LiveAction

LiveWire

User Guide

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

20240325-LWG2U_241a

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

In this chapter:

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 both LiveAction's LiveNX and ThreatEye. 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 ThreatEye. See Chapter 3, *Sending Telemetry to LiveNX and ThreatEye* for the additional tasks you must perform in order to export LiveFlow data from LiveWire to LiveNX and ThreatEye. Please also refer to the LiveNX and ThreatEye documentation for more information on using the LiveFlow data exported to LiveNX and ThreatEye.

LiveWire is available in the following configurations:

	LiveWire Edge	**LiveWire Core**	**LiveWire PowerCore**
Chassis	Mini Network Appliance	1U	2U
Processor **Base Frequency** **Cores** **Thread**	Intel® Atom® C3758 2.2 GHz 8	AMD® 1x7313 3.0 GHz 16 32	AMD® 2x EPYC 73F3 3.5 GHz 12 24
Memory	16 GB	64 GB	256 GB
Expansion Slots	N/A	1 x 16 full-height PCI Express 3.0 slot **NOTE**: A total of one capture adapter can be added to the LiveWire Core.	Eight available PCI Express 3.0 slots **NOTE**: A total of three high speed capture adapters can be added to the LiveWire PowerCore.
Integrated Network Interfaces	• Mini-USB console port • Management port • Three Ethernet ports • Two bridge ports	4 x 1GBASE-T iDRAC	4 x 1GBASE-T iDRAC
Storage-OS	Included as part of Storage-Data	Included as part of Storage-Data	Two 2 TB SSD SAS ISE drives for OS
Storage-Data	1 TB SSD	Available with 32 TB SAS ISE storage, RAID 0 with optional RAID 10	200 TB SAS storage, RAID 6 (240 TB, optional RAID 0) **NOTE**: Optional external storage with LiveWire TeraVault — Up to 800 TB, RAID 6 (960 TB, optional RAID 0) of additional storage (4x 2U TeraVaults)
Capture Adapter Options (High performance network analysis cards)	N/A	1G Capture Adapter (4-port) **NOTE**: A total of one capture adapter can be added to the LiveWire Core.	1G Capture Adapter (4-port) 10G Capture Adapter (2- or 4-port) 40G Capture Adapter (2-port) 100G Capture Adapter (2-port) **NOTE**: A total of three capture adapters can be added to the LiveWire PowerCore.
Additional			PERC H840 Adapter (used only for storage subsystem)

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

What's included

Your standard LiveWire package includes:

LiveWire Edge:

- 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
- Mini-USB console cable

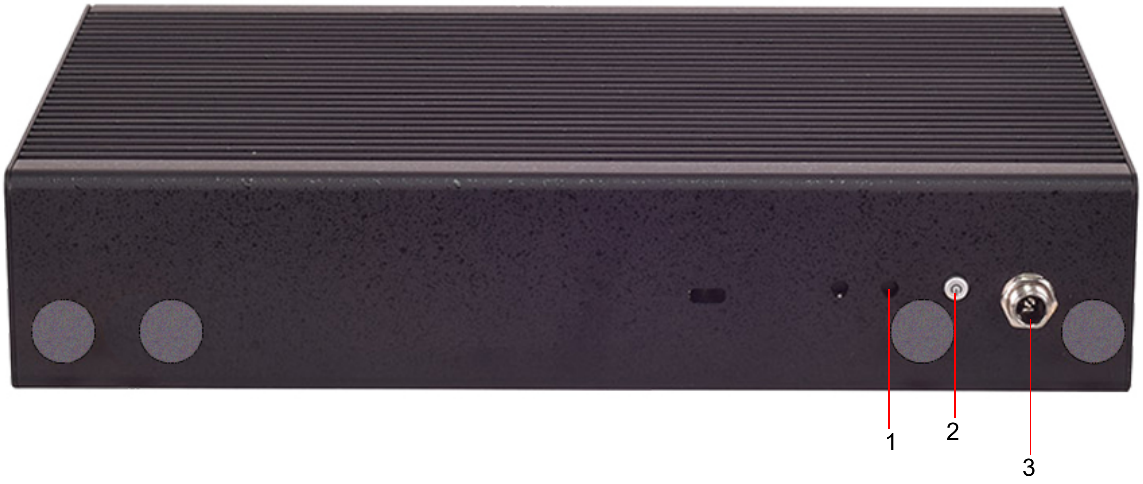
LiveWire Core/Power:

- 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 (1)
- Two power cords
- Rack-mount rails
- Chassis bezel

Front / rear panels

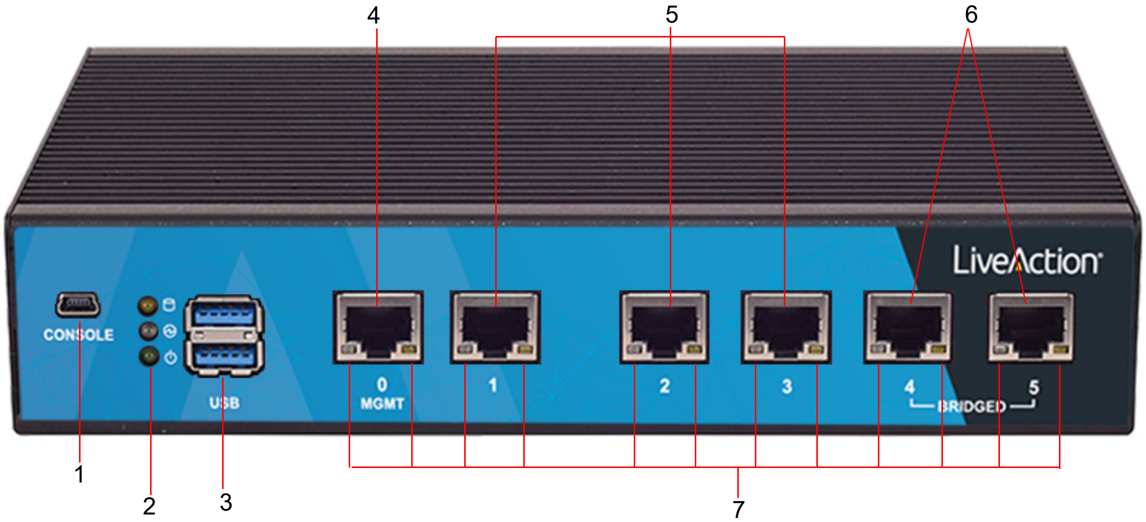
See the illustrations and descriptions of the front and back panel of LiveWire in the sections below.

LiveWire Edge front panel



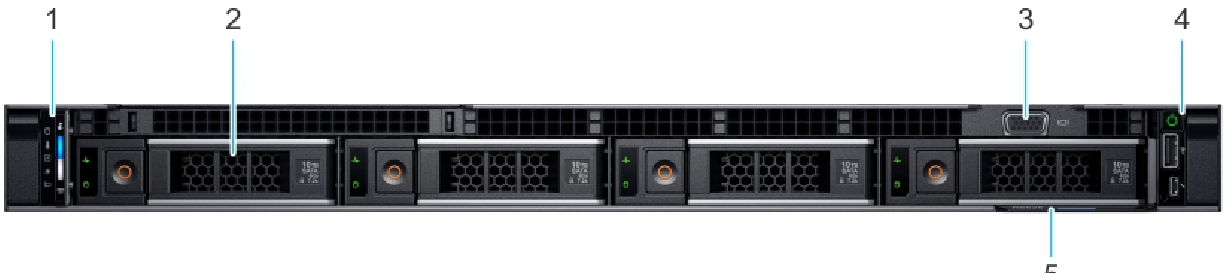
Item	Indicator, Button, or Connector	Description
1	Reset Button	Insert a paper clip, and press and hold the reset button for three seconds to reset LiveWire Edge to its factory settings. You will lose all saved settings and data on LiveWire Edge when it is reset to its factory settings. Once LiveWire Edge has reset, you will need to run the configuration utility again as described in 'Using the LiveAdmin utility' on page 27.
2	Power-on Button with LED	Press to power-on or power-off LiveWire Edge. When in Standby mode, the LED lights red; in Power-on mode, the LED lights green; when Off, the LED does not light.
3	Power-in Socket	Connects to the screw-on connector on the power adapter included with LiveWire Edge. **Note**: Make sure the screw-on connector on the power adapter is connected to the Power-in Socket on LiveWire Edge before the power adapter is plugged into an AC power source.

LiveWire Edge rear panel



Item	Indicator, Button, or Connector	Description
1	Mini-USB Port	The Mini-USB port (console port) lets you connect to another computer terminal for advanced diagnostics or recovery access using a mini-USB console cable (not included with LiveWire Edge) connected from the USB port on your PC/laptop to the Mini-USB Port on the rear panel of LiveWire Edge. See ’Connecting to LiveWire through the serial port’ on page 80.
2	Storage/Status/Power LEDs	Storage: If the LED blinks, it indicates data access activities; otherwise, it remains off. Status: When LiveWire Edge is first powered on, the LED momentarily blinks green, and then remains off. Power: If the LED is on it indicates that the system is powered on. If it is off, it indicates that the system is powered off.
3	USB 3.0 Ports	The USB ports are reserved for future expansion.
4	‘MGMT’ Port	This 1GbE Ethernet port is the management port that lets you configure LiveWire Edge (see ’Using the LiveAdmin utility’ on page 27). Connect a standard Ethernet cable from your network to the ‘MGMT’ port.
5	‘1–3’ Ports	These 1GbE Ethernet ports are used for capturing packets from your network. Connect a standard Ethernet cable from your network to the desired port on LiveWire Edge.
6	‘4–5 Bridged’	These 1GbE Ethernet ports are configured as a bridge and are used when you want to insert LiveWire Edge in-line between two network devices. This configuration allows the capture of traffic flowing between the two network nodes without requiring a tap. In this implementation, packets enter LiveWire Edge through one of the bridge ports, and then exit LiveWire Edge through the remaining bridge port. Essentially, any traffic that gets to one bridge port is copied to the other bridge port. In cases where power is turned off or is lost to LiveWire Edge, the two bridge ports are connected as if they are a wire (‘fail to wire’), so Internet connectivity is not lost. To establish the bridge, connect standard Ethernet cables so that LiveWire Edge is between your cable modem (Internet connection) and the LAN. One of the bridge ports on LiveWire Edge is connected to the cable modem, while the other bridge port is connected to the LAN. Both bridge ports must be connected in this fashion in order to properly establish the bridge. Do not connect each of the bridge ports to the same IP routed network; otherwise, a routing loop is created, and can cause the network to be inoperable. **Note**: When powering the LiveWire Edge on or off, there will be a short network disruption when the hardware bypass (bridge port) is enabled or disabled.
7	Port LEDs	The two LEDs on the bottom of the Ethernet ports light to indicate activity. A green and yellow LED light to indicate a connection has been established. A flashing yellow LED indicates data access activities.

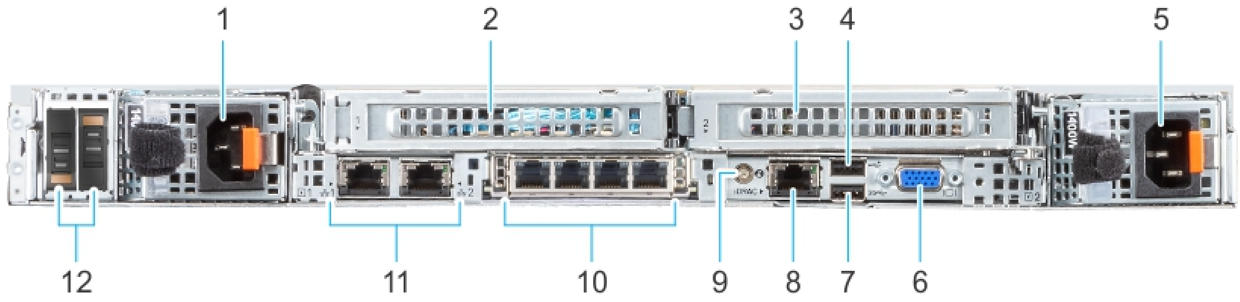
LiveWire Core front panel



Item	Ports, Panels, or Slots	Description
1	Left control panel	Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless) LED.
2	Hard drive (4)	3.5 inch hot-swappable hard drive/SSD.
3	VGA port	Enables you to connect a display device to the system.
4	Right control panel	Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED.
5	Information tag	The Information tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on.

Note To access the front panel, the front bezel must be removed.

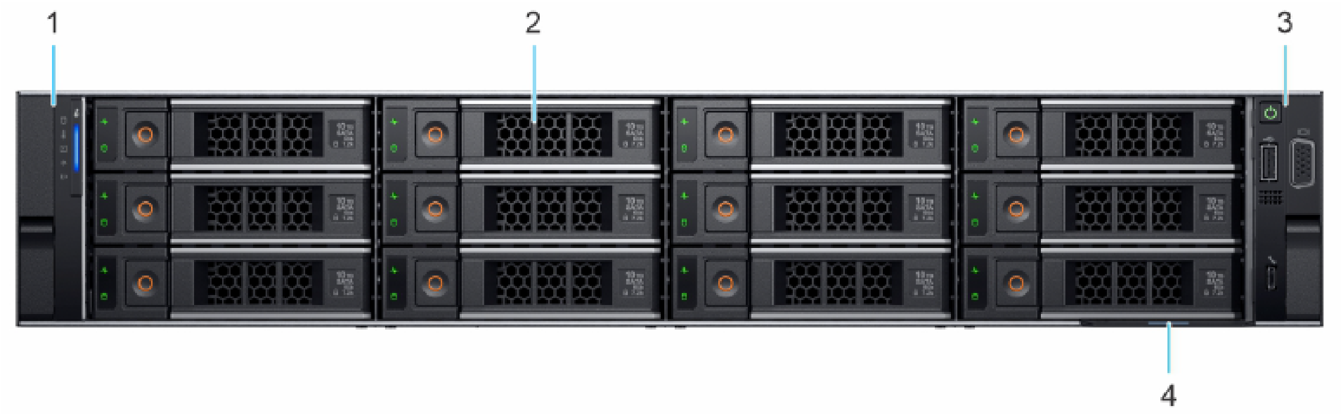
LiveWire Core back panel



Item	Ports, Panels, or Slots	Description
1	Power supply unit (PSU 1)	AC 800 W. Both power supplies should be plugged in to power to provide redundancy.
2	PCIe expansion card riser (slot 1)	The expansion card riser enables you to connect PCI Express expansion cards.
3	PCIe expansion card riser (slot 2)	The expansion card riser enables you to connect PCI Express expansion cards.
4	USB 2.0 port (1)	Use the USB 2.0 port to connect USB devices to the system. These ports are 4-pin, USB 2.0-compliant.
5	Power supply unit (PSU 2)	AC 800 W. Both power supplies should be plugged in to power to provide redundancy.
6	VGA port	Use the VGA port to connect a display to the system.
7	USB 3.0 port (1)	Use the USB 3.0 port to connect USB devices to the system. These ports are 4-pin, USB 3.0-compliant.
8	iDRAC dedicated port	Enables you to remotely access iDRAC. iDRAC is very useful for remote management and direct access of the appliance.
9	System identification button	The System Identification (ID) button is available on the 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.
10	OCP NIC port (optional)	This port supports OCP 3.0. The NIC ports are integrated on the OCP card which is connected to the system board.

Item	Ports, Panels, or Slots	Description
11	NIC port (2)	The NIC ports are embedded on the LOM card that is connected to the system board.
12	BOSS S2 card (optional)	This slot supports the BOSS S2 module.

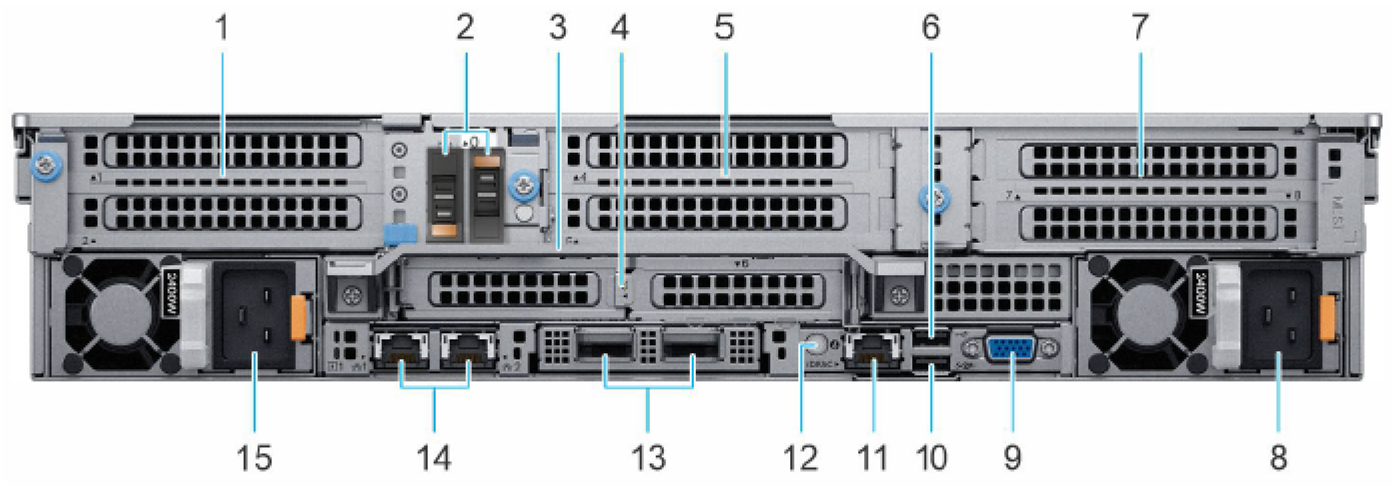
LiveWire PowerCore front panel



Item	Indicator, Button, or Connector	Description
1	Left control panel	Contains system health and system ID, status LED, and iDRAC Quick Sync 2 (wireless) LED.
2	Drive (12)	3.5 inch hot-swappable hard drive (12)
3	Right control panel	Contains the power button, VGA port, USB 2.0 port, and iDRAC Direct micro USB port.
4	Information tag	The information tag is a slide-out label panel that contains system information such as service tag, NIC, MAC address, and so on.

Note To access the front panel, the front bezel must be removed.

LiveWire PowerCore back panel

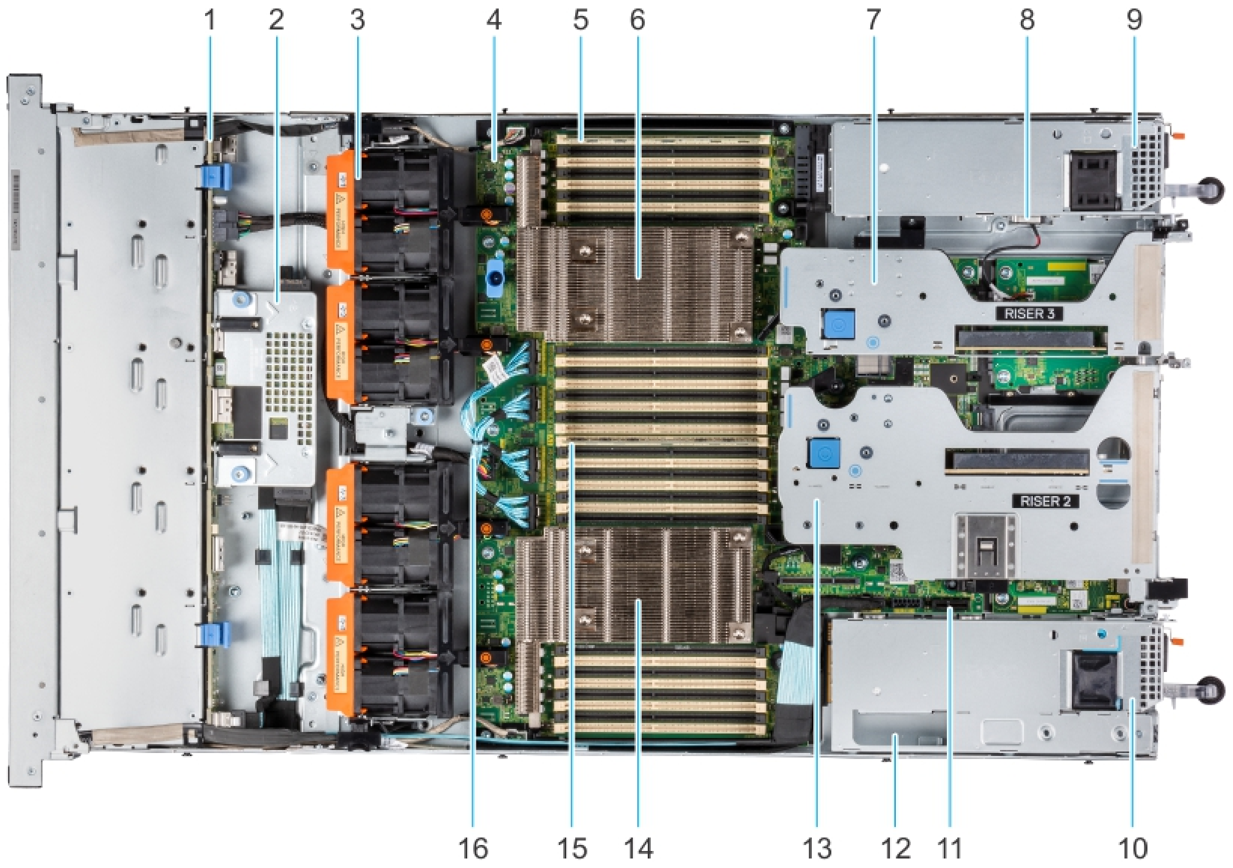


Item	Ports, Panels, or Slots	Description
1	PCIe expansion card riser 1 (slot 1 and slot 2)	The expansion card riser enables you to connect PCI Express expansion cards.
2	BOSS S2 card (optional)	This slot supports the BOSS S2 module.
3	Rear handle	To lift the system.
4	PCIe expansion card riser 2 (slot 3 and slot 6)	The expansion card riser enables you to connect PCI Express expansion cards.
5	PCIe expansion card riser 3 (slot 4 and slot 5)	The expansion card riser enables you to connect PCI Express expansion cards.
6	USB 2.0 port (1)	This port is USB 2.0-compliant.
7	PCIe expansion card riser 4 (slot 7 and slot 8)	The expansion card riser enables you to connect PCI Express expansion cards.
8	Power supply unit (PSU 2)	AC 1100 W Both power supplies should be plugged in to power to provide redundancy.
9	VGA port	Enables you to connect a display device to the system.
10	USB 3.0 port (1)	The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
11	iDRAC dedicated port. Enables you to remotely access iDRAC.	Enables you to remotely access iDRAC. iDRAC is very useful for remote management and direct access of the appliance.
12	System identification button	The System Identification (ID) button is available on the 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.
13	OCP NIC port (optional)	This port supports OCP 3.0. The NIC ports are integrated on the OCP card which is connected to the system board.
14	NIC port (1, 2)	The NIC ports are embedded on the LOM card that is connected to the system board.
15	Power supply unit (PSU 1)	AC 1100 W Both power supplies should be plugged in to power to provide redundancy.

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 internal components

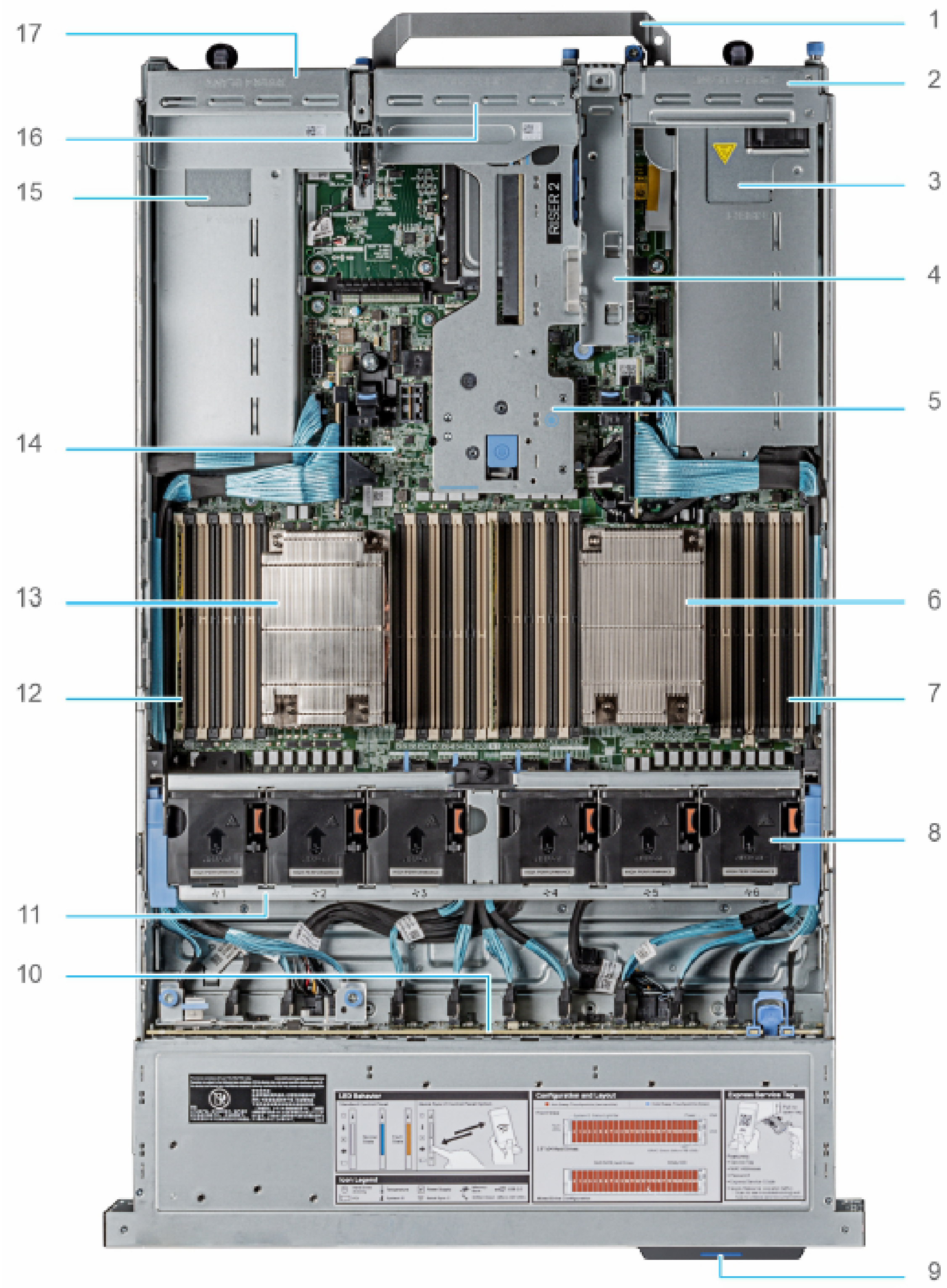


Item	Description
1	Drive backplane
2	Rear mounting front PERC module
3	Dual fan module (4)
4	System board
5	Memory DIMM socket for processor 2 (B1)
6	Heat sink for processor 2
7	Riser 3
8	Intrusion switch
9	Power supply unit (PSU 2)
10	Power supply unit (PSU 1)
11	IDSDM/Internal USB card port
12	BOSS slot
13	Riser 2
14	Heat sink for processor 1

Item	Description
15	Memory DIMM socket for processor 1 (A1)
16	xGMI cables

Note A defective drive should have a consistent RED blinking LED which should make it easier to detect.

LiveWire PowerCore internal components



Item	Description
1	Handle
2	Riser 1 blank
3	Power supply unit (PSU 1)
4	BOSS S2 card slot
5	Riser 2
6	Heat sink for processor 1
7	Memory DIMM socket for processor 1 (E,F,G,H)
8	Cooling fan assembly
9	Service tag
10	Drive backplane
11	Cooling fan cage assembly
12	Memory DIMM socket for processor 2 (A,B,C,D)
13	Heat sink for processor 2
13	System board
15	Power supply unit (PSU 2)
16	Riser 3 blank
17	Riser 4 blank

Note A defective drive should have a consistent RED blinking LED which should make it easier to detect.

Installing LiveWire

LiveWire Edge

To install LiveWire Edge:

1. Attach the rubber feet to the bottom of LiveWire Edge and place LiveWire Edge 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. Any obstructions to the heat sink located on top of LiveWire Edge can cause the unit to overheat.

4. Connect LiveWire Edge to the network to capture traffic:
   - From the Bridge ports: To use the Bridge ports, connect LiveWire Edge inline on a network segment. In this mode, connect the eth 4 port to the side of the network with the upstream router; and connect eth 5 to the LAN side of the network.

- From the Span ports: To use the span ports, connect LiveWire Edge directly to a span port from a switch or router.

5. To configure and use the LiveWire Edge, connect the 'MGMT' port to the network.

Connect to LiveWire Edge via the Mini-USB port

The Mini-USB port (Console port) on LiveWire Edge lets you connect to another computer terminal for advanced diagnostics or recovery access using a mini-USB console cable (included with LiveWire Edge) connected from the USB port on your PC/laptop to the Mini-USB Port of LiveWire Edge.

Using the Mini-USB port on LiveWire Edge, a laptop, and a terminal program of your choice, you can log into LiveWire Edge and access the LiveWire command prompt (admin@ivewire).

To connect to LiveWire Edge:

1. Connect the mini-USB console cable from your laptop to the Mini-USB port on LiveWire Edge.
2. Using any serial terminal program (e.g., HyperTerminal or Putty), establish a connection to LiveWire. Make sure the appropriate terminal settings match the default settings below for LiveWire Edge:
   - 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]
3. Once a connection to LiveWire Edge has been established, the LiveWire Edge login prompt appears.
4. Log into LiveWire Edge as you normally would. The LiveWire Edge command prompt (admin@livewire) appears.

LiveWire Core/PowerCore

LiveWire Core

LiveWire PowerCore

To install LiveWire:

1. Place LiveWire 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/PowerCore has two redundant high-efficiency “hot-swappable” power supplies. If a power module fails, it should be replaced immediately. If your LiveWire Core/PowerCore 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/PowerCore includes Gigabit Ethernet ports and Integrated Remote Access Controller (iDRAC) ports used for remotely accessing and troubleshooting LiveWire Core/PowerCore. LiveWire Edge includes Gigabit Ethernet ports, but no iDRAC port. See ‘Front / rear panels’ on page 3 for the location of these ports. For information on using iDRAC, see ’Integrated Remote Access Controller (iDRAC)’ on page 81.

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/PowerCore 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/PowerCore 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

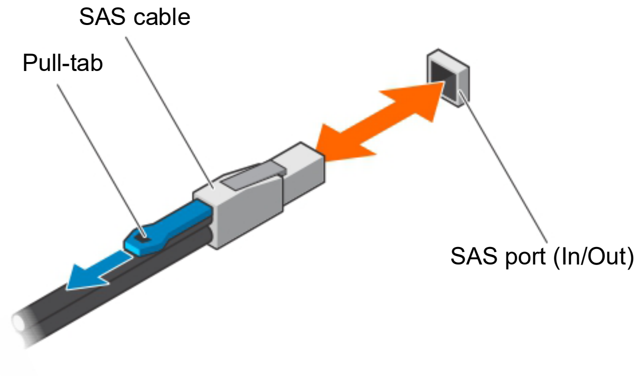
The storage capacity of any LiveWire PowerCore with 200 TB, RAID 6 (240 TB, optional RAID 0) of total hard disk capacity can be increased through the addition of TeraVault for LiveWire PowerCore. TeraVault is available in a configuration of 200 TB, RAID 6 (240 TB, optional RAID 0). Up to four TeraVault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

To connect TeraVault to LiveWire PowerCore:

1. Make sure both TeraVault and LiveWire PowerCore are powered OFF.
2. Select a suitable location for both TeraVault and LiveWire PowerCore. 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.

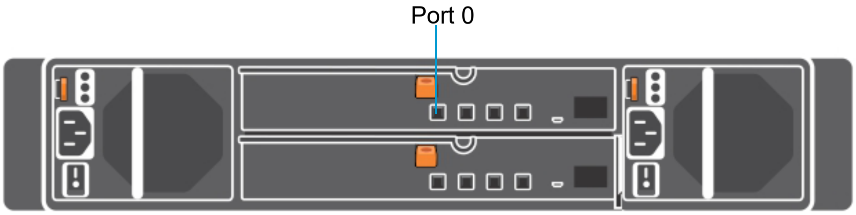
Note If you have multiple TeraVault boxes, and the system is disconnected for any reason, the cabling of the boxes needs to be exactly as it was before, otherwise the RAID won't be seen correctly. To assist you with the cabling, every TeraVault box is labeled with a number, and every TeraVault cable is labeled to the exact port it needs to get plugged into. See 'Connecting multiple TeraVault units' on page 16.

4. Facing the rear of LiveWire PowerCore, insert one connector of the SAS external cascading cable into the left RAID port (Port 0) of the RAID controller on LiveWire PowerCore so that the release pull-tab is on the top.



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 of the RAID controller.

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



TeraVault Unit

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.

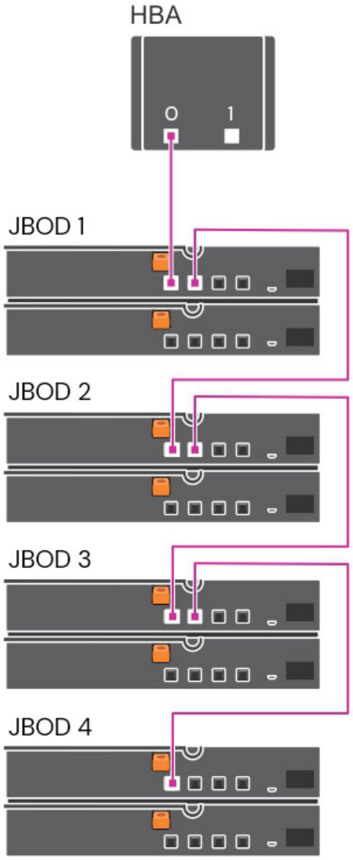
6. Turn on power to TeraVault by pressing the power button on the front of the chassis. You may see brief bursts of LED activity as the expander in TeraVault scans the drives.
7. Turn on the power to LiveWire PowerCore. The system is ready for use as soon as the LiveWire PowerCore boot sequence completes.

Connecting multiple TeraVault units

When connecting multiple TeraVault (JBOD) units to LiveWire PowerCore, it is important to note that each LiveWire PowerCore 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 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 and TeraVault unit. Make sure the LiveAction serial numbers are the same on LiveWire PowerCore 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 as described in 'Connecting TeraVault to LiveWire PowerCore' on page 14. Make sure the release pull-tab on the cable is on 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 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.



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:

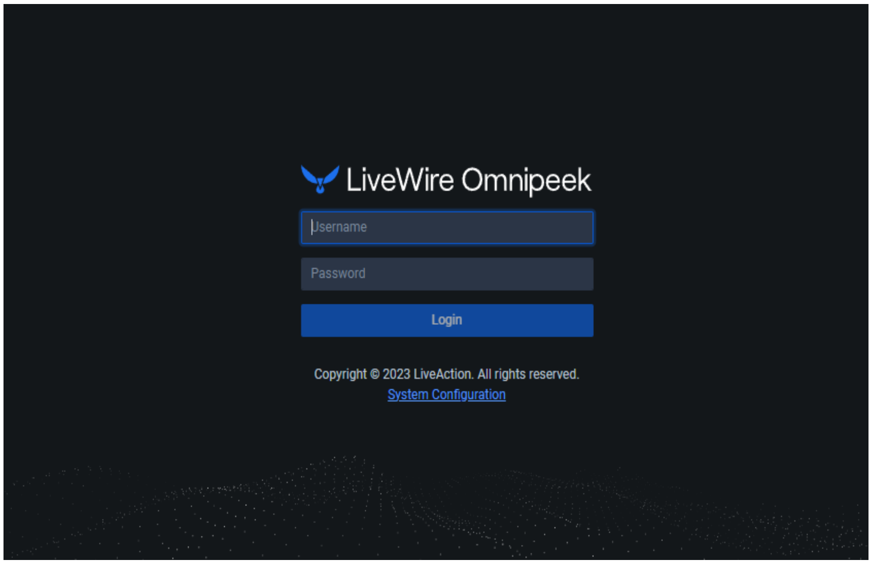
- IP address of LiveWire
- Product key
- User name
- Company name
- Email address
- Version number

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.

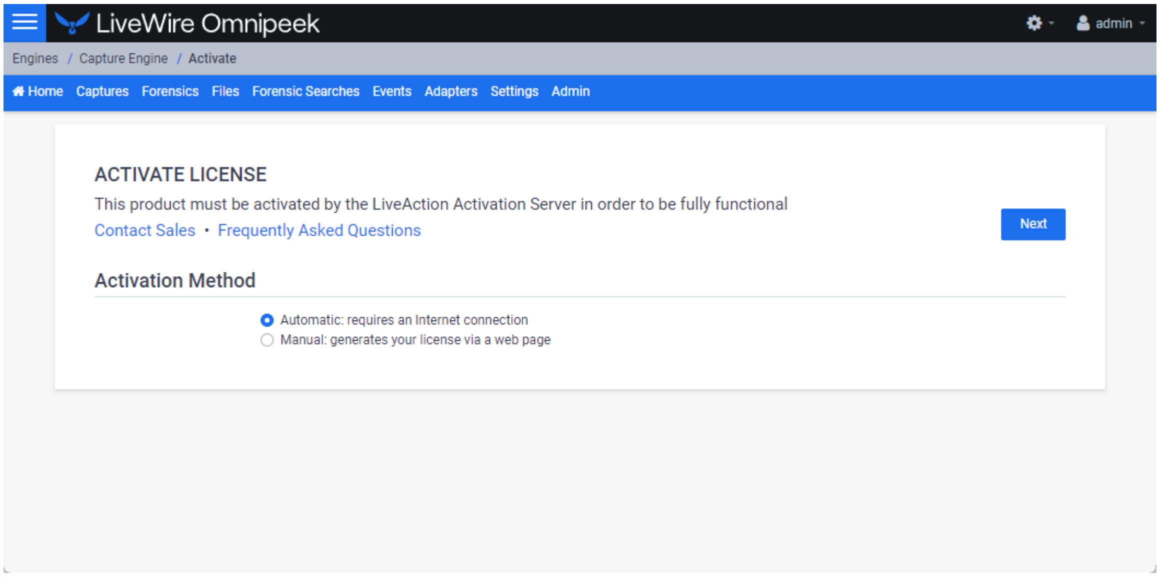


Copyright © 2023 LiveAction. All rights reserved.
System Configuration

   - *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.



ACTIVATE LICENSE

This product must be activated by the LiveAction Activation Server in order to be fully functional

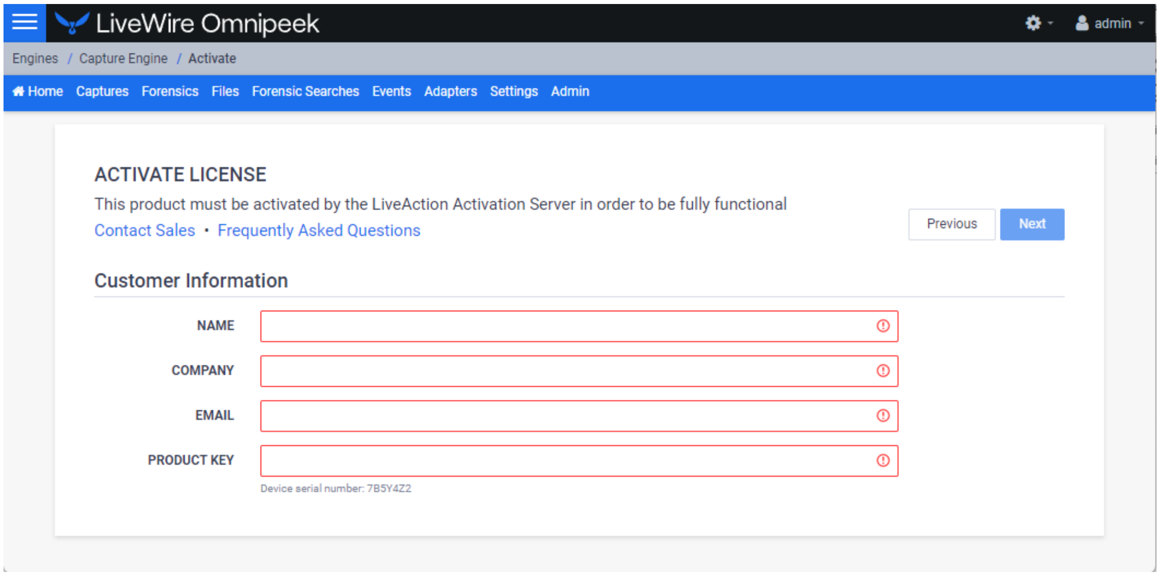
Contact Sales • Frequently Asked Questions

Activation Method

● Automatic: requires an Internet connection

○ Manual: generates your license via a web page

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

Customer Information

NAME

COMPANY

EMAIL

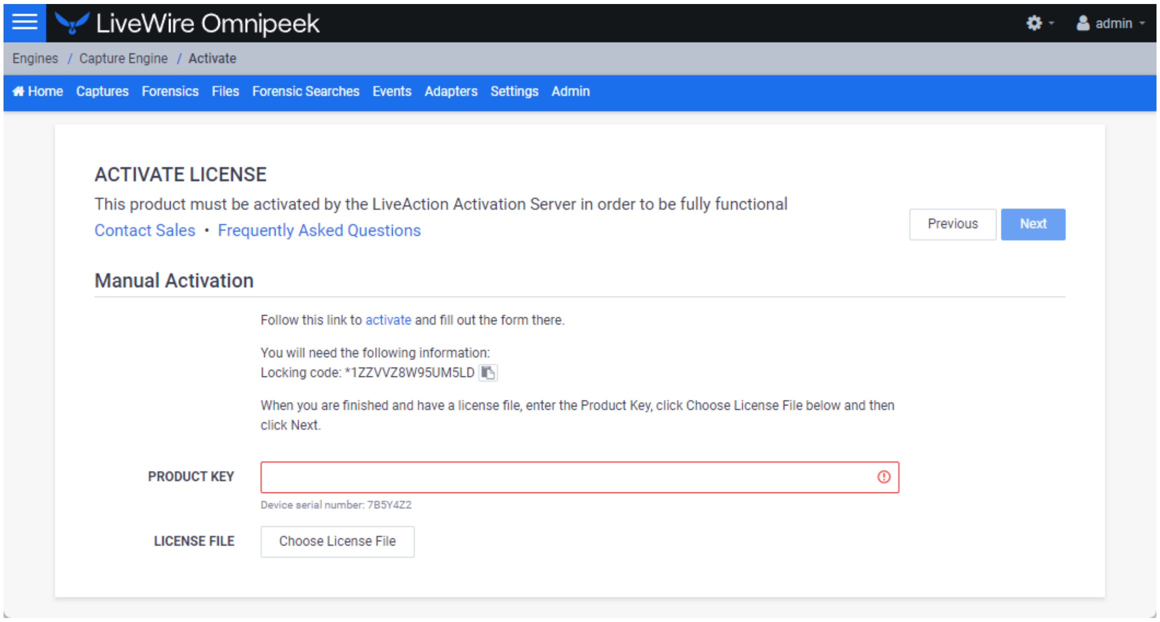
PRODUCT KEY

Device serial number: 7B5Y4Z2

- *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.


