time:** Click the Select date and Select time icons to set the date and time in which the API token expires and can no longer be used.

4. Click **OK**. A blue banner appears and displays the API token along with its *Label*. You can now use the new token from the blue banner for REST-API authentication.



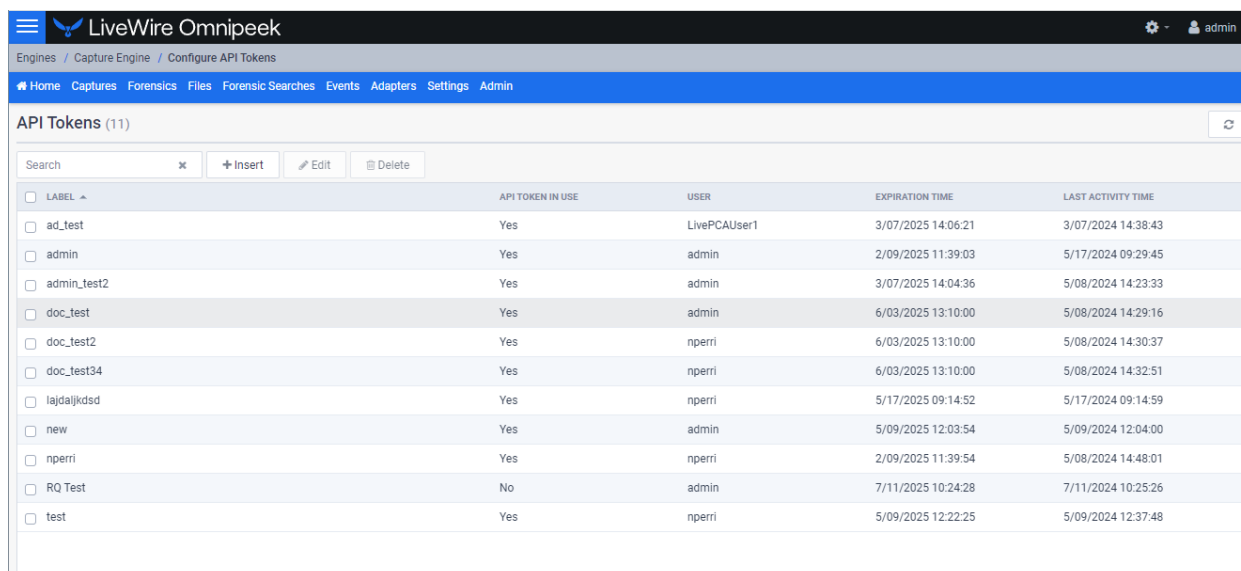
The screenshot shows the LiveWire Omnipeek interface. At the top, a blue banner displays the API token `eb22d8f69b1186a779e4625eecd998e` and the label `API Tokens Example`. Below the banner, the **API Tokens (12)** table is visible. The table has columns for **LABEL**, **API TOKEN IN USE**, **USER**, **EXPIRATION TIME**, and **LAST ACTIVITY TIME**.

LABEL	API TOKEN IN USE	USER	EXPIRATION TIME	LAST ACTIVITY TIME
ad_test	Yes	LivePCAUser1	3/07/2025 14:06:21	3/07/2024 14:38:43
admin	Yes	admin	2/09/2025 11:39:03	5/17/2024 09:29:45
admin_test2	Yes	admin	3/07/2025 14:04:36	5/08/2024 14:23:33
API Tokens Example	No	admin	7/11/2025 10:31:10	7/11/2024 10:31:26
doc_test	Yes	admin	6/03/2025 13:10:00	5/08/2024 14:29:16
doc_test2	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:30:37
doc_test34	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:32:51
lajdaljkdsd	Yes	nperrri	5/17/2025 09:14:52	5/17/2024 09:14:59
new	Yes	admin	5/09/2025 12:03:54	5/09/2024 12:04:00
nperrri	Yes	nperrri	2/09/2025 11:39:54	5/08/2024 14:48:01
RQ Test	No	admin	7/11/2025 10:24:28	7/11/2024 10:25:26
test	Yes	nperrri	5/09/2025 12:22:25	5/09/2024 12:37:48

Important! Please copy the token from the blue banner and save it to a safe location. For security reasons, the token will not be displayed again.

Managing API Tokens

You can manage API tokens from the *API Tokens* page.



The screenshot shows the LiveWire Omnipeek interface with the **API Tokens (11)** table. The table has columns for **LABEL**, **API TOKEN IN USE**, **USER**, **EXPIRATION TIME**, and **LAST ACTIVITY TIME**.

LABEL	API TOKEN IN USE	USER	EXPIRATION TIME	LAST ACTIVITY TIME
ad_test	Yes	LivePCAUser1	3/07/2025 14:06:21	3/07/2024 14:38:43
admin	Yes	admin	2/09/2025 11:39:03	5/17/2024 09:29:45
admin_test2	Yes	admin	3/07/2025 14:04:36	5/08/2024 14:23:33
doc_test	Yes	admin	6/03/2025 13:10:00	5/08/2024 14:29:16
doc_test2	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:30:37
doc_test34	Yes	nperrri	6/03/2025 13:10:00	5/08/2024 14:32:51
lajdaljkdsd	Yes	nperrri	5/17/2025 09:14:52	5/17/2024 09:14:59
new	Yes	admin	5/09/2025 12:03:54	5/09/2024 12:04:00
nperrri	Yes	nperrri	2/09/2025 11:39:54	5/08/2024 14:48:01
RQ Test	No	admin	7/11/2025 10:24:28	7/11/2024 10:25:26
test	Yes	nperrri	5/09/2025 12:22:25	5/09/2024 12:37:48

- *Search*: Type in the search bar to filter the table of API tokens by the 'Label' column.
- *Insert*: Click to insert a new API token. See 'Creating an API Token' on page 88.
- *Edit*: Click to edit the selected API token.
- *Delete*: Click to edit the selected API token.
- *Refresh*: Click to refresh the list of API tokens.
- *Check Box*: Select the check box of the API token you wish to manage. Selecting the check box at the top of the column selects all of the API tokens displayed in the tabel.
- *Label*: Displays the label for the API token.
- *Enabled*: Displays whether or not the API token can be used.
- *Expiration Time*: Displays the date and time in which the API token expires and can no longer be used.
- *Last Activity Time*: Displays the date and time at which the API token was last used or modified.

Important! When a new API token is successfully created, a blue banner is displayed across the top of the *API Tokens* window displaying the API token associated label for the API token. Please copy the token from the blue banner and save it to a safe location. For security reasons, the token is displayed only once and will not be displayed again.

Configuring Access Control

In this chapter:

- About Access Control* 93
- Enabling Access Control* 93
- About Roles* 97
- Configuring Roles* 97
- Adding a Role* 106
- Enabling Third-Party Authentication* 107
- When Upgrading From LiveWire v23.3.1 or Earlier* 113

About Access Control

The Access Control List (ACL) feature in LiveWire provides the ability to restrict access of predefined actions to a particular set of roles and users. This allows users to be given different privileges for when they are using LiveWire. These predefined actions are called policies. A full list of these policies are described in 'Policy Descriptions' on page 99. To learn about roles, see 'About Roles' on page 97. To manage users and groups assigned to the roles, see 'Manage Users for Roles' on page 102 and 'Manage Groups for Roles' on page 103.

Enabling Access Control

Access control is enabled via the *Engine* screen in Omnipeek.

To enable Access Control:

1. Use Omnipeek to view the *Home* page.

NAME Capture Engine
 HOST NAME liveaction
 ADDRESS 10.8.100.141
 USER admin
 ENGINE TYPE LiveWire
 VERSION 23.4 (build 23.4.0.6)
 ENGINE LOCAL TIME 11/07/2023 09:53:34
 TIME ZONE GMT-08:00
 UPTIME 17:05:29
 OPERATING SYSTEM Ubuntu 22.04.3 LTS
 IPMI ADDRESS 10.8.100.142
 MEMORY 31,722 MB Total Phys; 26,047 MB Avail Phys
 CPU TYPE Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz
 CPU COUNT 8
 DATA FOLDER /var/lib/omni/data/
 CAPTURE STORAGE 14,428 GB Total; 14,304 GB Avail

Configure Engine
 Configure System
 Update License

0 CAPTURES
 7 CAPTURE SESSIONS
 25 FILES
 0 FORENSIC SEARCHES
 319 EVENTS
 5 ADAPTERS
 113 FILTERS
 29 SETTINGS
 60 ALARMS
 1 NOTIFICATIONS
 0 PROTOCOL TRANSLATIONS
 33,864 NAMES
 4 HARDWARE PROFILES
 0 DECRYPTION KEYS

2. Click **Configure Engine**. The *Configure Engine* page appears.

The screenshot shows the 'CONFIGURE ENGINE' page in the LiveWire Omnipeek interface. The 'General' tab is selected. The page includes a navigation bar at the top with links to Home, Captures, Forensics, Files, Forensic Searches, Events, Adapters, Settings, and Admin. The main content area contains the following settings:

- NAME:** Capture Engine
- IP ADDRESS:** Any address (with a dropdown arrow and a note: 'Choose the IP address used with Omnipeek')
- PORT:** 6367
- MAX CONNECTIONS:** 100
- ☐ Enable auto discovery
- ☒ Automatically restart captures
- DATA FOLDER:** /var/lib/omni/data (with a 'Browse' button)
- LOG MAX:** 200000
- LOG ADJUST:** 100000

At the bottom right, there are three buttons: 'Close', 'Apply to Other Engines', and 'Apply'.

3. Scroll down to the *Access Control* settings.

The screenshot shows the 'CONFIGURE ENGINE' page with the 'Security' tab selected. The 'Access Control' section is highlighted with a red rectangle. The settings in this section are:

- ☒ Enable OS authentication only
- ☐ Enable third-party authentication
- ☐ Enable two-factor authentication
- ☐ Send audit log messages to syslog
- ☐ Enable access control

At the bottom right, there are three buttons: 'Close', 'Apply to Other Engines', and 'Apply'.

4. Select *Enable access control* to expand the access control settings.

Note If *Roles* have not yet been enabled as shown below, you must manually convert access control to a roles-based approach by clicking **Convert Access Control To Roles** when the button is displayed in the *Access Control* settings. Although you can choose to not manually opt-in to the role-based approach, it is advisable to switch to a roles-based approach in order to have the ability to assign ACL policies to multiple users simultaneously rather than having to assign them to each user individually. This is incredibly useful if you have a large number of users using LiveWire.

Additionally, a roles-based approach is required to use the data exclusion feature in LiveWire, which allows you to filter packet data to only analyze and reveal a filtered subset of the packet data in a forensic search, distributed forensic search, or MSA search. This filtering is accomplished by using a specific Capture Engine filter specified in an ACL role. Therefore, the data exclusion feature is restricted to ACL roles.