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

ACTIVATE LICENSE

This product must be activated by the LiveAction Activation Server in order to be fully functional

Contact Sales • Frequently Asked Questions

Manual Activation

Follow this link to activate and fill out the form there.

You will need the following information:
Locking code: *1ZZVVZ8W95UM5LD

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: 7B5Y4Z2

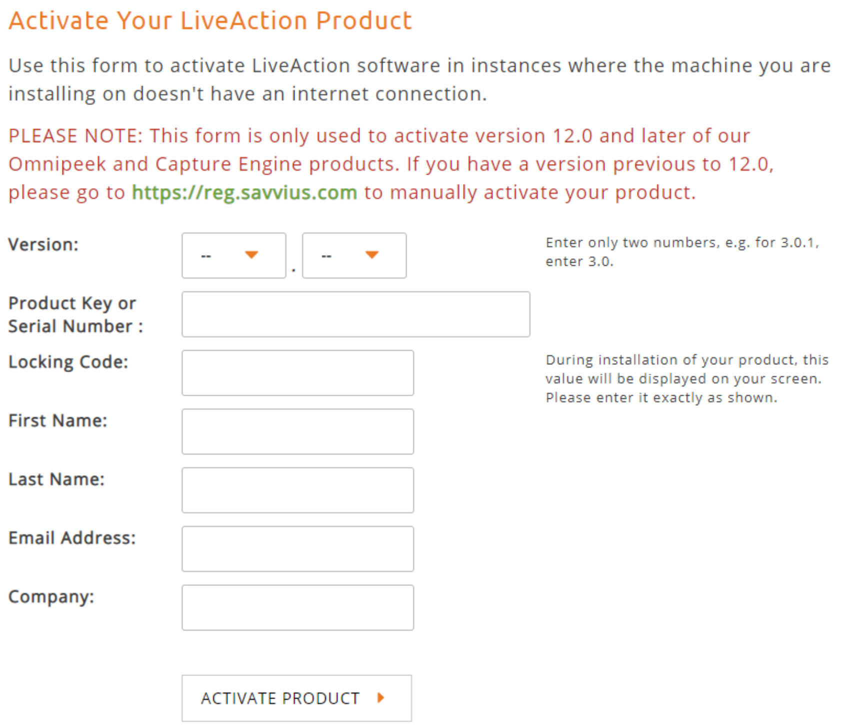
LICENSE FILE Choose License File

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: -- . -- Enter only two numbers, e.g. for 3.0.1, enter 3.0.

Product Key or Serial Number :

Locking Code: During installation of your product, this value will be displayed on your screen. Please enter it exactly as shown.

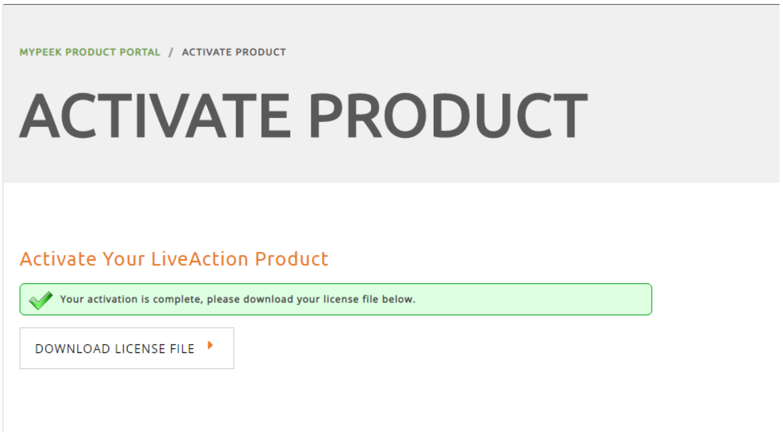
First Name:

Last Name:

Email Address:

Company:

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



MYPEEK PRODUCT PORTAL / ACTIVATE PRODUCT

ACTIVATE PRODUCT

Activate Your LiveAction Product

Your activation is complete, please download your license file below.

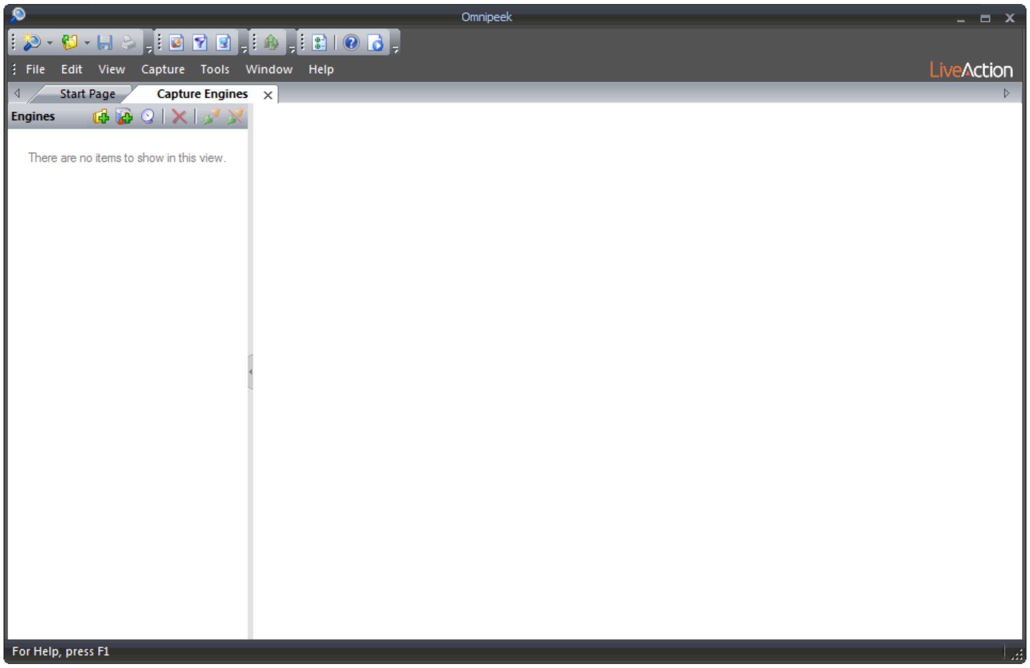
7. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in the following steps.
8. Return back to the to the **Manual Activation** window, and click **Choose License File**.
9. Navigate to the license file downloaded above and click **Open**.
10. Click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

Activation via Omnipeek

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

To activate LiveWire via Omnipeek:

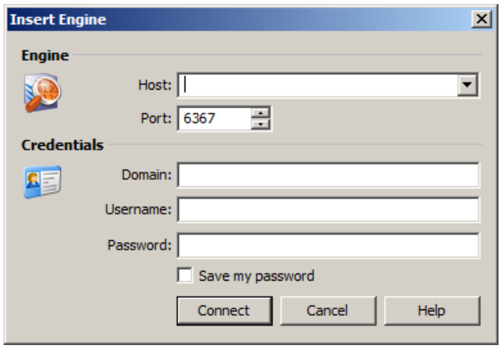
1. From the Omnipeek Start Page, click **View Capture Engines** to display the **Capture Engines** window.



There are no items to show in this view.

For Help, press F1

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



Host:

Port: 6367

Domain:

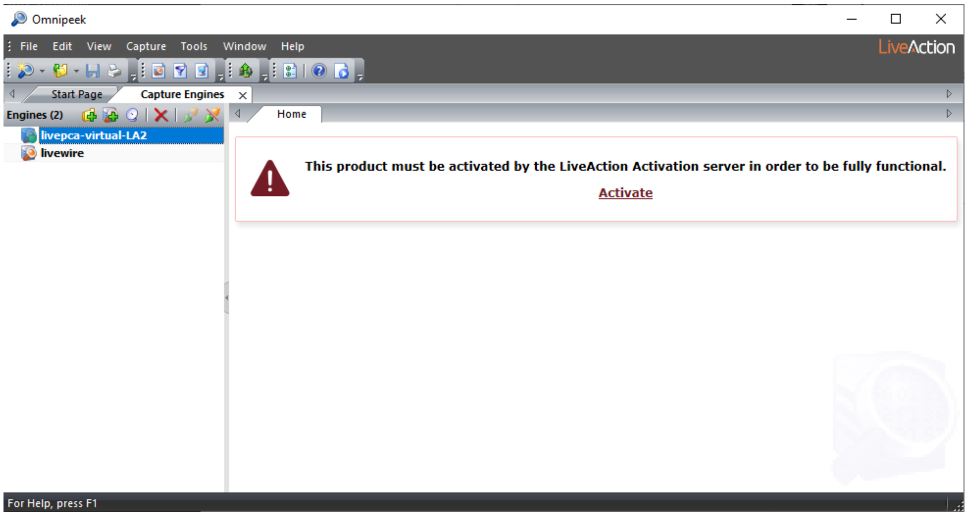
Username:

Password:

☐ Save my password

- *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.

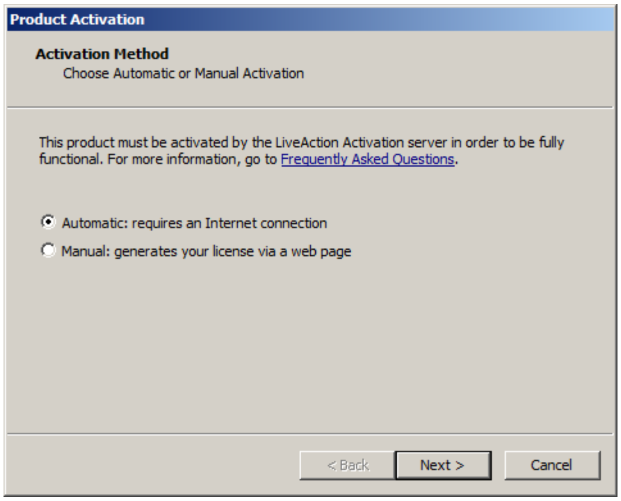
3. Click **Connect** to connect to LiveWire. If LiveWire has not yet been activated, the activation message appears in the **Capture Engines** window.



This product must be activated by the LiveAction Activation server in order to be fully functional.

Activate

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



Product Activation

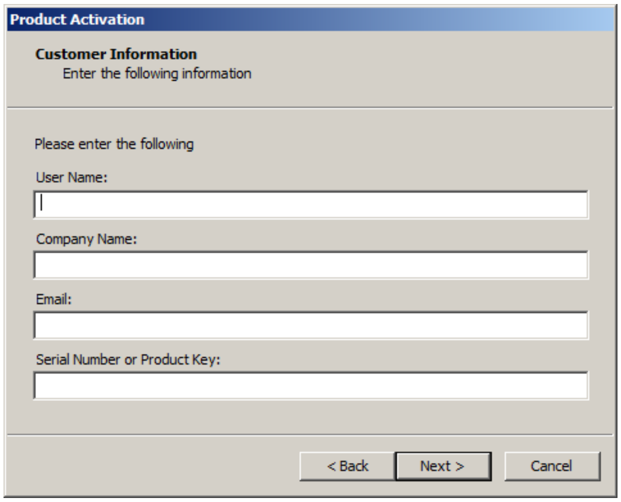
Activation Method
Choose Automatic or Manual Activation

This product must be activated by the LiveAction Activation server in order to be fully functional. For more information, go to Frequently Asked Questions.

● Automatic: requires an Internet connection

○ Manual: generates your license via a web page

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.



Product Activation

Customer Information
Enter the following information

Please enter the following

User Name:

Company Name:

Email:

Serial Number or Product Key:

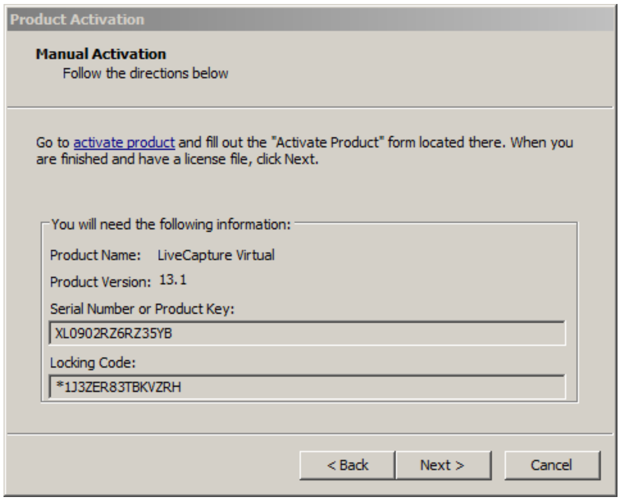
- *User Name*: Type the user name of the customer.
- *Company Name*: Type the company name.

- *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.



Manual Activation

Follow the directions below

Go to activate product and fill out the "Activate Product" form located there. When you are finished and have a license file, click Next.

You will need the following information:

Product Name: LiveCapture Virtual

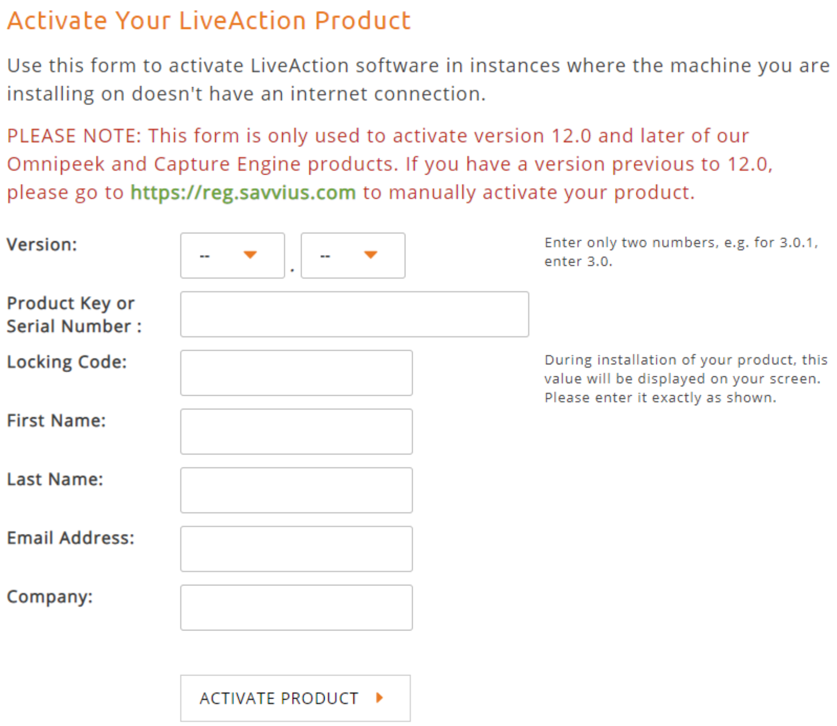
Product Version: 13.1

Serial Number or Product Key: XL0902RZ6RZ35YB

Locking Code: *1J3ZER83TBKVZRH

   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.

7. 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 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: -- . -- Enter only two numbers, e.g. for 3.0.1, enter 3.0.

Product Key or Serial Number :

Locking Code: During installation of your product, this value will be displayed on your screen. Please enter it exactly as shown.

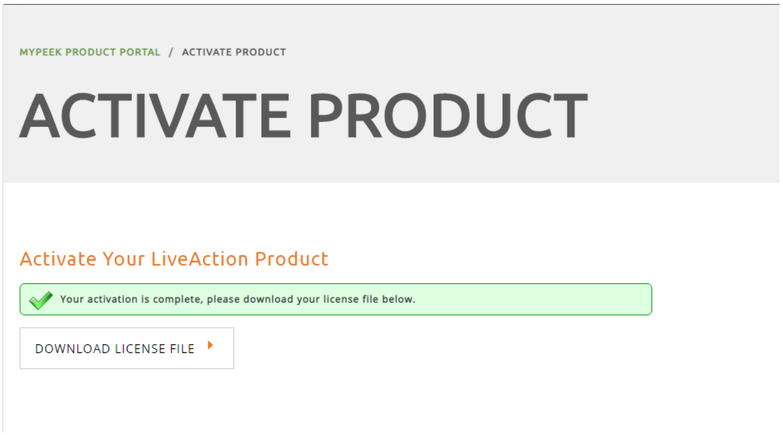
First Name:

Last Name:

Email Address:

Company:

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



MYPEEK PRODUCT PORTAL / ACTIVATE PRODUCT

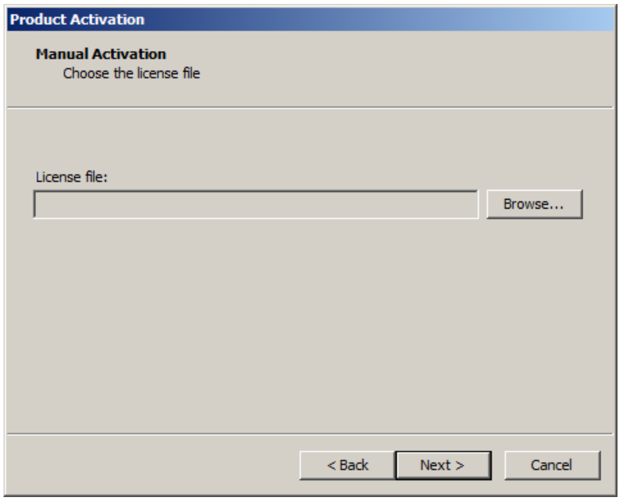
ACTIVATE PRODUCT

Activate Your LiveAction Product

Your activation is complete, please download your license file below.

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.



Product Activation

Manual Activation

Choose the license file

License file:

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.

Starting / shutting down LiveWire

To start LiveWire:

- LiveWire Edge: Press the power-on button on the back panel of LiveWire Edge.
- LiveWire Core/PowerCore: Press the power button in the upper right corner on the front of the chassis.

To shutdown LiveWire:

- LiveWire Edge: Press the power-on button briefly on the back panel of LiveWire Edge.
- 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/PowerCore. See 'Starting / Shutting down LiveWire' on page 88**.**

Attaching the front bezel

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

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

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.

CHAPTER 2

Configuring LiveWire

In this chapter:

Logging-in to LiveWire command line

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

- Remotely, using remote SSH software such as *Putty*
- Locally, by connecting a monitor, mouse and keyboard to LiveWire (LiveWire Core/PowerCore only)
- Locally, via the serial port

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

username: *admin*

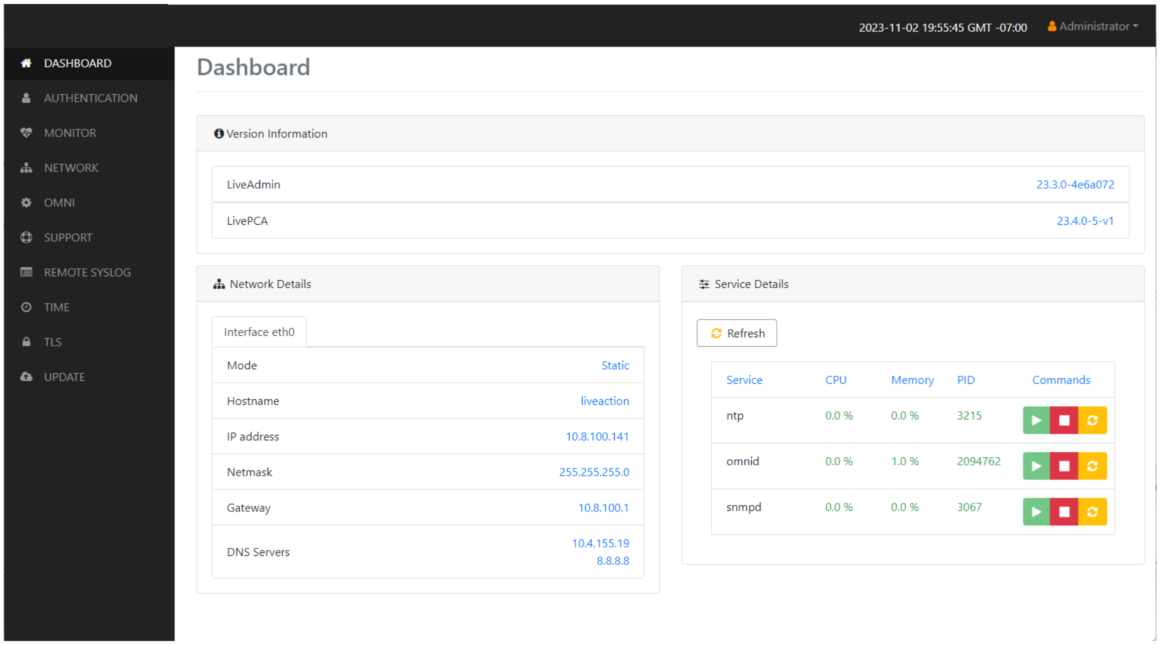
password: *admin*

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

Version Information

LiveAdmin	23.3.0-4e6a072
LivePCA	23.4.0-5-v1

Network Details

Interface eth0

Mode	Static
Hostname	liveaction
IP address	10.8.100.141
Netmask	255.255.255.0
Gateway	10.8.100.1
DNS Servers	10.4.155.19 8.8.8.8

Service Details

Service	CPU	Memory	PID	Commands
ntp	0.0 %	0.0 %	3215	▶ ■ ⟳
omnid	0.0 %	1.0 %	2094762	▶ ■ ⟳
snmpd	0.0 %	0.0 %	3067	▶ ■ ⟳

- *Dashboard*: The *Dashboard* view provides you with some very basic information about the system. See 'Dashboard' on page 29.
- *Authentication*: The *Authentication* view lets you change the password for LiveWire. See 'Authentication' on page 30.
- *Monitor*. The *Monitor* view displays the health of the overall system. See 'Monitor' on page 31.
- *Network*: The *Network* view lets you configure the primary network interfaces network settings and the hostname of the system. See 'Network' on page 32.
- *Omni*: The *Omni* view lets you configure *Centralized Management*, *Factory Reset*, *Backup*, *Restore*, *SFTP*, and *SNMP* for the appliance. See 'Omni' on page 34.

- *Support*: The *Support* view lets you download logs from the system that would be helpful in troubleshooting issues. See 'Support' on page 39.
- *Remote Syslog*: The Remote Syslog view lets you configure a remote syslog server that receives all system logs. See 'Remote Syslog' on page 40.
- *Time*: The *Time* view lets you configure the system's Timezone and NTP servers. See 'Time' on page 40.
- *TLS*: The *TLS* view lets you change the self-signed certificates that LiveAdmin and Omnipeek use for HTTPS. See 'TLS' on page 41.
- *Update*: The *Update* view lets you update the appliance using a software update package. See 'Update' on page 41.
- *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 42.

Important! LiveWire comes pre-configured to obtain its IP address via DHCP. The IP address is required to configure LiveWire, as described below. You can obtain the IP address by logging into Grid as described in 'Using Grid to manage and configure LiveAction appliances' on page 42.

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.

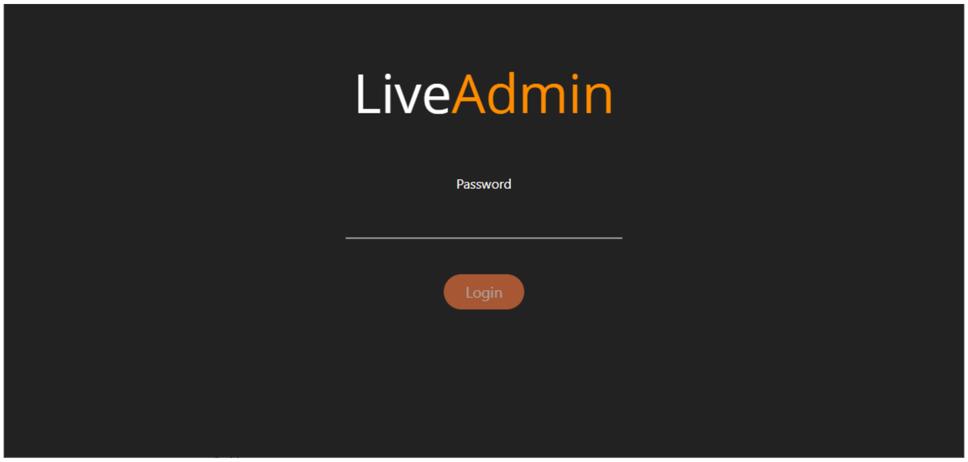
Login

To log into the LiveAdmin utility:

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

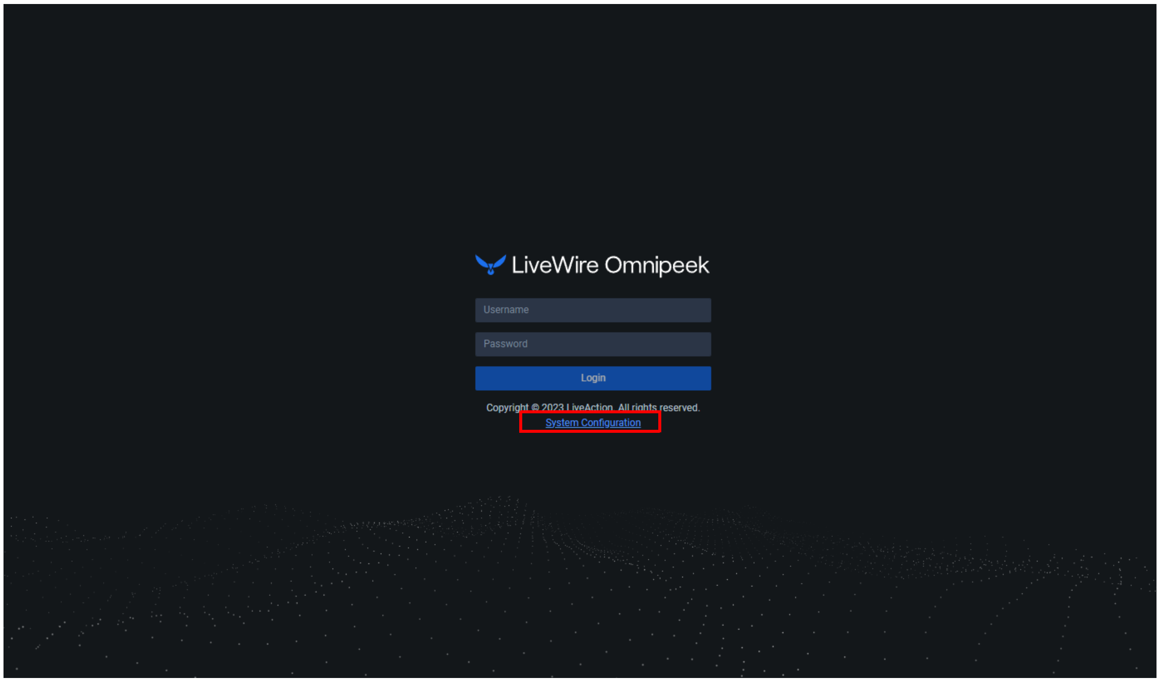
   LiveWire Edge: Connect the '0 MGMT' port on LiveWire Edge to your network router or switch with an Ethernet cable.

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.

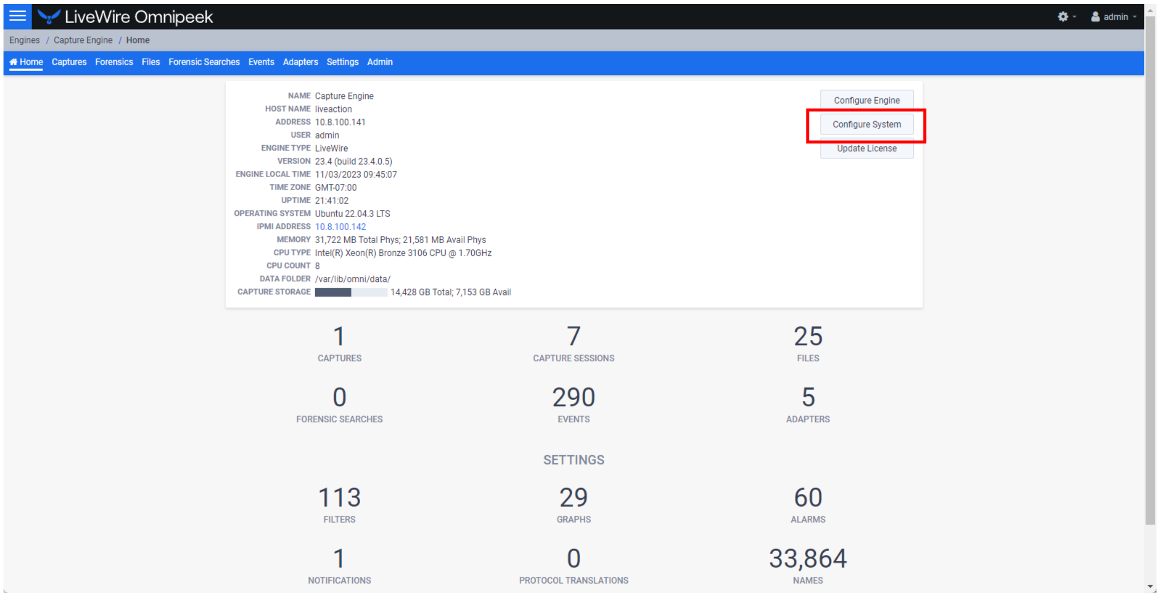


3. Enter the default password 'admin' and click **Login**.

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



Copyright © 2023 LiveAction. All rights reserved.



NAME	Capture Engine
HOST NAME	liveaction
ADDRESS	10.8.100.141
USER	admin
ENGINE TYPE	LiveWire
VERSION	23.4 (build 23.4.0.5)
ENGINE LOCAL TIME	11/03/2023 09:45:07
TIME ZONE	GMT-07:00
UPTIME	21:41:02
OPERATING SYSTEM	Ubuntu 22.04.3 LTS
IPMI ADDRESS	10.8.100.142
MEMORY	31,722 MB Total Phys; 21,581 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; 7,153 GB Avail

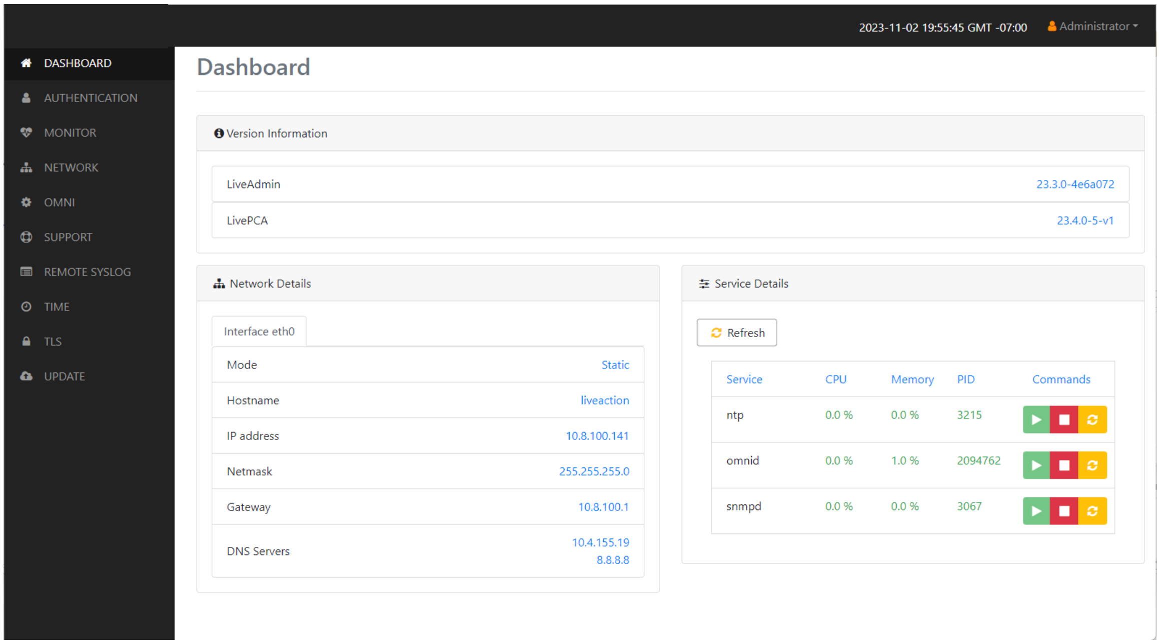
1 CAPTURES	7 CAPTURE SESSIONS	25 FILES
0 FORENSIC SEARCHES	290 EVENTS	5 ADAPTERS

SETTINGS

113 FILTERS	29 GRAPHS	60 ALARMS
1 NOTIFICATIONS	0 PROTOCOL TRANSLATIONS	33,864 NAMES

Dashboard

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



Dashboard

Version Information

LiveAdmin	23.3.0-4e6a072
LivePCA	23.4.0-5-v1

Network Details

Interface eth0

Mode	Static
Hostname	liveaction
IP address	10.8.100.141
Netmask	255.255.255.0
Gateway	10.8.100.1
DNS Servers	10.4.155.19 8.8.8.8

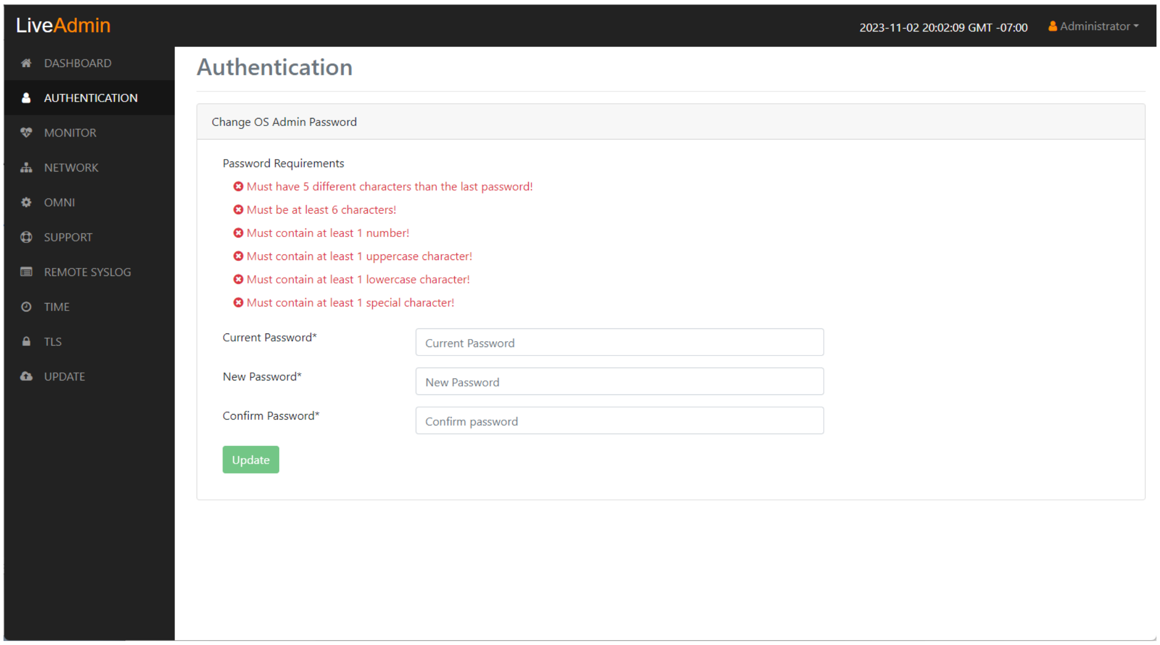
Service Details

Service	CPU	Memory	PID	Commands
ntp	0.0 %	0.0 %	3215	▶ ■ ⟳
omnid	0.0 %	1.0 %	2094762	▶ ■ ⟳
snmpd	0.0 %	0.0 %	3067	▶ ■ ⟳

- *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 32.
- *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.



Authentication

Change OS Admin Password

Password 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!

Current Password* Current Password

New Password* New Password

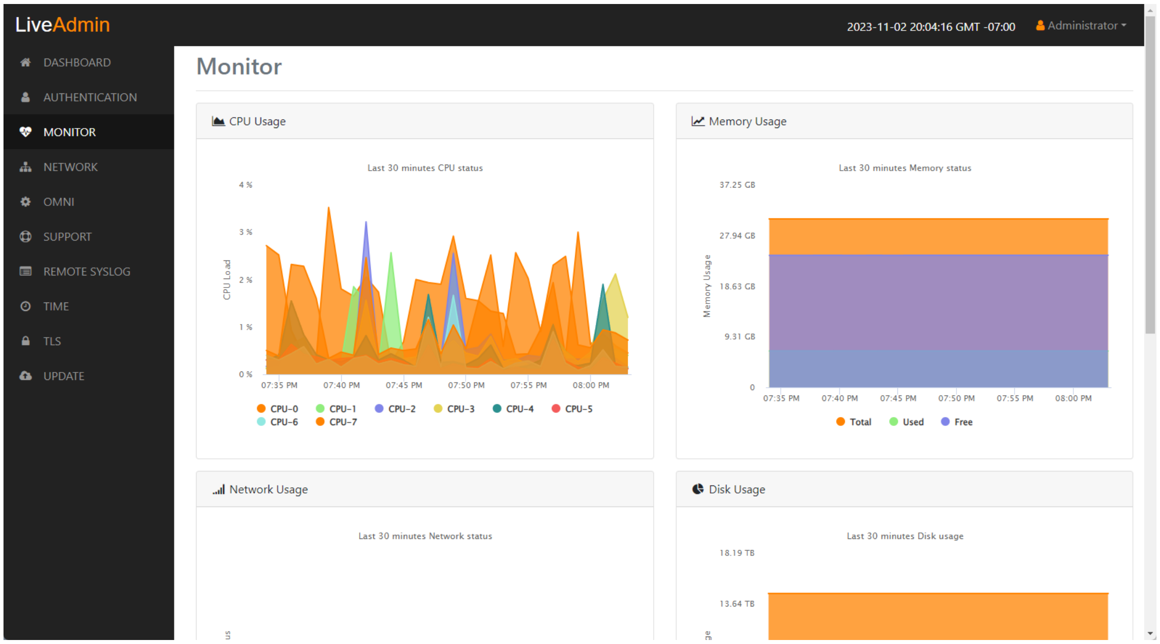
Confirm Password* Confirm password

- *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.

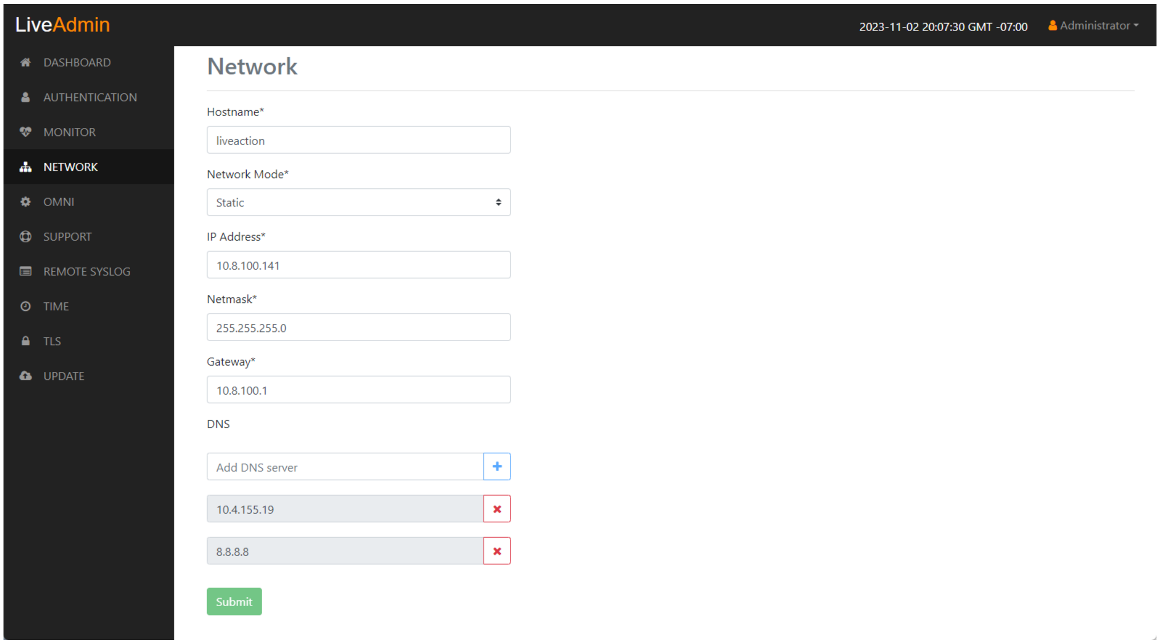


- *CPU Usage*: This chart displays the current usage of individual CPUs on the system. Click the CPU label in the legend to enable/disable its data displayed in the chart.
- *Memory Usage*: This chart displays the current amount of memory being consumed on the system. Click the *Total*, *Used*, or *Free* 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.



Network

Hostname*: liveaction

Network Mode*: Static

IP Address*: 10.8.100.141

Netmask*: 255.255.255.0

Gateway*: 10.8.100.1

DNS: Add DNS server +

10.4.155.19 ✖

8.8.8.8 ✖

- *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

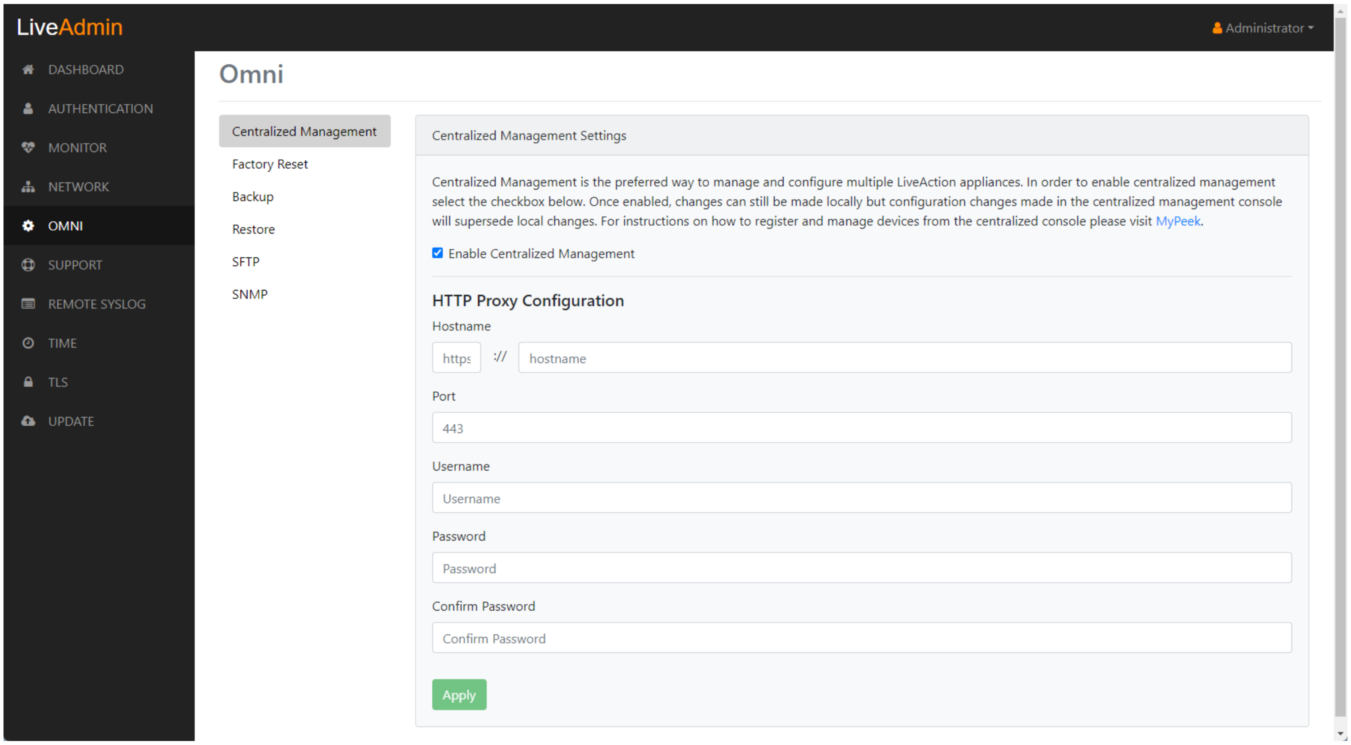
To configure a static IP address:

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.



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: https :// hostname

Port: 443

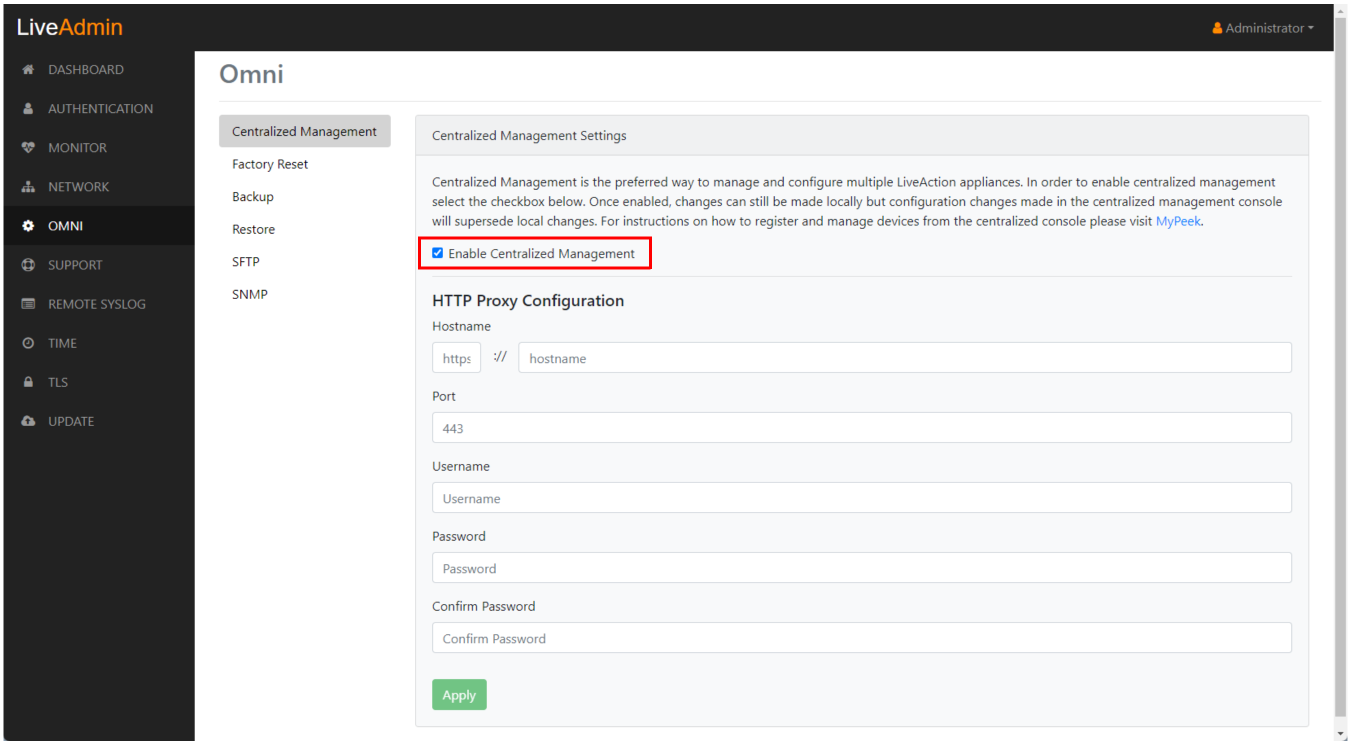
Username: Username

Password: Password

Confirm 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*.



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: https :// hostname

Port: 443

Username: Username

Password: Password

Confirm Password: Confirm Password

- *Enable Centralized Management*: Select this check box to enable Grid for LiveWire to manage and configure LiveWire from the cloud. See ‘Using Grid to manage and configure LiveAction appliances’ on page 42.

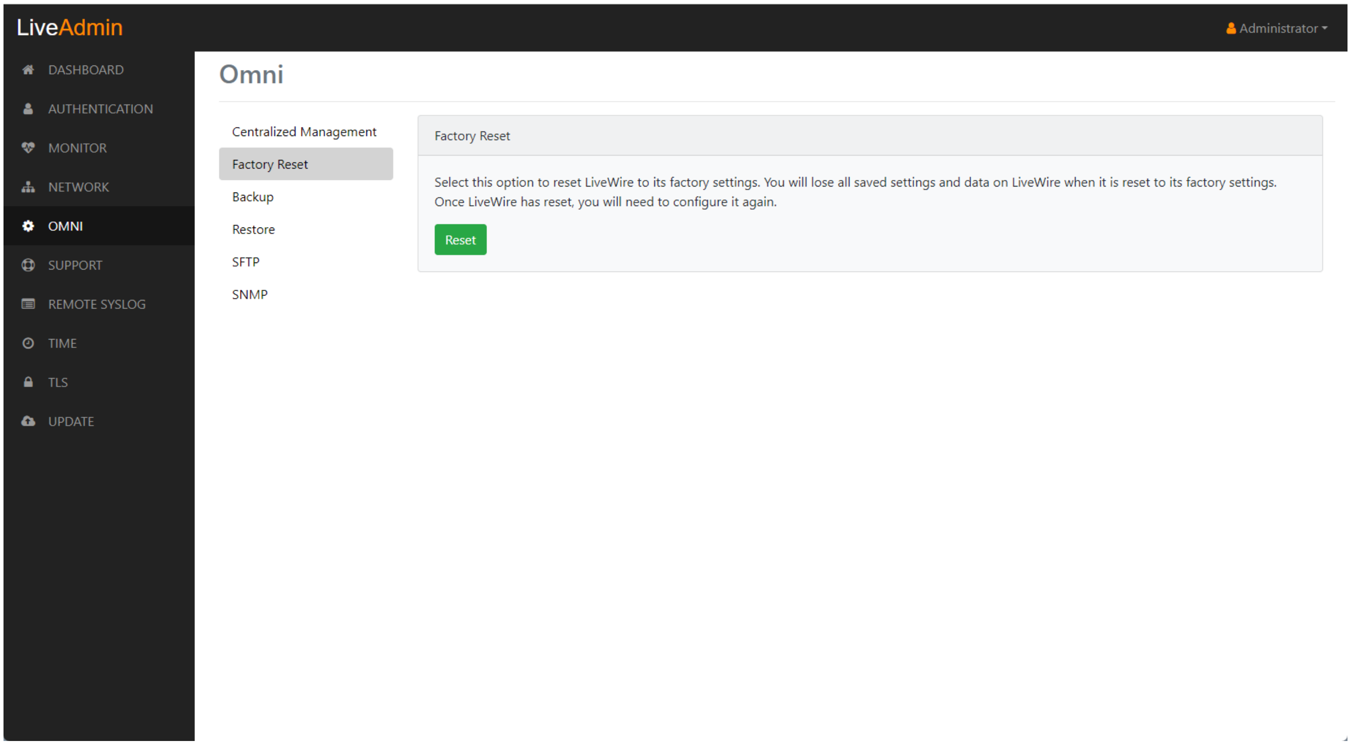
Note When Centralized Management is enabled, you can make local changes to LiveWire using the LiveAdmin utility; however, changes made with Grid will overwrite any local changes made with the LiveAdmin utility.

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.

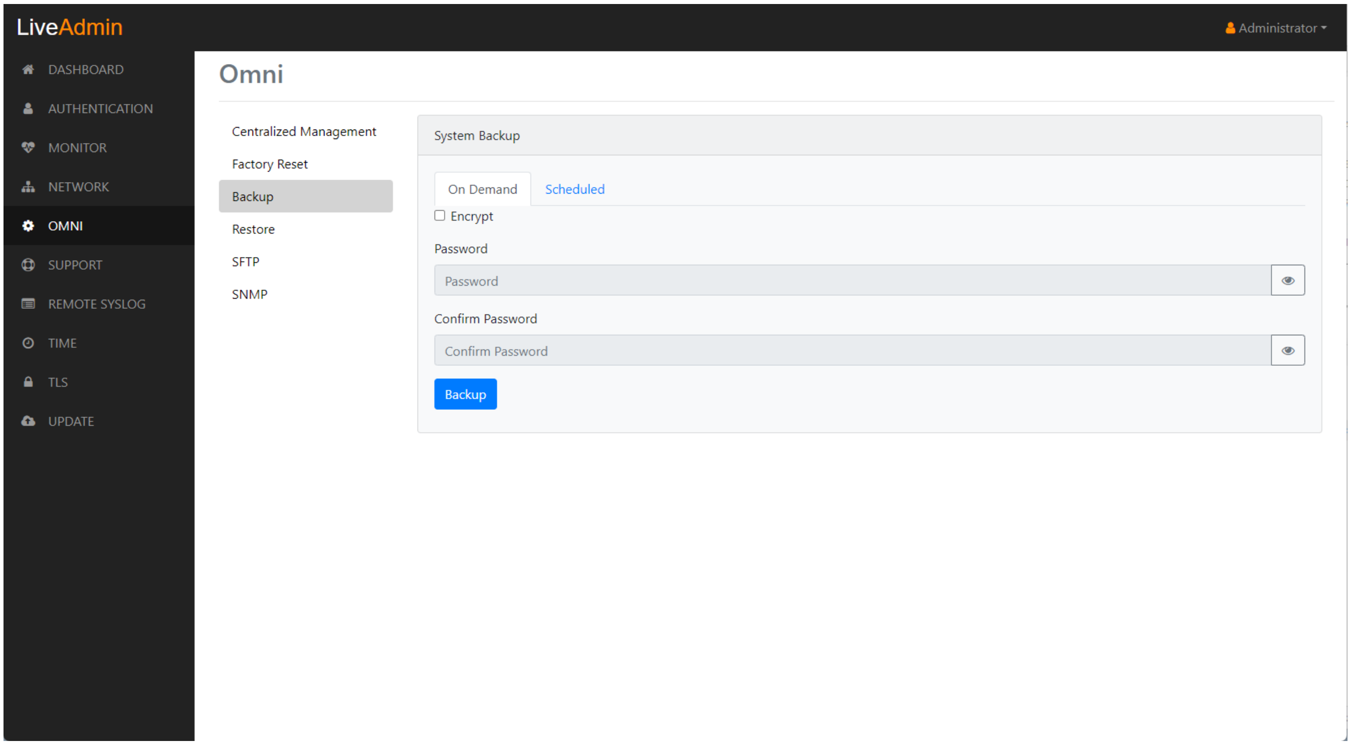
CAUTION! All data captured by the LiveAction software will be deleted. All configuration settings will revert to their factory defaults, including the IP address of the management port.



Select this option to reset LiveWire to its factory settings. You will lose all saved settings and data on LiveWire when it is reset to its factory settings. Once LiveWire has reset, you will need to configure it again.

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.

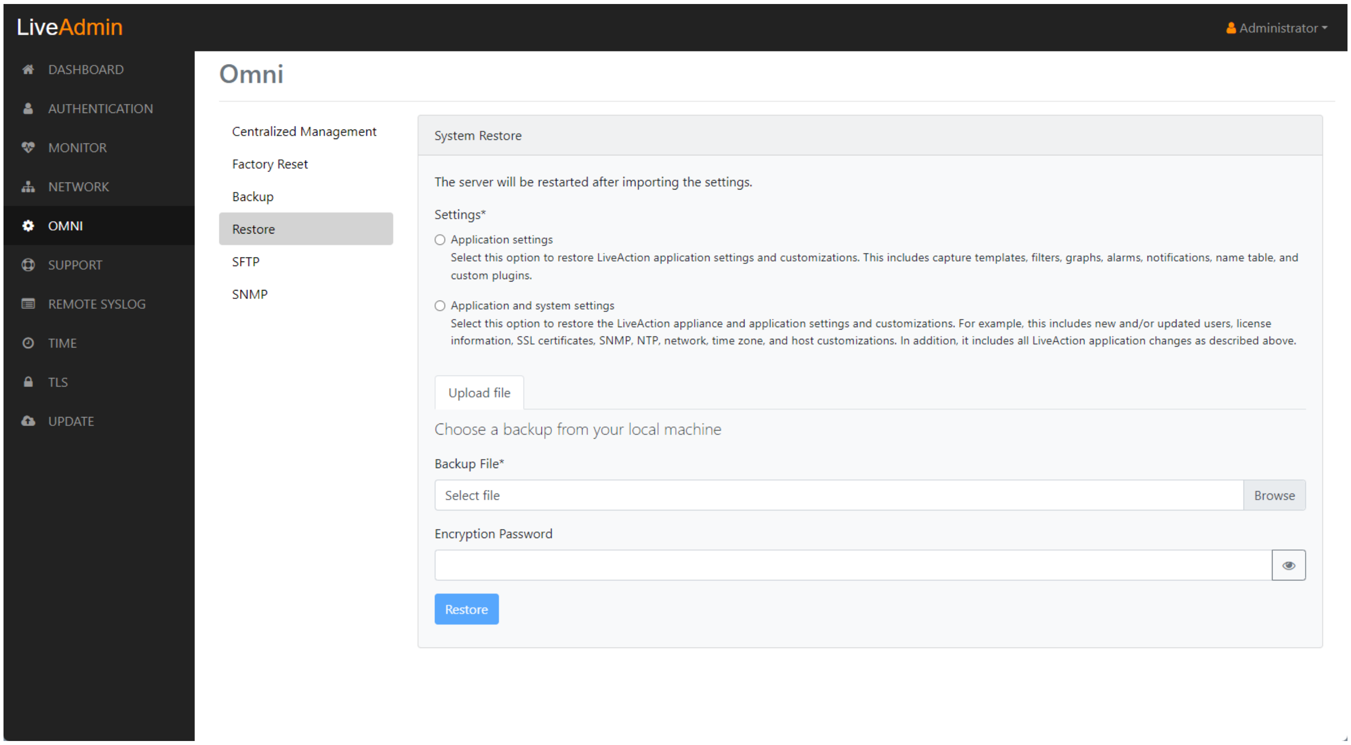
- *Confirm Password*: Type the password again to confirm the password.
- *Backup*: Click to start the backup.

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.



System Restore

The server will be restarted after importing the settings.

Settings*

○ Application settings
Select this option to restore LiveAction application settings and customizations. This includes capture templates, filters, graphs, alarms, notifications, name table, and custom plugins.

○ Application and system settings
Select this option to restore the LiveAction appliance and application settings and customizations. For example, this includes new and/or updated users, license information, SSL certificates, SNMP, NTP, network, time zone, and host customizations. In addition, it includes all LiveAction application changes as described above.

Upload file

Choose a backup from your local machine

Backup File*

Select file | Browse

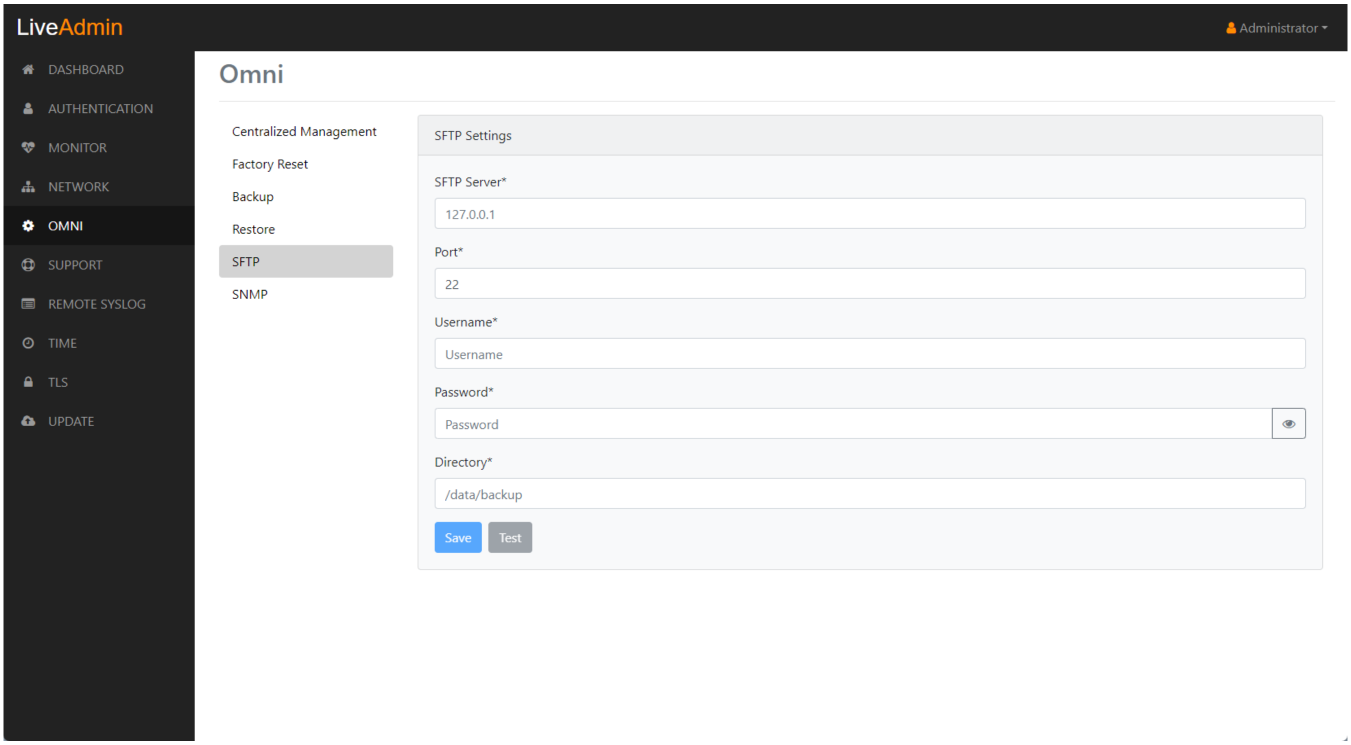
Encryption Password

Restore

- *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.



SFTP Settings

SFTP Server*
127.0.0.1

Port*
22

Username*
Username

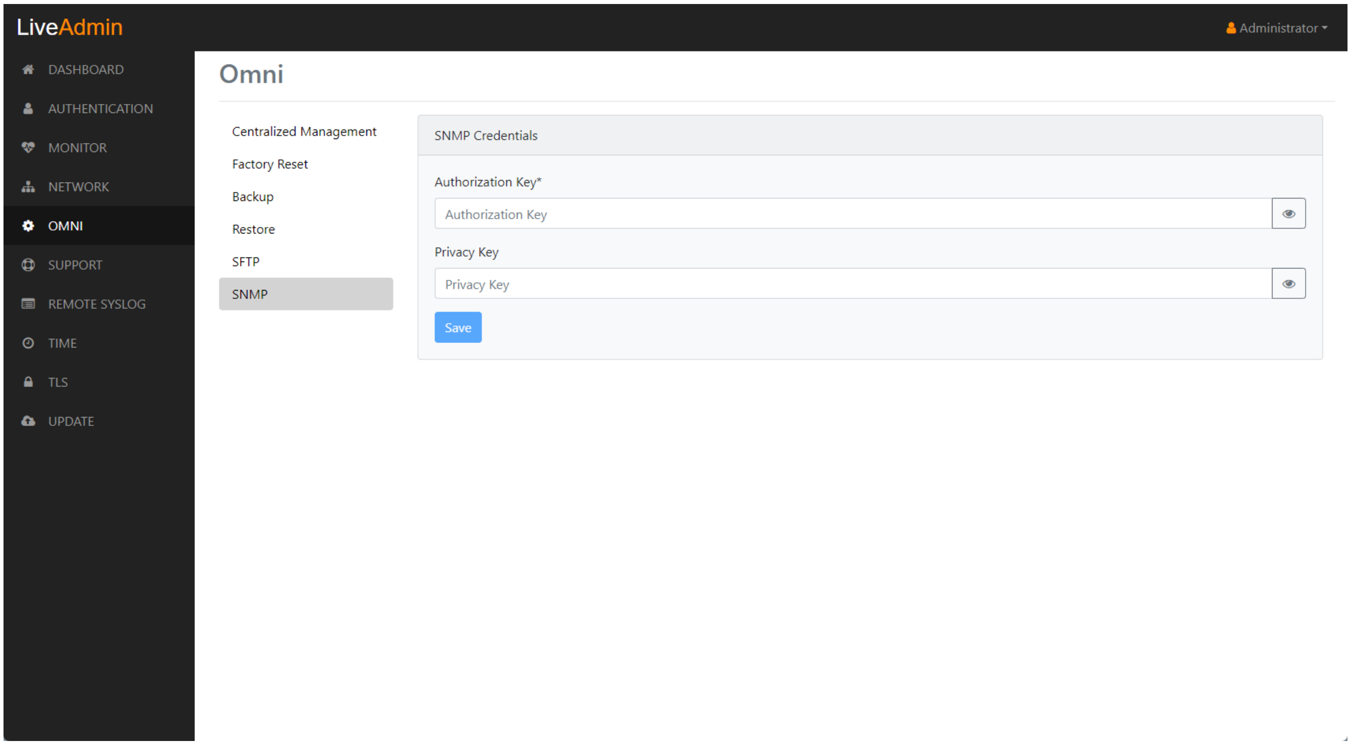
Password*
Password

Directory*
/data/backup

- *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

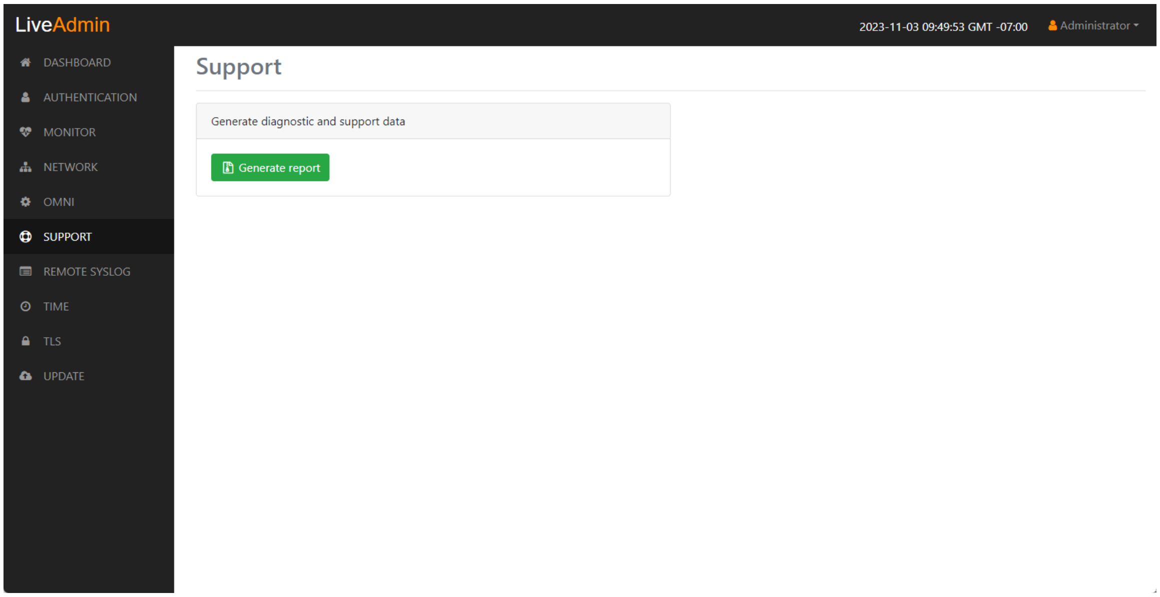
SNMP settings allow you to configure the SNMP Credentials *Authentication Key* and *Privacy Key* for LiveWire.



- *Authorization Key*: Type a new *Authorization Key* to change it from the default *Authorization Key* displayed in ‘LiveNX SNMP Configuration’ in ‘LiveFlow’ on page 96.
- *Privacy Key*: Type a new *Privacy Key* to change it from the default *Privacy Key* displayed in ‘LiveNX SNMP Configuration’ in ‘LiveFlow’ on page 96.
- *Save*: Click to apply the SNMP credentials to the device.

Support

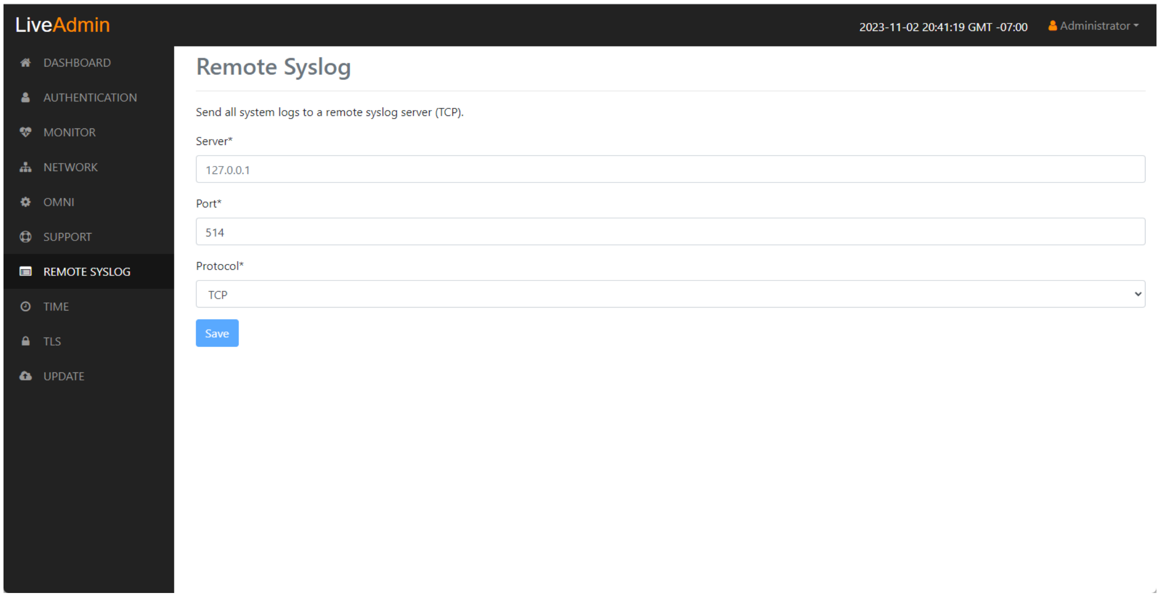
The *Support* view lets you generate a diagnostic and support data report from LiveWire that would be helpful in troubleshooting issues.



- *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.



Remote Syslog

Send all system logs to a remote syslog server (TCP).

Server*: 127.0.0.1

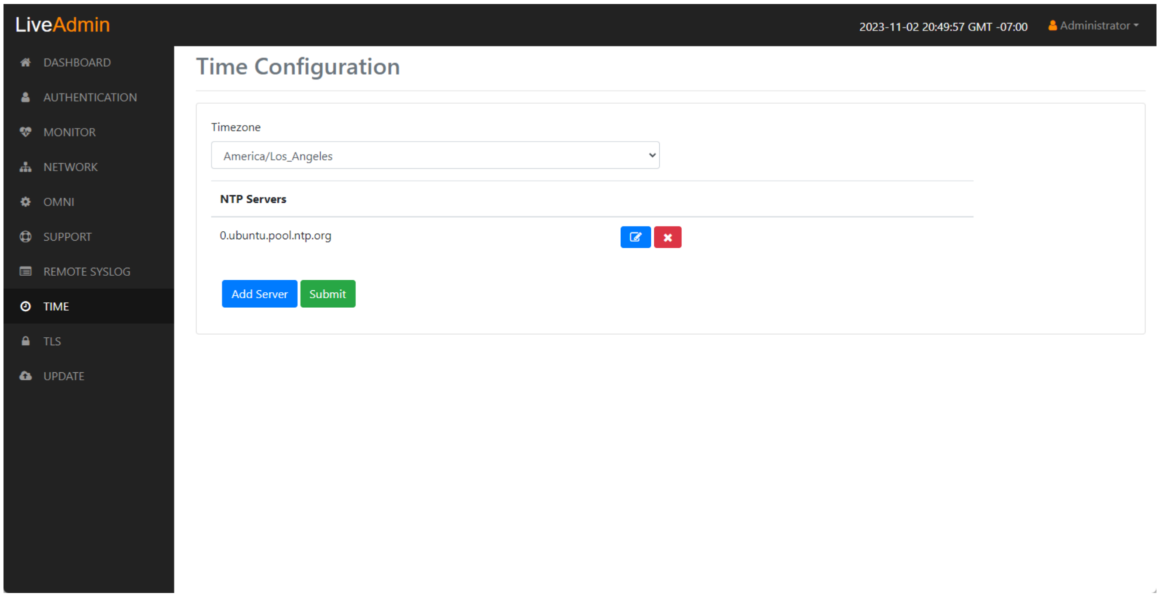
Port*: 514

Protocol*: TCP

- *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.



Time Configuration

Timezone: America/Los_Angeles

NTP Servers

0.ubuntu.pool.ntp.org

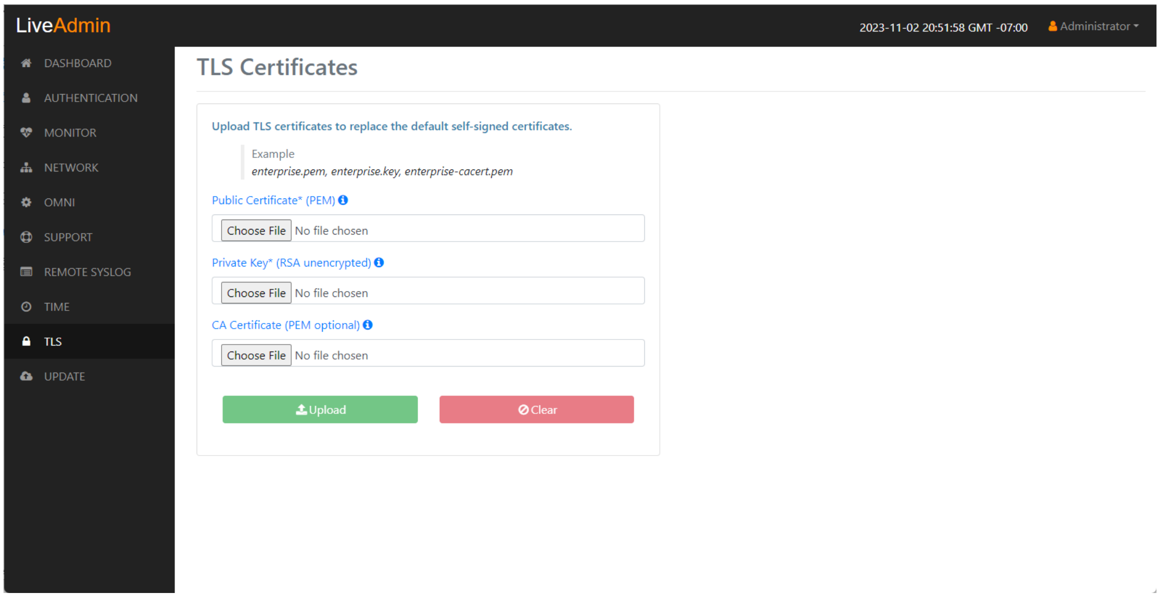
- *Timezone*: The Timezone setting lets you specify the physical location of LiveWire. Select from the list the location closest to your LiveWire.

- *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 LiveWiref 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 Omnipeek and LiveAdmin use for HTTPS.



TLS Certificates

Upload TLS certificates to replace the default self-signed certificates.

> Example
> *enterprise.pem, enterprise.key, enterprise-cacert.pem*

Public Certificate* (PEM)

No file chosen

Private Key* (RSA unencrypted)

No file chosen

CA Certificate (PEM optional)

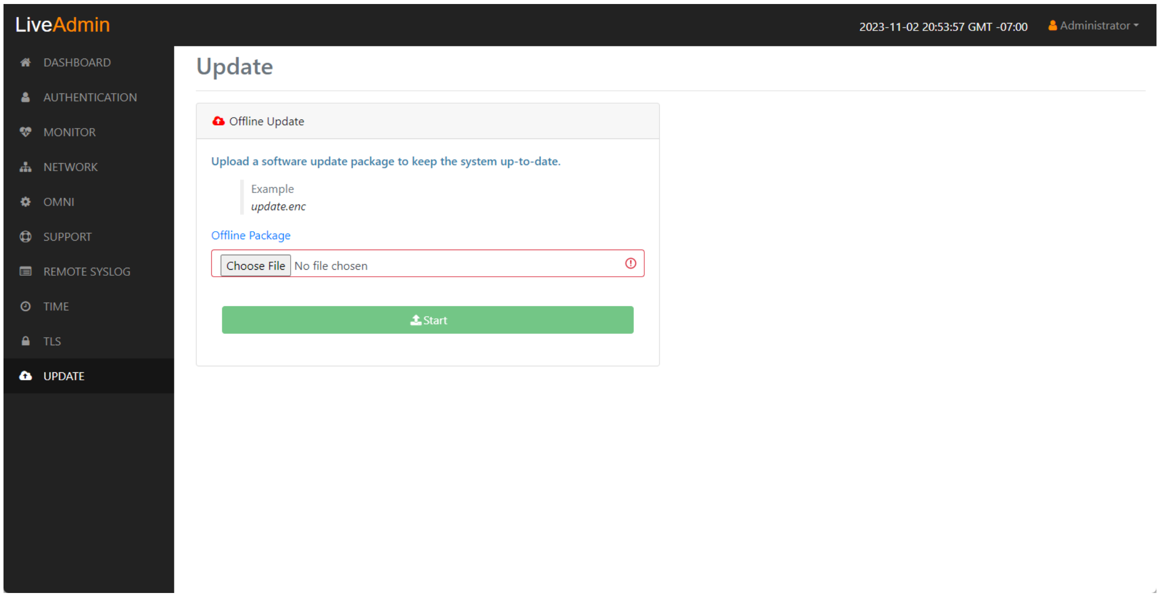
No file chosen

- *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.



Update

Offline Update

Upload a software update package to keep the system up-to-date.

Example
update.enc

Offline Package

No file chosen

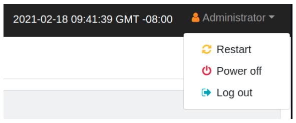
To update the software:

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**.

Using Grid to manage and configure LiveAction appliances

If you have one or more LiveAction appliances, you can use LiveAction Grid to manage and configure these appliances from the cloud. In order to use the Grid server for the LiveAction appliance, you must first enable the *Enable Centralized Management Settings* option in the LiveAdmin utility as described in 'Omni' on page 34.

Note When *Centralized Management Settings* are enabled, you can make local changes to the LiveAction appliance using the LiveAdmin utility; however, changes made with Grid will overwrite any local changes made with the utility.

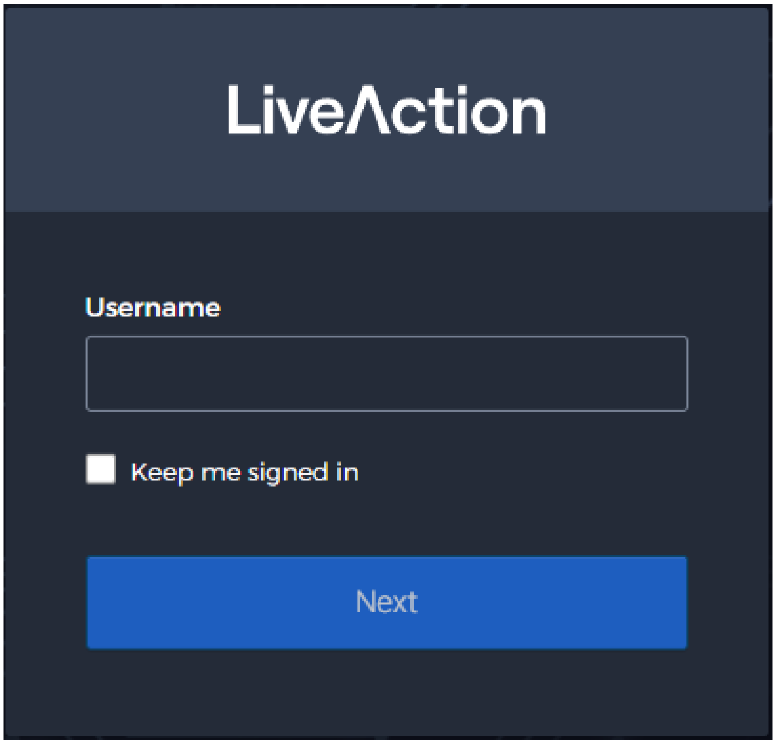
Note All Grid communications require that the LiveAction appliance has Internet access and is able to access various websites including *https://mypeek.liveaction.com* and *https://cloudkeys.liveaction.com* using TCP over port 443. If necessary, configure a DNS server to resolve the URLs above.

Additionally, all Grid communications are initiated by the LiveAction appliance, so it is not necessary to open a port in the firewall for communications.

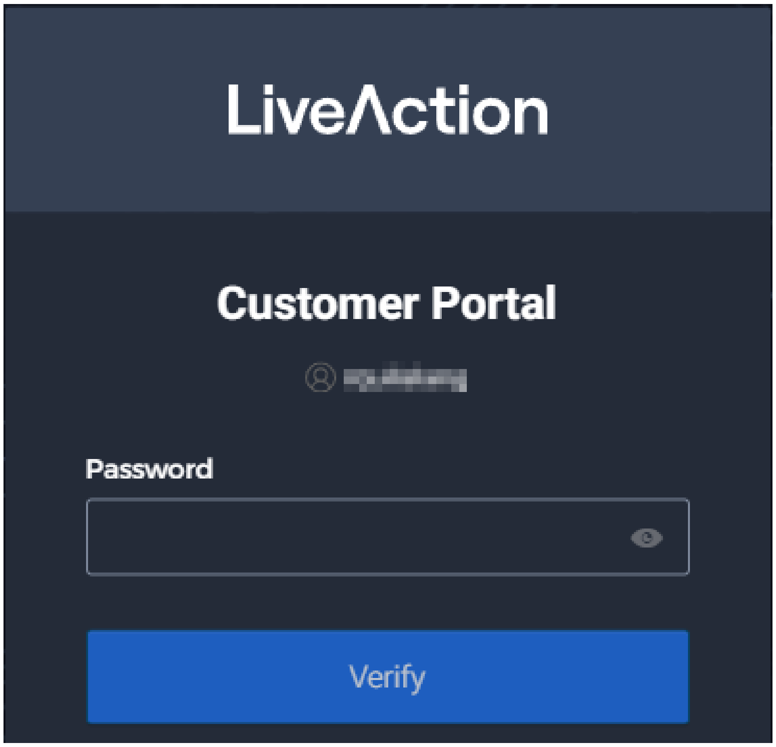
To use Grid to manage and configure LiveAction appliances:

1. Log into LiveAction Grid using the link provided by LiveAction when the appliance was purchased.

Note A link to LiveAction Grid and a temporary password is emailed to the customer whenever a LiveAction appliance is purchased. Use the customer email and temporary password to log into Grid. You will be required to change the temporary password upon first login.



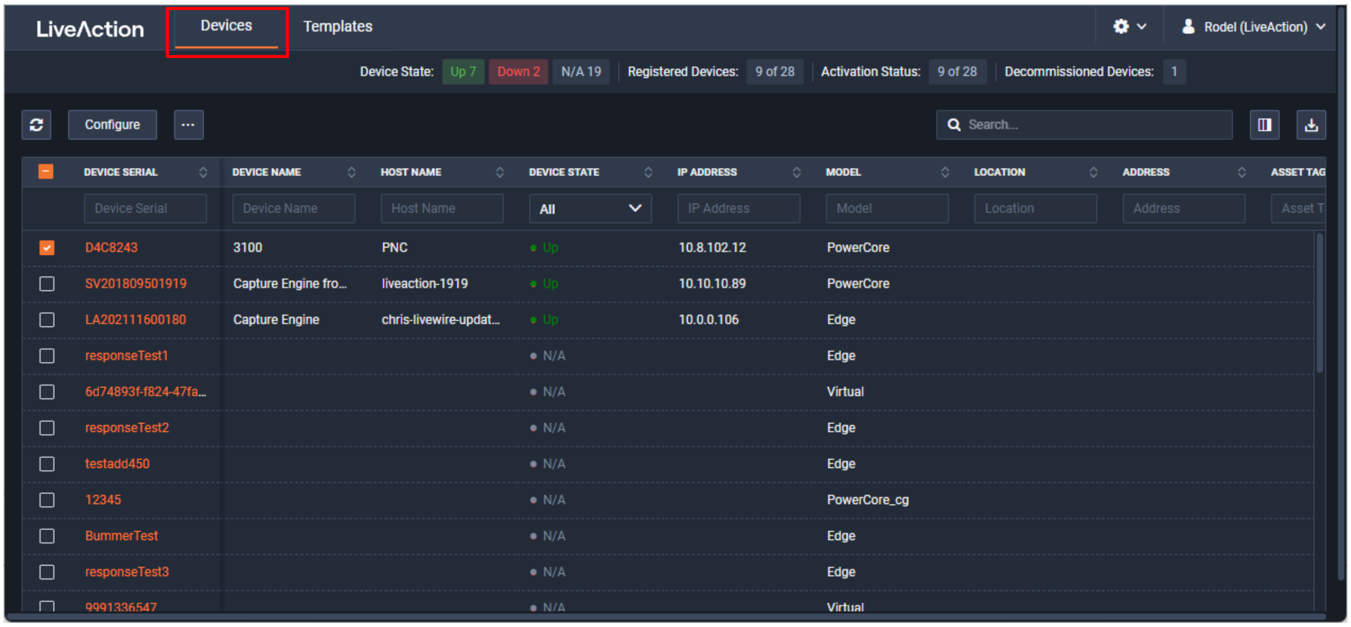
2. Enter the Username, and click **Next**.



3. Enter your Password, and click **Verify**.

Grid Devices tab

The Grid *Devices* tab displays the LiveWire devices associated with the user's account. A description of each of the available options and settings in the *Devices* tab is provided below:

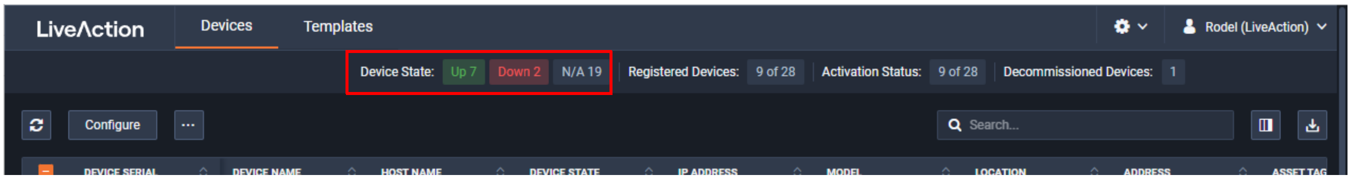


Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

	DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION	ADDRESS	ASSET TAG
	Device Serial	Device Name	Host Name	All	IP Address	Model	Location	Address	Asset T
☑	D4C8243	3100	PNC	● Up	10.8.102.12	PowerCore			
☐	SV201809501919	Capture Engine fro...	liveaction-1919	● Up	10.10.10.89	PowerCore			
☐	LA202111600180	Capture Engine	chris-livewire-updat...	● Up	10.0.0.106	Edge			
☐	responseTest1			● N/A		Edge			
☐	6d74893f-f824-47fa...			● N/A		Virtual			
☐	responseTest2			● N/A		Edge			
☐	testadd450			● N/A		Edge			
☐	12345			● N/A		PowerCore_cg			
☐	BummerTest			● N/A		Edge			
☐	responseTest3			● N/A		Edge			
☐	9991336547			● N/A		Virtual			

Device State

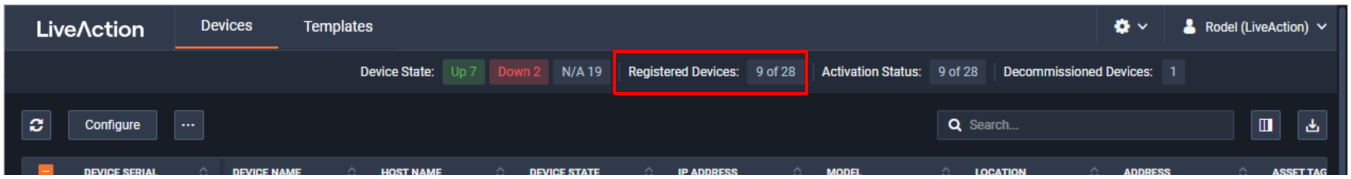
The *Device State* displays whether the device is able to connect to Grid.