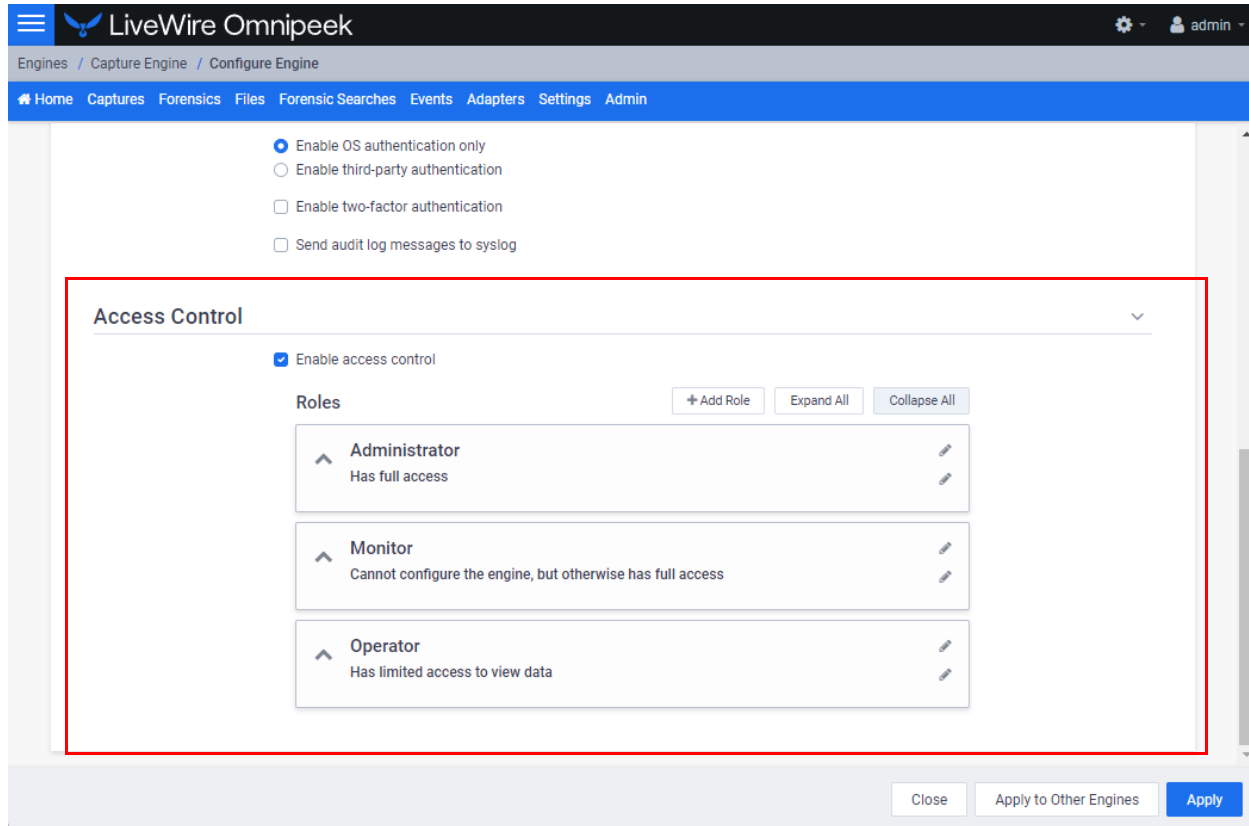
Non role-based access control settings:

The screenshot shows the 'Access Control' configuration page in LiveWire Omnippeek. The page has a header with the LiveWire logo and 'admin' user. The main content area is titled 'Access Control' and includes a checkbox 'Enable access control' which is checked. Below this is a table with two columns: 'POLICY' and 'USERS'. The table lists various policies and the users assigned to them. At the bottom of the table, there is a button labeled 'Convert Access Control To Roles' which is highlighted with a red rectangle. A 'Close' button is located at the bottom right of the page.

POLICY	USERS
Allow Capture Engine usage	admin, local_user_1, local_user_2, LivePCAUser1
Capture: Create new capture	admin, local_user_1, LivePCAUser1
Capture: Delete captures created by other users	admin, local_user_1, LivePCAUser1
Capture: Start/stop captures created by other users	admin
Capture: Modify captures created by other users	admin
Capture: View captures created by other users	admin, local_user_1, LivePCAUser1
Capture / Forensic Search: View packets from captures and forensic searches created by other users	admin, local_user_1, LivePCAUser1
Capture / Forensic Search: View statistics from captures and forensic searches created by other users	admin, local_user_1, LivePCAUser1
Capture: Delete files created by other users	admin
Configuration: Configure engine settings	admin
Configuration: View the audit log	admin, local_user_2
Configuration: Upload files	admin, local_user_2
Configuration: Download packet data	admin, local_user_2
Forensic Search: Create new forensic search	admin, local_user_1, LivePCAUser1
Forensic Search: Delete forensic searches created by other users	admin, local_user_1, LivePCAUser1
Forensic Search: View forensic searches created by other users	admin, local_user_1, LivePCAUser1

Convert Access Control To Roles

Role-based access control settings:



- *Enable access control:* Select this setting to enable access control.
- *Add Role:* Click to add a new role to the list of roles. You will need to provide a unique name for the role.
- *Expand All:* Click to expand the settings displayed for each of the roles.
- *Collapse All:* Click to collapse the settings displayed for each of the roles.
- *Roles:* Displays the set of *roles* for LiveWire.
 - *Administrator:* The default *Administrator* role is configured to provide full access to LiveWire to users or groups that have been assigned to this role.
 - *Monitor:* The default *Monitor* role is configured so that users or groups assigned to this role cannot configure LiveWire, but otherwise have full access to LiveWire.
 - *Operator:* The default *Operator* role is configured so that users assigned to this role have limited access to view data.

Apply to Other Engines

- *Apply to Other Engines:* Click to open a wizard that allows you to send all of the current engine configurations (security, authentication, and access control settings) to multiple other engines. All of the other engines must be running the same engine version of the current engine.

Apply

- *Apply:* Click to apply all Access Control settings to LiveWire.

About Roles

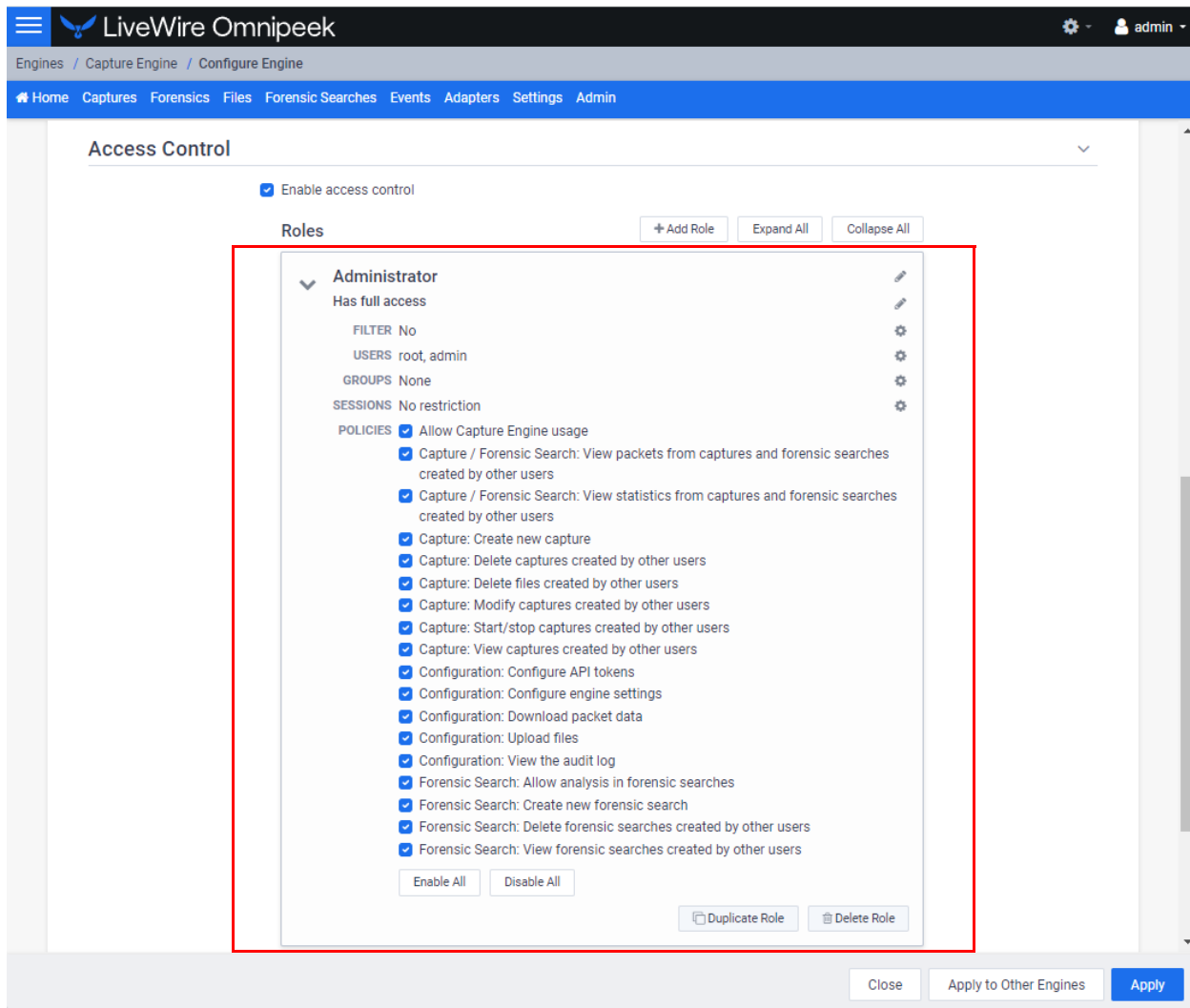
Roles are a collection of pre-defined policies for specific actions within LiveWire. For each role, one or more Policies are selected, and users or Active Directory groups are assigned. LiveWire includes a default set of roles (*Administrator*, *Monitor*, and *Operator*), with each providing a unique set of policies to the users and Active Directory groups assigned to the role. A user with the policy to configure the engine (*Configuration: Configure engine settings*) shall have the ability to adjust the policies within each of these roles and also add additional roles.

Each role has the following components:

- *Role name*: The name given to the role.
- *Role description*: A short description that describes the role.
- *Filters*: Filters can be configured to limit access to certain data in addition to global policies. See 'Configuring Filters for Roles' on page 100.
- *Users*: Users are the list of individual users of a system with a valid username/password that are assigned to a role.
- *Groups*: Groups are a list of the Active Directory groups assigned to a role. See also 'Manage Groups for Roles' on page 103.
- *Policy/Policies*: Policies are specific actions within the product that LiveAction chooses to control with permissions, for example, starting a capture. Policies are applied to users or roles only. See 'Policy Descriptions' on page 99.

Configuring Roles

Roles are configured in the *Access Control* settings in Omnipeek.



- **Role Name:** A descriptive name for the role. For example, *Administrator*, *Monitor*, and *Operator*. Click the *edit* icon to change the name. Click the up and down arrow next to the name to expand or collapse the role.
- **Role Description:** A short description of the role. For example, *Has full access*. Click the *edit* icon to change the description.
- **Filter:** Displays whether or not (Yes or No) filter rules have been configured for the role. Filters can be configured to limit access to certain data in addition to global policies. See also 'Configuring Filters for Roles' on page 100. Click the *Filter* gear icon to configure a filter.
- **Users:** Displays the users associated with the role. Click the *Users* gear icon to select one or more users. See also 'Manage Users for Roles' on page 102.
- **Groups:** Displays the Active Directory groups associated with the role. Click the *Groups* gear icon to select one or more groups. See also 'Manage Groups for Roles' on page 103.
- **Policies:** Select one or more policies associated with a role. See also 'Policy Descriptions' on page 99.
- **Enable All:** Click to enable all policies for the role.
- **Disable All:** Click to disable all policies for the role.
- **Duplicate Role:** Click to duplicate a role with the same configuration of the existing role. You will need to provide a unique name of the duplicate role.
- **Delete Role:** Click to delete the role.