- *Up*: Displays the number of devices that were able to connect to Grid.
- *Down*: Displays the number of devices Grid has not heard from in the last two intervals. The default interval is 10 minutes.
- *N/A*: Displays the number of devices that are not available to Grid.

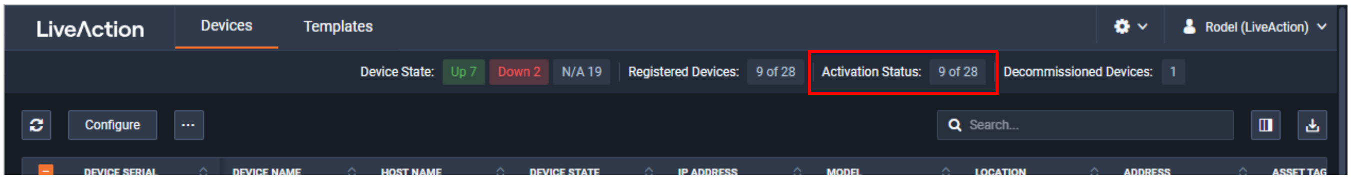
Registered Devices

The *Registered Devices* displays the number of devices that have registered with Grid.



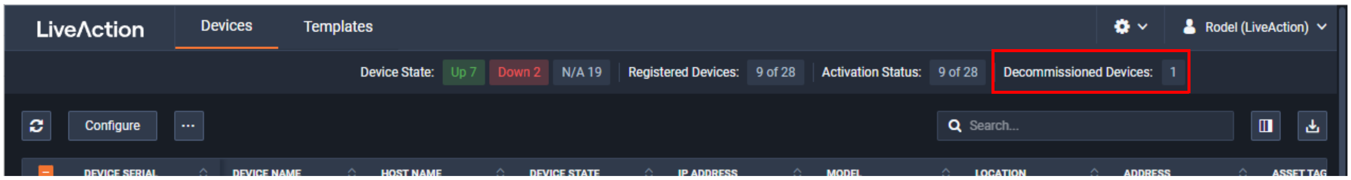
Activation Status

The *Activation Status* displays the number of devices that have been activated.



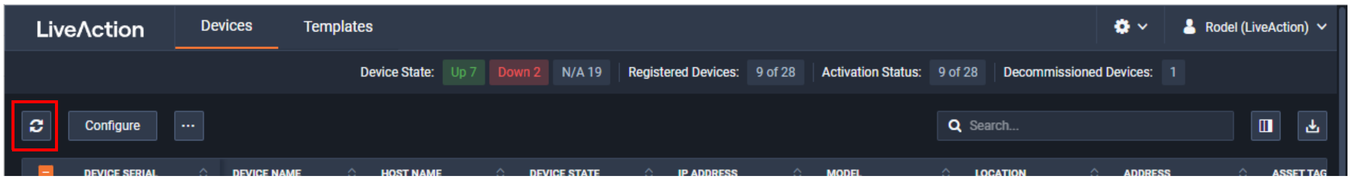
Decommissioned Devices

The *Decommissioned Devices* displays the number of devices that have been deactivated.



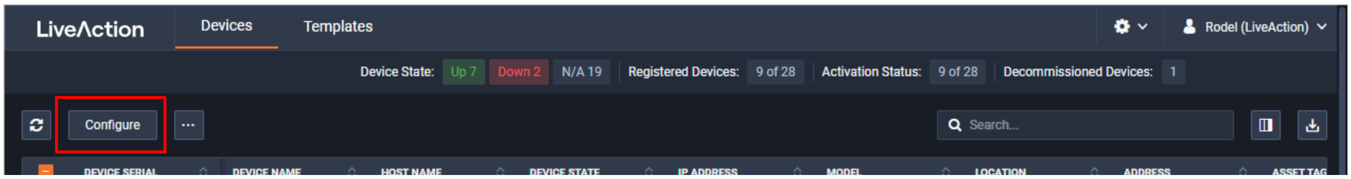
Refresh

Click **Refresh** to refresh the list of devices.



Configure

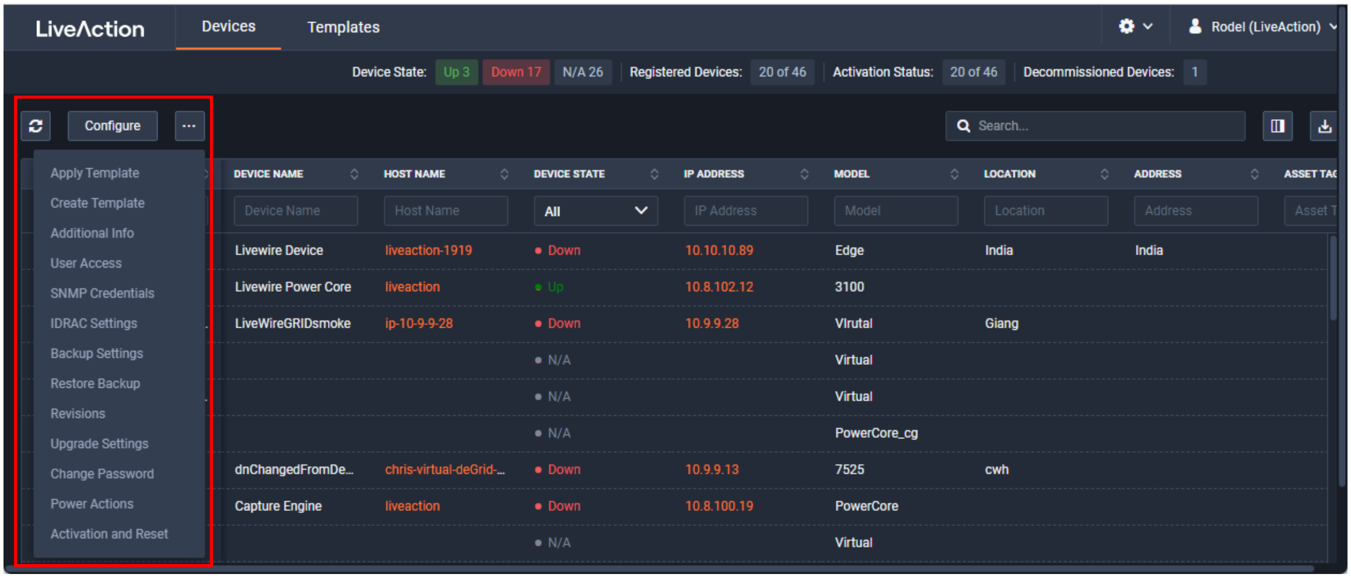
Click to display the *Configure* settings to configure the selected device. See 'Configuring a Device' on page 49 for descriptions of each of the settings.



Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

Elipsis (...)

Click the **Elipsis** (...) to view the following settings for the selected devices:



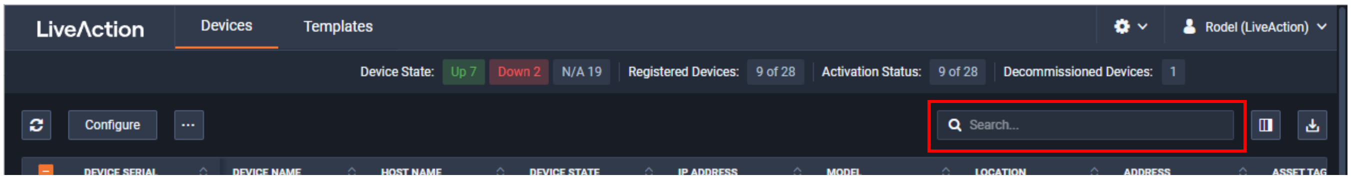
Device State: Up 3 Down 17 N/A 26 Registered Devices: 20 of 46 Activation Status: 20 of 46 Decommissioned Devices: 1

DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION	ADDRESS	ASSET TAG
Device Name	Host Name	All	IP Address	Model	Location	Address	Asset T
Livewire Device	liveaction-1919	● Down	10.10.10.89	Edge	India	India	
Livewire Power Core	liveaction	● Up	10.8.102.12	3100			
LiveWireGRIDsmoke	ip-10-9-9-28	● Down	10.9.9.28	VIrtual	Giang		
		● N/A		Virtual			
		● N/A		Virtual			
		● N/A		PowerCore_cg			
dnChangedFromDe...	chris-virtual-deGrid-...	● Down	10.9.9.13	7525	cwh		
Capture Engine	liveaction	● Down	10.8.100.19	PowerCore			
		● N/A		Virtual			

- *Apply Template. See 'Grid Templates tab' on page 66*
- *Create Template. See 'Grid Templates tab' on page 66*
- *Additional Info*. See 'Additional Info' on page 55.
- *User Access*. See 'Additional Info' on page 55.
- *SNMP Credentials*. See 'SNMP Credentials' on page 56.
- *IDRAC Settings*. See 'IDRAC Settings' on page 57.
- *Backup Settings*. See 'Backup Settings' on page 59.
- *Restore Backup*. See 'Restore Backup' on page 61.
- *Revisions*. See 'Revisions' on page 62.
- *Upgrade Settings*. See 'Upgrade Settings' on page 62.
- *Change Password*. See 'Change Password' on page 63.
- *Power Actions*. See 'Power Actions' on page 64.
- *Activation and Reset*. See 'Activation and Reset' on page 65.

Search

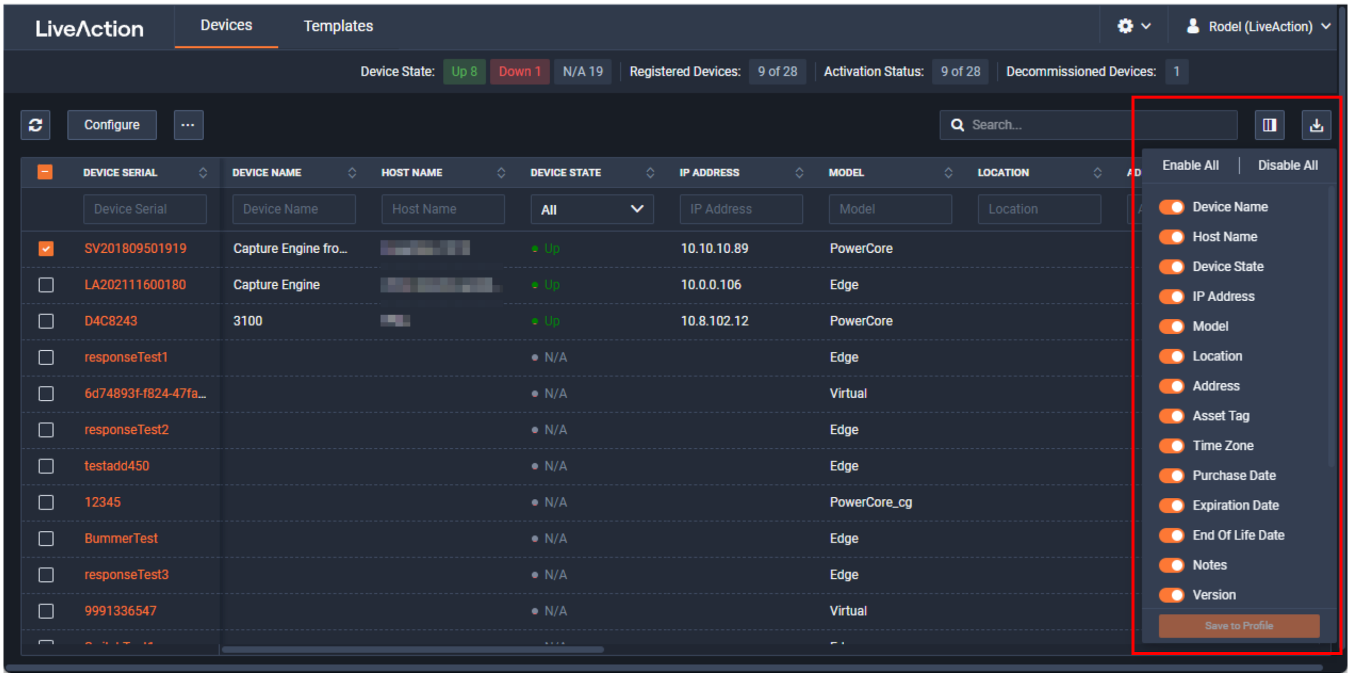
Use the *Search* field to locate a specific device in the list of devices. Simply enter a text string to display all appliances that match the text string.



Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

Display Columns

Click the **Display Columns** icon and then select the columns you want to display in the list of devices.

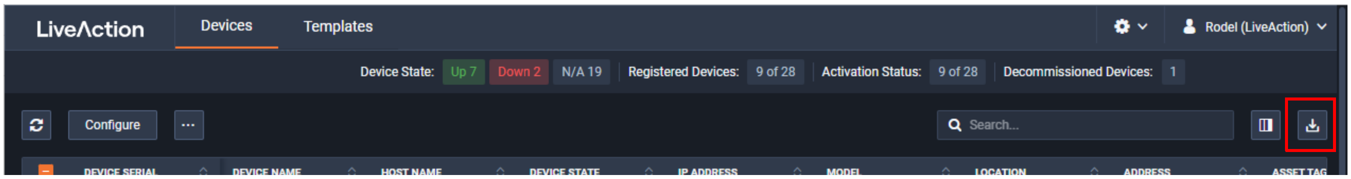


Device State: Up 8 Down 1 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

	DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION
	Device Serial	Device Name	Host Name	All	IP Address	Model	Location
☑	SV201809501919	Capture Engine fro...	[redacted]	● Up	10.10.10.89	PowerCore	
☐	LA202111600180	Capture Engine	[redacted]	● Up	10.0.0.106	Edge	
☐	D4C8243	3100	[redacted]	● Up	10.8.102.12	PowerCore	
☐	responseTest1			● N/A		Edge	
☐	6d74893f-f824-47fa...			● N/A		Virtual	
☐	responseTest2			● N/A		Edge	
☐	testadd450			● N/A		Edge	
☐	12345			● N/A		PowerCore_cg	
☐	BummerTest			● N/A		Edge	
☐	responseTest3			● N/A		Edge	
☐	9991336547			● N/A		Virtual	

Export to CSV

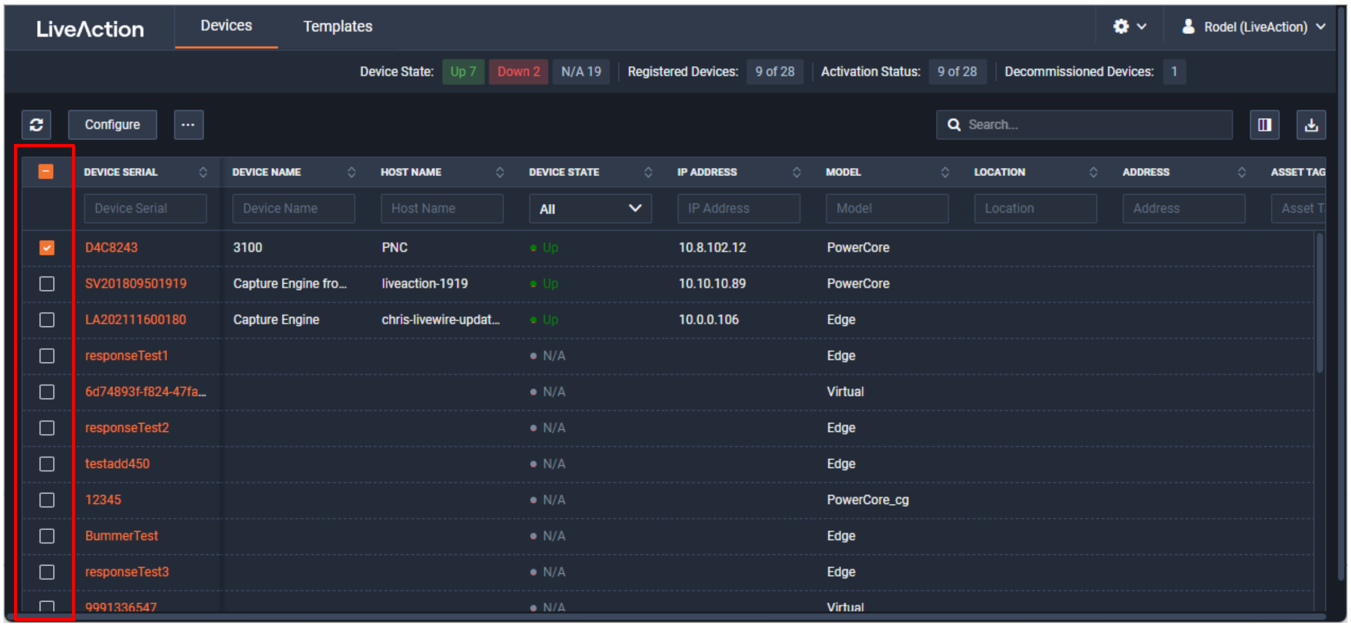
Click the **Export to CSV** icon (...) to export the list of devices to a *.csv* file.



Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

Check Box

To select a device in the list of devices, select the check box of the desired devices. Selecting the check box at the top of the column allows you to select or clear the check boxes of all devices in the list of devices.



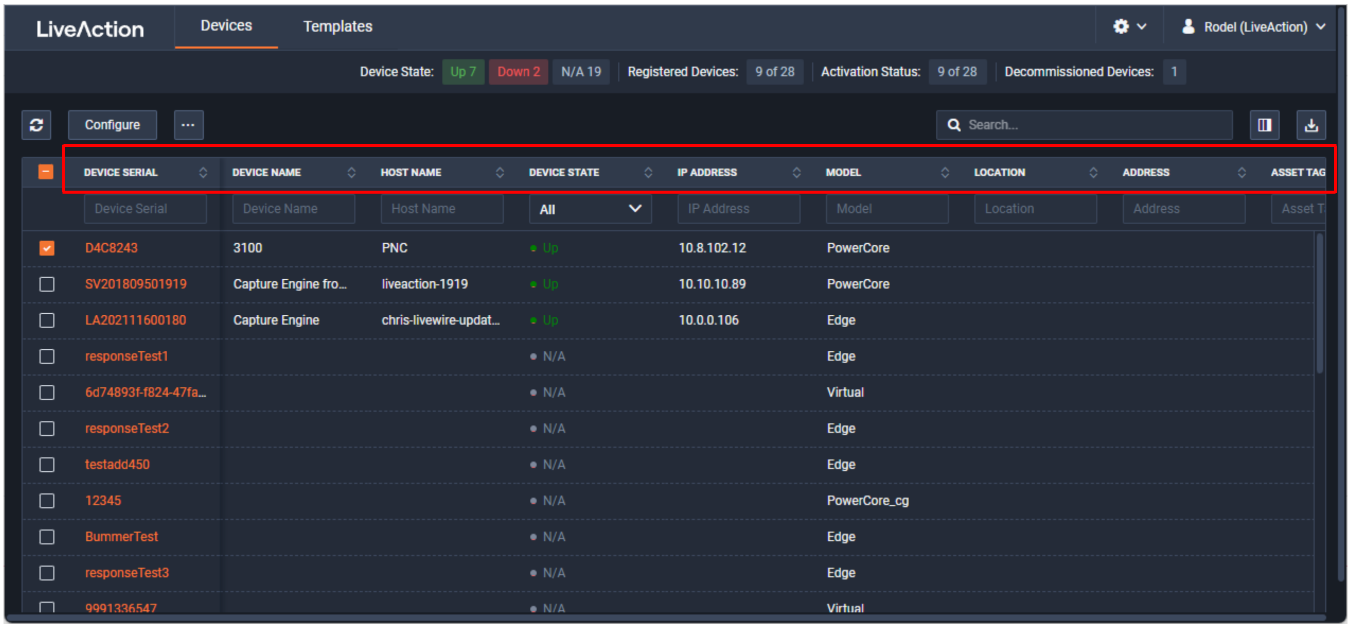
Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

☐	DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION	ADDRESS	ASSET TAG
	Device Serial	Device Name	Host Name	All	IP Address	Model	Location	Address	Asset T
☑	D4C8243	3100	PNC	● Up	10.8.102.12	PowerCore			
☐	SV201809501919	Capture Engine fro...	liveaction-1919	● Up	10.10.10.89	PowerCore			
☐	LA202111600180	Capture Engine	chris-livewire-updat...	● Up	10.0.0.106	Edge			
☐	responseTest1			● N/A		Edge			
☐	6d74893f-f824-47fa...			● N/A		Virtual			
☐	responseTest2			● N/A		Edge			
☐	testadd450			● N/A		Edge			
☐	12345			● N/A		PowerCore_cg			
☐	BummerTest			● N/A		Edge			
☐	responseTest3			● N/A		Edge			
☐	9991336547			● N/A		Virtual			

Devices column headings

Descriptions of the columns displayed in the list of devices are provided below.

> **Tip** Below each of the column headings is either a text box or list box that you can use to filter the devices displayed in the list of Devices. To filter using the text box, simply enter a text string to display the devices that match the text string. To filter using a list box, click the box and select an option to display the devices that match that option.


Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

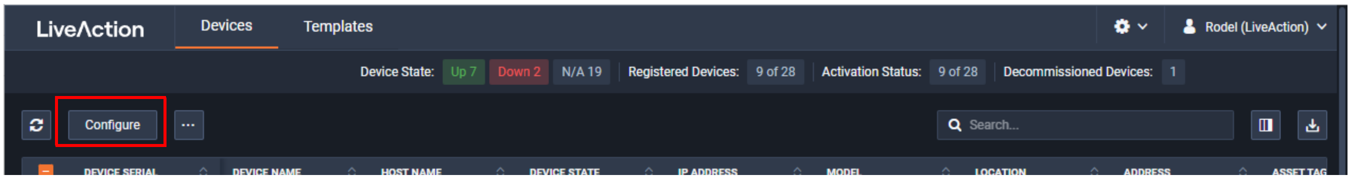
☐	DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION	ADDRESS	ASSET TAG
	Device Serial	Device Name	Host Name	All	IP Address	Model	Location	Address	Asset T
☑	D4C8243	3100	PNC	● Up	10.8.102.12	PowerCore			
☐	SV201809501919	Capture Engine fro...	liveaction-1919	● Up	10.10.10.89	PowerCore			
☐	LA202111600180	Capture Engine	chris-livewire-updat...	● Up	10.0.0.106	Edge			
☐	responseTest1			● N/A		Edge			
☐	6d74893f-f824-47fa...			● N/A		Virtual			
☐	responseTest2			● N/A		Edge			
☐	testadd450			● N/A		Edge			
☐	12345			● N/A		PowerCore_cg			
☐	BummerTest			● N/A		Edge			
☐	responseTest3			● N/A		Edge			
☐	9991336547			● N/A		Virtual			

- *Device Serial*: Displays the serial number of the device.
- *Device Name*: Displays the name of the device.
- *Host Name*: Displays the host name of the device used by DNS.
- *Device State*: Displays whether the device is *Up* or *Down*. A device is up if it has contacted Grid in the last 20 minutes.

- *IP Address*: Displays the IP address of the device. The *IP Address* value is a link which can be used to connect directly to Omnipeek running on the device. This makes it easy to use the Grid as a launch pad to access all of the devices being managed. It can also be used to discover the *IP Address* in the case where the device is set to DHCP, or for some other reason the *IP Address* is not known. The *IP Address* is provided by the device every time the device connects back to the portal, which by default is every 10 minutes. This way, if the *IP Address* of the device changes, the *IP Address* value displayed in Grid will reflect that.
- *Model*: Displays the model of the device (*e.g., Edge*, Core, PowerCore, or *Virtual*).
- *Location*: Displays the location of the device.
- *Address*: Displays the address of the device. Typically, this is the mailing address where the device is located.
- *Asset Tag*: Displays the asset tag of the device.
- *Time Zone*: Displays the time zone of the device.
- *Purchase Date*: Displays the purchase date of the device.
- *Expiration Date*: Displays the date that the maintenance on the device will expire. Once the expiration date has passed, you can still access Grid and use it to manage most of the device configuration; however, until the maintenance is renewed, the device cannot be upgraded to a newer version. As LiveAction releases new versions a few times a year with significant improvements, we recommend keeping the devices up to date with the latest releases of the software.
- *End Of Life Date*: Displays the date for when the device should be replaced.
- *Notes*: Displays any notes entered for the device.
- *Version*: Displays the version number of the software installed on the device.
- *Engine Type*: Displays the type of device, which can be *LiveWire*, *LiveCapture*, or *LiveWire Virtual*.
- *User Count*: Displays the number of secondary users that have access to the device.
- *Scheduled Action(s)*: Displays any 'Actions' scheduled for the device.
- *Configuration Status*: Displays any status associated with configuration of the device.
- *Registered*: Displays a check mark if the device has been registered with LiveAction.
- *Activation Status*: Displays a check mark if the license on the device is valid and not expired.

Configuring a Device

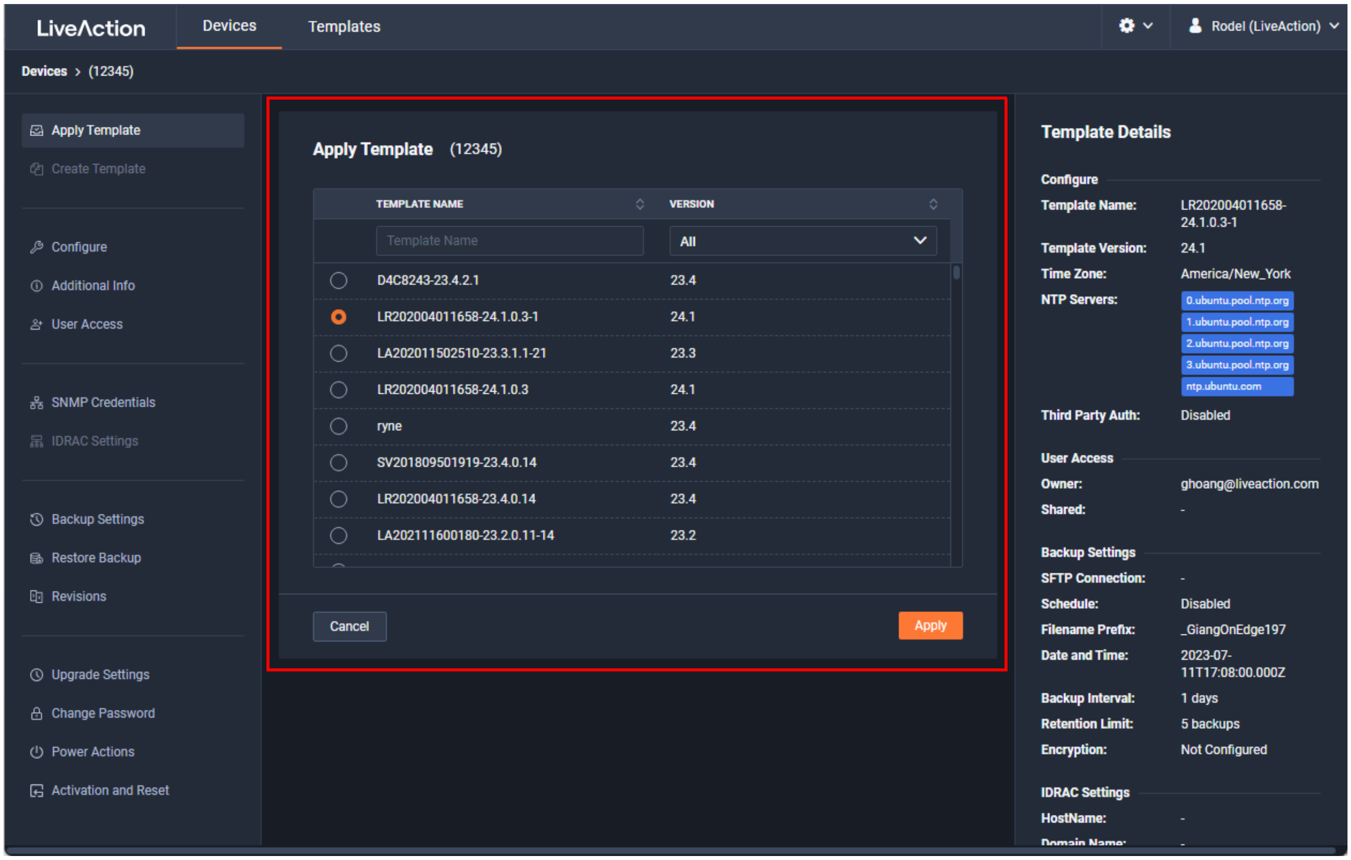
Click the *Configure* button to configure the selected devices. If multiple devices are selected, certain configuration options will not be available and greyed out; for example, the *Device Name*. The options to configure a device are available in the left-hand pane of the window. Each of the options are described below.



Device State: Up 7 Down 2 N/A 19 Registered Devices: 9 of 28 Activation Status: 9 of 28 Decommissioned Devices: 1

Apply Template

Apply Template lets you apply the settings from templates that have been saved to Grid.



Apply Template (12345)

	TEMPLATE NAME	VERSION
	Template Name	All
○	D4C8243-23.4.2.1	23.4
●	LR202004011658-24.1.0.3-1	24.1
○	LA202011502510-23.3.1.1-21	23.3
○	LR202004011658-24.1.0.3	24.1
○	ryne	23.4
○	SV201809501919-23.4.0.14	23.4
○	LR202004011658-23.4.0.14	23.4
○	LA202111600180-23.2.0.11-14	23.2

Template Details

Configure

Template Name:	LR202004011658-24.1.0.3-1
Template Version:	24.1
Time Zone:	America/New_York
NTP Servers:	0.ubuntu.pool.ntp.org 1.ubuntu.pool.ntp.org 2.ubuntu.pool.ntp.org 3.ubuntu.pool.ntp.org ntp.ubuntu.com
Third Party Auth:	Disabled

User Access

Owner:	ghoang@liveaction.com
Shared:	-

Backup Settings

SFTP Connection:	-
Schedule:	Disabled
Filename Prefix:	_GiangOnEdge197
Date and Time:	2023-07-11T17:08:00.000Z
Backup Interval:	1 days
Retention Limit:	5 backups
Encryption:	Not Configured

IDRAC Settings

HostName:	-
Domain Name:	-

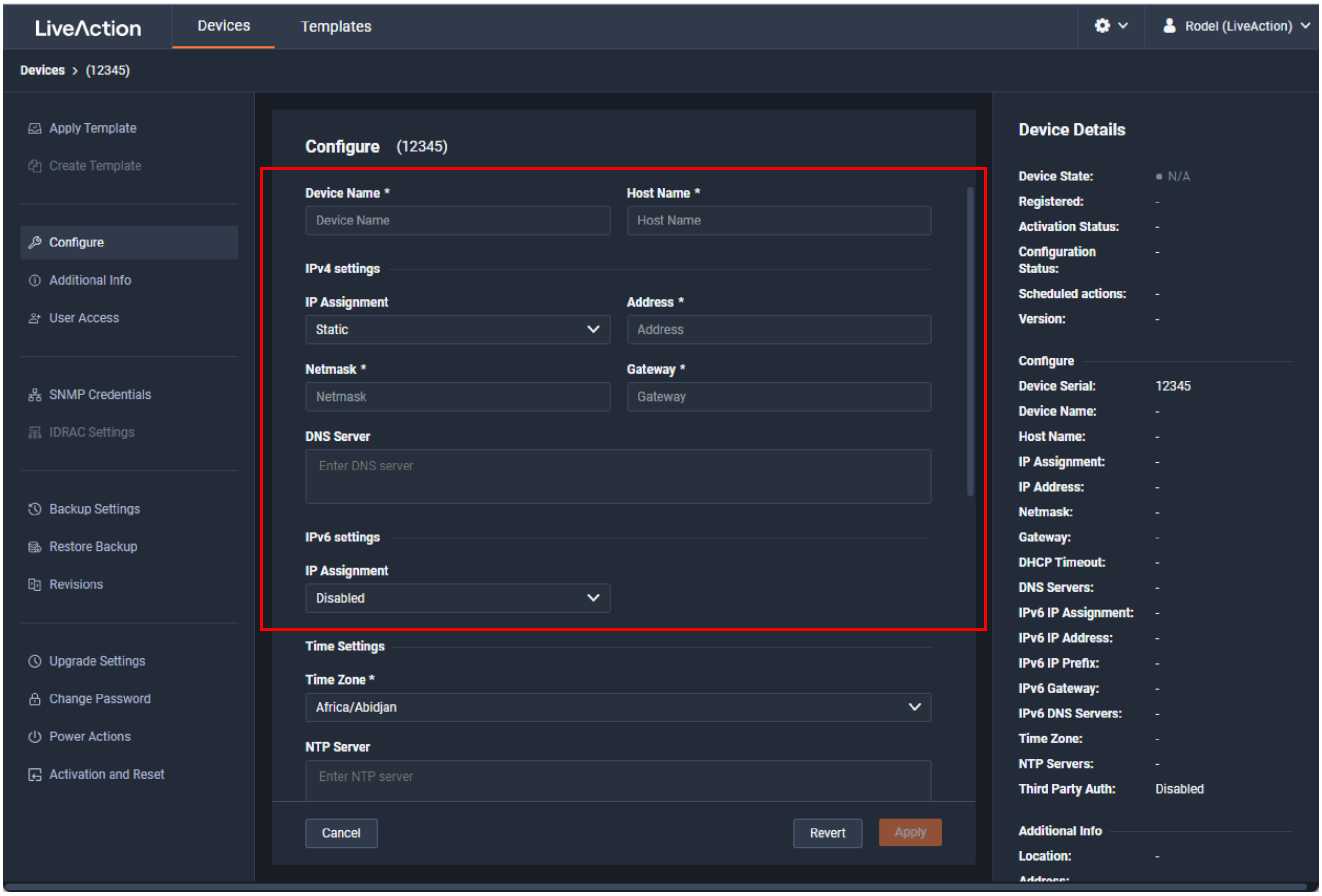
- *Template Name*: Displays the template name. Select the template to apply to the selected device.
- *Version*: Displays the version number of the template. You can select the template versions to display.
- *Apply*: Click to apply the template to the selected device.

Create Template

Select *Create Template* to create a template based on the settings of the selected device. The template is created immediately and is made available in the *Templates* tab.

Configure

Select *Configure* to view and modify settings of the selected devices.



IP Assignment: Static

IPv6 IP Assignment: Disabled

Time Zone *: Africa/Abidjan

Device State: N/A
Registered: -
Activation Status: -
Configuration Status: -
Scheduled actions: -
Version: -

Configure
Device Serial: 12345
Device Name: -
Host Name: -
IP Assignment: -
IP Address: -
Netmask: -
Gateway: -
DHCP Timeout: -
DNS Servers: -
IPv6 IP Assignment: -
IPv6 IP Address: -
IPv6 IP Prefix: -
IPv6 Gateway: -
IPv6 DNS Servers: -
Time Zone: -
NTP Servers: -
Third Party Auth: Disabled

Additional Info
Location: -
Address:

Settings

- *Device Name*: Displays the unique name given to the device. Type a new name to change the name.
- *Host Name*: Displays the host name of the device used by DNS. Type a new name to change the name.

IPv4 settings

- *IP Assignment*: Displays the current IP assignment for the device. You can select either *DHCP* or *Static*. If the IP Assignment is *DHCP*, then the IP assignment is configured automatically via the DHCP server. If the IP Assignment is *Static*, then the options below are available:

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.

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.

- *Address*: Displays the IP address assigned to the device. Type a new address to change the IP address.

  - *Netmask*: Displays the netmask address assigned to the device. A netmask address, combined with the IP address, defines the network associated with device. Type a new address to change the netmask address.
  - *Gateway*: Displays the gateway address, also known as 'default gateway,' assigned to the device. When the device 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. Type a new address to change the gateway address.
  - *DNS*: Enter the address of any DNS (Domain Name Server) servers to add to the configuration. 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. Multiple DNS name servers can be defined. You can also delete any defined DNS servers.

IPv6 settings

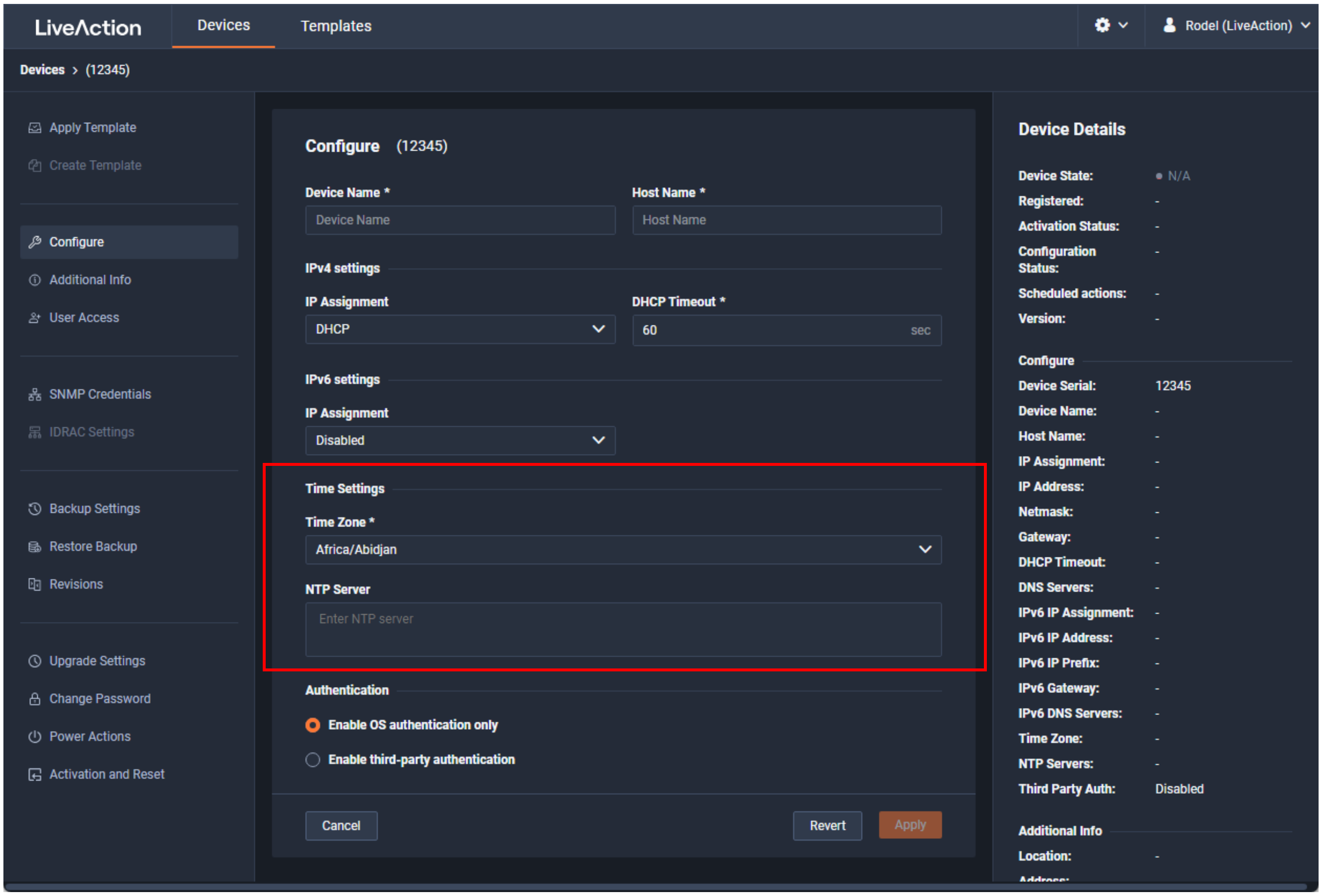
- *IP Assignment*: Displays the current IP assignment for the device. You can select either *DHCP* or *Static*. If the IP Assignment is *DHCP*, then the IP assignment is configured automatically via the DHCP server. If the IP Assignment is *Static*, then the options below are available:

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.

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.

  - *Address*: Displays the IP address assigned to the device. Type a new address to change the IP address.
  - *Netmask*: Displays the netmask address assigned to the device. A netmask address, combined with the IP address, defines the network associated with device. Type a new address to change the netmask address.
  - *Gateway*: Displays the gateway address, also known as 'default gateway,' assigned to the device. When the device 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. Type a new address to change the gateway address.
  - *DNS*: Enter the address of any DNS (Domain Name Server) servers to add to the configuration. 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. Multiple DNS name servers can be defined. You can also delete any defined DNS servers.
  - *Add Server*: Click to add the DNS server to the configuration.
  - *DNS Servers*: Displays the DNS servers added to the configuration.
  - *Edit DNS*: Click to edit or update the DNS server in the configuration.
  - *Delete DNS*: Click to delete the DNS server from the configuration.
- *DHCP Timeout*: Displays the amount of time (in seconds) the device will wait for a DHCP address.