Note If the same user is added to multiple roles, policy permissions will be ORed together but filters will be ANDed together.

Policy Descriptions

The following table provides a description of the policies available to enable for any role:

Policy	Description
Allow Capture Engine usage	This policy allows a user to use any REST-API or Omni protocol command, which effectively includes all Capture Engine functionality.
Capture / Forensic Search: View packets from captures and forensic searches create by other users	This policy allows a user to view packets from captures and forensic searches created by other users.
Capture / Forensic Search: View statistics from captures and forensic searches create by other users	This policy allows a user to view statistics from captures and forensic searches created by other users. This policy also allows access to MSA projects the user doesn't own.
Capture: Create new capture	This policy allows a user to create a new capture.
Capture: Delete captures created by other users	This policy allows a user to delete captures created by other users.
Capture: Delete files created by other users	This policy allows a user to delete capture files created by other users.
Capture: Modify captures create by other users	This policy allows a user to modify the capture settings for captures created by other users.
Capture: Start/stop captures created by other users	This policy allows a user to start and stop captures created by other users.
Capture: View captures created by other users	This policy allows a user to view captures and capture data created by other users. The user must also have either the View Packets ACL or View Statistics ACL permission (first two policies in this table) as well to open a capture window for a capture the user doesn't own.
Configuration: Configure API tokens	This policy allows a user to configure and view API tokens.
Configuration: Configure engine settings	This policy allows a user to configure and view engine settings.
Configuration: Download packet data	This policy allows a user to download packet files from captures and distributed forensic searches.
Configuration: Save packet data	This policy allows users to save packet data from captures and forensic searches.
Configuration: Upload files	This policy allows a user to upload or open packet files.
Configuration: View the audit log	This policy allows a user to view the Audit Log.
Forensic Search: Allow analysis in forensic searches	This policy allows the user to perform analysis in forensic searches. Without this policy, users will only be able to perform a forensic search that shows packets and only packets.
Forensic Search: Create new forensic search	This policy allows a user to create forensic searches and distributed forensic searches, and to perform a cross launch from LiveNX.
Forensic Search: Delete forensic searches created by other users	This policy allows the user to delete a forensic search, distributed forensic search, or MSA project created by others.
Forensic Search: View forensic searches created by other user	This policy allows a user to view forensic searches and distributed forensic searches created by others. The user must also have either the View Packets ACL or View Statistics ACL permission (first two policies in this table) as well to view the forensic search for a forensic search the user doesn't own.

Policy Description notes:

- In order to delete capture sessions from the Forensics view, the user must have the *Delete Captures* and the *Delete Files* policies.
- The *View Captures*, *Save Packet Data* and *Create Forensic Search* policies will affect which capture sessions are available to the user when performing a distributed forensic search or creating an MSA project. The user must have the *View Captures* policy on the target engine to see capture sessions for captures the user doesn't own. The user must have the *Save Packet Data* and *Create Forensic Search* policies on the target engine to see any of its capture sessions.
- The user must have the *Upload Files* and *Create Forensic Search* policies to create a distributed forensic search and to create an MSA project.
- Users always maintain control over their own data, for example, deleting a capture they started. See also 'Manage Users for Roles' on page 102.

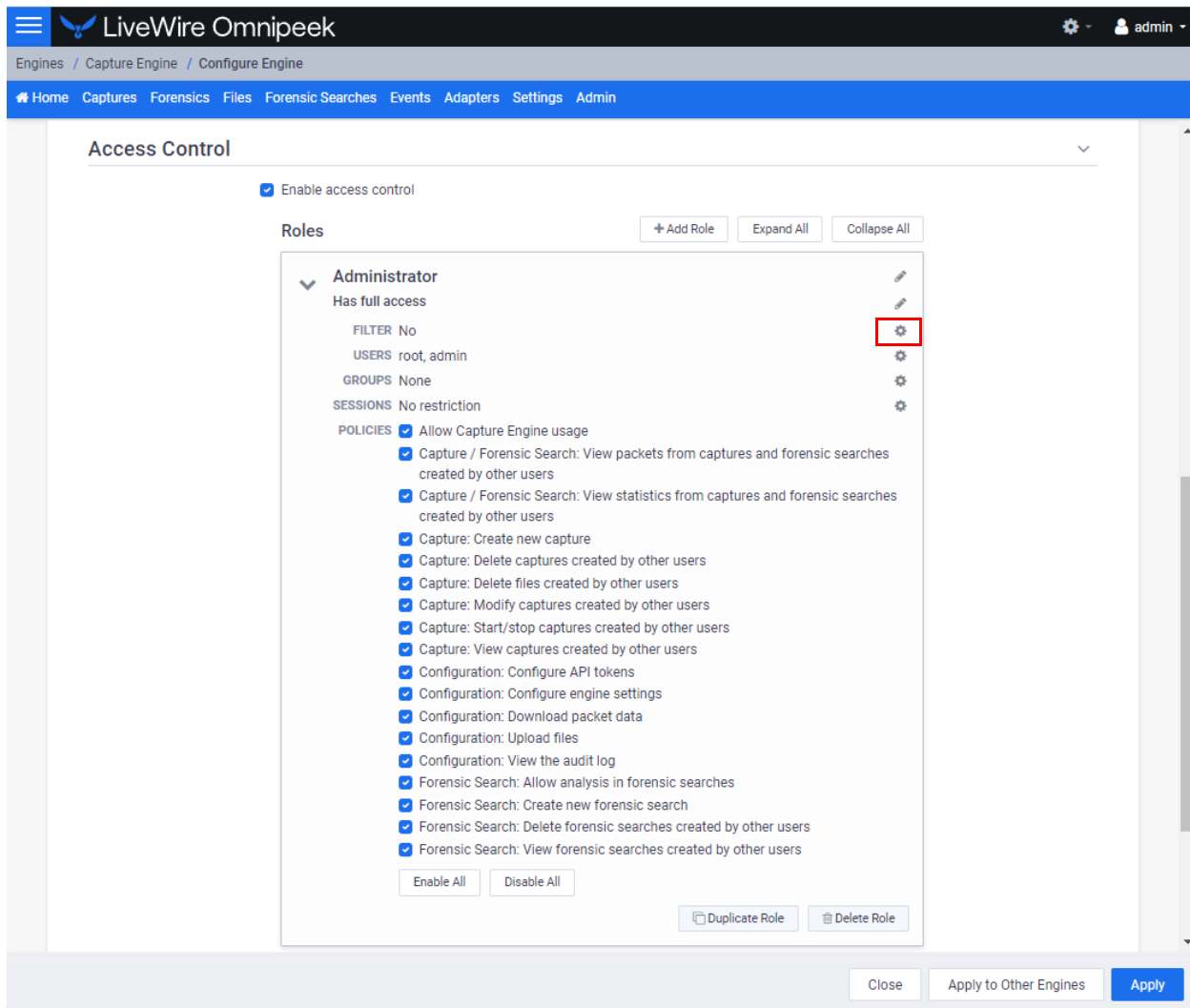
Configuring Filters for Roles

Filters can be configured to limit access to certain data in addition to global policies for each role.

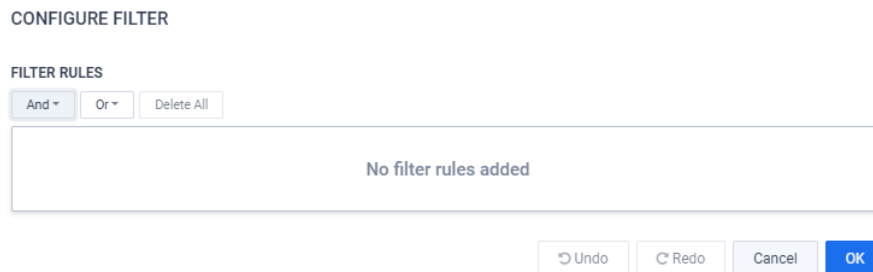
Note Any filters supplied when creating a forensic search will be 'ANDed' together with the role filter.

To configure filters for roles:

1. Click the *Filter* gear icon. The *Configure Filter* dialog appears.



2. Configure the filter.

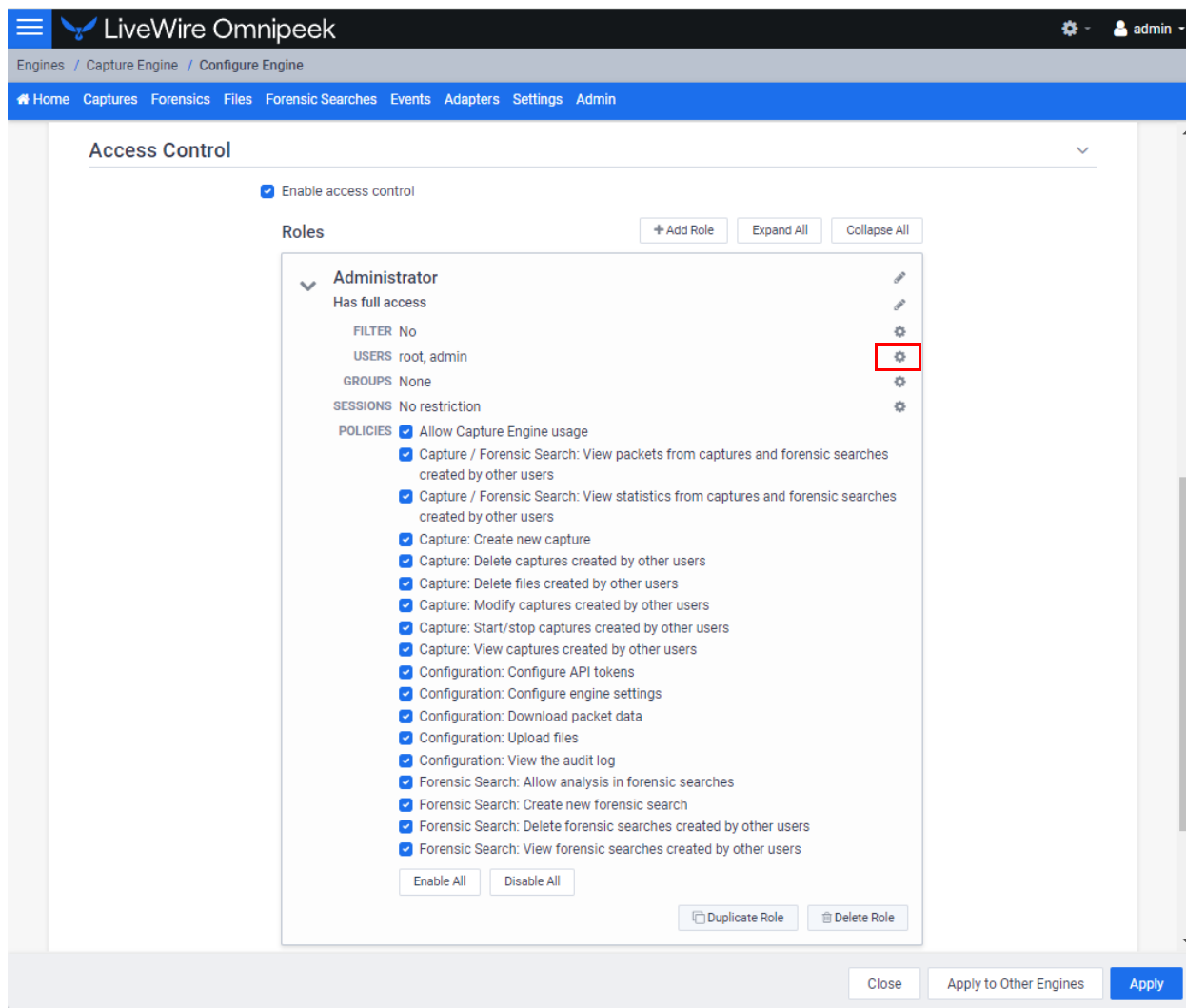


- *And*: Click to select the type of data to include in your *And* filter. You can further refine your filter by clicking the filter rule once it is added to the *Filter Rules*.
- *Or*: Click to select the type of data to include in your *Or* filter. You can further refine your filter by clicking the filter rule once it is added to the *Filter Rules*.
- *Delete All*: Click to delete all filter rules displayed in the *Filter Rules*.