Time Settings



Configure (12345)

Device Name * Device Name

Host Name * Host Name

IPv4 settings

IP Assignment: DHCP

DHCP Timeout *: 60 sec

IPv6 settings

IP Assignment: Disabled

Time Settings

Time Zone *: Africa/Abidjan

NTP Server: Enter NTP server

Authentication

● Enable OS authentication only

○ Enable third-party authentication

Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-

Configure

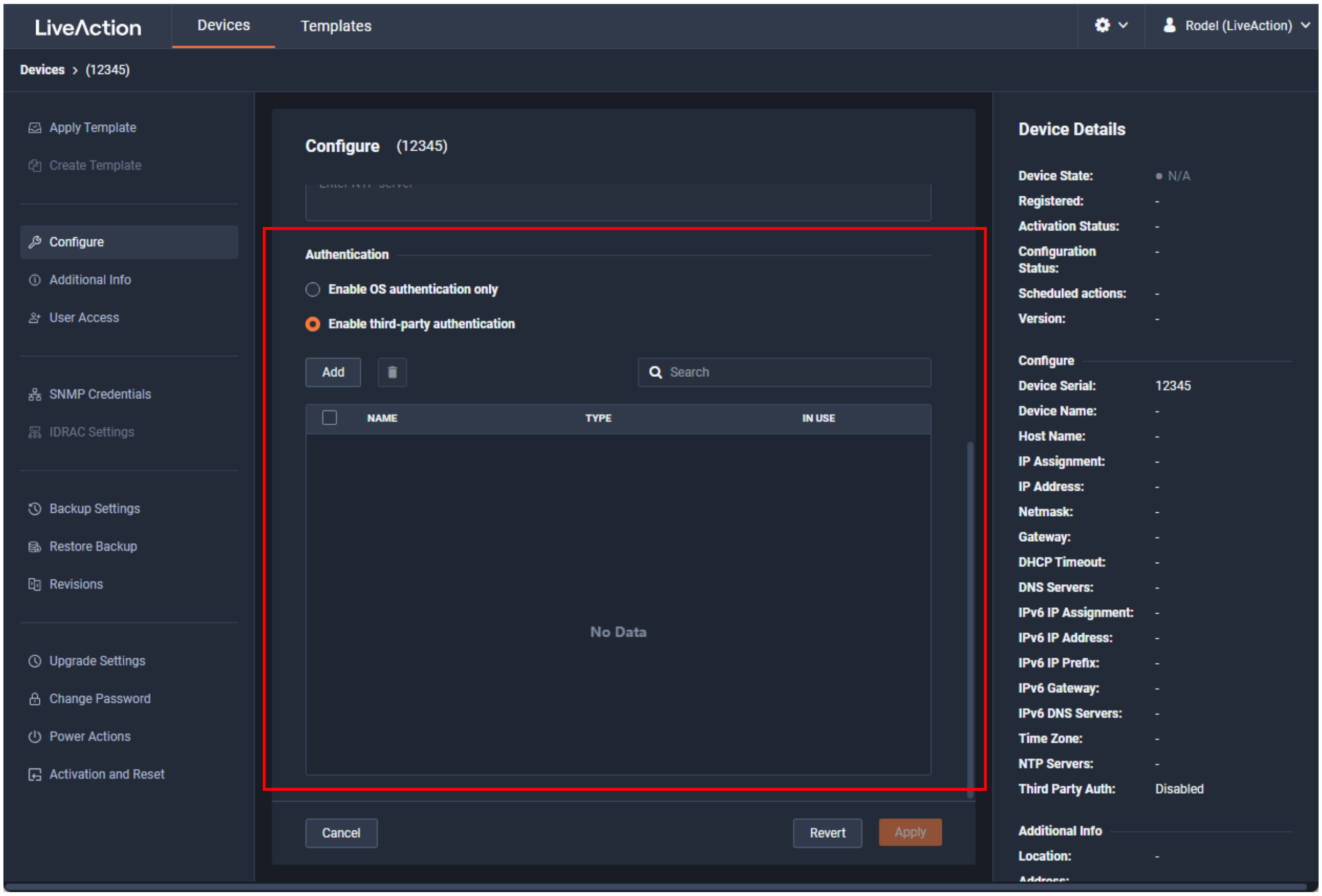
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled

Additional Info

Location:	-

- *Time Zone*: Displays the time zone of the device. Select a different time zone to change the time zone.
- *NTP Server*: Enter the address of any NTP servers to add to the configuration, and then click **Add Server**.
- *NTP Servers*: Displays the list of NTP servers added to *Time Settings*. To add an NTP server, enter the address of the server. Multiple NTP servers can be defined. You can also delete any defined NTP servers.

Authentication



Configure (12345)

Authentication

○ Enable OS authentication only

● Enable third-party authentication

☐	NAME	TYPE	IN USE

No Data

Device Details

Device State: N/A
Registered: -
Activation Status: -
Configuration Status: -
Scheduled actions: -
Version: -

Configure
Device Serial: 12345
Device Name: -
Host Name: -
IP Assignment: -
IP Address: -
Netmask: -
Gateway: -
DHCP Timeout: -
DNS Servers: -
IPv6 IP Assignment: -
IPv6 IP Address: -
IPv6 IP Prefix: -
IPv6 Gateway: -
IPv6 DNS Servers: -
Time Zone: -
NTP Servers: -
Third Party Auth: Disabled

Additional Info
Location: -

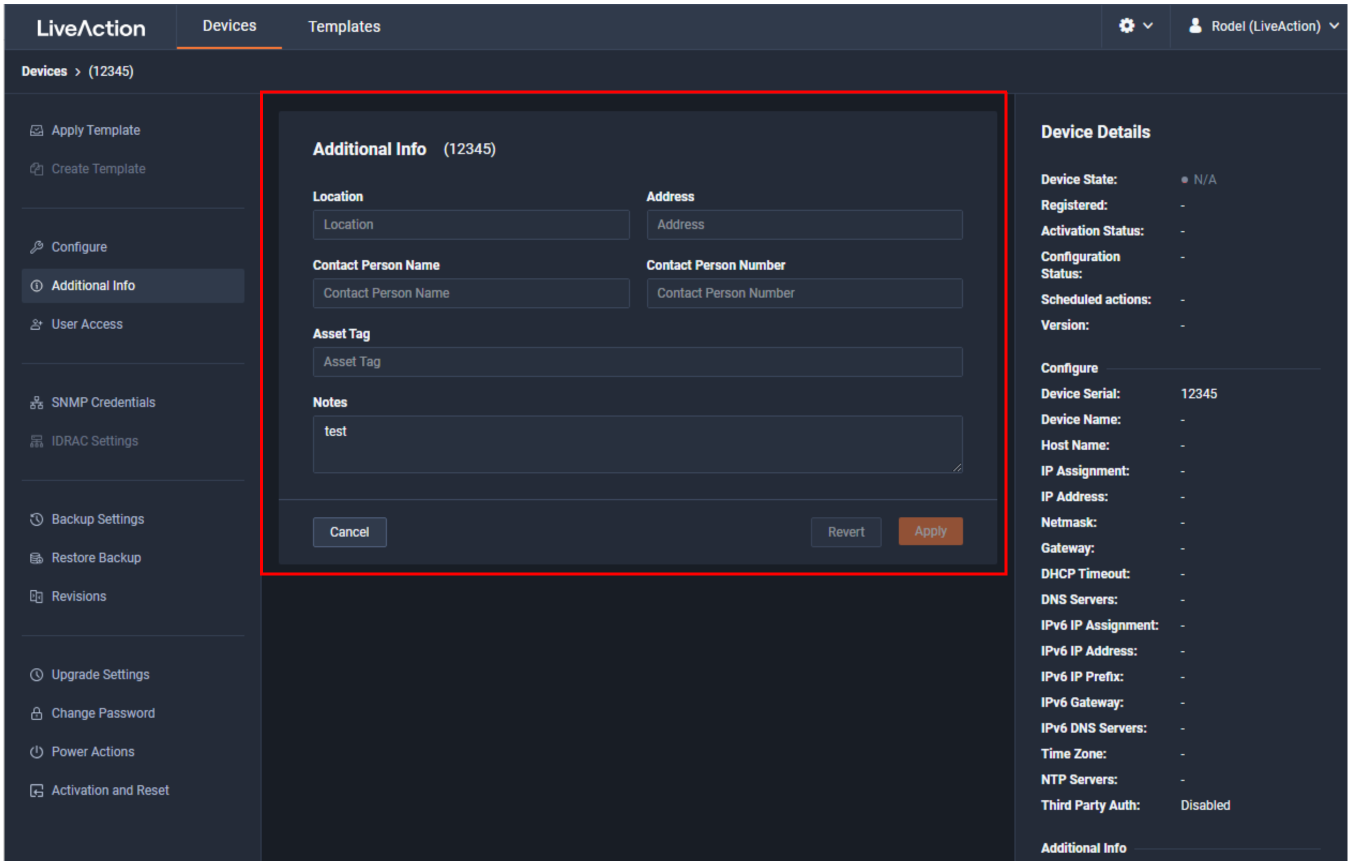
- *Enable OS authentication only*: Select this option to use the local OS authentication.
- *Enable third-party authentication*: Select this option to use Active Directory, TACACS+, or RADIUS authentication. If this option is selected, click **Add** to configure the new authentication setting. The available settings will change depending on which type of authentication is selected by the user:

Note These options will change depending on which type of authentication is selected by the user.

  - *Add*: Click to add a new authentication setting. You will need to configure the new authentication setting.
  - *Delete*: Click to delete the selected authentication setting.
  - *Search*: Enter the text string to search the list of authentication settings.
  - *Name*: Enter the name of the authentication setting.
  - *Type*: Select the type of authentication, which can be 'TACACS+.' 'RADIUS' or 'Active Directory.'
  - *Host*: Enter the host of the authentication setting.
  - *Port*: Enter the port of the authentication setting.
  - *Secret*: Enter the secret key of the authentication setting.
  - *Use Now*: Enable or disable whether or not the authentication setting is in use.

Additional Info

Select *Additional Info* to edit various settings of the selected devices.



Additional Info (12345)

Location	Location
Address	Address
Contact Person Name	Contact Person Name
Contact Person Number	Contact Person Number
Asset Tag	Asset Tag
Notes	test

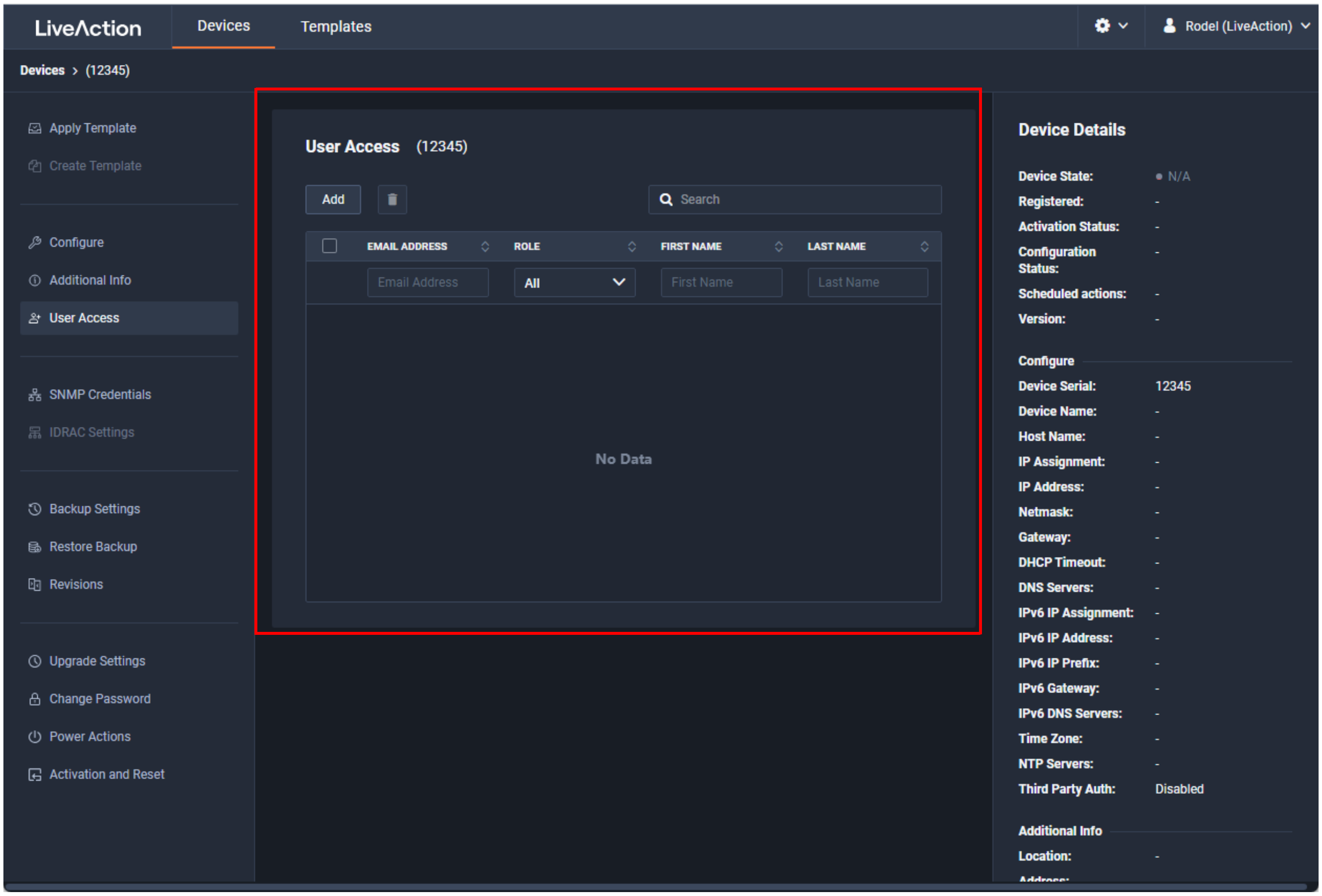
Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled
Additional Info	

- *Location*: Displays the general location of the device. Type a new location to change the location. We suggest entering the physical location of the device for the organization. For example, 'Office.'
- *Address*: Displays the mailing address of the device. For example, 123 Main St., New York, NY. Type a new address to change the address.
- *Contact Person Name*: Displays the contact person of the device. Type a new name to change the contact person.
- *Contact Person Number*: Displays the phone number of the contact person. Type a new number to change the phone number.
- *Asset Tag*: Displays the asset tag of the device. Type a new asset tag to change the asset tag.
- *Notes*: Displays any notes for the device. Type any new notes to update the notes.
- *Revert*: Click to clear the *Edit Additional Info* values.
- *Apply* Click to apply the additional info to the device.

User Access

Select *User Access* to add or remove authorized users for your organization that have access to the selected devices.



User Access (12345)

☐	EMAIL ADDRESS	ROLE	FIRST NAME	LAST NAME
	Email Address	All	First Name	Last Name

No Data

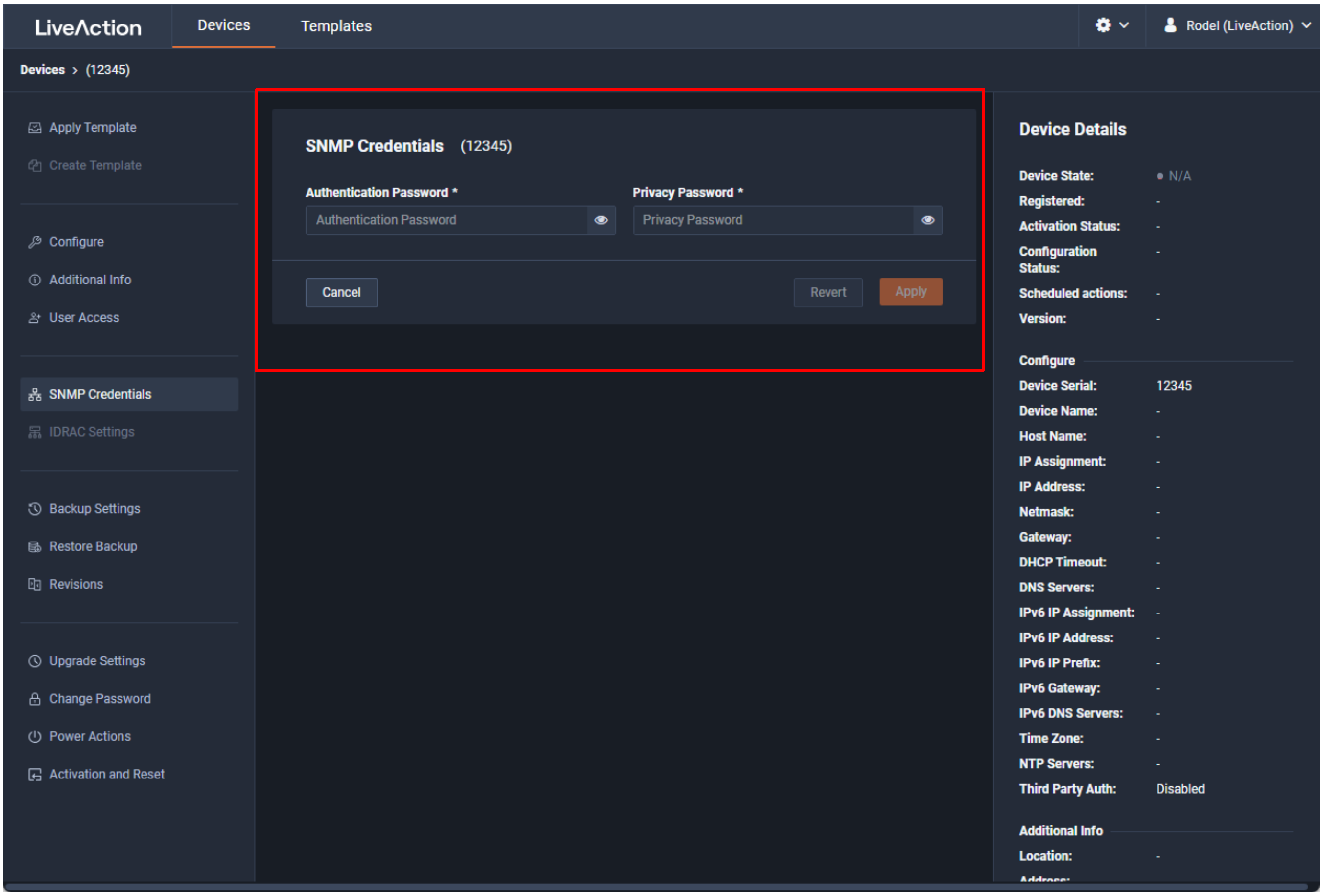
Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled
Additional Info	
Location:	-

- *Add*: Click to add an authorized user to have access to the device.
- *Delete*: Click to delete the selected user from list of users.
- *Search*: Use the *Search* field to locate a specific user in the list of users. Simply enter a text string to display all users that match the text string..
- *Email Address*: Displays the email address of the user.
- *Role*: Displays the role assigned to the user. A user can have the following roles.
  - *Admin*: Users in this role are able to view and modify/configure all devices and users that belong to the organization. Additionally they can add new users to the organization and are allowed to configure Single Sign On (SSO).
  - *Config*: Users in this role are able to view and configure any devices that have been shared to them by another user that has access. They cannot perform operations on user accounts or SSO.
  - *View*: Users in this role can only view devices that have been assigned to them and are not able to effect any changes within the system.
- *First Name*: Displays the first name of the user.
- *Last Name*: Displays the last name of the user.

SNMP Credentials

Select *SNMP Credentials* to configure the SNMP *Authentication Password* and *Privacy Password* for the selected devices.



SNMP Credentials (12345)

Authentication Password *: Authentication Password

Privacy Password *: Privacy Password

Device Details

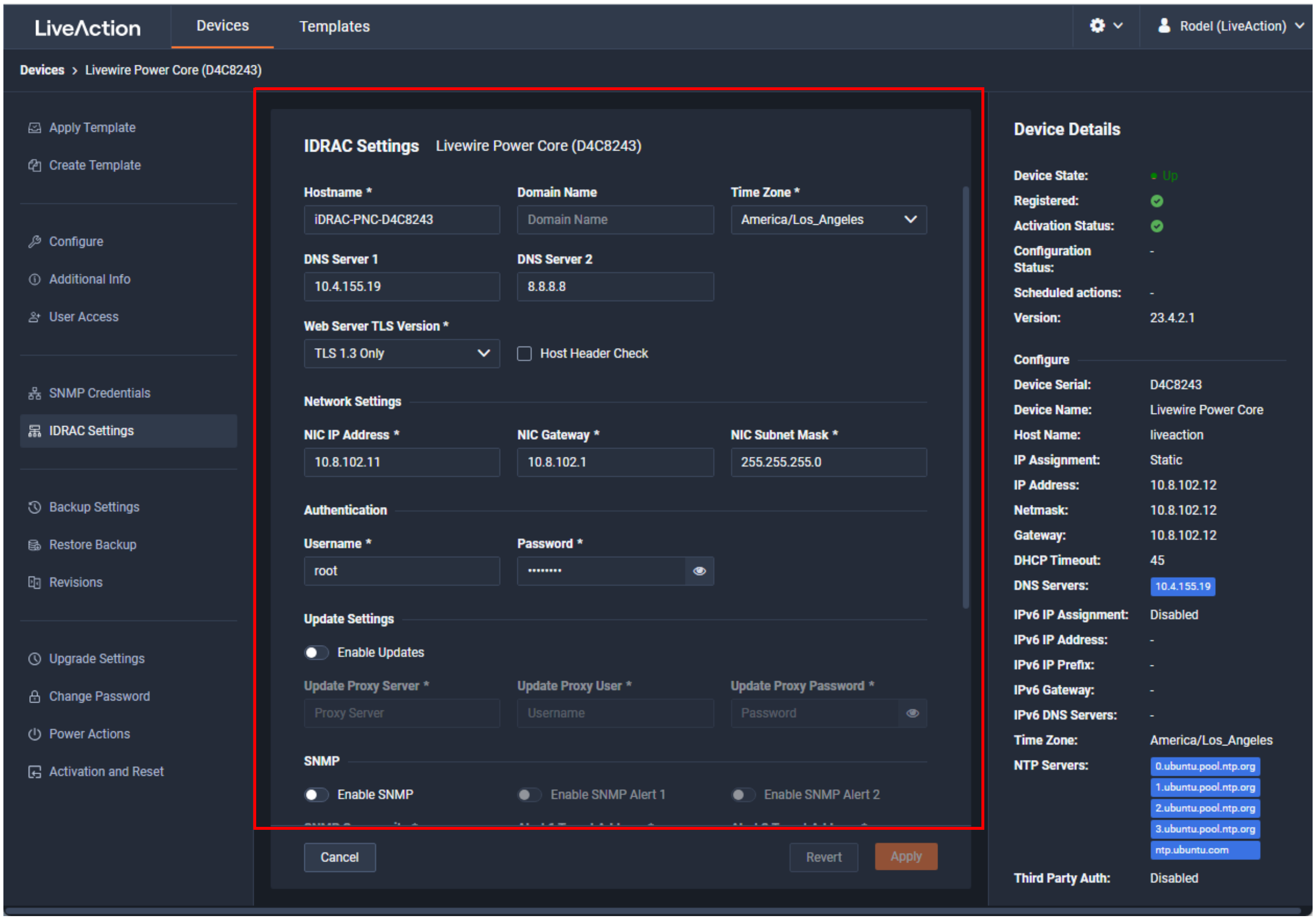
Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled
Additional Info	
Location:	-
Address:	

- *Authentication Password*: Type a new *Authentication Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 96.
- *Privacy Password*: Type a new *Privacy Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 96.
- *Revert*: Click to clear the *Edit Additional Info* values.
- *Apply* Click to apply the SNMP credentials to the device.

IDRAC Settings

Select the *iDRAC Settings* to configure various options for LiveWire that would normally be configured by using the iDRAC utility on LiveWire. See also 'Integrated Remote Access Controller (iDRAC)' on page 81.

Note Only selected options available from the iDRAC utility are available and configurable below.



IDRAC Settings Livewire Power Core (D4C8243)

Hostname *: iDRAC-PNC-D4C8243
Domain Name: Domain Name
Time Zone *: America/Los_Angeles
DNS Server 1: 10.4.155.19
DNS Server 2: 8.8.8.8
Web Server TLS Version *: TLS 1.3 Only
□ Host Header Check

Network Settings

NIC IP Address *: 10.8.102.11
NIC Gateway *: 10.8.102.1
NIC Subnet Mask *: 255.255.255.0

Authentication

Username *: root
Password *: ••••••••

Update Settings

○ Enable Updates
Update Proxy Server *: Proxy Server
Update Proxy User *: Username
Update Proxy Password *: Password

SNMP

○ Enable SNMP
○ Enable SNMP Alert 1
○ Enable SNMP Alert 2

Device Details

Device State: ● Up
Registered: ✓
Activation Status: ✓
Configuration Status: -
Scheduled actions: -
Version: 23.4.2.1

Configure
Device Serial: D4C8243
Device Name: Livewire Power Core
Host Name: liveaction
IP Assignment: Static
IP Address: 10.8.102.12
Netmask: 10.8.102.12
Gateway: 10.8.102.12
DHCP Timeout: 45
DNS Servers: 10.4.155.19
IPv6 IP Assignment: Disabled
IPv6 IP Address: -
IPv6 IP Prefix: -
IPv6 Gateway: -
IPv6 DNS Servers: -
Time Zone: America/Los_Angeles
NTP Servers: 0.ubuntu.pool.ntp.org 1.ubuntu.pool.ntp.org 2.ubuntu.pool.ntp.org 3.ubuntu.pool.ntp.org ntp.ubuntu.com
Third Party Auth: Disabled

- *Hostname*: Displays the *Hostname* of the device. Type a new *Hostname* to change it.
- *Domain Name*: Displays the *Domain Name* of the device. Type a new *Domain Name* to change it.
- *Time Zone*: Displays the *Time Zone* of the device. Select a new *Time Zone* to change it.
- *DNS Server 1*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *DNS Server 2*: Displays the *DNS Server* used by the device. Enter a new *DNS Server* to change it.
- *Web Server TLS Version*: Displays the TLS protocol version support used by the device. You can select from the following: TLS 1.1 and Higher, TLS 1.2 Only, TLS 1.2 and Higher, and TLS 1.3
  - *Host Header Check*: Select to enable *Host Header Check* requests.

Network Settings

- *NIC IP Address*: Displays the static *NIC IP Address* of the device. Type a new *NIC IP Address* to change it.
- *NIC Gateway*: Displays the *NIC Gateway* of the device. Type a new *NIC Gateway* to change it.
- *NIC Subnet Mask*: Displays the *NIC Subnet Mask* of the device. Type a new *NIC Subnet Mask* to change it.

Authentication

- *Username*: Displays the *Username* of the device. Type a new *Username* to change it.
- *Password*: Configures the *Password* of the device. Type a new *Password* to change it.

Update Settings

- *Enable Updates*: Select to enable updates on the device. If enabled, you must configure the Update Proxy Server, Update Proxy User, and Update Proxy Password.
- *Update Proxy Server*: Displays the *Update Proxy Server* of the device. Type a new *Update Proxy Server* to change it.
- *Update Proxy User*: Displays the *Update Proxy User* of the device. Type a new *Update Proxy User* to change it.
- *Update Proxy Password*: Displays the *Update Proxy Password* of the device. Type a new *Update Proxy Password* to change it.

SNMP

- *Enable SNMP*: Select to enable the SNMP Agent on the iDRAC. If enabled, you must configure the *SNMP Community.*
  - *SNMP Community*: Configures the *SNMP Community* name used for SNMP Agents. Type a new *SNMP Community* name to change it
- *Enable SNMP Alert 1*: Select to enable the *SNMP Alert 1* on the iDRAC. If enabled, you must configure the *Alert 1 Target Address*.
  - *Alert 1 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.
- *Enable SNMP Alert 2*: Select to enable the *SNMP Alert 2* on the iDRAC. If enabled, you must configure the *Alert 2*. If enabled, you must configure the *Alert 2 Target Address*.
  - *Alert 2 Target Address*: Displays the IPv4, IPv6, FQDN address, or hostname of the target destination to receive alerts. Must be valid IPv4, IPv6, FQDN address, or hostname.

NTP

- *Enable NTP*: Select to enable an *NTP* server on the iDRAC. If enabled, you must configure the *NTP Server*.
  - *NTP Server*: Displays the name or IP address of the *NTP Server*. Type a new name or IP address to change it.

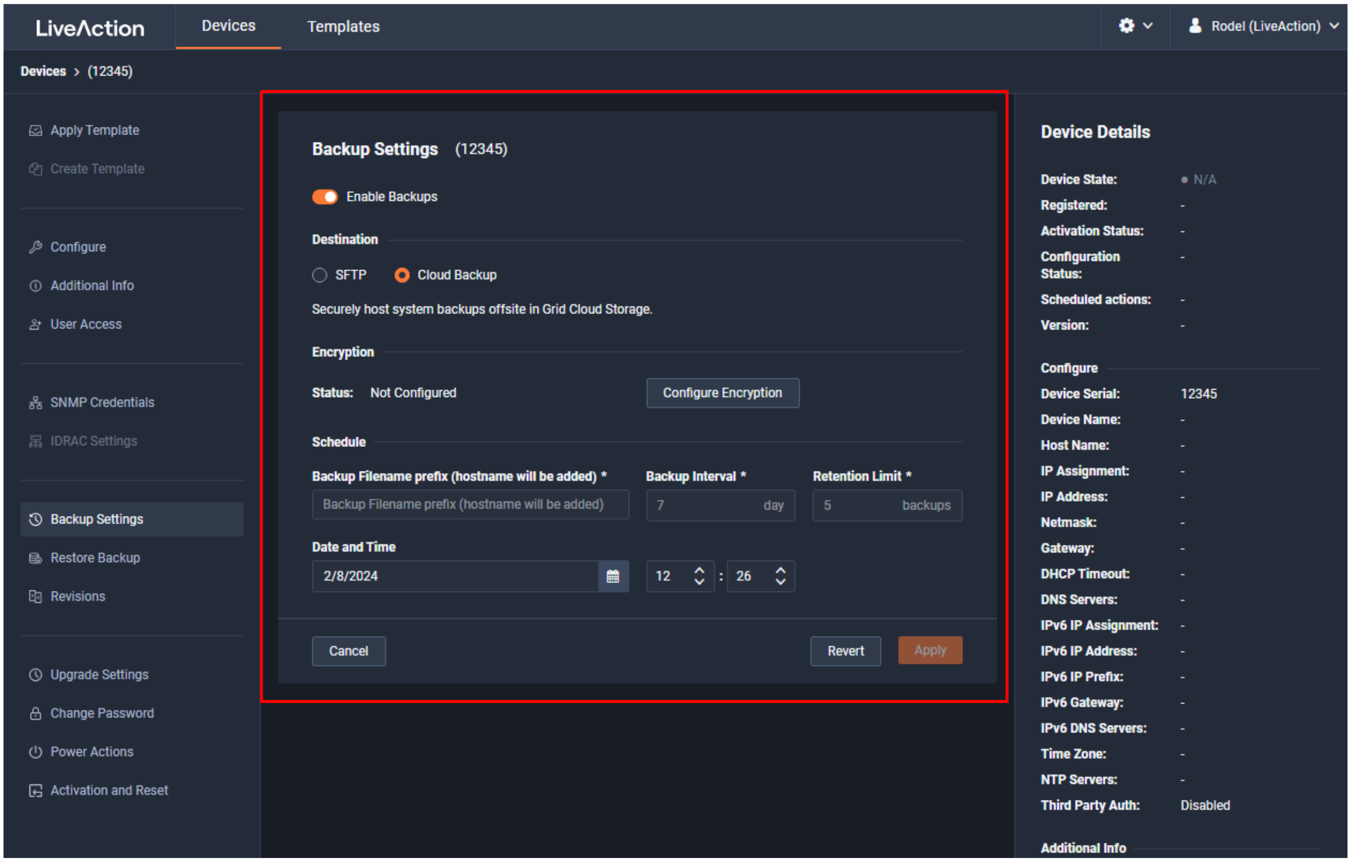
Event Filters

- *Alert*: Displays any iDRAC Event filters configured for the device.
- *Add*: Click to add a new Event filter configured in the text box. You must provide any parameters by defining what you want to be alerted to and how you want to be notified. You can configure as may event filter commands as you want. The general format of an alert category:

  idrac.alert.category.[subcategory].[severity]
- *Revert*: Click to clear the *iDRAC Settings* values.
- *Apply* Click to apply the *iDRAC Settings* to the device.

Backup Settings

Select *Backup Settings* to set up and configure a backup for the selected device. See 'Backup and restore' on page 77 for instructions on performing an actual backup.



Backup Settings (12345)

Enable Backups

Destination

○ SFTP ● Cloud Backup

Securely host system backups offsite in Grid Cloud Storage.

Encryption

Status: Not Configured

Schedule

Backup Filename prefix (hostname will be added) *	Backup Interval *	Retention Limit *
Backup Filename prefix (hostname will be added)	7 day	5 backups

Date and Time

2/8/2024 12 : 26

Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-

Configure

Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled

Additional Info

- *Enable Backups*: Select to enable or disable the backups configured below.

Destination

- *SFTP*: Select to configure the SFTP (Secure FTP) server for the backup, and then click *Configure SFTP*.
  - *Hostname*: 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.
- *Delete*: Click to delete the configured SFTP server for the backup.
- *Cloud Backup*: Select to securely host system backups offsite in Grid Cloud Storage.

Encryption

- *Status*: Displays whether or not encryption is configured for each scheduled backup.
- *Configure Encryption*: Click to configure security settings to encrypt each scheduled backup.
  - *Encrypt backups*: Select this option to encrypt each scheduled backup.
  - *Password*: Type the password for each scheduled backup.
  - *Repeat Password*: Tye the password again to verify the password.

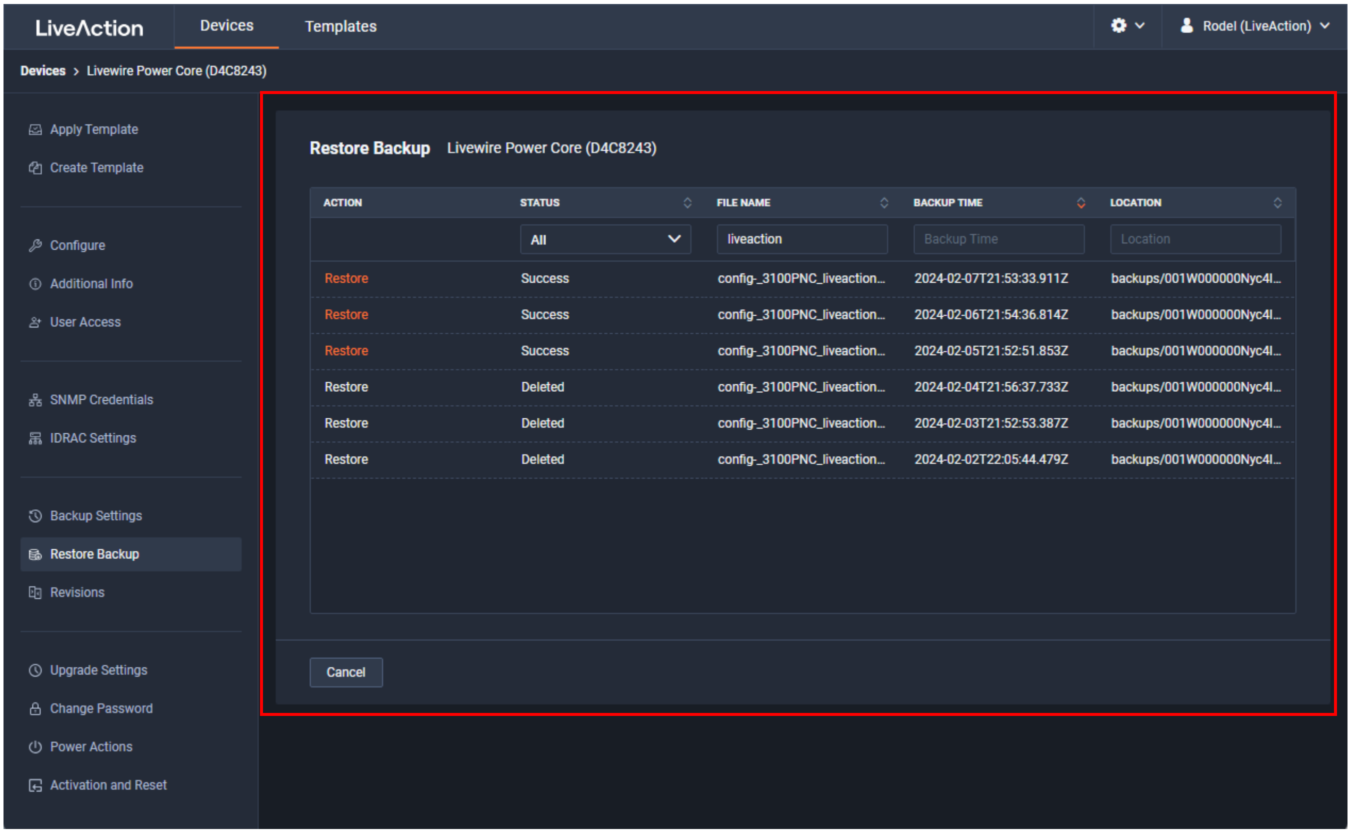
Schedule

- *Backup Filename prefix*: Type a prefix filename for the backup. Each scheduled backup that is created will append the prefix to the beginning of the backup filename.

- *Backup Interval*: Type the number of days between YADA.
- *Retention Limit*: Type the number backups to YADA.
- *GMT Date and Time*: Type or select the GMT date and time the backup will complete.

Restore Backup

Select *Restore Backup* to restore a backup from an earlier backup. See 'Backup and restore' on page 77 for instructions on performing an actual restore.



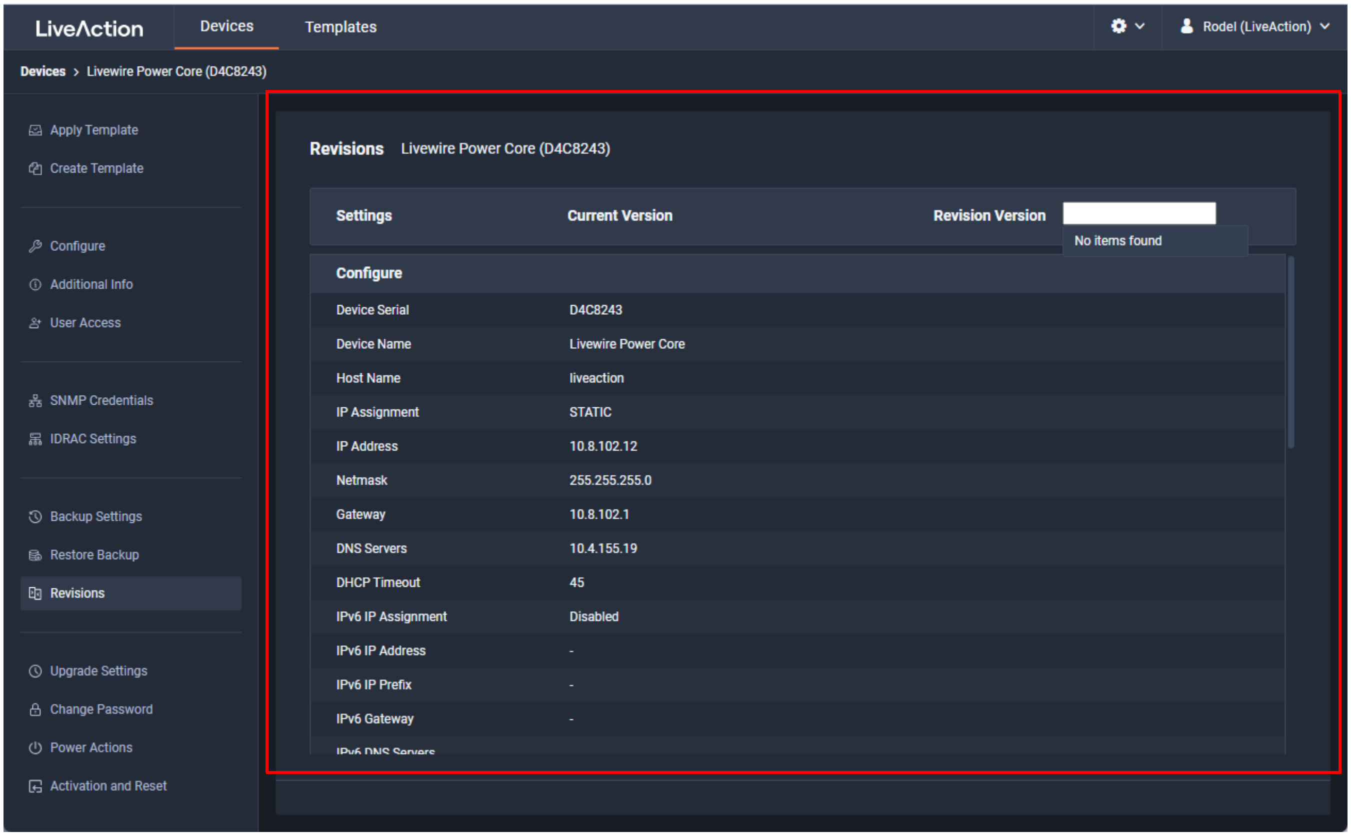
Restore Backup Livewire Power Core (D4C8243)

ACTION	STATUS	FILE NAME	BACKUP TIME	LOCATION
	All	liveaction	Backup Time	Location
Restore	Success	config-_3100PNC_liveaction...	2024-02-07T21:53:33.911Z	backups/001W000000Nyc4l...
Restore	Success	config-_3100PNC_liveaction...	2024-02-06T21:54:36.814Z	backups/001W000000Nyc4l...
Restore	Success	config-_3100PNC_liveaction...	2024-02-05T21:52:51.853Z	backups/001W000000Nyc4l...
Restore	Deleted	config-_3100PNC_liveaction...	2024-02-04T21:56:37.733Z	backups/001W000000Nyc4l...
Restore	Deleted	config-_3100PNC_liveaction...	2024-02-03T21:52:53.387Z	backups/001W000000Nyc4l...
Restore	Deleted	config-_3100PNC_liveaction...	2024-02-02T22:05:44.479Z	backups/001W000000Nyc4l...

- *Action*: Click **Restore** to restore a backup for the device. You will need to select to restore either *Application Settings* or *Application and System Settings*.
  - *Application Settings*: Select this option to restore all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins.
  - *Application and System Settings*: Select this option to restore all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins. Additionally, all system settings are restored and include all new and/or updated users, SNMP, NTP, network, time zone, and host customizations.
  - *Password*: Type the password of the backup you are restoring.
  - *Restore*: Click to perform the restore.
- *Status*: Displays the status of the backup.
- *File Name*: Displays the name of the backup.
- *Backup TIme*: Displays the date and time the backup was completed
- *Location*: Displays the location of the backup.

Revisions

Select *Revisions* to view the current settings of the device. You can also select a *Revision Version* to view settings previously applied to the device, and if necessary apply those previous settings to the device.



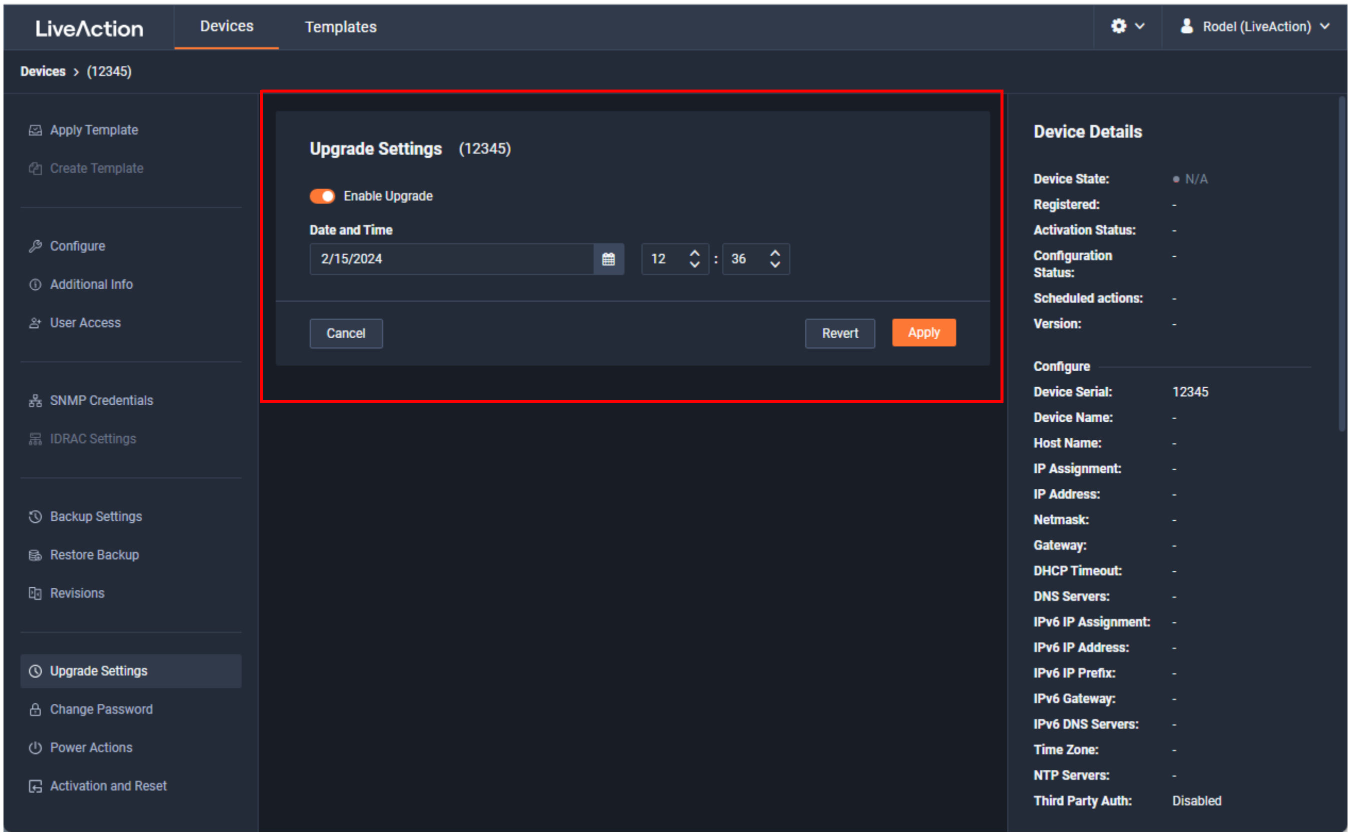
Revisions Livewire Power Core (D4C8243)

Settings	Current Version	Revision Version
Configure		
Device Serial	D4C8243	
Device Name	Livewire Power Core	
Host Name	liveaction	
IP Assignment	STATIC	
IP Address	10.8.102.12	
Netmask	255.255.255.0	
Gateway	10.8.102.1	
DNS Servers	10.4.155.19	
DHCP Timeout	45	
IPv6 IP Assignment	Disabled	
IPv6 IP Address	-	
IPv6 IP Prefix	-	
IPv6 Gateway	-	
IPv6 DNS Servers		

- *Settings*: Displays the settings that can be applied to a device.
- *Current Version*: Displays the settings currently applied to a device.
- *Revision Version*: Displays the settings previously applied to a device. You must select the *Revision Version* to display.
- *Apply*: Click to apply the settings from the *Revision Version* currently displayed above to a device.

Upgrade Settings

Select *Upgrade Settings* to upgrade the selected appliance remotely through Grid. The version that the appliance is upgraded to is the latest shipping version of the appliance. There is no capability to upgrade to a previously released version.



Upgrade Settings (12345)

Enable Upgrade

Date and Time: 2/15/2024 12 : 36

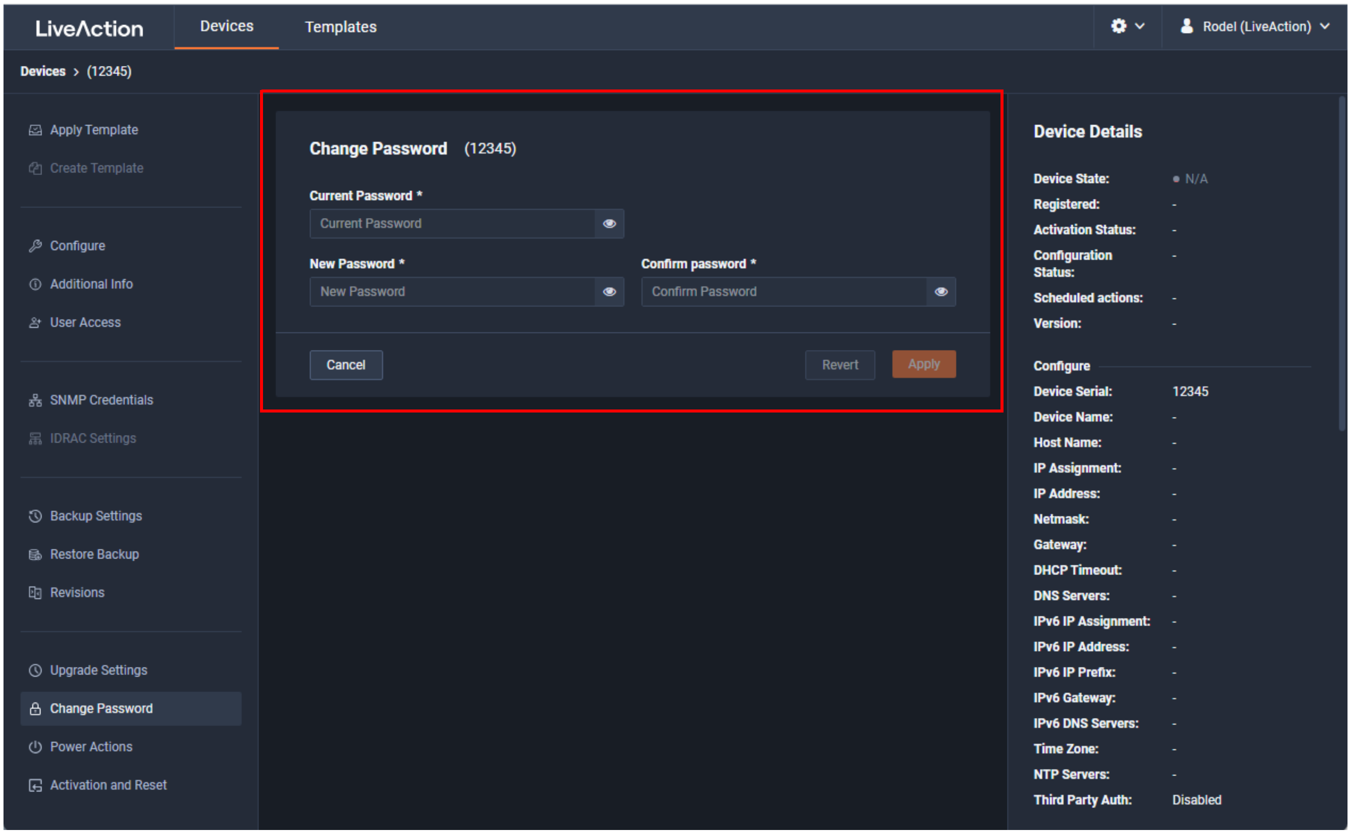
Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled

- *Enable Upgrade*: Select to enable or disable the upgrade on the selected devices.
- *GMT Date and Time*: Type or select the GMT date and time the upgrade should take place. Because all communications are initiated from the device once every ten minutes, the upgrade will happen as the result of the device communicating with the network, sometime on or after the selected time.
- *Revert*: Click to clear the *Upgrade Settings* values.
- *Apply* Click to apply the *Upgrade Settings* to the device.

Change Password

Select *Change Password* to change the password of the selected devices.



Change Password (12345)

Current Password * : Current Password

New Password * : New Password

Confirm password * : Confirm Password

Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-

Configure

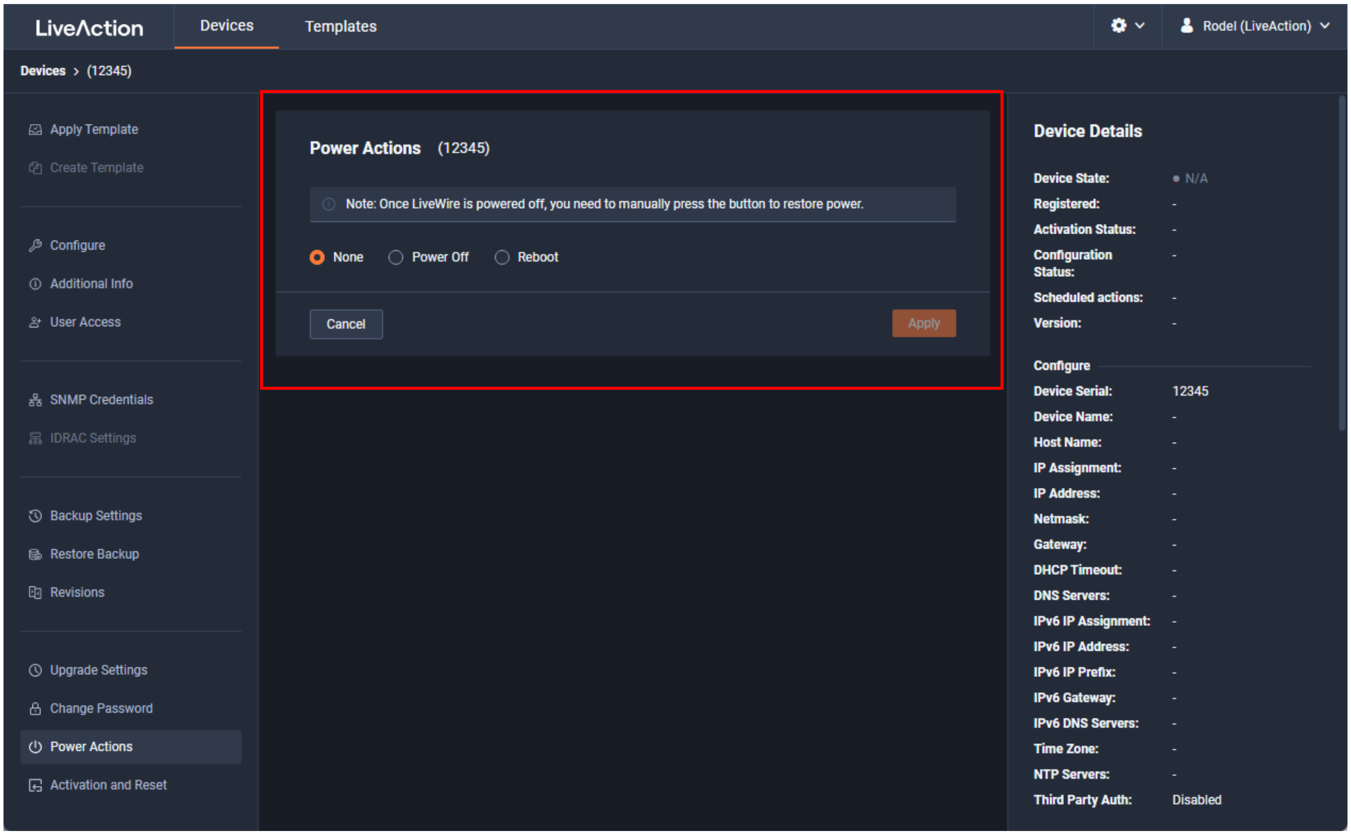
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled

- *Current Password*: Enter the current password.
- *New Password*: Enter the new password. 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 again.
- *Revert*: Click to clear the *Change Password* values.
- *Apply* Click to apply the *Change Password* to the device.

Power Actions

Select *Power Actions* to perform the actions below on the selected devices.



Power Actions (12345)

Note: Once LiveWire is powered off, you need to manually press the button to restore power.

● None ○ Power Off ○ Reboot

Device Details

Device State: N/A
Registered: -
Activation Status: -
Configuration Status: -
Scheduled actions: -
Version: -

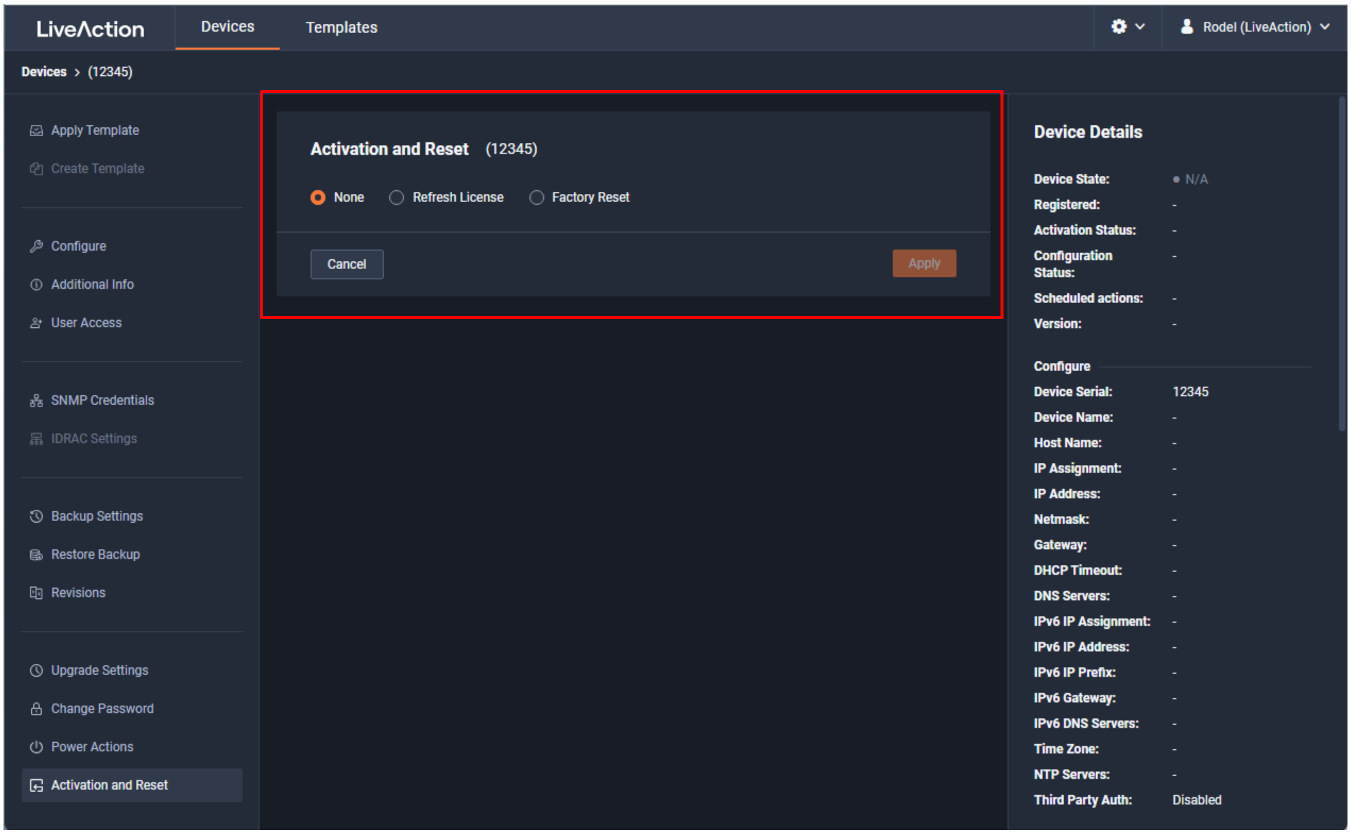
Configure

Device Serial: 12345
Device Name: -
Host Name: -
IP Assignment: -
IP Address: -
Netmask: -
Gateway: -
DHCP Timeout: -
DNS Servers: -
IPv6 IP Assignment: -
IPv6 IP Address: -
IPv6 IP Prefix: -
IPv6 Gateway: -
IPv6 DNS Servers: -
Time Zone: -
NTP Servers: -
Third Party Auth: Disabled

- *None*: Select to not perform an action on the selected device.
- *Power Off*: Select to power off the selected device. Once the device is powered off, you must manually press the power-on button on each of the devices to power them back on.
- *Reboot*: Select to reboot the selected appliances.
- *Factory Reset*: Select to reset the selected appliances to their factory default settings.

Activation and Reset

Select *Activation and Reset* to perform one of the three options below on the selected devices.



Activation and Reset (12345)

● None ○ Refresh License ○ Factory Reset

Cancel   Apply

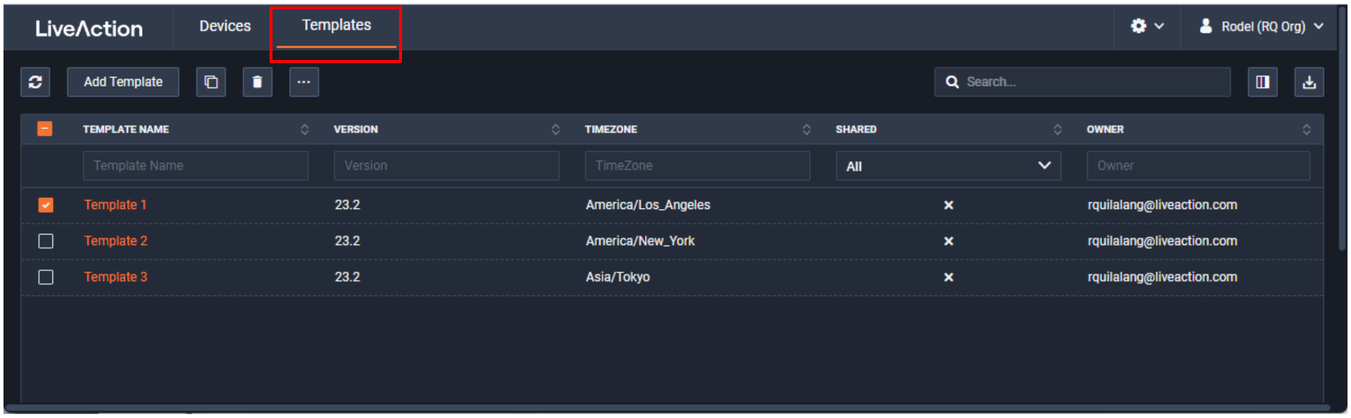
Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Assignment:	-
IP Address:	-
Netmask:	-
Gateway:	-
DHCP Timeout:	-
DNS Servers:	-
IPv6 IP Assignment:	-
IPv6 IP Address:	-
IPv6 IP Prefix:	-
IPv6 Gateway:	-
IPv6 DNS Servers:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled

- *None*: Select to not perform an action on the selected device.
- *Refresh License*: Select to refresh the license on the selected device.
- *Factory Reset*: Select to reset the selected devices to their factory default settings.

Grid Templates tab

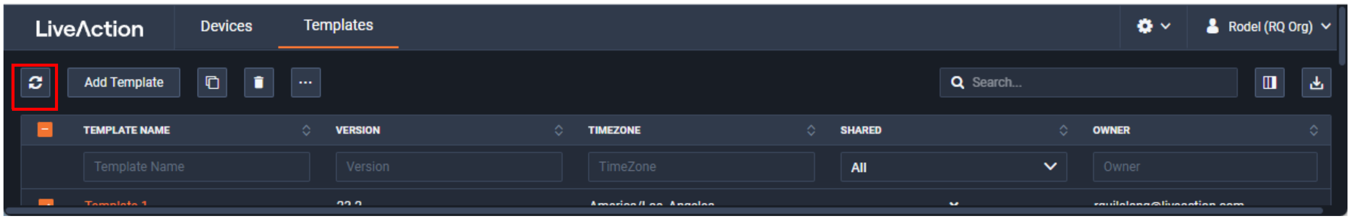
The Grid *Templates* tab displays the templates saved to your account. Templates allow you to configure settings independent of a particular device, and then apply the template, and thus the settings, to a device, or multiple devices in bulk at the same time. A description of each of the available options and settings in the *Templates* tab is provided below:



	TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
	Template Name	Version	TimeZone	All	Owner
☑	Template 1	23.2	America/Los_Angeles	✕	rquilalang@liveaction.com
□	Template 2	23.2	America/New_York	✕	rquilalang@liveaction.com
□	Template 3	23.2	Asia/Tokyo	✕	rquilalang@liveaction.com

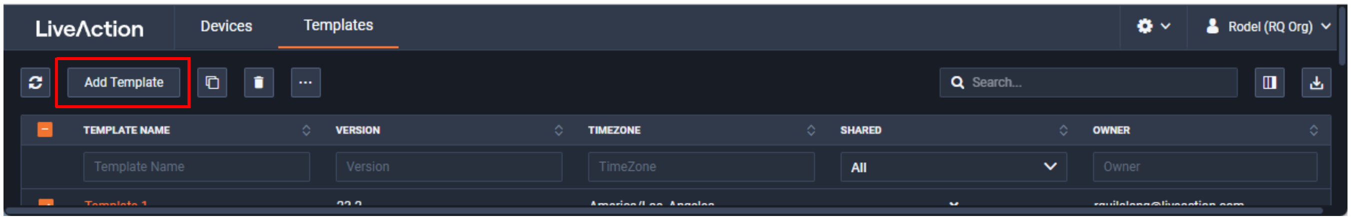
Refresh

Click *Refresh* to refresh the list of templates.



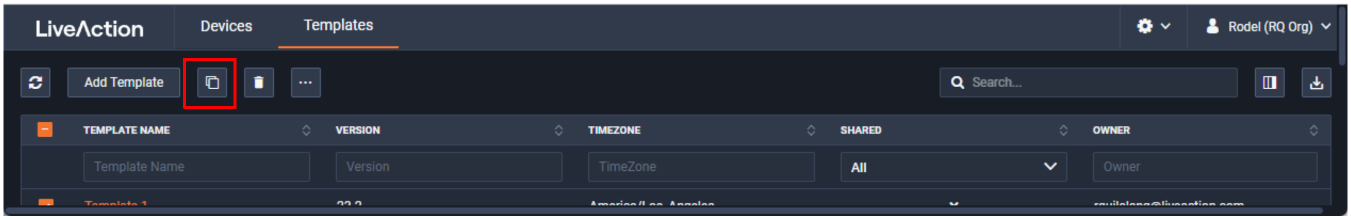
Add Template

Click *Add Template* to display the *Configure* settings to configure the new template. See 'Configure' on page 50 for descriptions of each of the settings.



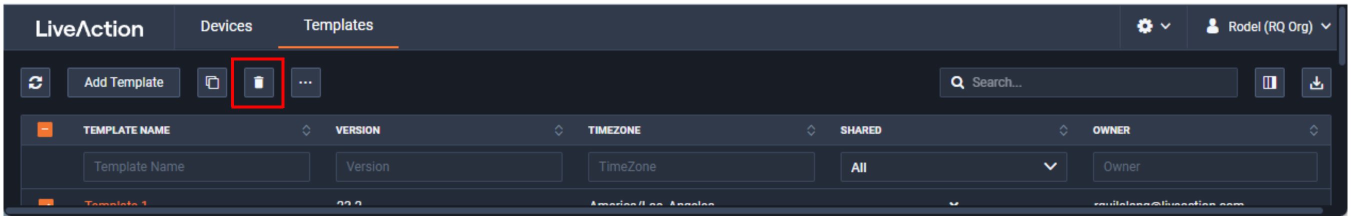
Duplicate Template

Click *Duplicate Template* to copy the selected template and add the copied template to the list of templates.



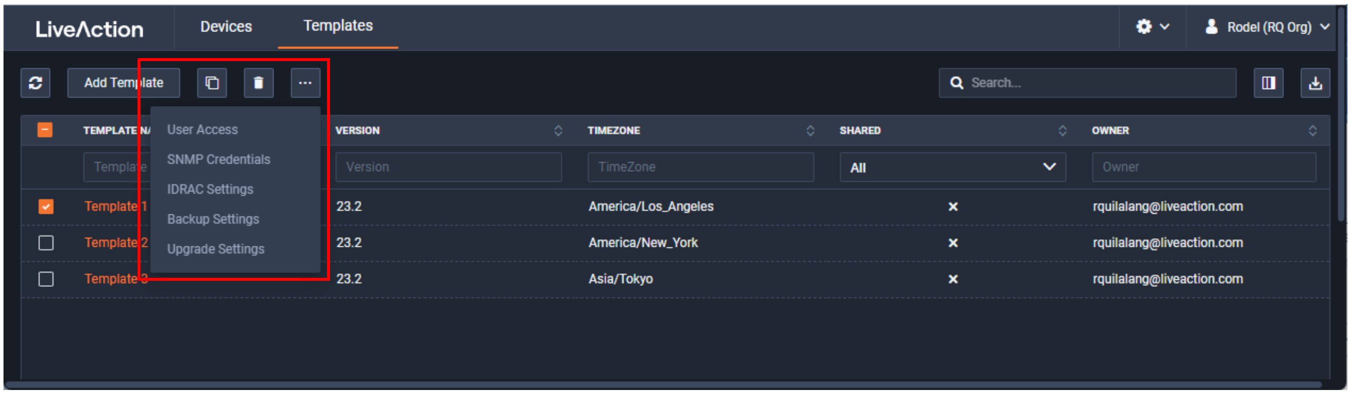
Delete Template

Click *Delete Template* to remove the selected template from the list of templates.



Elipsis (...)

Click the **Elipsis** (...) to view options for the selected template: The options available to configure templates are the same options used to configure a device. Follow the links below for descriptions of the settings.

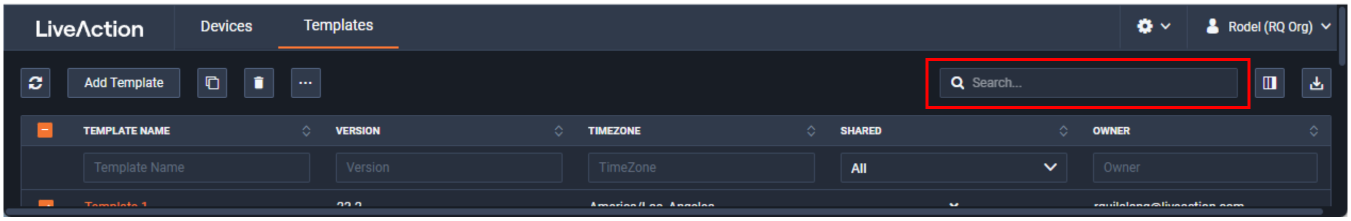


TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
Template	Version	TimeZone	All	Owner
☑ Template 1	23.2	America/Los_Angeles	×	rquilalang@liveaction.com
□ Template 2	23.2	America/New_York	×	rquilalang@liveaction.com
□ Template 3	23.2	Asia/Tokyo	×	rquilalang@liveaction.com

- *User Access*. See 'User Access' on page 55
- *SNMP Credentials*. See 'SNMP Credentials' on page 56
- *IDRAC Settings*. See 'IDRAC Settings' on page 57
- *Backup Settings*. See 'Backup Settings' on page 59
- *Upgrade Settings*. See 'Upgrade Settings' on page 62

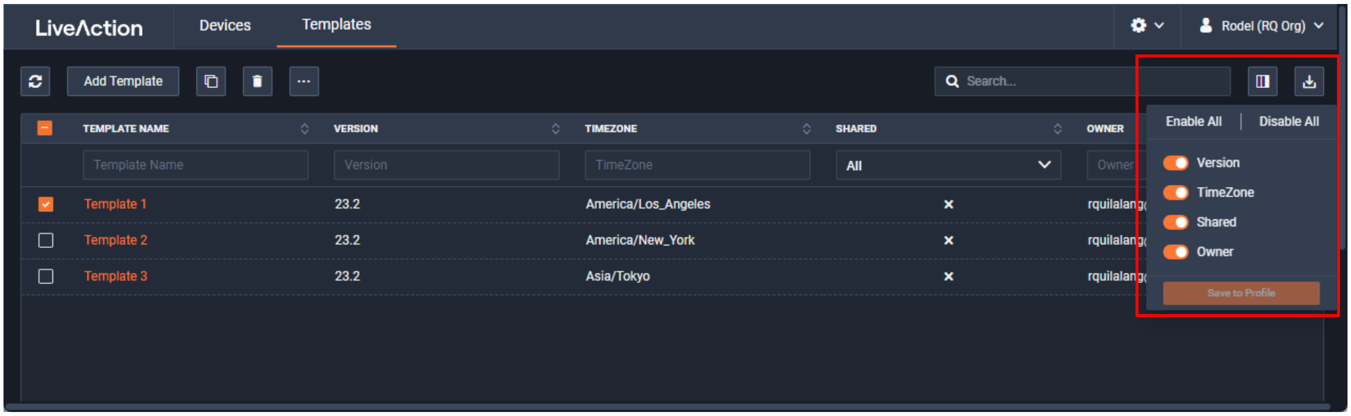
Search

Use the *Search* field to locate a specific template in the list of templates. Simply enter a text string to display all templates that match the text string.



Display Columns

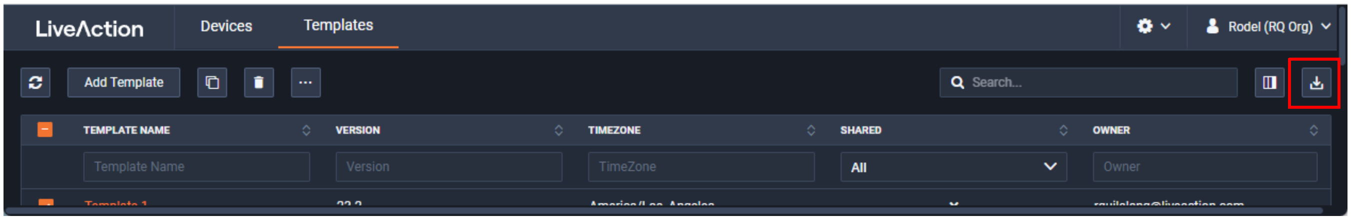
Click the *Display Columns* icon and then select the columns you want to display in the list of templates.



TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
Template Name	Version	TimeZone	All	Owner
☑ Template 1	23.2	America/Los_Angeles	×	rquilalang
□ Template 2	23.2	America/New_York	×	rquilalang
□ Template 3	23.2	Asia/Tokyo	×	rquilalang

Export to CSV

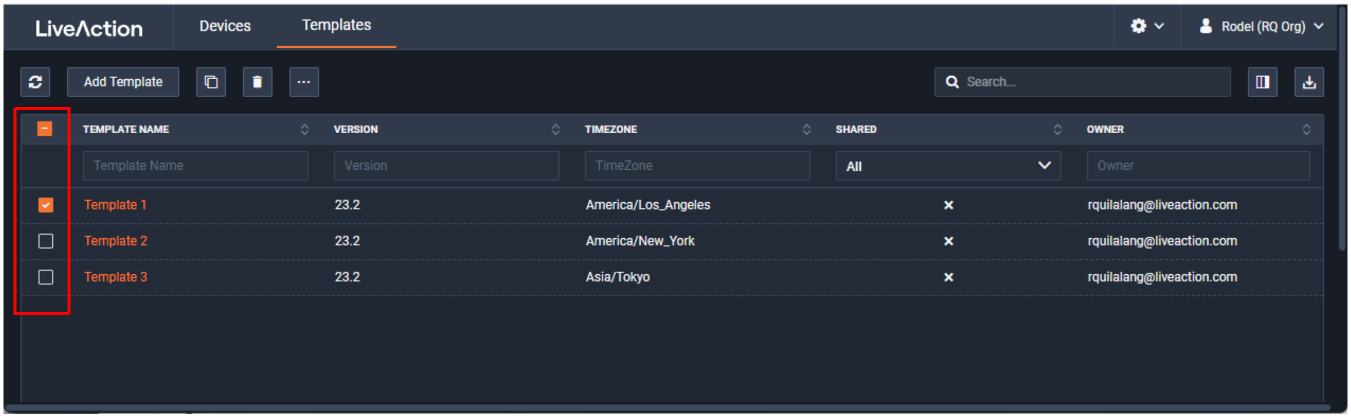
Click the *Export to CSV* icon (...) to export the list of templates to a *.csv* file.



TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
Template Name	Version	TimeZone	All	Owner

Check Box

To select a template in the list of templates, select the check box of the desired templates. Selecting the check box at the top of the column allows you to select or clear the check boxes of all templates in the list of templates.

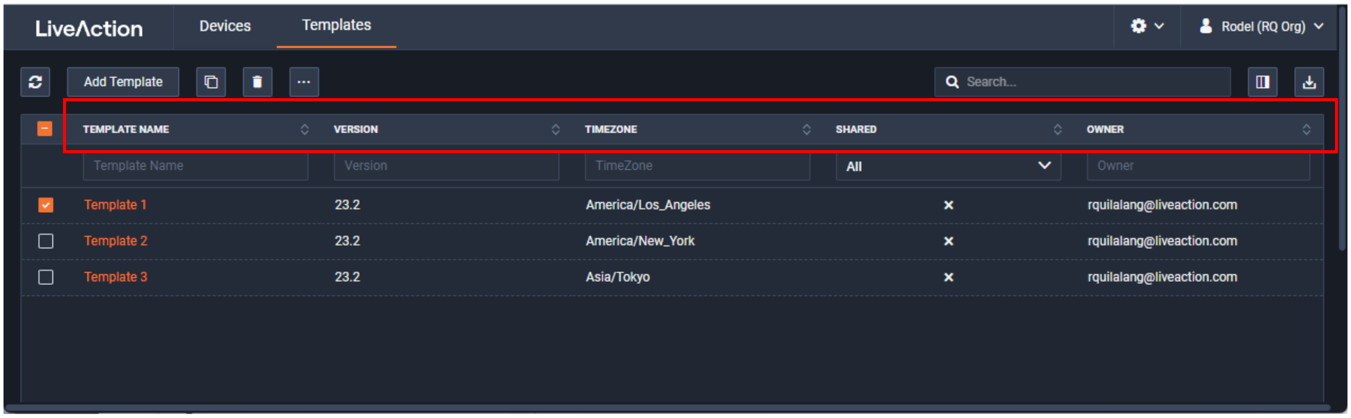


	TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
	Template Name	Version	TimeZone	All	Owner
☑	Template 1	23.2	America/Los_Angeles	×	rquilalang@liveaction.com
□	Template 2	23.2	America/New_York	×	rquilalang@liveaction.com
□	Template 3	23.2	Asia/Tokyo	×	rquilalang@liveaction.com

Devices column headings

Descriptions of the columns displayed in the list of templates are provided below.

Tip Below each of the column headings is either a text box or list box that you can use to filter the devices displayed in the list of Devices. To filter using the text box, simply enter a text string to display the devices that match the text string. To filter using a list box, click the box and select an option to display the devices that match that option.



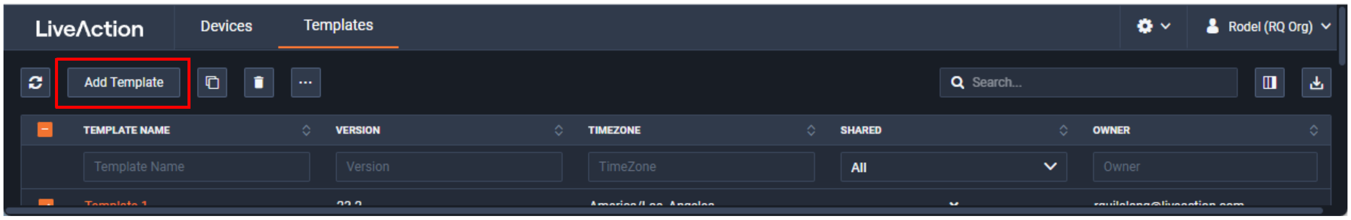
	TEMPLATE NAME	VERSION	TIMEZONE	SHARED	OWNER
	Template Name	Version	TimeZone	All	Owner
☑	Template 1	23.2	America/Los_Angeles	×	rquilalang@liveaction.com
□	Template 2	23.2	America/New_York	×	rquilalang@liveaction.com
□	Template 3	23.2	Asia/Tokyo	×	rquilalang@liveaction.com

- *Template Name*: Displays the name of the template. Click the name to display details about the template.
- *Version*: Displays the version number of the template.
- *Timezone*: Displays the time zone of the template.
- *Shared*: Displays the users that have been shared with the device. Shared users can fully configure a device from Grid.

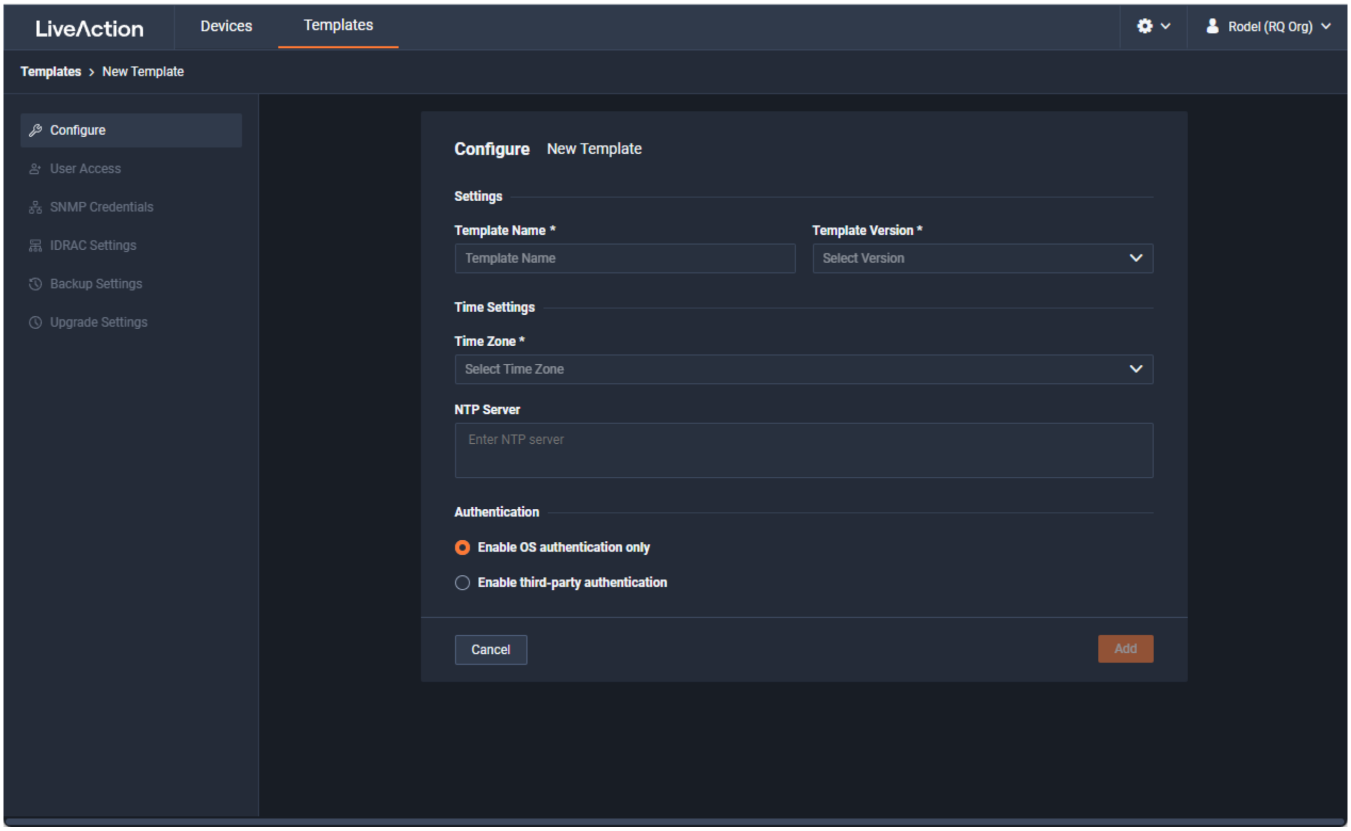
- *Owner*. Displays the owner of the device. There can only be one owner of the device.

Adding a template

Click *Add Template* to display the *Configure* settings to configure the new template.



With the exception of the *Template Name* and *Template Version* settings, the settings available to configure templates are the same settings used to configure a device. Follow the links below for descriptions of the settings.



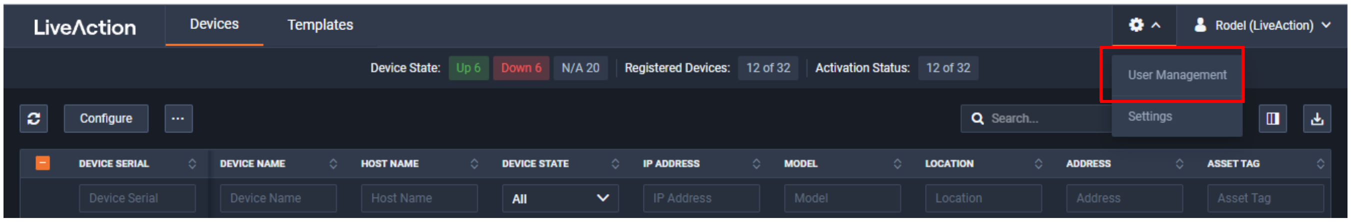
To add a new template:

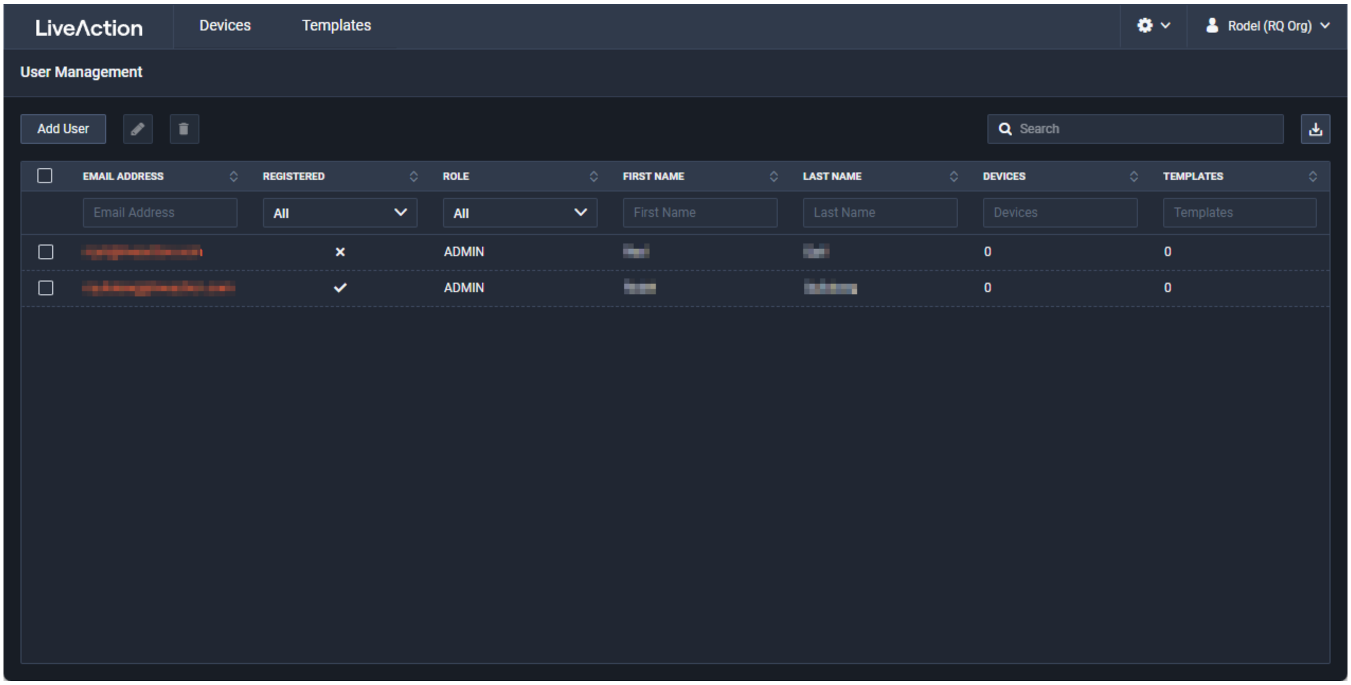
1. Click the **Add Template** button to display the *Configure* dialog.
2. Configure the new template:
   - *Template Name*: Type a name for the template.
   - *Template Version*: Click to select the version of the template you are configuring.
   - *Time Settings*: See 'Time Settings' on page 53.
   - *Authentication*: See 'Authentication' on page 54.
3. Click **Add**. The new template is created and you will now have access to the options below in the left-hand pane to further configure settings for the template.