Manage Users for Roles

To manage the users assigned to a role:

1. Click the *Users* gear icon. The *Add/Remove Users* dialog appears.



2. Configure the users.

ADD/REMOVE USERS
×

LOCAL USERS

root	Add
root	
nobody	Add
nobody	
nperr	Add
...	

THIRD-PARTY AUTHENTICATION USER

	Add
--	-----

SELECTED USERS

admin	Remove
Administrator	

Remove All

Cancel

OK

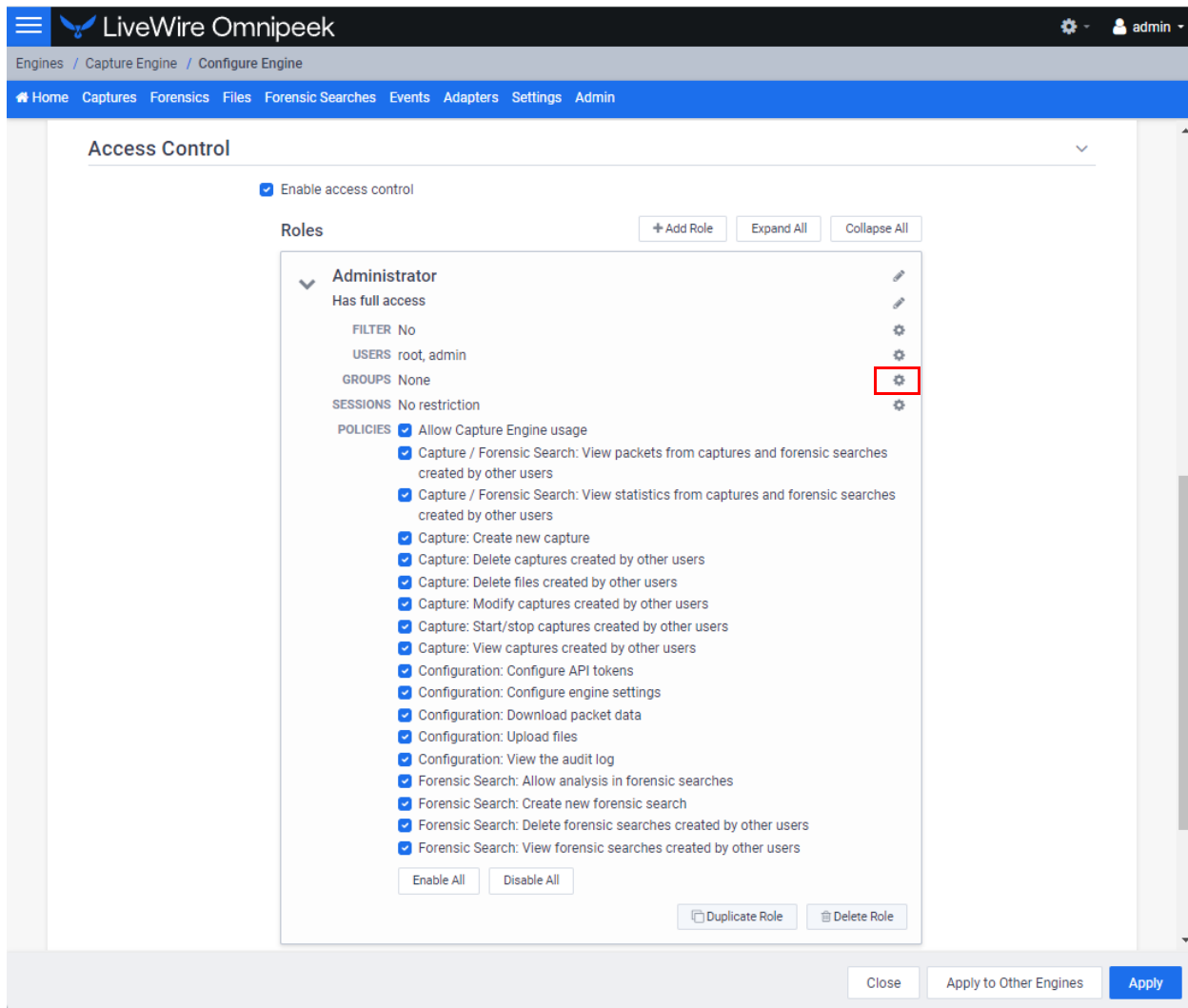
- *Local Users*: Displays the local users that can be added to a role. Click *Add* to add a user to the *Selected Users* list.
- *Third-Party Authentication User*: Allows users to type in third-party users from third-party authentication servers. Click *Add* to add a user to the *Selected Users* list.
- *Selected Users*: Displays the users added to the role. Click *Remove* to remove a user from the *Selected Users* list.
- *Remove All*: Click to remove all the users from the *Selected Users* list.

Manage Groups for Roles

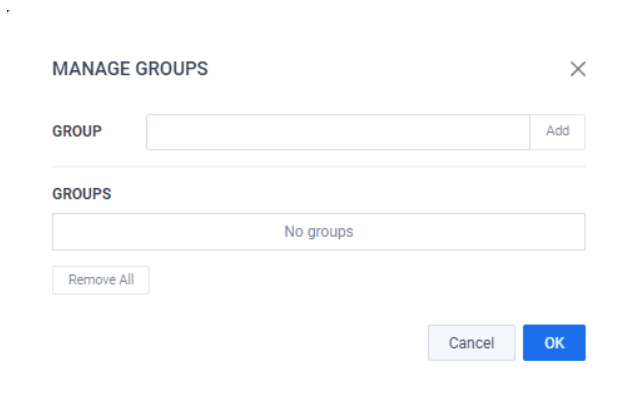
Note If you assign a group to any of the Access Control roles, third-party authentication must also be enabled. See 'Enabling Third-Party Authentication' on page 107. Additionally, a valid Active Directory entry must be added and enabled as well.

To manage the groups assigned to a role:

1. Click the *Groups* gear icon. The *Manage Groups* dialog appears.



2. Configure the groups.



- *Group*: Type in a group name to be added to a role. Click *Add* to add a group to the *Groups* list.
- *Groups*: Displays the groups added to the role. For each Active Directory group in the list, there are three buttons for the following:
 - *Validate*: Click to validate the group exists in the Active Directory server supplied in third-party authentication.

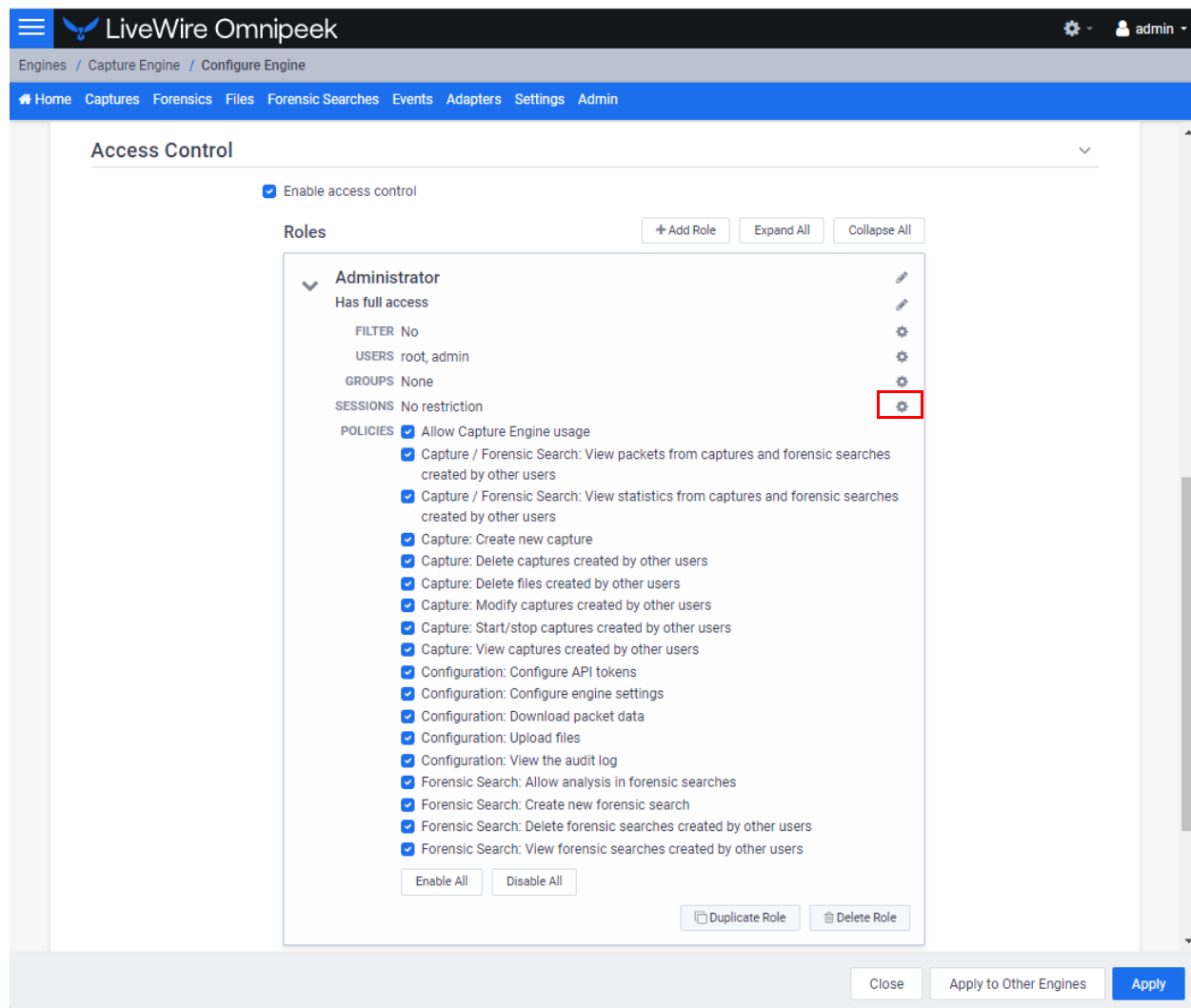
- *Users*: Click to validate a given user is found in the Active Directory group; the *Test User* dialog appears.
- *Remove*: Click to remove the group from the list.
- *Remove All*: Click to remove all groups from the *Groups* list.

Manage Sessions for Roles

Sessions are for limiting the number of concurrent login sessions for a user assigned to a specific role. For example, if there is a role called *Monitor* and it's session limit is set to 2, then any user who is assigned to that role can only have a maximum of two concurrent sessions.

To manage the sessions assigned to a role:

1. Click the *Sessions* gear icon. The *Manage Sessions* dialog appears.



2. Configure the sessions.

MANAGE SESSIONS


☐ Enable session control

0

Cancel

OK

- *Enable session control:* Select this option to enable session control, and set the session limit to a number > 0.