- *Configure*: See 'Configure' on page 50.
- *User Access*: See 'User Access' on page 55.
- *SNMP Credentials*: See 'SNMP Credentials' on page 56.
- *iDRAC Settings*: See 'IDRAC Settings' on page 57.
- *Backup Settings*: See 'Backup Settings' on page 59.
- *Upgrade Settings*: See 'Upgrade Settings' on page 62.

User Management

Select *User Management* to add or remove authorized users for your organization that have access to Grid. For each user, you can specify the roles that define the user's level of access to Grid.

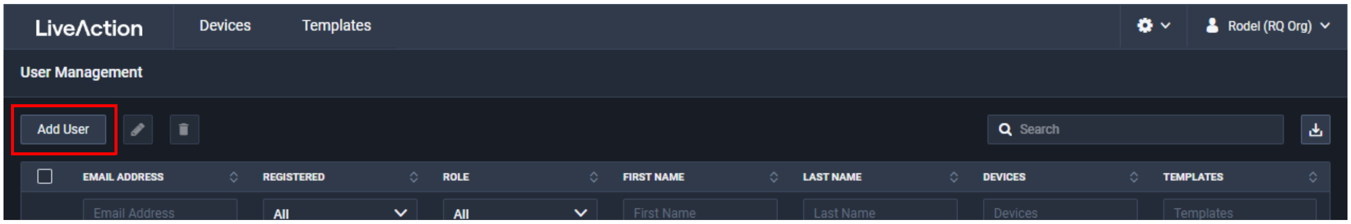




	EMAIL ADDRESS	REGISTERED	ROLE	FIRST NAME	LAST NAME	DEVICES	TEMPLATES
	Email Address	All	All	First Name	Last Name	Devices	Templates
□	[redacted]	×	ADMIN	[redacted]	[redacted]	0	0
□	[redacted]	✓	ADMIN	[redacted]	[redacted]	0	0

Add User

Click *Add User* to add an authorized user to have access to Grid.

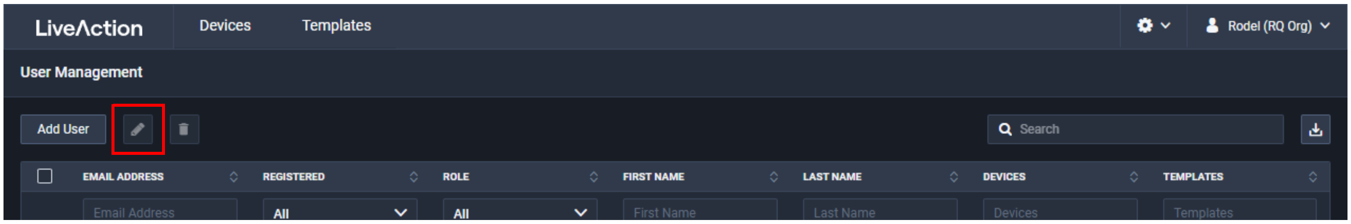


- *Email*: Type the email of the user.

- *Role*: Select the role assigned to the user. A user can be assigned the following roles:
    - *Admin*: Users in this role are able to view and modify/configure all devices and users that belong to the organization. Additionally they can add new users to the organization and are allowed to configure Single Sign On (SSO).
    - *Config*: Users in this role are able to view and configure any devices that have been shared to them by another user that has access. They cannot perform operations on user accounts or SSO.
    - *View*: Users in this role can only view devices that have been assigned to them and are not able to effect any changes within the system.
- *First Name*: Type of the first name of the user.
- *Last Name*: Type the last name of the user.

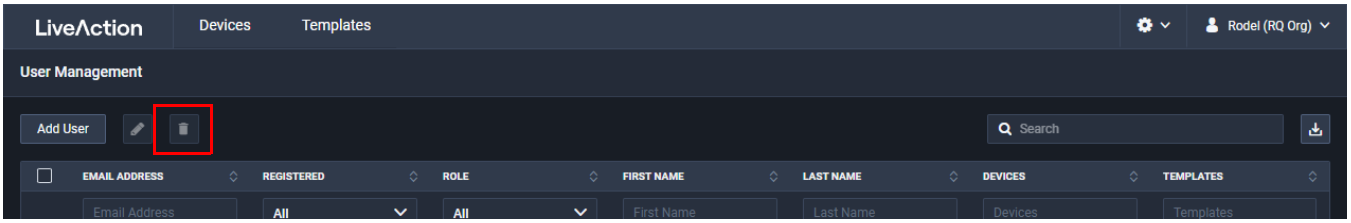
Edit User

Click *Edit User* to edit the details of the selected user.



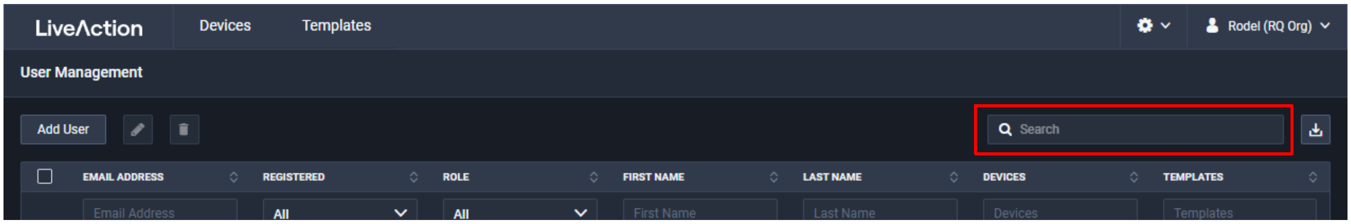
Delete User

Click Delete User to delete the selected user from the list of users.



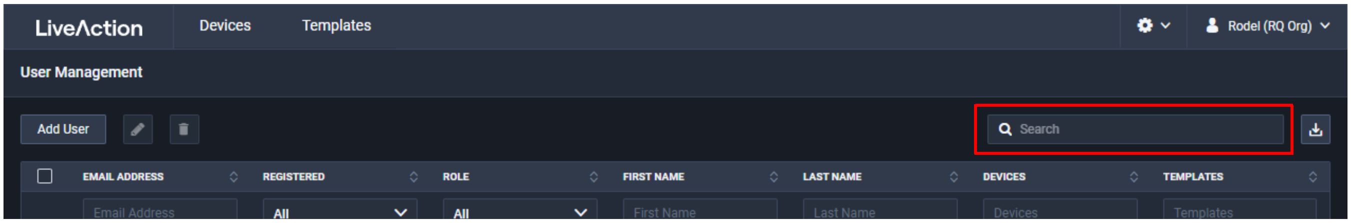
Search

Use the *Search* field to locate a specific user in the list of users. Simply enter a text string to display all users that match the text string.



Download

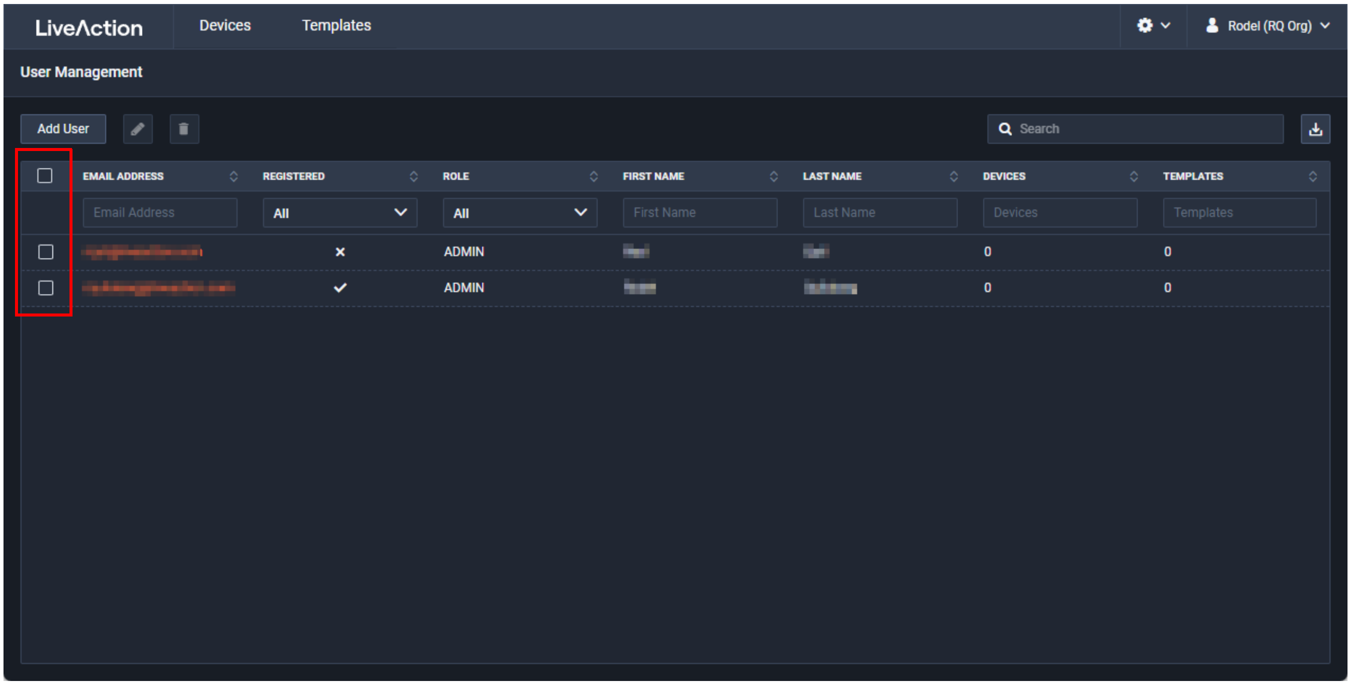
Click *Download* to create and download a *.csv* file of the list of users.



□	EMAIL ADDRESS	REGISTERED	ROLE	FIRST NAME	LAST NAME	DEVICES	TEMPLATES
	Email Address	All	All	First Name	Last Name	Devices	Templates

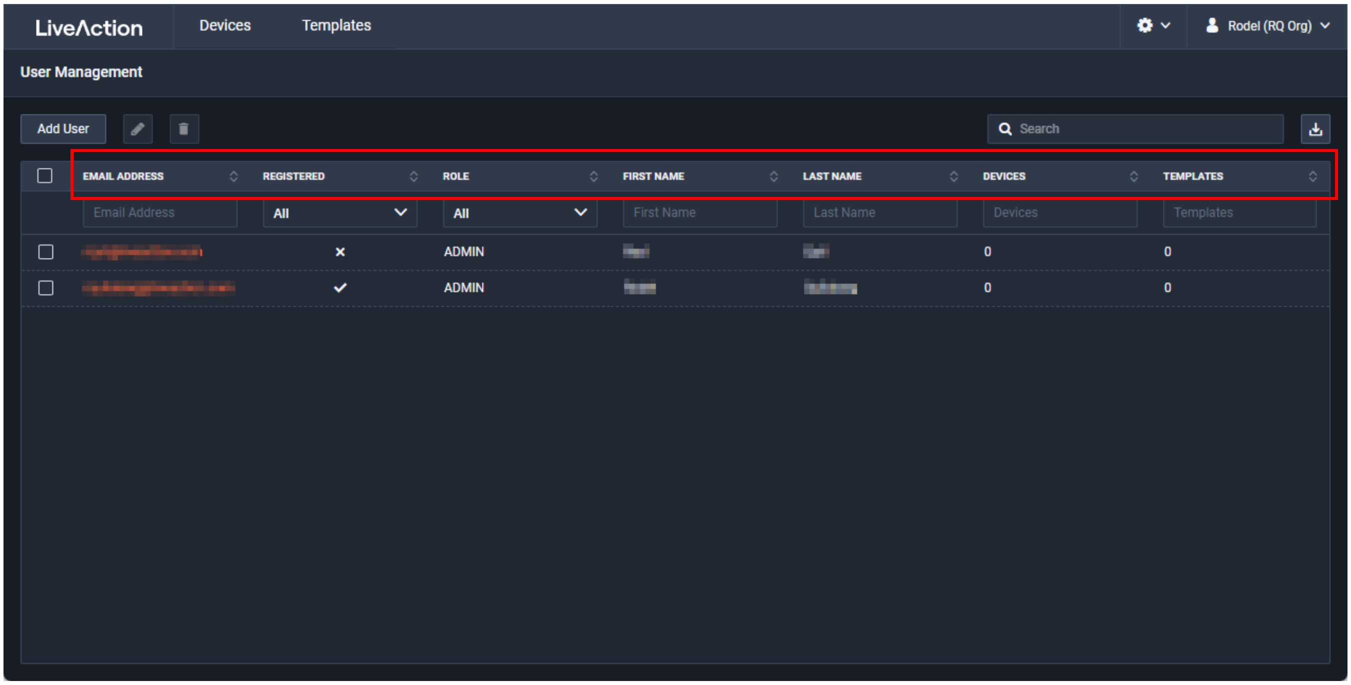
Check Box

To select a user in the list of users, select the check box of the desired users. Selecting the check box at the top of the column allows you to select or clear the check boxes of all users in the list of users.



□	EMAIL ADDRESS	REGISTERED	ROLE	FIRST NAME	LAST NAME	DEVICES	TEMPLATES
	Email Address	All	All	First Name	Last Name	Devices	Templates
□	[redacted]	✕	ADMIN	[redacted]	[redacted]	0	0
□	[redacted]	✓	ADMIN	[redacted]	[redacted]	0	0

User Management Column Headings

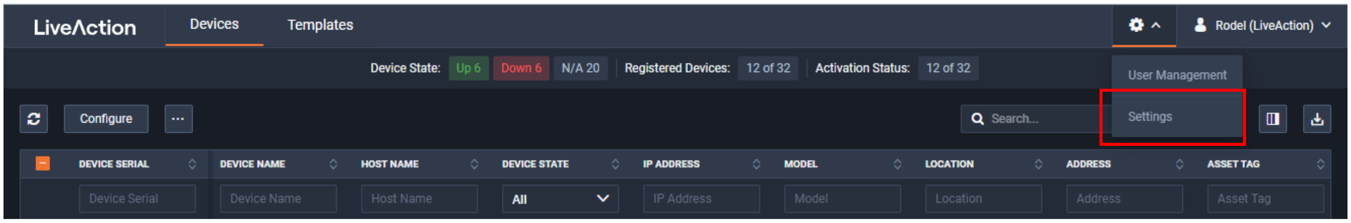


EMAIL ADDRESS	REGISTERED	ROLE	FIRST NAME	LAST NAME	DEVICES	TEMPLATES
[redacted]	✕	ADMIN	[redacted]	[redacted]	0	0
[redacted]	✓	ADMIN	[redacted]	[redacted]	0	0

- *Email Address*: Displays the email address of the user.
- *Registered*: Displays a check mark if the user has been registered with LiveAction. An X indicates the user is not registered with LiveAction.
- *Role*: Displays the role assigned to the user.
- *First Name*: Displays the first name of the user.
- *Last Name*: Displays the last name of the user.
- *Devices*: Displays the number of devices the user has registered.
- *Templates*: Displays the number of templates the user has defined.

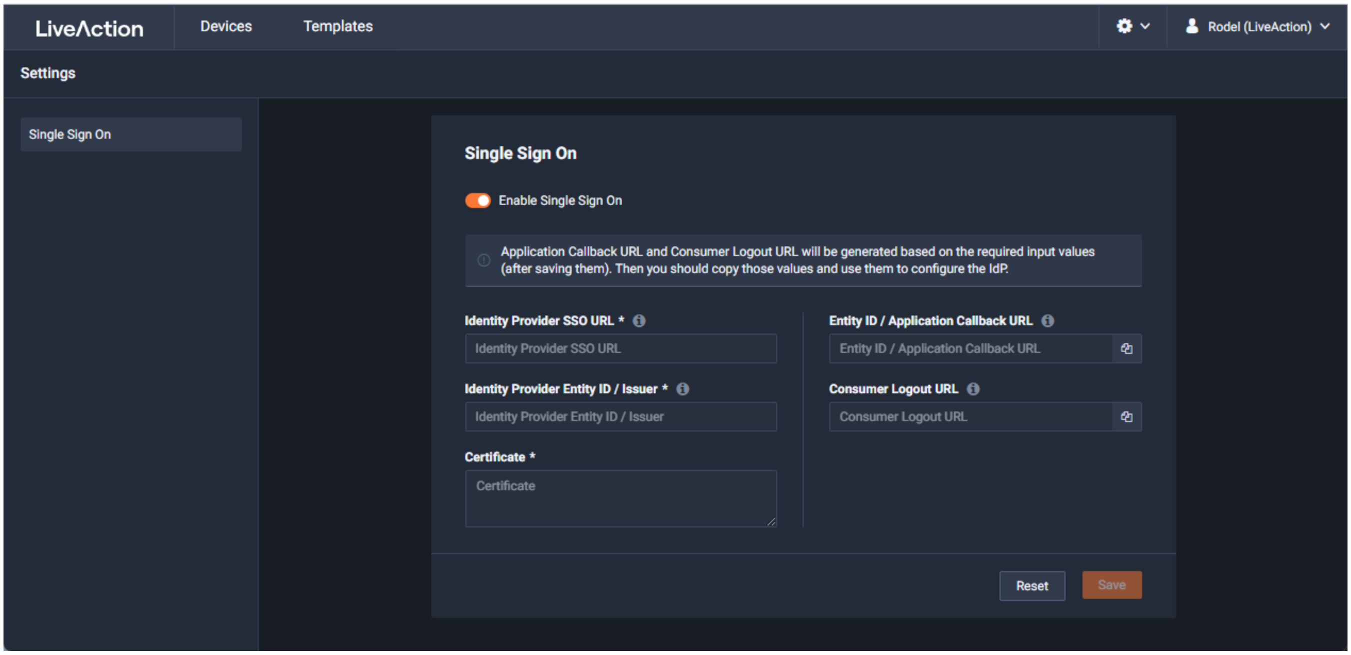
Settings

Select *Settings* to configure Grid's *Single Sign On* settings.



Single Sign On

The *Single Sign On* settings allows you to use an organization's identity provider (e.g, Okta, Ping, Auth0, etc.) for authentication.


LiveAction
Devices
Templates
Rodel (LiveAction)
Settings
Single Sign On
Single Sign On
Enable Single Sign On
Identity Provider SSO URL *
Identity Provider SSO URL
Identity Provider Entity ID / Issuer *
Identity Provider Entity ID / Issuer
Certificate *
Certificate
Entity ID / Application Callback URL
Entity ID / Application Callback URL
Consumer Logout URL
Consumer Logout URL
Reset
Save

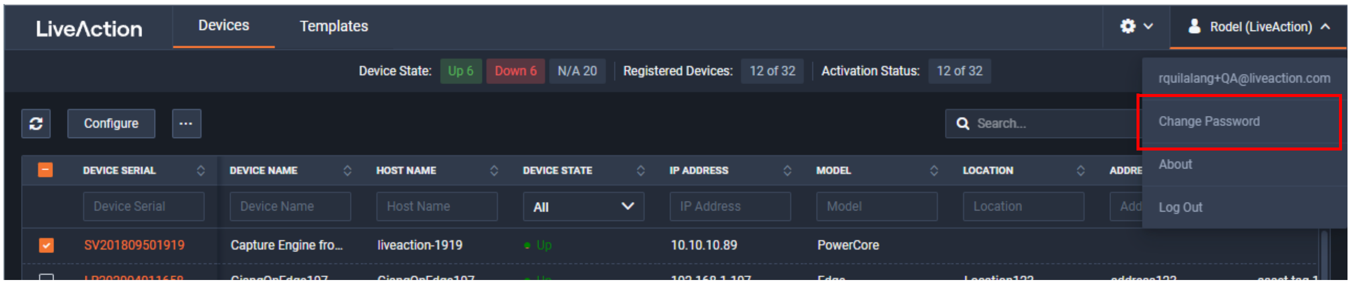
Application Callback URL and Consumer Logout URL will be generated based on the required input values (after saving them). Then you should copy those values and use them to configure the IdP.

- *Enable Single Sign On*: Click to enable or disable Single Sign On.
- *Identify Provider SSO URL*: Enter the *Single Sign On Service* (Ping) or *Idp Single Sign-On URL* (Okta).
- *Entity ID/Application Callback URL*: Enter the *ACS URL* (Ping) or *Assertion Consumer Service (ACS) URL* (Okta).
- *Identify Provider Entity ID/Issuer*: Enter *Issuer ID* (Ping) or *IdP Issuer URI* (Okta).
- *Consumer Logout URL*: Enter the *SLO Endpoint* (Ping).
- *Certificate*: Enter the *Signing Certificate* (Ping) or *IdP Signature Certificate* (Okta).
- *Reset*: Click to reset the *Single Sign On* settings.
- *Save*: Click to save the *Single Sign On* settings.

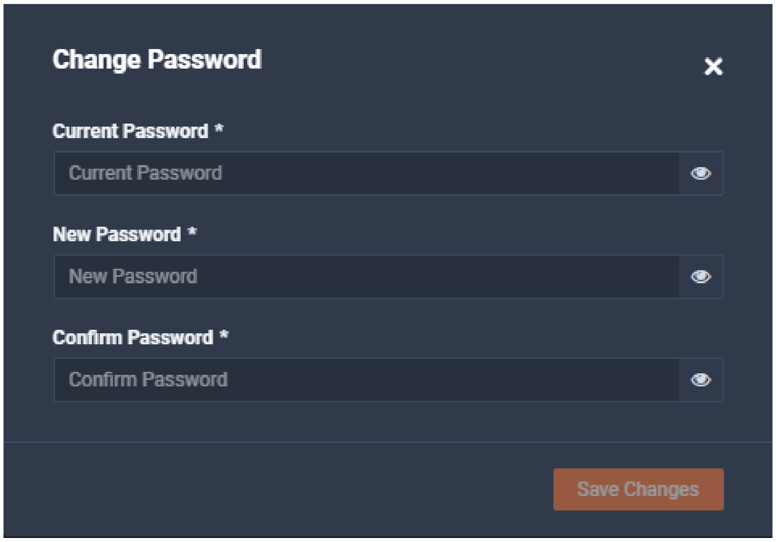
Note The *Consumer Logout URL* and *Application Callback URL* settings in Grid are generated by Grid after you save the *Single Sign On* settings.

Change Password

Select *Change Password* to change the password for logging into Grid.



Configure the *Change Password* dialog to change the password of Grid.

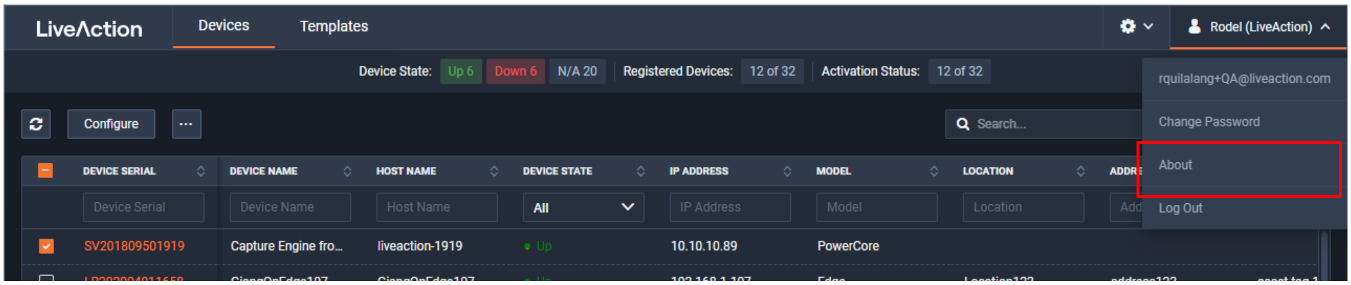


- *Current Password*: Enter the current password.
- *New Password*: Enter the new password. The new password must meet the following requirements:

  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 again.
- *Save Changes*: Click to apply the new password for Grid.

About

Select *About* to view the *Application version* of Grid.

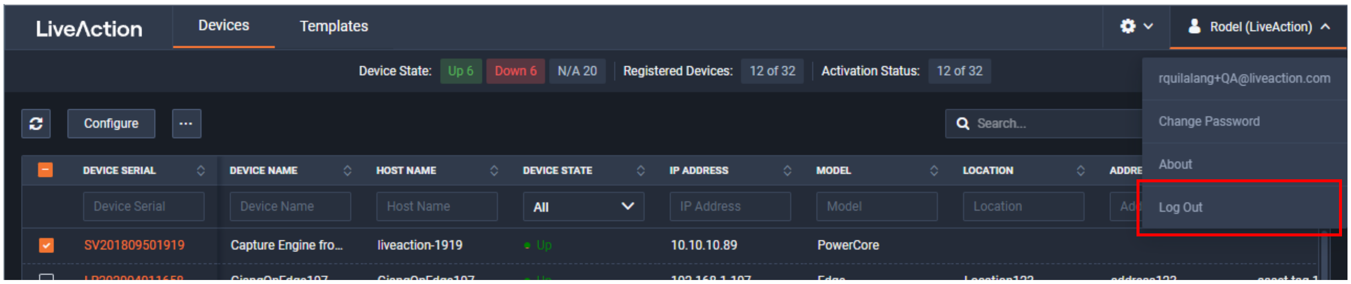


Device State: Up 6 Down 6 N/A 20 Registered Devices: 12 of 32 Activation Status: 12 of 32

DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION
SV201809501919	Capture Engine fro...	liveaction-1919	● Up	10.10.10.89	PowerCore	

Log Out

Select *Log Out* to log out of Grid.



Device State: Up 6 Down 6 N/A 20 Registered Devices: 12 of 32 Activation Status: 12 of 32

DEVICE SERIAL	DEVICE NAME	HOST NAME	DEVICE STATE	IP ADDRESS	MODEL	LOCATION
SV201809501919	Capture Engine fro...	liveaction-1919	● Up	10.10.10.89	PowerCore	

Backup and restore

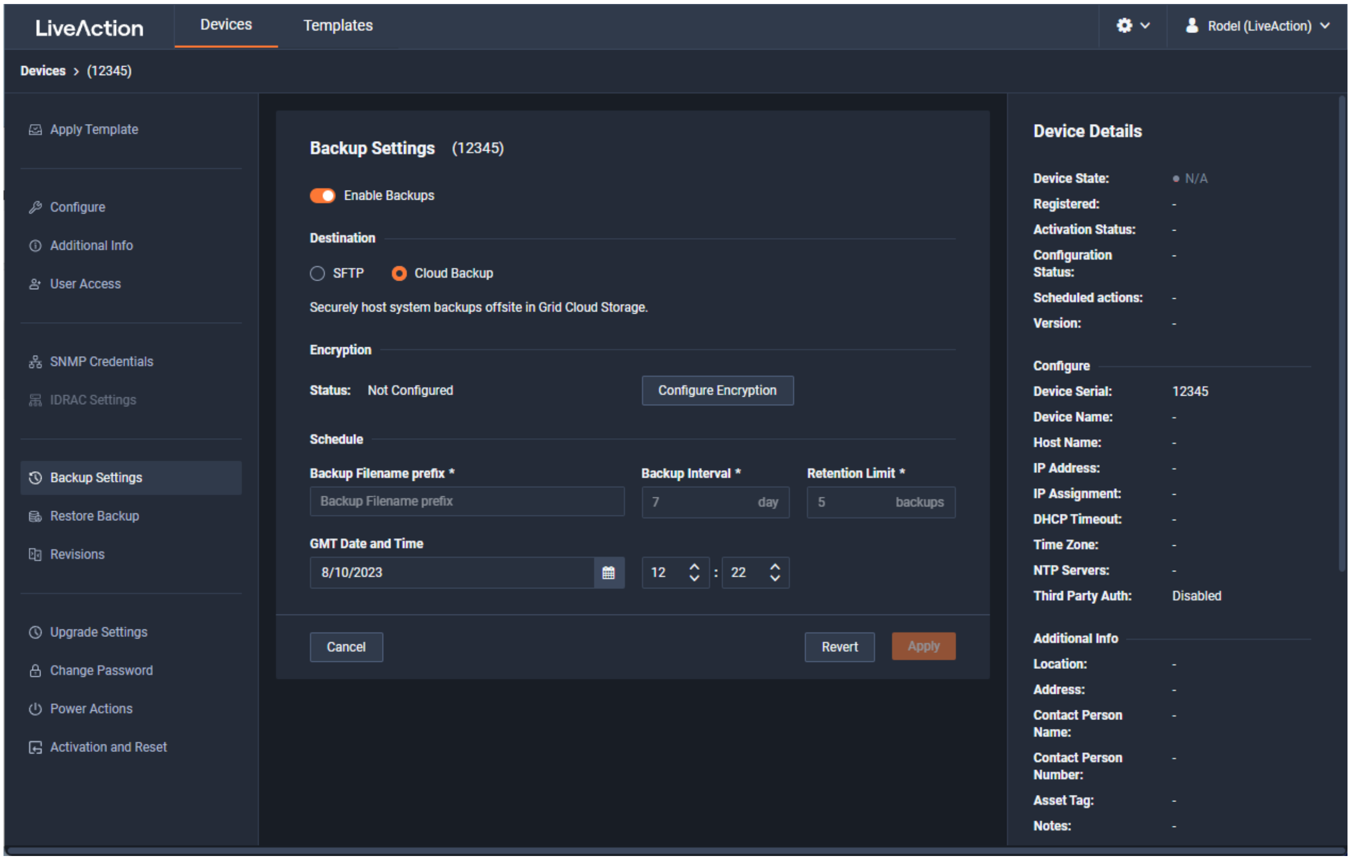
The *Backup Settings* in Grid let you configure and designate either an *SFTP* (Secure FTP) server or *Cloud Backup* for backing up the application and system settings on the LiveWire device. Once a backup is created, you can use the *Restore Backup* settings to restore either the application settings, or both the application and system settings to the same or different LiveWire device.

Here are descriptions of the *Application* and *System* settings that are included in a backup:

- *Application* settings: These are all application settings and customizations, including capture templates, filters, graphs, alarms, notifications, name table, SSL certificates, and custom plugins.
- *System* settings: These are new and/or updated users, SNMP, NTP, network, time zone, and host customizations.

Creating a backup

1. Click the **Elipsis** (...) in Grid and select *Backup Settings*. The *Backup Settings* dialog appears. See 'Backup Settings' on page 59 for a description of each of the settings.



Backup Settings (12345)

Enable Backups

Destination

○ SFTP ● Cloud Backup

Securely host system backups offsite in Grid Cloud Storage.

Encryption

Status: Not Configured

Schedule

Backup Filename prefix *: Backup Filename prefix

Backup Interval *: 7 day

Retention Limit *: 5 backups

GMT Date and Time: 8/10/2023 12 : 22

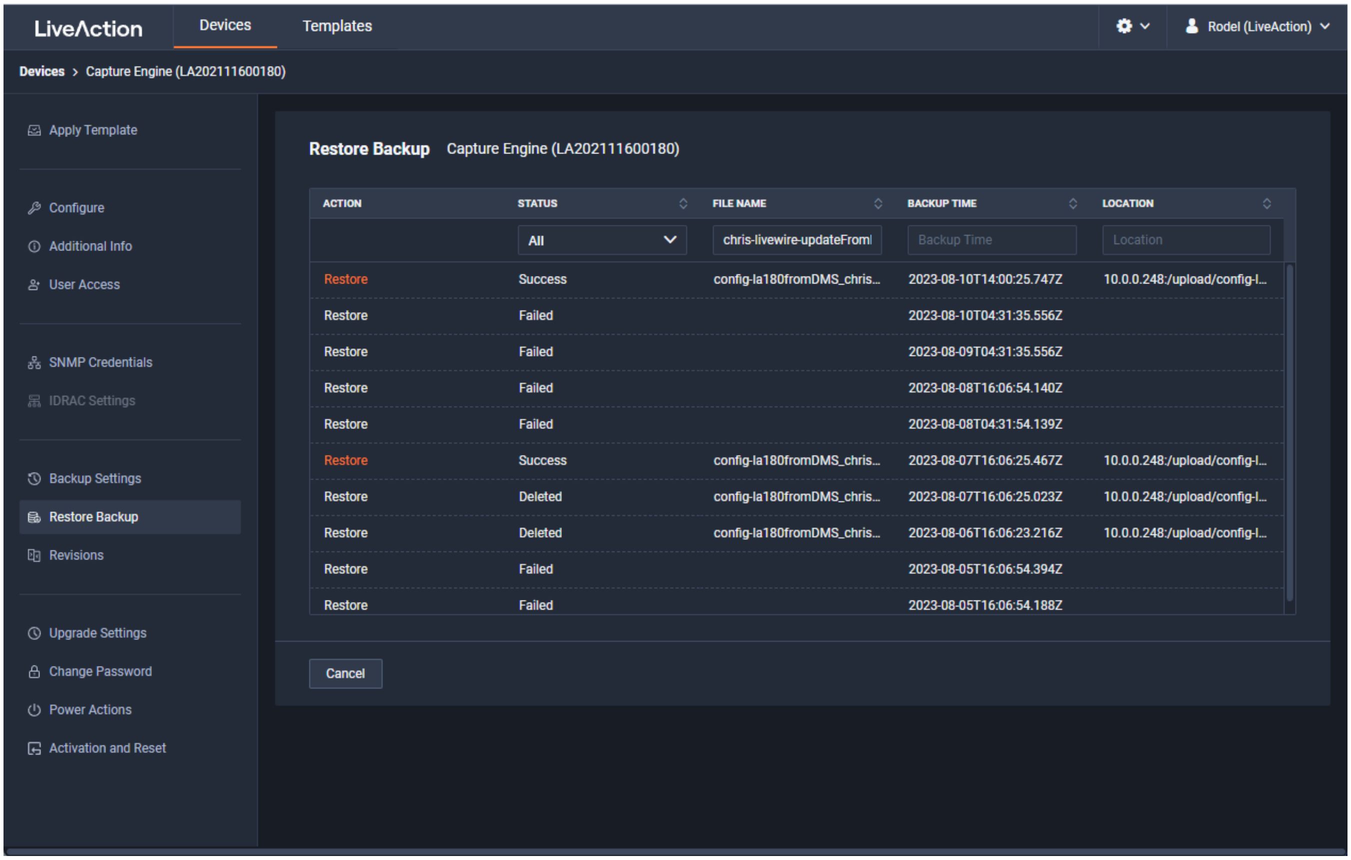
Device Details

Device State:	● N/A
Registered:	-
Activation Status:	-
Configuration Status:	-
Scheduled actions:	-
Version:	-
Configure	
Device Serial:	12345
Device Name:	-
Host Name:	-
IP Address:	-
IP Assignment:	-
DHCP Timeout:	-
Time Zone:	-
NTP Servers:	-
Third Party Auth:	Disabled
Additional Info	
Location:	-
Address:	-
Contact Person Name:	-
Contact Person Number:	-
Asset Tag:	-
Notes:	-

2. In the *Destination* section, choose one of the following:
   - *SFTP*: Select this option to back up to the SFTP (Secure FTP) server. You will need to configure the SFTP server you want to use as the backup server.
   - *Cloud Backup*: Select this option to back up to Grid Cloud Storage.
3. In the *Encryption* section, click *Configure Encryption* to set up encryption.
4. In the *Schedule* section, configure the *Schedule* settings.
5. Click **Apply**.

Restoring a backup

1. Click the **Elipsis** (...) in Grid and select *Restore Backup*. The *Restore Backup* dialog appears. See 'Restore Backup' on page 61 for a description of each of the settings.



Restore Backup Capture Engine (LA202111600180)

ACTION	STATUS	FILE NAME	BACKUP TIME	LOCATION
	All	chris-livewire-updateFroml	Backup Time	Location
Restore	Success	config-la180fromDMS_chris...	2023-08-10T14:00:25.747Z	10.0.0.248:/upload/config-l...
Restore	Failed		2023-08-10T04:31:35.556Z	
Restore	Failed		2023-08-09T04:31:35.556Z	
Restore	Failed		2023-08-08T16:06:54.140Z	
Restore	Failed		2023-08-08T04:31:54.139Z	
Restore	Success	config-la180fromDMS_chris...	2023-08-07T16:06:25.467Z	10.0.0.248:/upload/config-l...
Restore	Deleted	config-la180fromDMS_chris...	2023-08-07T16:06:25.023Z	10.0.0.248:/upload/config-l...
Restore	Deleted	config-la180fromDMS_chris...	2023-08-06T16:06:23.216Z	10.0.0.248:/upload/config-l...
Restore	Failed		2023-08-05T16:06:54.394Z	
Restore	Failed		2023-08-05T16:06:54.188Z	

2. In the *Action* column, select the backup (in orange) you want to restore.
3. Select either the *Application Settings* or *Application and System Settings* option, enter the *Password* for the backup, and click **Restore**.

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

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

Usage: *omni-interface [options]*

options:

-a, --adapter	adapter to modify
-f, --wifi	enable or disable Remote AP Capture capability [on|off]
-c, --dhcp	configure dhcp
-s, --static	configure static
-l, --manual	configure manual

-r, --address	static adapter address
-m, --netmask	static adapter netmask
-b, --broadcast	static adapter broadcast address
-w, --network	static adapter network address
-g, --gateway	static adapter gateway address
-h, --hwaddress	static adapter mac address
-d, --dns	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 Omnipeek.

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

Connecting to LiveWire Edge via the Mini-USB Console Port

The Mini-USB port (Console port) on LiveWire Edge lets you connect to another computer terminal for advanced diagnostics or recovery access using a mini-USB console cable (included with LiveWire Edge) connected from the USB port on your PC/laptop to the Mini-USB Port of LiveWire Edge.

Using the Mini-USB port on LiveWire Edge, a laptop, and a terminal program of your choice, you can log into LiveWire Edge and access the LiveWire command prompt (admin@ivewire).

To connect to LiveWire Edge:

1. Connect the mini-USB console cable from your laptop to the Mini-USB port on LiveWire Edge.
2. Using any serial terminal program (e.g., HyperTerminal or Putty), establish a connection to LiveWire. Make sure the appropriate terminal settings match the default settings below for LiveWire Edge:
   - 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]
3. Once a connection to LiveWire Edge has been established, the LiveWire Edge login prompt appears.
4. Log into LiveWire Edge as you normally would. The LiveWire Edge command prompt (admin@livewire) appears.

Connecting to LiveWire through the serial port

Using the serial port on LiveWire, a laptop, and a terminal program of your choice, you can log into LiveWire and access the LiveWire command prompt (*admin@ivewire*).

To connect to LiveWire:

1. Connect a serial console cable from your laptop to the serial port on the back of LiveWire. The cable must be an RS-232 (null modem) cable with a female DB-9 connector for the serial port on LiveWire.
2. Using any serial terminal program (e.g., HyperTerminal or Putty), establish a connection to LiveWire. Make sure the appropriate terminal settings match the default settings below for LiveWire:
   - 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]
3. Once a connection to LiveWire has been established, the LiveWire login prompt appears.
4. Log into LiveWire as you normally would. The LiveWire command prompt (*admin@livewire*) appears.
5. At this point, you can configure network settings by using the ‘omni-interface’ command script, as described in ’Configuring network settings by command script’ on page 78. Additionally, please configure an NTP server as described in ‘Time’ on page 40.

Using LiveWire with Omnipeek

Any computer on the network with the Omnipeek Windows software installed can now access the Capture Engine running on LiveWire. From the **Capture Engine** window in Omnipeek, 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 Omnipeek console, please see ‘Using Capture Engines with Omnipeek’ on page 115, and also the *Omnipeek User Guide* or Omnipeek 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).

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 83.
- **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

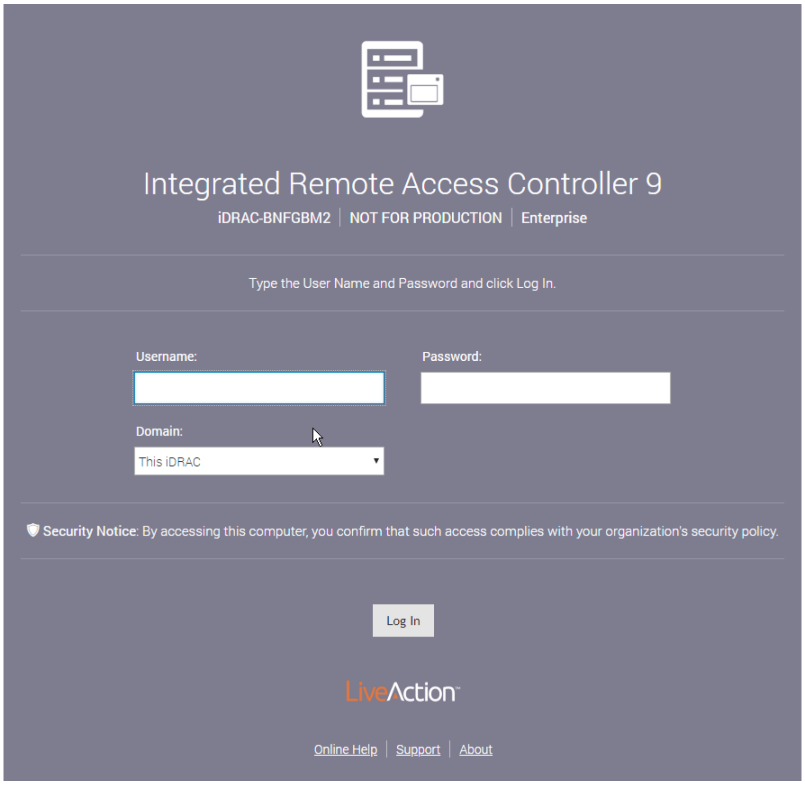
You can use an Internet browser window to connect to iDRAC on LiveWire. Additionally, you must make sure the following ports are accessible through any firewall:

- 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.



Integrated Remote Access Controller 9

iDRAC-BNFGBM2 | NOT FOR PRODUCTION | Enterprise

Type the User Name and Password and click Log In.

Username:

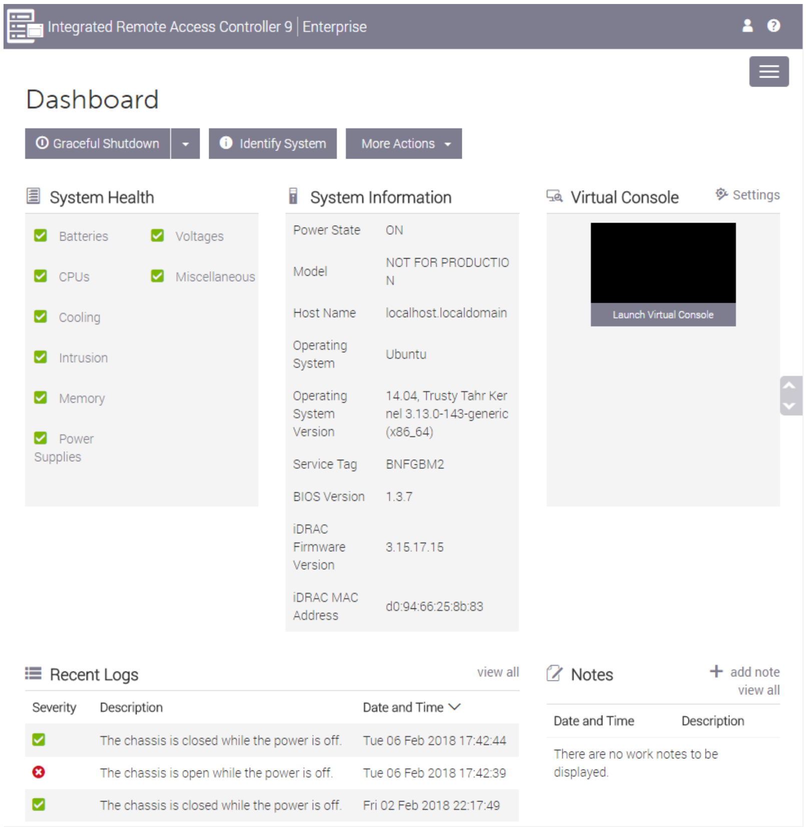
Password:

Domain: This iDRAC

Security Notice: By accessing this computer, you confirm that such access complies with your organization's security policy.