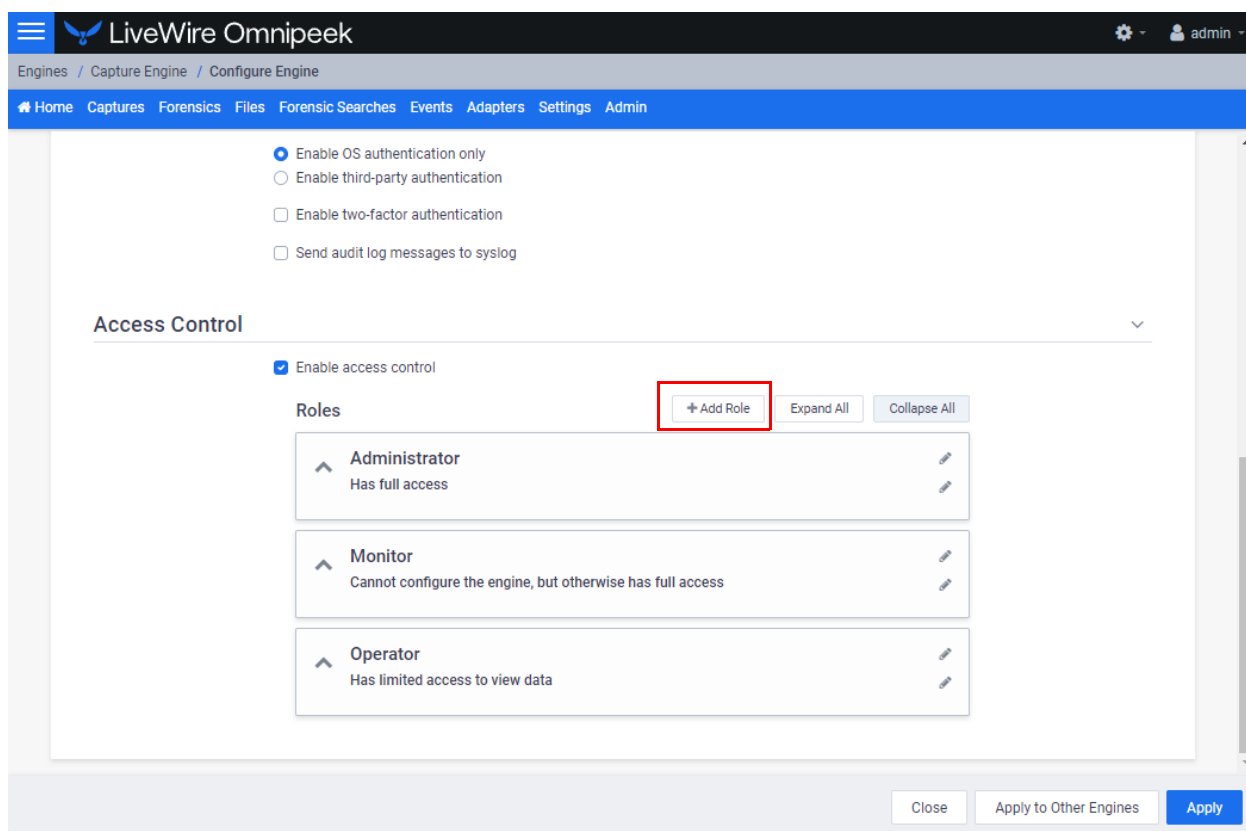
Adding a Role

In addition to the default set of roles included with LiveWire, additional roles can be added and configured.

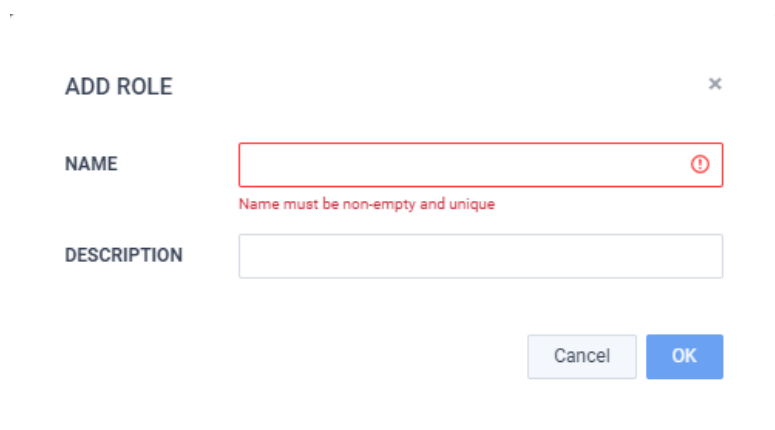
To add a role:

1. Click *Add Role*. The *Add Role* dialog appears.

Note You can also duplicate an existing role and its settings. You will need to provide a unique name for the role when you duplicate a role. See 'Configuring Roles' on page 97.



2. Configure the dialog.



ADD ROLE

NAME

DESCRIPTION

Cancel OK

Name must be non-empty and unique

- *Name*: Type a unique name for the role.
- *Description*: Type a description for the role.
- *OK*: Click to save the role and add it to list of roles.

Enabling Third-Party Authentication

If you assign a group to any of the Access Control roles, third-party authentication must also be enabled and include at least one Active Directory entry that is active with a non-empty *Base DN* (Domain Name), *Application Username*, and *Application Password*.

To enable third-party authentication:

1. Scroll down to the *Security* settings.

The screenshot shows the LiveWire Omnipeek configuration interface. The top navigation bar includes a hamburger menu, the LiveWire Omnipeek logo, and a settings icon with a user profile labeled 'admin'. Below the navigation bar is a breadcrumb trail: 'Engines / Capture Engine / Configure Engine'. A secondary navigation bar contains links: 'Home', 'Captures', 'Forensics', 'Files', 'Forensic Searches', 'Events', 'Adapters', 'Settings', and 'Admin'. The main configuration area is divided into sections. The 'Security' section is highlighted with a red border and contains four radio button options: 'Enable OS authentication only' (selected), 'Enable third-party authentication', 'Enable two-factor authentication', and 'Send audit log messages to syslog'. Below the 'Security' section is the 'Access Control' section, which includes a checked checkbox for 'Enable access control'. Under 'Access Control', there are buttons for '+ Add Role', 'Expand All', and 'Collapse All'. A list of roles is shown, each with an expand/collapse icon, a role name, a description, and an edit icon. The roles are: 'Administrator' (Has full access), 'Monitor' (Cannot configure the engine, but otherwise has full access), and 'Operator' (Has limited access to view data). At the bottom right of the configuration area are three buttons: 'Close', 'Apply to Other Engines', and 'Apply'.

Engines / Capture Engine / Configure Engine

Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin

DATA FOLDER Browse

LOG MAX

LOG ADJUST

Security

- ☒ Enable OS authentication only
- ☐ Enable third-party authentication
- ☐ Enable two-factor authentication
- ☐ Send audit log messages to syslog

Access Control

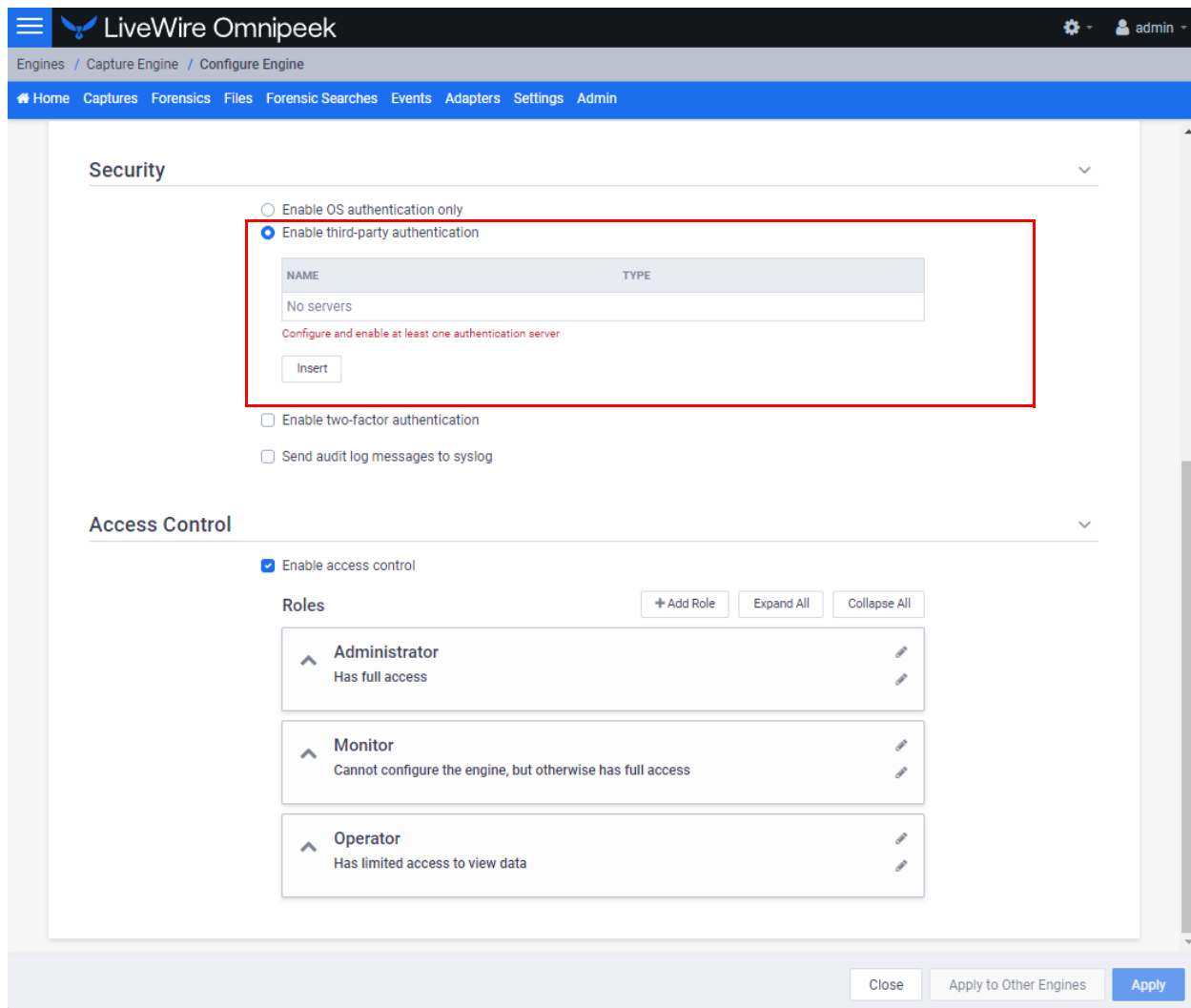
☒ Enable access control

Roles

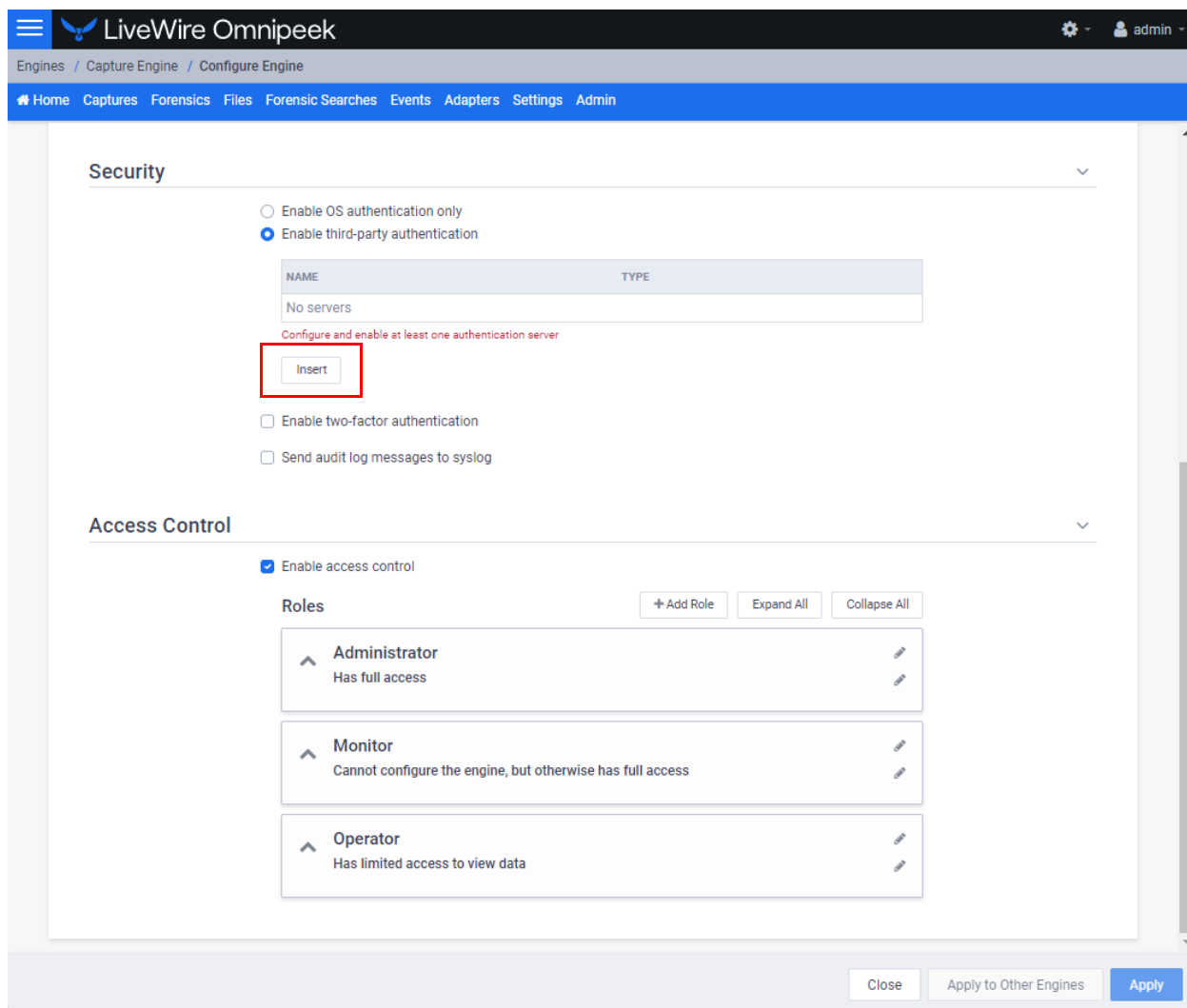
^	Administrator Has full access	
^	Monitor Cannot configure the engine, but otherwise has full access	
^	Operator Has limited access to view data	

Close Apply to Other Engines Apply

2. Select *Enable third-party authentication*.



- Click **Insert**. The **Edit Authentication Setting** dialog appears.



4. Select *Active Directory* as the *Type* of authentication setting. The settings for the Active Directory appear and must be configured.

EDIT AUTHENTICATION SETTING

×

NAME

TYPE

Active Directory

SERVER ADDRESS/HOSTNAME

May be a Hostname/IP address, or a Hostname/IP address and a port separated by a colon
Must be non-empty and cannot contain any of the special characters " , ~ ! @ # \$ % ^ & * () ; : " "

PROTOCOL

LDAP

BASE DN

Must be non-empty

APPLICATION USERNAME

Must be non-empty

APPLICATION PASSWORD

Must be non-empty

Test Connection

Test User

Cancel

OK

- Once the settings are configured, click **Test Connection** to test the Active Directory connection.

EDIT AUTHENTICATION SETTING

×

NAME

TYPE

Active Directory

SERVER ADDRESS/HOSTNAME

May be a Hostname/IP address, or a Hostname/IP address and a port separated by a colon
Must be non-empty and cannot contain any of the special characters " , ~ ! @ # \$ % * & ' () : . "

PROTOCOL

LDAP

BASE DN

Must be non-empty

APPLICATION USERNAME

Must be non-empty

APPLICATION PASSWORD

Must be non-empty

Test Connection

Test User

Cancel

OK

- Click **Test User** to check if a particular user exists within the specified Active Directory.

EDIT AUTHENTICATION SETTING X

NAME

TYPE

Active Directory

SERVER ADDRESS/HOSTNAME

May be a Hostname/IP address, or a Hostname/IP address and a port separated by a colon
Must be non-empty and cannot contain any of the special characters " , ~ ! @ # \$ % ^ & * () ; : . "

PROTOCOL

LDAP

BASE DN

Must be non-empty

APPLICATION USERNAME

Must be non-empty

APPLICATION PASSWORD

Must be non-empty

Test Connection Test User

Cancel OK

7. Click **OK**.

When Upgrading From LiveWire v23.3.1 or Earlier

When upgrading from LiveWire v23.3.1 or earlier to LiveWire v23.4.0 or later, there are two possible upgrade scenarios that affect the Access Control List (ACL):

- If you are upgrading from LiveWire 23.3.1 or earlier, and the ACL policy list is empty (no users are assigned to any of the policies), regardless of whether ACL is enabled or disabled:

In this case, upon upgrading to v23.4.0 or later, LiveWire automatically upgrades the ACL from the policy-based approach to the role-based approach described in this chapter.

- If you are upgrading from LiveWire 23.3.1 or earlier, and the Access Control List policy list is NOT empty (at least one user is assigned to at least one policy), regardless of whether ACL is enabled or disabled:

In this case, upon upgrading to v23.4.0 or later, LiveWire keeps the policy-based approach. You will need to manually opt-in to the role-based approach. If you decide to upgrade to a role-based approach, and upon your confirmation, LiveWire completely clears the current ACL settings and forces you to redefine your ACL settings using the role-based approach as explained in this chapter.

LiveWire Omnipeek

Engines / livepca-virtual-lauren8 / Configure

Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin

Access Control

☒ Enable access control

POLICY	USERS	
Allow Capture Engine usage	admin, local_user_1, local_user_2, LivePCAUser1	
Capture: Create new capture	admin, local_user_1, LivePCAUser1	
Capture: Delete captures created by other users	admin, local_user_1, LivePCAUser1	
Capture: Start/stop captures created by other users	admin	
Capture: Modify captures created by other users	admin	
Capture: View captures created by other users	admin, local_user_1, LivePCAUser1	
Capture / Forensic Search: View packets from captures and forensic searches created by other users	admin, local_user_1, LivePCAUser1	
Capture / Forensic Search: View statistics from captures and forensic searches created by other users	admin, local_user_1, LivePCAUser1	
Capture: Delete files created by other users	admin	
Configuration: Configure engine settings	admin	
Configuration: View the audit log	admin, local_user_2	
Configuration: Upload files	admin, local_user_2	
Configuration: Download packet data	admin, local_user_2	
Forensic Search: Create new forensic search	admin, local_user_1, LivePCAUser1	
Forensic Search: Delete forensic searches created by other users	admin, local_user_1, LivePCAUser1	
Forensic Search: View forensic searches created by other users	admin, local_user_1, LivePCAUser1	

Convert Access Control To Roles

Close

CONVERT ACCESS CONTROL TO ROLES

Are you sure you would like to clear your current Access Control settings and begin using roles?

No Yes

Capture Adapters for LiveWire

In this chapter:

- About capture adapters* 116
- 1G capture adapter* 116
- 10G capture adapter* 117
- 40G capture adapter* 119
- 100G capture adapter* 120
- Enabling PTP support for capture adapters* 121
- Connecting the external time synchronization adapter* 124
- Troubleshooting the capture adapters* 124

About capture adapters

The capture adapters for LiveWire (LiveWire Core/PowerCore only) are high performance network analysis cards that allow you to perform advanced recording, monitoring and troubleshooting of Gigabit, 10 Gigabit, and 40 Gigabit Ethernet networks. The capture adapters for LiveWire are available in the following configurations:

- 1G capture adapter—Four port PCI Express Gigabit adapter (see '1G capture adapter' on page 116)
- 10G capture adapter—Two or four port 10 Gigabit adapter (see '10G capture adapter' on page 117)
- 40G capture adapter—Two port 40 Gigabit adapter (see '40G capture adapter' on page 119)
- 100G capture adapter—Two port 100 Gigabit adapter (see '100G capture adapter' on page 120)

If your capture adapter supports Precision Time Protocol (PTP), instructions for manually enabling PTP support and connecting the PTP adapter on LiveWire are included.

For more information on using capture adapters with LiveWire and Omnipeek, please refer to the documentation and online help that ships with the Omnipeek. Additionally, the LiveAction website has up-to-date software and support at <https://www.liveaction.com>.

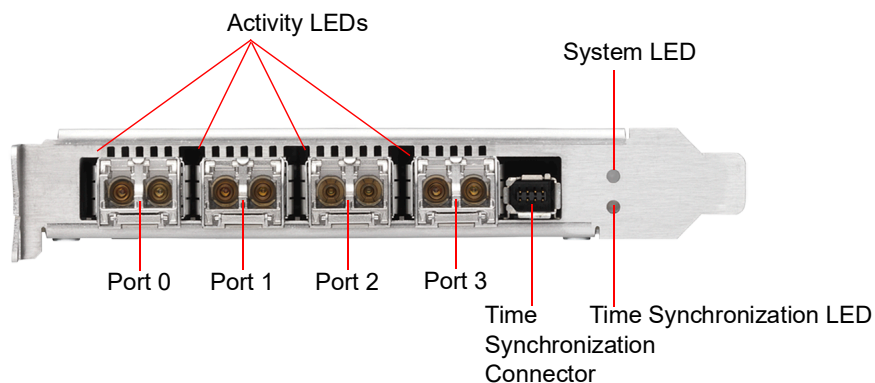
1G capture adapter

The 1G capture adapter is a four port PCI Express Gigabit adapter that supports up to four half-duplex Gigabit Ethernet channels (two full-duplex links). The 1G capture adapter can be connected via taps, matrix switches, or at a switch span port. Taps and matrix switches provide completely passive monitoring that does not affect the network, even in power loss conditions.

1G capture adapter I/O bracket

The I/O bracket of the 1G capture adapter has four SFP cages, a time synchronization connector, and status LEDs. The SFP cages accommodate either fiber or copper modules, which allows you to match different media for your network: copper, single mode fiber (SX), multi-mode fiber (LX), and 10/100/1000 Base-T.

Note Each SFP cage accommodates a single SFP module (not included). A pair of SFP modules are required for full-duplex links.



LED status

The following table describes the LED status on the 1G capture adapter.

LED	State and Color	Condition
System LED	Off	The power is off.
	Constant red	During start-up: Power is on. The adapter is checking the power supplies.
	Flashing red	After start-up: The power is on. There is a fatal hardware error.
	Constant yellow	During start-up: The power is on. The power supplies are working.
	Flashing yellow	There is a new entry in the hardware log.
	Constant green	The FPGA is loaded, and the system is running.
Activity LEDs	Off	The driver is not loaded, the Ethernet link is down, or the port is disconnected.
	Constant Green	The driver is loaded and the Ethernet link is up, but there is no RX or TX traffic.
	Flashing Green	The driver is loaded and there is RX or TX traffic on the Ethernet link
External Time Synchronization LED	Off	No driver is loaded, or no valid PPS or NT-TS signal is detected or generated on the SMA port of the external time synchronization connector, and the Ethernet link on the PTP port is down.
	Constant yellow	The Ethernet link on the PTP port is up.
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the PTP port is down and the following condition is fulfilled: When the SMA port of the external time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.
	Yellow with flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link is up. When the corresponding time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated

10G capture adapter

The 10G capture adapter is a two or four port 10 Gigabit adapter specifically designed to handle 10 Gigabit capture and analysis. Capturing 10 Gigabit network traffic, it can slice and filter packets in order to focus the traffic stream and optimize analysis. The 10G capture adapter can be used in fiber environments, or via SPAN or mirror ports.

The 10G capture adapter is available in the following configurations:

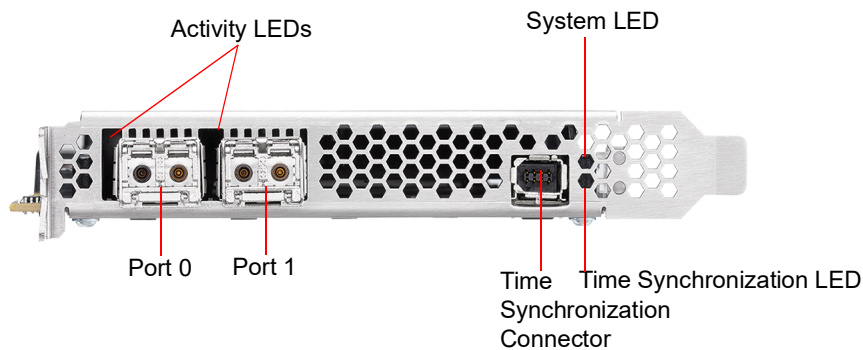
- Two or four 850nm MMF SFP+ optical transceivers with LC connectors
- Two or four 1310nm SMF SFP+ optical transceivers with LC connectors

Note If you are using a variable rate 1 GB SFP+, you will need to cd into `/opt/Napatech/bin` and issue the following command to set the port rate to 1 GB:

```
config --cmd set --port 1 --speed 1G
```

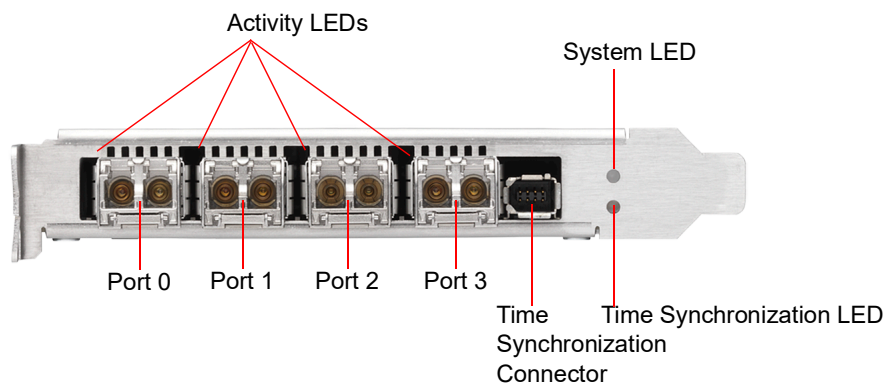
10G capture adapter (2-port) I/O bracket

The I/O bracket of the 10G capture adapter (2-port) has two SFP+ cages, a time synchronization connector, and status LEDs. Each SFP+ cage accommodates a single SFP+ module. A pair of SFP+ modules are required for full-duplex links.



10G capture adapter (4-port) I/O bracket

The I/O bracket of the 10G capture adapter (4-port) has four SFP+ cages, a time synchronization connector, and status LEDs. Each SFP+ cage accommodates a single SFP+ module (not included). A pair of SFP+ modules are required for full-duplex links.



LED status

The following table describes the LED status on the 10G capture adapter.

LED	State and Color	Condition
System LED	Off	The power is off.
	Constant red	During start-up: Power is on. The adapter is checking the power supplies.
	Flashing red	After start-up: The power is on. There is a fatal hardware error.
	Constant yellow	During start-up: The power is on. The power supplies are working.
	Flashing yellow	There is a new entry in the hardware log.
	Constant green	The FPGA is loaded, and the system is running.
Activity LEDs	Off	The driver is not loaded, the Ethernet link is down, or the port is disconnected.
	Constant Green	The driver is loaded and the Ethernet link is up, but there is no RX or TX traffic.
	Flashing Green	The driver is loaded and there is RX or TX traffic on the Ethernet link

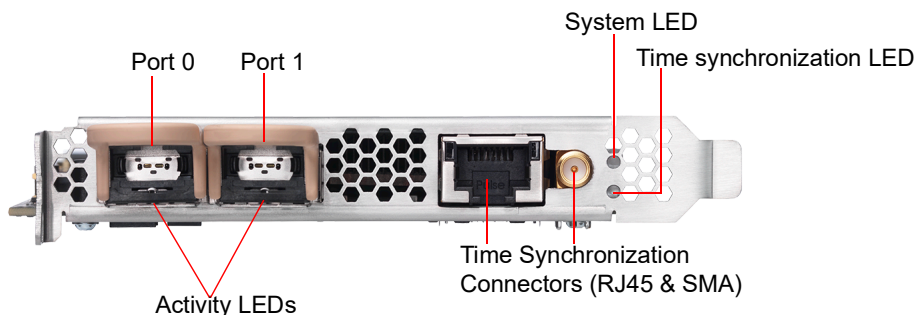
LED	State and Color	Condition
External Time Synchronization LED	Off	No driver is loaded, or no valid PPS or NT-TS signal is detected or generated on the SMA port of the external time synchronization connector, and the Ethernet link on the PTP port is down.
	Constant yellow	The Ethernet link on the PTP port is up.
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the PTP port is down and the following condition is fulfilled: When the SMA port of the external time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.
	Yellow with flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link is up. When the corresponding time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.

40G capture adapter

The 40G capture adapter is a two port, PCI Express 40 Gigabit adapter with optical interfaces that are optimized for recording, monitoring, and troubleshooting traffic on 40 Gigabit Ethernet networks. The 40G capture adapter provides tracing and dynamically configurable filtering together with high precision time-stamping. The 40G Adapter is available with two QSFP+ interfaces.

40G capture adapter I/O bracket

The I/O bracket of the 40G capture adapter has two QSFP+ cages, a time synchronization connector, and status LEDs. Each QSFP+ cage accommodates a single QSFP+ module (not included).



LED status

The following table describes the LED status on the 40G capture adapter.

LED	State and Color	Condition
System LED	Off	The power is off.
	Constant red	During start-up: Power is on. The adapter is checking the power supplies.
	Flashing red	After start-up: The power is on. There is a fatal hardware error.
	Constant yellow	During start-up: The power is on. The power supplies are working.
	Flashing yellow	There is a new entry in the hardware log.
	Constant green	The FPGA is loaded, and the system is running.

LED	State and Color	Condition
Activity LEDs	Off	The driver is not loaded, the Ethernet link is down or the port is disconnected.
	Constant Green	The driver is loaded and the Ethernet link is up, but there is no RX or TX traffic.
	Flashing Green	The driver is loaded and there is RX or TX traffic on the Ethernet link
External Time Synchronization LED	Off	No driver is loaded, or no valid PPS or NT-TS signal is detected or generated.
	Constant Yellow	The Ethernet link on the external RJ45 time synchronization connector is up.
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the external RJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.
	Yellow with flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the external RJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.

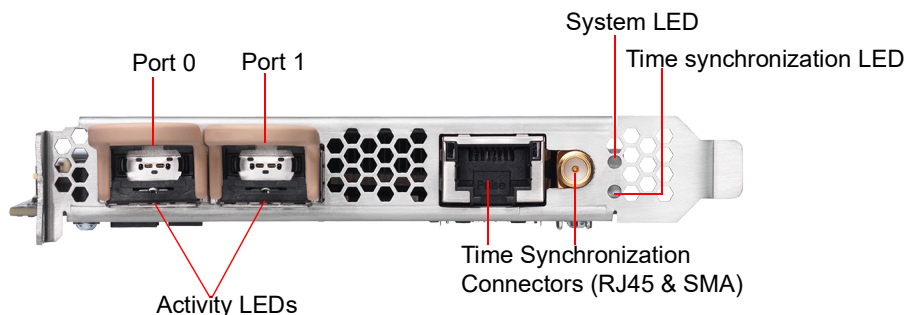
100G capture adapter

The 100G capture adapter is a two port, PCI Express 100 Gigabit adapter with optical interfaces that are optimized for recording, monitoring, and troubleshooting traffic on 100 Gigabit Ethernet networks. The 100G capture adapter provides tracing and dynamically configurable filtering together with high precision time-stamping. The 100G capture adapter is available with two QSFP28 interfaces.

Note Both a 25G and 80G capture adapter configuration that is based on the 100G capture adapter form factor are also available. If you are interested in obtaining either a 25G or 80G capture adapter configuration, please contact LiveAction Technical Support.

100G capture adapter I/O bracket

The I/O bracket of the 100G capture adapter has two QSFP28 cages, a time synchronization connector, and status LEDs. Each QSFP28 cage accommodates a single QSFP28 module (not included).



LED status

The following table describes the LED status on the 100G capture adapter.

LED	State and Color	Condition
System LED	Off	The power is off.
	Constant red	During start-up: Power is on. The adapter is checking the power supplies.
	Flashing red	After start-up: The power is on. There is a fatal hardware error.
	Constant yellow	During start-up: The power is on. The power supplies are working.
	Flashing yellow	There is a new entry in the hardware log.
	Constant green	The FPGA is loaded, and the system is running.
Activity LEDs	Off	The driver is not loaded, the Ethernet link is down or the port is disconnected.
	Constant Green	The driver is loaded and the Ethernet link is up, but there is no RX or TX traffic.
	Flashing Green	The driver is loaded and there is RX or TX traffic on the Ethernet link
External Time Synchronization LED	Off	No driver is loaded, or no valid PPS or NT-TS signal is detected or generated.
	Constant Yellow	The Ethernet link on the external RJ45 time synchronization connector is up.
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the external RJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.
	Yellow with flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the external RJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: <ul style="list-style-type: none"> • PPS or NT-TS input connector: A driver is loaded, and a valid PPS or NT-TS signal as relevant is detected. • PPS or NT-TS output connector: A driver is loaded, and a PPS or NT-TS signal is generated.

Enabling PTP support for capture adapters

The capture adapters for LiveWire support the Precision Time Protocol (PTP). This protocol allows the adapters to sync to a time source on the network that may be more accurate than the clock on LiveWire. If you have multiple capture adapters, you can sync the adapters to a single clock source, as well as allow the packets received on the adapters to have more accurate timestamps. See also 'Synchronizing the capture engine clock' on page 123.

To enable PTP support for the adapters, you must manually edit a config file and restart some services on the Capture Engine. The instructions for enabling PTP support on the Capture Engine are provided below.

To enable PTP support on the Capture Engine:

1. SSH into the Capture Engine.
2. Stop the Capture Engine service.
 - `service omnid stop`
3. Open the file `/etc/omni/ntservice.ini`
 - This file uses the INI format.

- The file is broken up into sections. Each section has a name wrapped in [] (e.g [Adapter0]), all of the fields below the section name apply to that section.
- 4. Find the adapter section corresponding to the adapter you wish to configure. Make note of the section name.
 - Adapter sections have section names which follow the format [AdapterN] where N is a number starting at 0 and incremented by one for each Napatech adapter present on the system.
- 5. Close the /etc/omni/ntservice.ini file.
- 6. Open the file /etc/omni/ntoverrides.ini
 - This file has the same format as the /etc/omni/ntservice.ini file.
 - This file is used to override the default settings of configuration parameters in the /etc/omni/ntservice.ini file.
- 7. Add the section name of the adapter retrieved in the /etc/omni/ntservice.ini file.
- 8. Below this section, add the necessary PTP configuration parameters.
 - If more than one card is being configured, add the next section name and the necessary PTP configuration parameters.
- 9. When all of the adapters have been configured, save and close the file.
- 10. Run the ntcards_setup script to update the configuration file with the PTP settings.
 - service ntcards_setup start
 - This script may take a couple of minutes to complete.
- 11. Once the script is finished, restart the Capture Engine service.
 - service omnid start

Configuration parameters

The minimum configuration parameters that must be set to enable PTP on an Adapter for LiveWire are described in the table below. For more complex configurations, contact LiveAction Tech Support to get a full list of all the PTP configuration parameters supported.

Note *PtPlpAddr*, *PtpGw* and *PtpNetmask* are only applicable if *PtpDhcp* is set to DISABLE. If *PtpDhcp* is set to ENABLE the static IP configuration parameters should not be added to the configuration file.

Section	Parameters	Description	Values	Default Value
System	TimeSyncOsTimeReference	This option can be used to synchronize the OS Time to a Napatech adapter clock The chosen adapter cannot specify OSTime as one of the options in the TimeSyncReferencePriority field	None - adapter-0 - adapter-1 - adapter-2...	None
AdapterN	PtpDhcp	Enables/disables DHCP support on the PTP port. Set to DISABLE if a static IP address will be used.	ENABLE - DISABLE	DISABLE
AdapterN	PtPlpAddr	Specifies a static IP address for the PTP port.	Any valid IPv4 address (e.g. 192.168.1.10)	Not set

Section	Parameters	Description	Values	Default Value
AdapterN	PtpGw	Specifies a gateway address for the PTP port.	Any valid IPv4 address (e.g. 192.168.1.10)	Not set
AdapterN	PtpNetMask	Specifies the netmask for the static address specified with PtpIPAddr.	Any valid IPv4 netmask (e.g. 255.255.255.0)	Not set
AdapterN	PtpUnicastMasterAddr<1...10>	<p>Adds an IP address of a PTP master to the unicast master table.</p> <p>Up to 10 IP addresses can be added.</p> <p>The order of the addresses is not important.</p>	Any valid IPv4 address (e.g. 192.168.1.10)	Not set
AdapterN	TimeSyncReferencePriority	<p>Comma separated list of clock sources.</p> <p>In order to enable PTP, PTP must be the first item in the list.</p> <p>The last item in the list must be either FreeRun or OStime.</p>	PTP - Ext1 - FreeRun - OStime	OStime

Example of /etc/omni/ntoverrides.ini:

```
## This file is used to specify overrides for the ntsservice configuration file
#
## Option to synchronize OS time to a Napatech adapter clock:
##   Note: The selected accelerator must not have OStime included in the
##   TimeSyncReferencePriority parameter, nor must it be synchronized to an accelerator
##   in OS synchronization mode.
[System]
TimeSyncOStimeReference = adapter-1

#
# Example for Configuring Multicast:
[Adapter0]
PtpDhcp = ENABLE
# Last item in list must be FreeRun or OStime, cannot include both in the list:
TimeSyncReferencePriority = PTP, OStime

##
# Example for Configuring Unicast using a Static IP Address:
[Adapter1]
PtpDhcp = DISABLE
PtpIPAddr = 192.168.1.15
PtpGw = 192.168.1.1
PtpNetMask = 255.255.255.0
PtpUnicastMasterAddr1 = 192.168.1.13
PtpUnicastMasterAddr2 = 192.168.1.29
TimeSyncReferencePriority = PTP, FreeRun
```

Synchronizing the capture engine clock

If PTP support is enabled on the capture adapter in a PTP network environment, to prevent inaccurate time-stamps from being reported, ensure that the Capture Engine's clock is synchronized with the PTP or NTP server (if NTP's time source is pointed at the PTP grandmaster clock).

To synchronize the Capture Engine clock, one of the following configurations is needed:

- Enable 'TimeSyncOsTimeReference' in `/etc/omni/ntoverrides.ini`—This option synchronizes the OS time to a Napatech adapter clock, which in turn should be configured to point to the PTP grandmaster clock as its time reference
- If NTP server references PTP as its time source, run 'ntpd' to synchronize the OS time with the NTP server, and then start up the NTP daemon

Connecting the external time synchronization adapter

For the capture adapters for LiveWire that support the Precision Time Protocol (PTP), a time synchronization adapter is included with your adapter. One end of the time synchronization adapter is connected to the external time synchronization connector on the capture adapter; the other end of the time synchronization adapter is connected to your PTP source via an Ethernet or GPS connection (blue cable).

Note For instructions on manually enabling PTP support on your Capture Engine, see 'Enabling PTP support for capture adapters' on page 121.

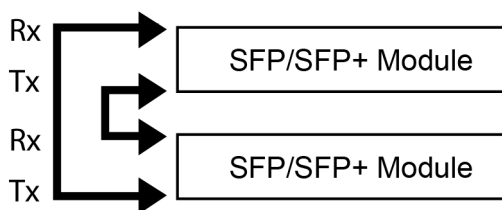


Troubleshooting the capture adapters

When the connection for one or more channels is down or degraded, you can use a known good test cable to connect the card to itself in order to facilitate troubleshooting and help to isolate the source of trouble.

Verifying link status

1. Remove the cables from two of the channels and replace with a crossover test cable connected as shown below:



2. If the two links are established, this will indicate that both channels, including the SFP/SFP+ modules, are functional. An external connection issue should then be investigated.

If both links are NOT established using the Link Status test steps above, users of fiber SFP/SFP+ modules may attempt a further test to isolate individual SFP/SFP+ modules.

Note Both the Rx and Tx sides of the connection are contained in a single jack for 1000Base-TX SFPs/SFP+ modules. The following steps can only be used to test fiber SFP (SX or LX) and SFP+ modules, which have separate Rx and Tx connectors.

To test fiber SFP/SFP+ modules individually:

1. Connect the crossover test cable as shown below:



2. Each channel should auto-negotiate with itself, turning its Link Status LED on.
3. If a single failing channel is identified, substitute the corresponding channel's SFP/SFP+ module.
4. If substitution of the SFP/SFP+ modules does not resolve the problem, replace the card.

Capture adapter technical specifications

1G capture adapter specifications

Specification	Description
Network Interfaces	
Standard:	IEEE 802.3 1 Gbps Ethernet support
Physical interface:	4x SFP ports
Supported SFP modules	Multi-mode SX (850 nm), single-mode LX (1310 nm), single-mode ZX (1550 nm), 1000BASE-T or 10/100/1000BASE-T
Environment	
Power consumption:	23.3 Watts including SFP SX modules
Operating temperature:	32° F to 113° F (0° to 45° C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	CE CB RoHS REACH cURus (UL) FCC CSA VCCI C-TICK

10G capture adapter (2-port) specifications

Specification	Description
Network interfaces	
Standard:	IEEE 802.3 10 Gbps Ethernet LAN
Physical interface:	2 x SFP or SFP+ ports
Supported SFP modules:	Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T
Supported SFP+ modules:	Multi-mode SR, single-mode LR and ER, 10GBASE-CR
Supported dual-rate modules:	Multi-mode SR and single-mode LR
Environment	
Operating temperature:	32°F to 113°F (0° to 45°C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	CE CB RoHS REACH cURus (UL) FCC CSA VCCI C-TICK

10G capture adapter (4-port) specifications

Specification	Description
Network interfaces	
Standard:	IEEE 802.3 10 Gbps Ethernet LAN
Physical interface:	4x SFP or SFP+ ports
Supported SFP modules:	Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T
Supported SFP+ modules:	Multi-mode SR, single-mode LR and ER, 10GBASE-CR
Supported dual-rate modules:	Multi-mode SR and single-mode LR
Environment	
Power consumption:	27 Watts including SFP+ SR modules
Operating temperature:	32° F to 113° F (0° C to 45° C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	PCI-SIG® CE CB RoHS REACH cURus (UL) FCC CSA VCCI C-TICK

40G capture adapter specifications

Specification	Description
Network interfaces	
Standard:	IEEE 802.3 40 Gbps Ethernet LAN
Physical interface:	2x QSFP+ ports
Supported optical transceivers:	
Supported QSFP+ modules:	40GBASE-SR4, 40GBASE-LR4, and 40GBASE-SR-BiDi
Supported QSFP28 modules:	100GBASE-SR4 and 100GBASE-LR4
Environment	
Operating temperature:	32°F to 113°F (0° to 45°C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	PCI-SIG® NEBS level 3 CE CB RoHS REACH cURus (UL) FCC ICES VCCI C-TICK

100G capture adapter specifications

Specification	Description
Network interfaces	
Standard:	IEEE 802.3 40 Gbps Ethernet LAN
Physical interface:	2x QSFP+ ports
Supported optical transceivers:	
Supported QSFP+ modules:	40GBASE-SR4, 40GBASELR4, and 40GBASE-SR-BiDi
Supported QSFP28 modules:	100GBASE-SR4 and 100GBASE-LR4
Environment	
Operating temperature:	32°F to 113°F (0° to 45°C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	PCI-SIG® NEBS level 3 CE CB RoHS REACH cURus (UL) FCC ICES VCCI C-TICK

Network Port Requirements

In this chapter:

<i>LiveWire/Omnipeek Port Information</i>	130
<i>NetFlow (NetFlow v5, NetFlow v9, and IPFix) (optional)</i>	130
<i>iDRAC (out-of-band LiveWire management) Default Port Requirements</i>	130

LiveWire/Omnipeek Port Information

Port	Protocol	Usage
22	TCP/UDP	SSH (device management; optional: tcpdump capabilities)
25	TCP/UDP	SMTP (optional alerting method)
49	TCP/UDP	TACACS (optional)
80	TCP	HTTP (optional: not recommended for use – should be closed/blocked)
88	TCP/UDP	Kerberos KDC (optional)
161	TCP/UDP	SNMP (optional)
443	TCP	HTTPS
514	TCP/UDP	RSYSLOG (optional)
749	TCP/UDP	Kerberos Admin Server (optional)
1812	TCP/UDP	RADIUS (optional)
2812	TCP	Monit (optional: can be TLS encrypted)
6367	TCP	LiveAction WP Omni protocol
6370	TCP	Capture Engine Manager
8443	TCP	HTTPS

NetFlow (NetFlow v5, NetFlow v9, and IPFix) (optional)

Port	Protocol	Usage
2055	UDP	Netflow v5 & v9
4739	TCP/UDP	IPFix

iDRAC (out-of-band LiveWire management) Default Port Requirements

Port	Protocol	Usage
22*	TCP	SSH
23*	TCP	Telnet (not recommended for use – should be closed/blocked)
80*	TCP	HTTP (not recommended for use – should be closed/blocked)
161*	UDP	SNMP
443*	TCP	HTTPS
623	UDP	RCMP/RCMP+
5900*	TCP	Virtual Console keyboard and mouse redirection, virtual media, virtual folders, and remote file share
5901	TCP	VNC (when VNC feature is enabled, the port 5901 opens)
*configurable port		