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.



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

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

Date and Time	Description

There are no work notes to be displayed.

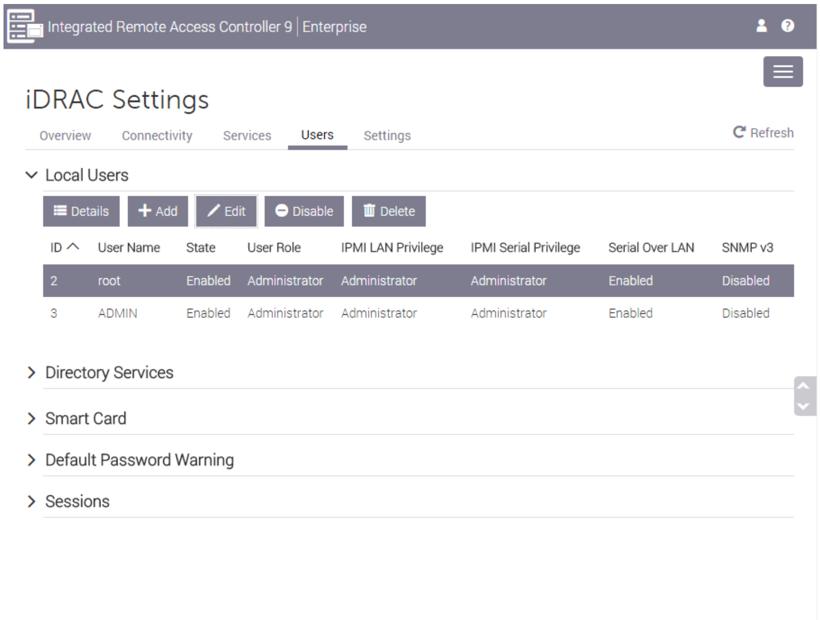
5. View the remaining instructions in this section for instructions on using iDRAC to perform tasks such as changing the default password, accessing a remote console, reimaging, rebooting, starting, and shutting down LiveWire.

Changing the default password

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

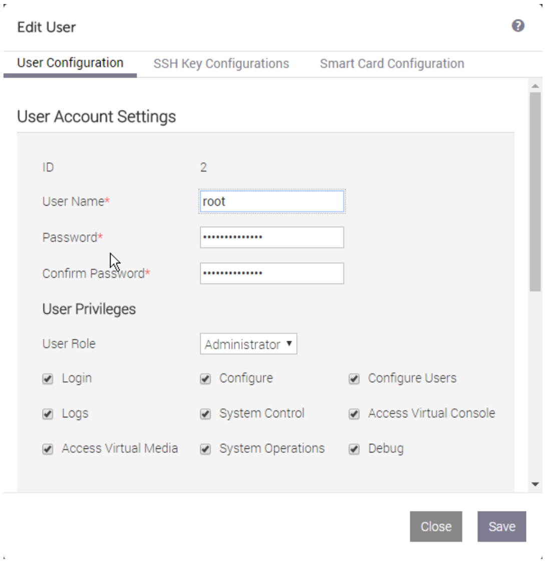
To change the default password:

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



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

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.



User Account Settings

ID: 2

User Name*: root

Password*: ••••••••••••••

Confirm Password*: ••••••••••••••

User Privileges

User Role: Administrator

☑ Login ☑ Configure ☑ Configure Users

☑ Logs ☑ System Control ☑ Access Virtual Console

☑ Access Virtual Media ☑ System Operations ☑ Debug

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

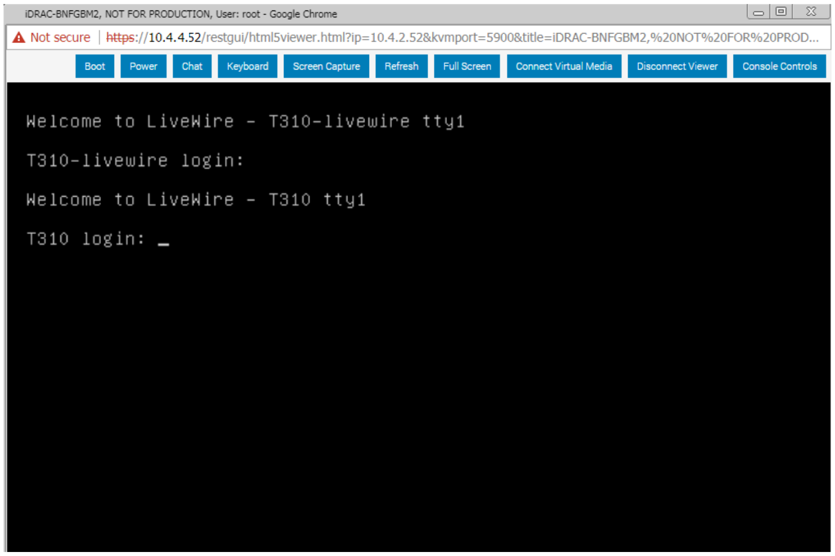
Accessing a remote console

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:

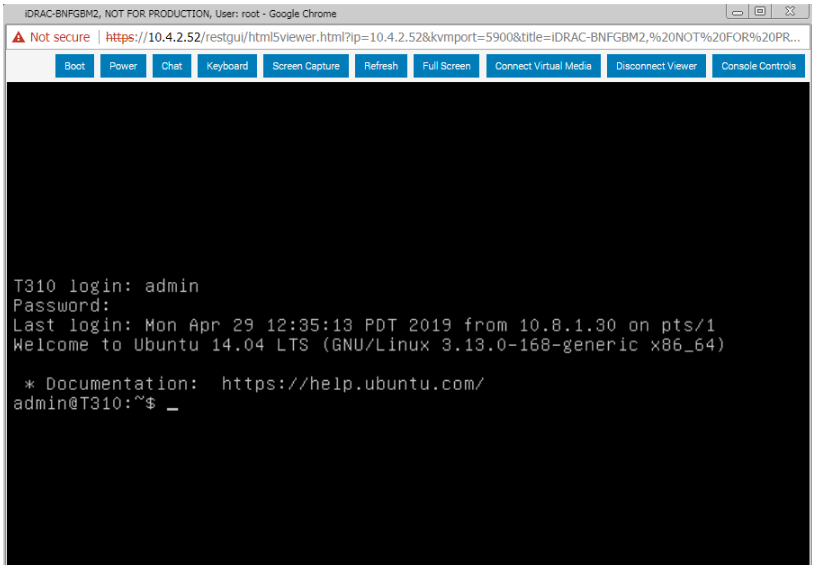
> **Note** The *Plug-in Type* was changed to 'HTML5' from the default of 'Native' for the instructions in this section. To change the *Plug-in Type*, click *Settings* in the *Virtual Console Preview*.

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


iDRAC-BNFGBM2, NOT FOR PRODUCTION, User: root - Google Chrome
Not secure | https://10.4.4.52/restgui/html5viewer.html?ip=10.4.2.52&kvmport=5900&title=iDRAC-BNFGBM2,%20NOT%20FOR%20PROD...
Boot
Power
Chat
Keyboard
Screen Capture
Refresh
Full Screen
Connect Virtual Media
Disconnect Viewer
Console Controls

```
Welcome to LiveWire - T310-livewire tty1

T310-livewire login:

Welcome to LiveWire - T310 tty1

T310 login: _
```

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


iDRAC-BNFGBM2, NOT FOR PRODUCTION, User: root - Google Chrome
Not secure | https://10.4.2.52/restgui/html5viewer.html?ip=10.4.2.52&kvmport=5900&title=iDRAC-BNFGBM2,%20NOT%20FOR%20PR...
Boot
Power
Chat
Keyboard
Screen Capture
Refresh
Full Screen
Connect Virtual Media
Disconnect Viewer
Console Controls

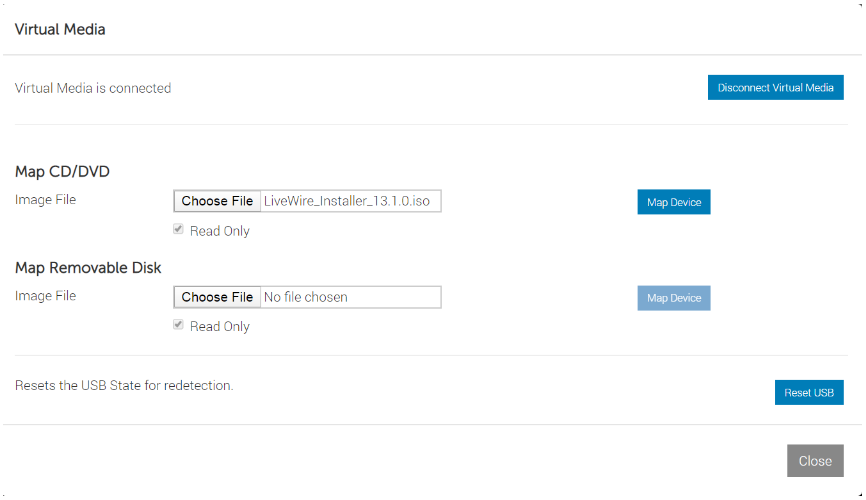
```
T310 login: admin
Password:
Last login: Mon Apr 29 12:35:13 PDT 2019 from 10.8.1.30 on pts/1
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-168-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
admin@T310:~$ _
```

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 25.

To reimage LiveWire:

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



Virtual Media

Virtual Media is connected

Map CD/DVD

Image File: Choose File LiveWire_Installer_13.1.0.iso

☑ Read Only

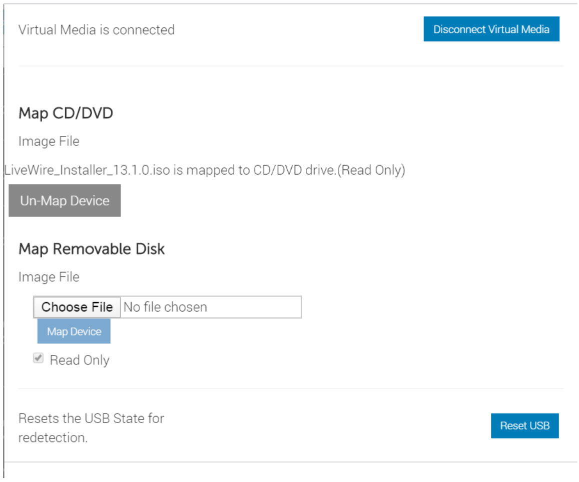
Map Removable Disk

Image File: Choose File No file chosen

☑ Read Only

Resets the USB State for redetection.

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

Map CD/DVD

Image File

LiveWire_Installer_13.1.0.iso is mapped to CD/DVD drive.(Read Only)

Map Removable Disk

Image File

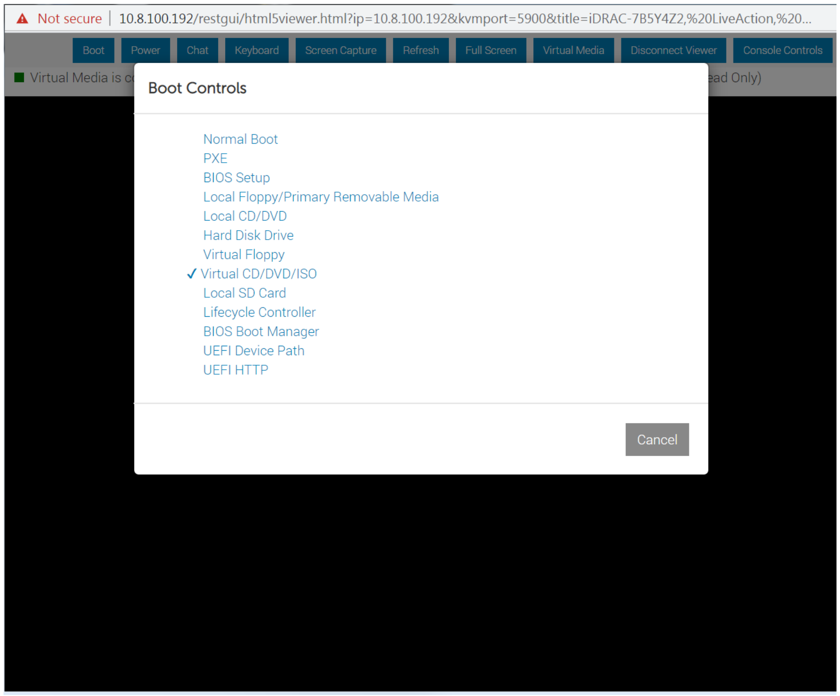
Choose File No file chosen

☑ Read Only

Resets the USB State for redetection.

3. Click **Close** to close the dialog.

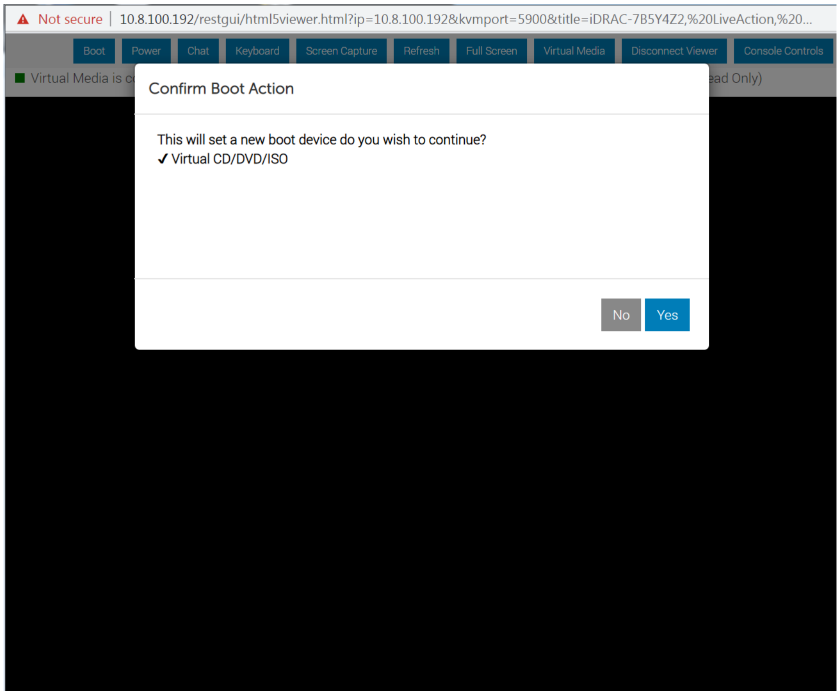
4. From the remote console, click **Boot** and select *Virtual CD/DVD/ISO* from the boot controls. The **Confirm Boot Action** dialog appears.



Not secure | 10.8.100.192/restgui/html5viewer.html?ip=10.8.100.192&kvmport=5900&title=iDRAC-7B5Y4Z2,%20LiveAction,%20...

Boot Controls

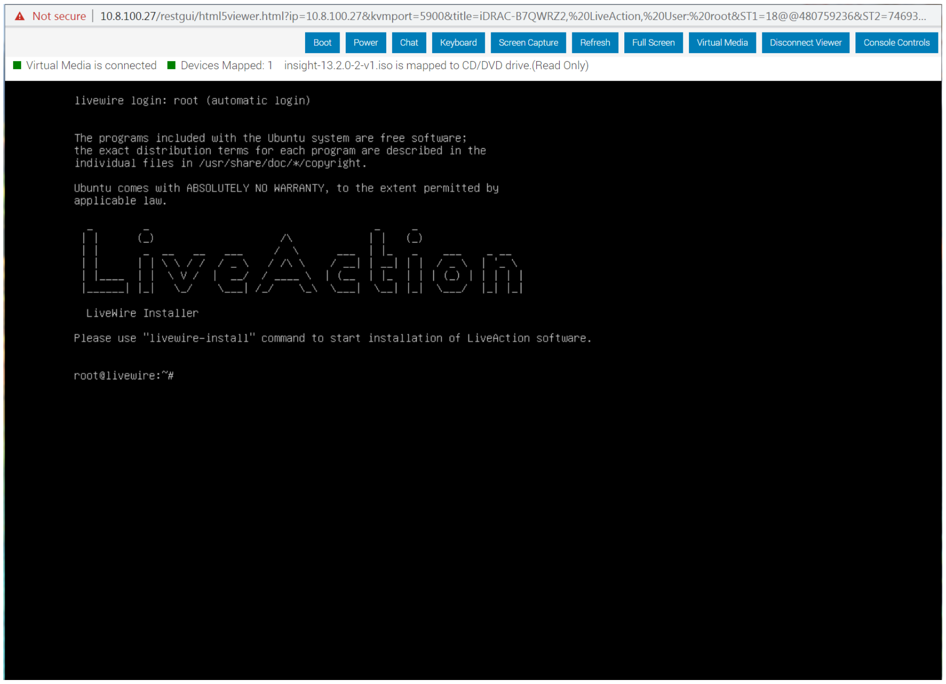
5. Click **Yes** to set the *Virtual CD/DVD/ISO* as the new boot device.



Confirm Boot Action

This will set a new boot device do you wish to continue?
✓ Virtual CD/DVD/ISO

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.


Not secure | 10.8.100.27/restgui/html5viewer.html?ip=10.8.100.27&kvmport=5900&title=iDRAC-B7QWRZ2,%20LiveAction,%20User:%20root&ST1=18@@480759236&ST2=74693...
Boot
Power
Chat
Keyboard
Screen Capture
Refresh
Full Screen
Virtual Media
Disconnect Viewer
Console Controls

🟩 Virtual Media is connected 🟩 Devices Mapped: 1 insight-13.2.0-2-v1.iso is mapped to CD/DVD drive.(Read Only)

```
livewire login: root (automatic login)


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

  _     _            _        _   _
 | |   (_)_   _____ / \   ___| |_(_) ___  _ __
 | |   | \ \ / / _ \ / _ \ / __| __| |/ _ \| '_ \
 | |___| |\ V /  __// ___ \ (__| |_| | (_) | | | |
 |_____|_| \_/ \___/_/   \_\___|\__|_|\___/|_| |_|

  LiveWire Installer

Please use "livewire-install" command to start installation of LiveAction software.


root@livewire:~#
```

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

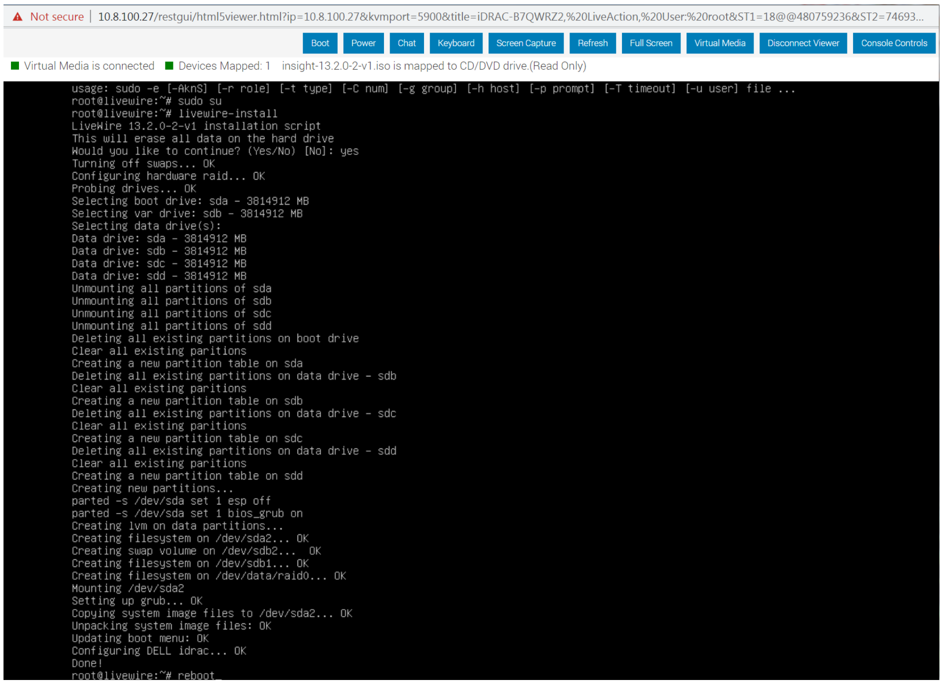
Note When running the *livewire-install* script though the remote console, do not close the console until the script completes. Closing the console prematurely causes the reimaging process to fail.

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.


▲ Not secure | 10.8.100.27/restgui/html5viewer.html?ip=10.8.100.27&kvmport=5900&title=iDRAC-B7QWRZ2,%20LiveAction,%20User:%20root&ST1=18@@480759236&ST2=74693...
Boot
Power
Chat
Keyboard
Screen Capture
Refresh
Full Screen
Virtual Media
Disconnect Viewer
Console Controls
🟩 Virtual Media is connected
🟩 Devices Mapped: 1
insight-13.2.0-2-v1.iso is mapped to CD/DVD drive.(Read Only)

```
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 paritions
Creating a new partition table on sda
Deleting all existing partitions on data drive - sdb
Clear all existing paritions
Creating a new partition table on sdb
Deleting all existing partitions on data drive - sdc
Clear all existing paritions
Creating a new partition table on sdc
Deleting all existing partitions on data drive - sdd
Clear all existing paritions
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 lvm 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.

CHAPTER 3

Sending Telemetry to LiveNX and ThreatEye

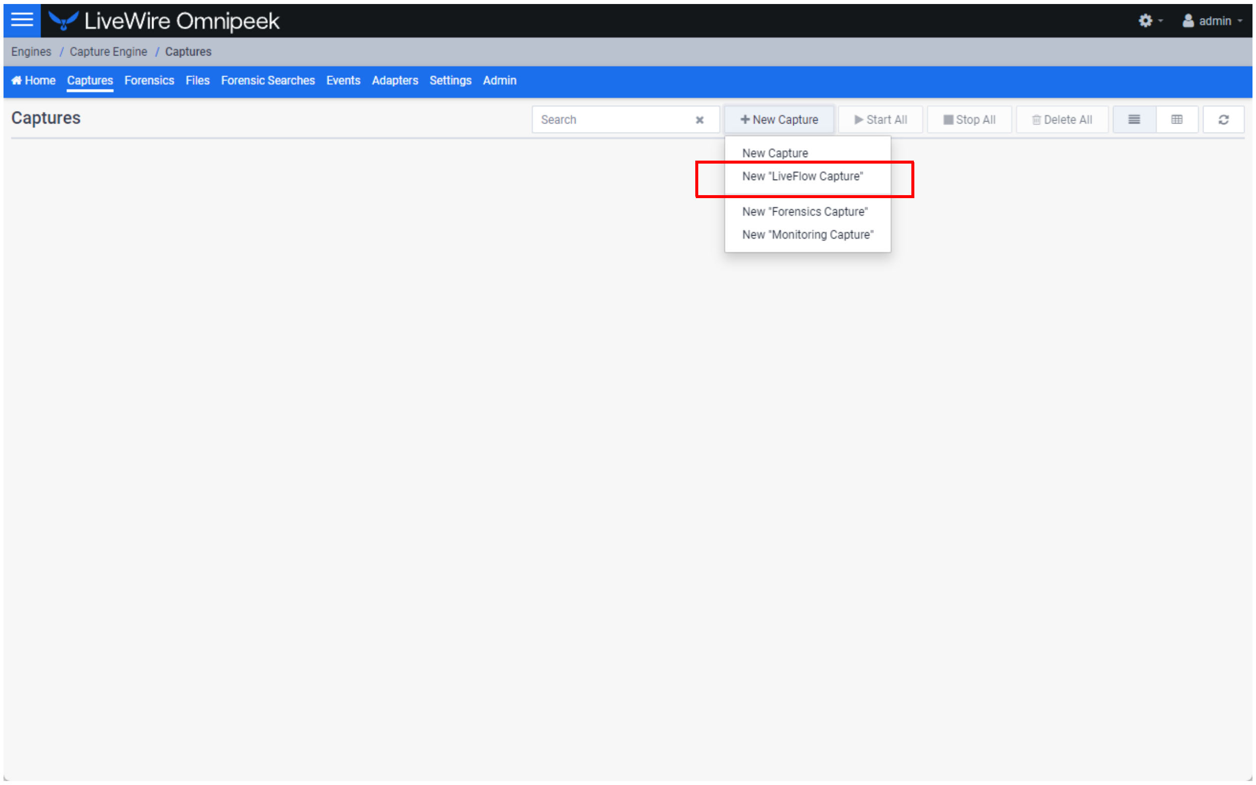
In this chapter:

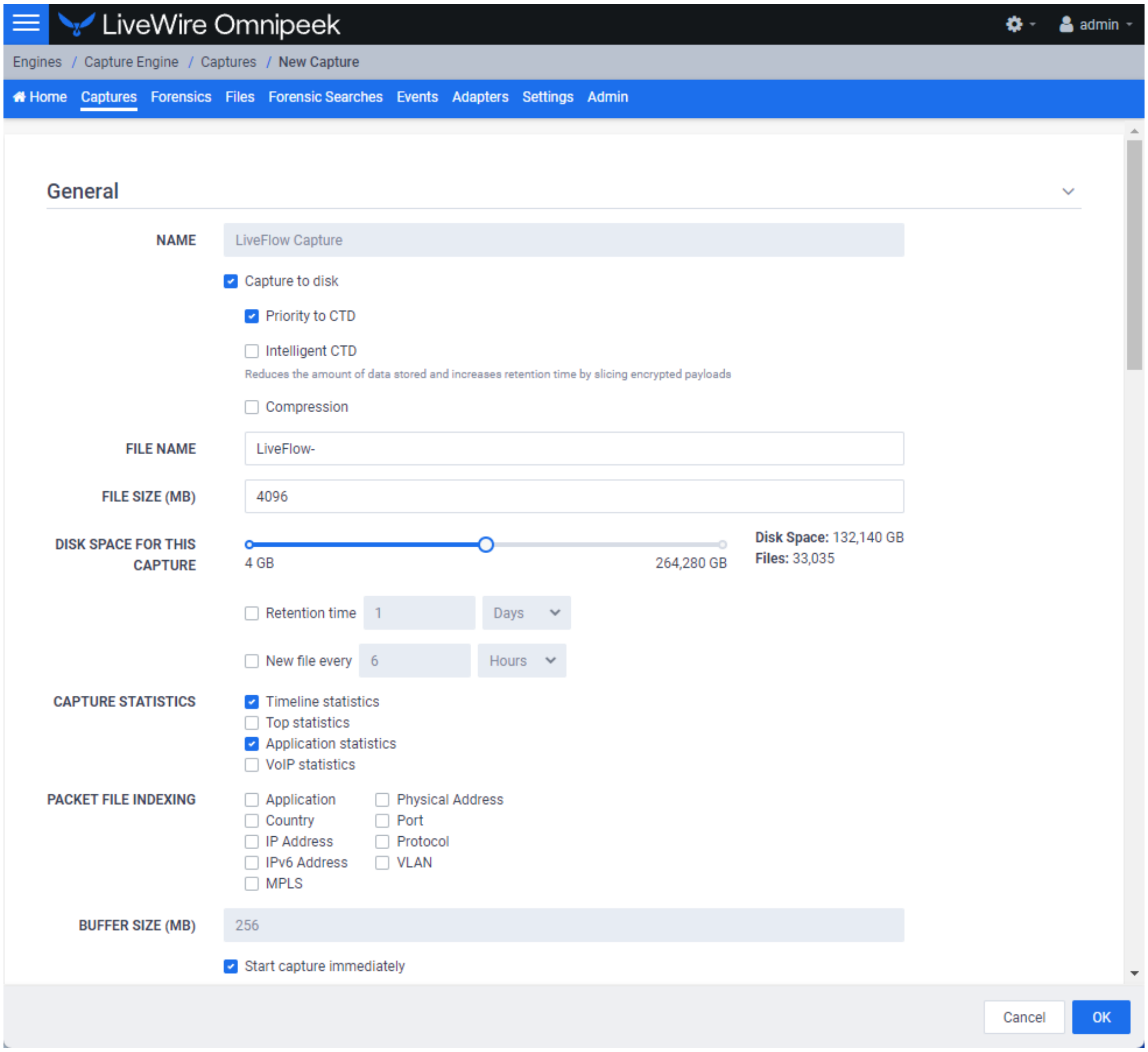
About sending telemetry to LiveNX and ThreatEye

LiveWire is designed to send LiveFlow telemetry data to LiveAction's LiveNX and ThreatEye 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. ThreatEye is a Network Detection & Response platform, unfazed by encrypted network traffic, that uses advanced behavioral analysis and machine learning for threat detection and security compliance. This chapter describes the tasks you must perform in order to properly send LiveFlow telemetry data from LiveWire to LiveNX and ThreatEye.

Configuring LiveFlow telemetry

To send the LiveFlow telemetry data that LiveNX or ThreatEye uses for its platform, you must use Omnipeek to first create a new LiveFlow capture and then configure the settings for that capture to send LiveFlow telemetry to either the LiveNX and/or ThreatEye platforms.





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

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 – 264,280 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
□ Country
□ IP Address
□ IPv6 Address
□ MPLS
□ Physical Address
□ Port
□ Protocol
□ VLAN

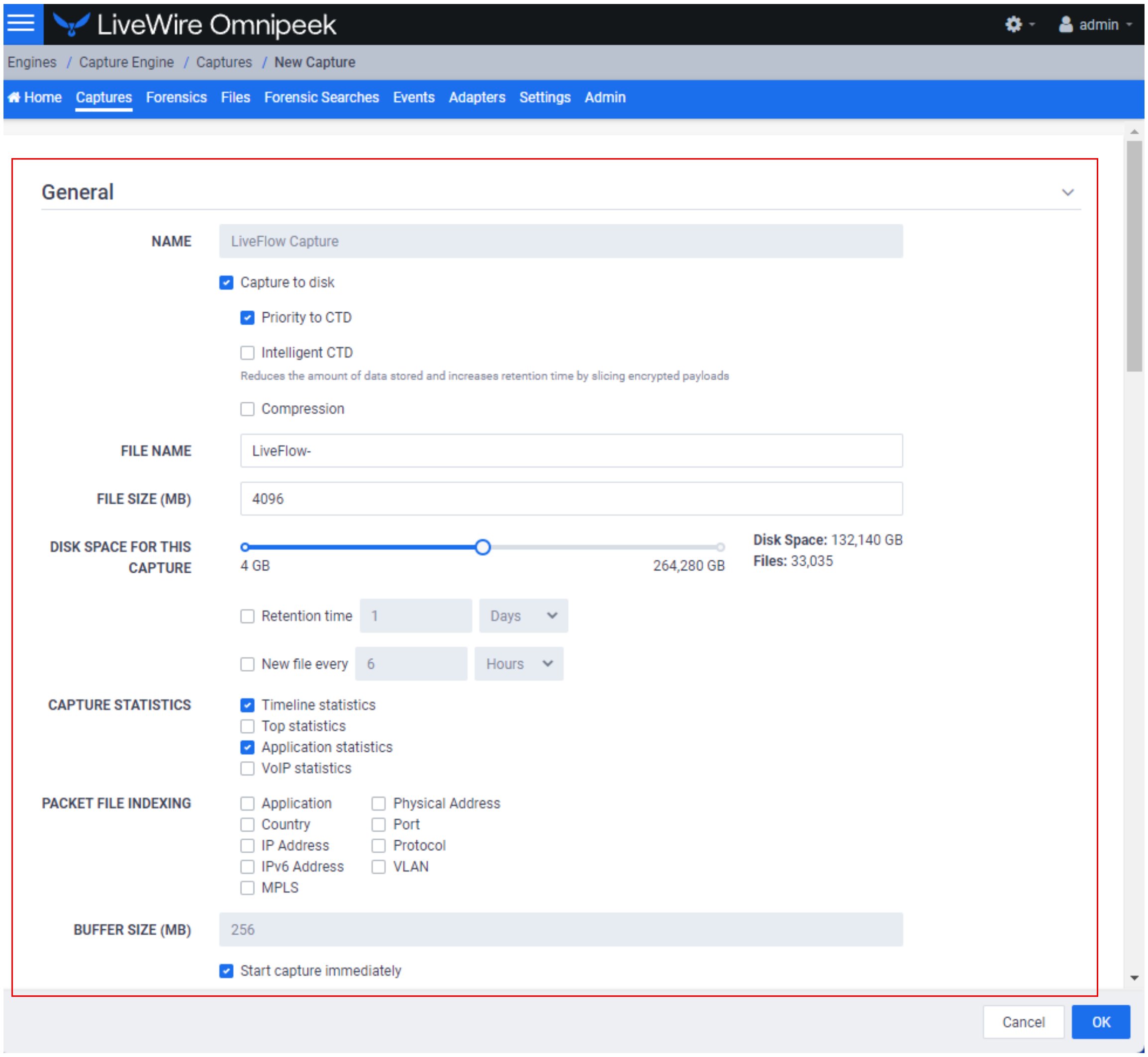
BUFFER SIZE (MB): 256

☑ Start capture immediately

Note Scroll down in the capture options to see LiveFlow settings for *Template Refresh Interval* and *Options Template Refresh Interval*. These settings let you configure the amount of time (in seconds) LiveWire sends template information to LiveNX. The templates provide the instructions to LiveNX 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 LiveNX and ThreatEye 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.


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

General

NAME: LiveFlow Capture

☑ Capture to disk

☑ Priority to CTD

☐ Intelligent CTD

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

☐ Compression

FILE NAME: LiveFlow-

FILE SIZE (MB): 4096

DISK SPACE FOR THIS CAPTURE: 4 GB – 264,280 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
☐ Country
☐ IP Address
☐ IPv6 Address
☐ MPLS
☐ Physical Address
☐ Port
☐ Protocol
☐ VLAN

BUFFER SIZE (MB): 256

☑ Start capture immediately

- *Name:* Type a descriptive name for the capture. Unique names can help you to identify and organize your captures.
- *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.

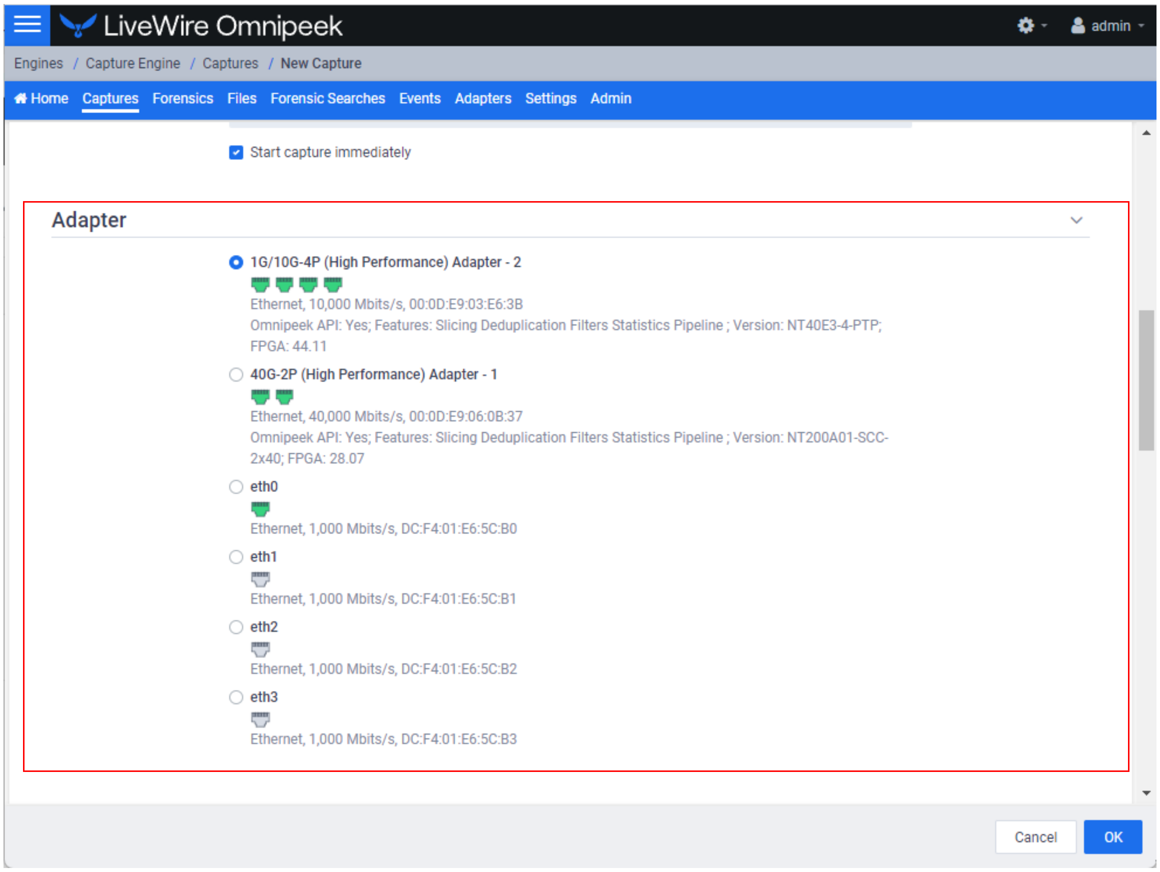
- *File Name:* Type the name used as a base file name prefix for each capture file that is created using the *Capture to disk* option. Additionally, each capture file is appended with a timestamp indicating the date and time the file was saved. The format of the timestamp is *YYYY-MM-DD-HH.MM.SS.mmm*.
- *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.



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

☑ Start capture immediately

Adapter

● 1G/10G-4P (High Performance) Adapter - 2
Ethernet, 10,000 Mbits/s, 00:0D:E9:03:E6:3B
Omnipeek API: Yes; Features: Slicing Deduplication Filters Statistics Pipeline ; Version: NT40E3-4-PTP; FPGA: 44.11

○ 40G-2P (High Performance) Adapter - 1
Ethernet, 40,000 Mbits/s, 00:0D:E9:06:0B:37
Omnipeek API: Yes; Features: Slicing Deduplication Filters Statistics Pipeline ; Version: NT200A01-SCC-2x40; FPGA: 28.07

○ eth0
Ethernet, 1,000 Mbits/s, DC:F4:01:E6:5C:B0

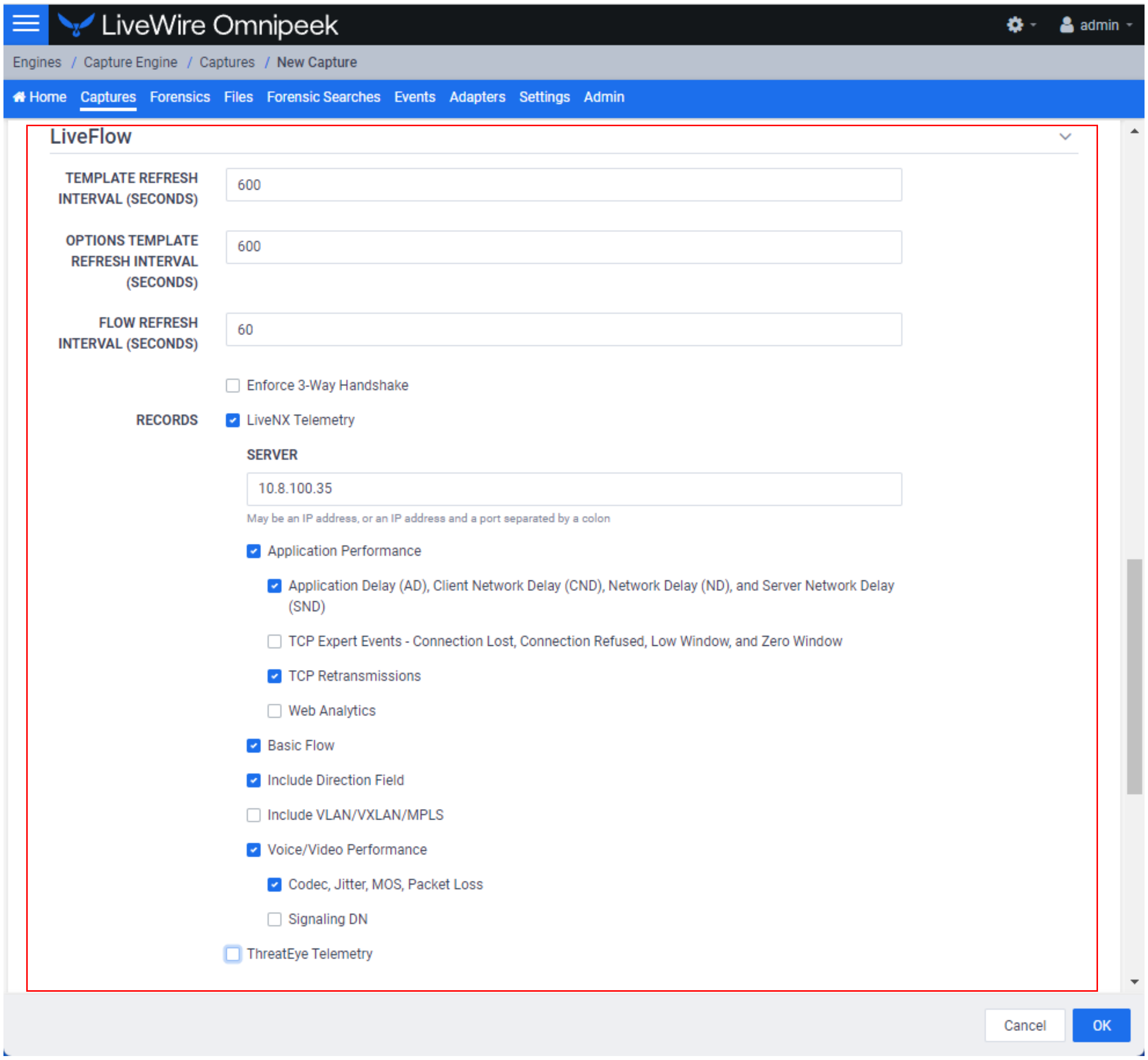
○ eth1
Ethernet, 1,000 Mbits/s, DC:F4:01:E6:5C:B1

○ eth2
Ethernet, 1,000 Mbits/s, DC:F4:01:E6:5C:B2

○ eth3
Ethernet, 1,000 Mbits/s, DC:F4:01:E6:5C:B3

LiveFlow

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


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

TEMPLATE REFRESH INTERVAL (SECONDS): 600

OPTIONS TEMPLATE REFRESH INTERVAL (SECONDS): 600

FLOW REFRESH INTERVAL (SECONDS): 60

□ Enforce 3-Way Handshake

RECORDS: ☑ LiveNX Telemetry

SERVER: 10.8.100.35

May be an IP address, or an IP address and a port separated by a colon

- ☑ Application Performance
  - ☑ Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)
  - □ TCP Expert Events - Connection Lost, Connection Refused, Low Window, and Zero Window
  - ☑ TCP Retransmissions
  - □ Web Analytics
- ☑ Basic Flow
- ☑ Include Direction Field
- □ Include VLAN/VXLAN/MPLS
- ☑ Voice/Video Performance
  - ☑ Codec, Jitter, MOS, Packet Loss
  - □ Signaling DN

□ ThreatEye Telemetry

Template Refresh Interval

- *Template Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire generates and sends IPFIX template records to LiveNX. The templates provide the instructions to LiveNX 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 LiveNX to see the LiveFlow data from LiveWire. You may want to adjust this setting to the desired intervals.

Options Template Refresh Interval

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

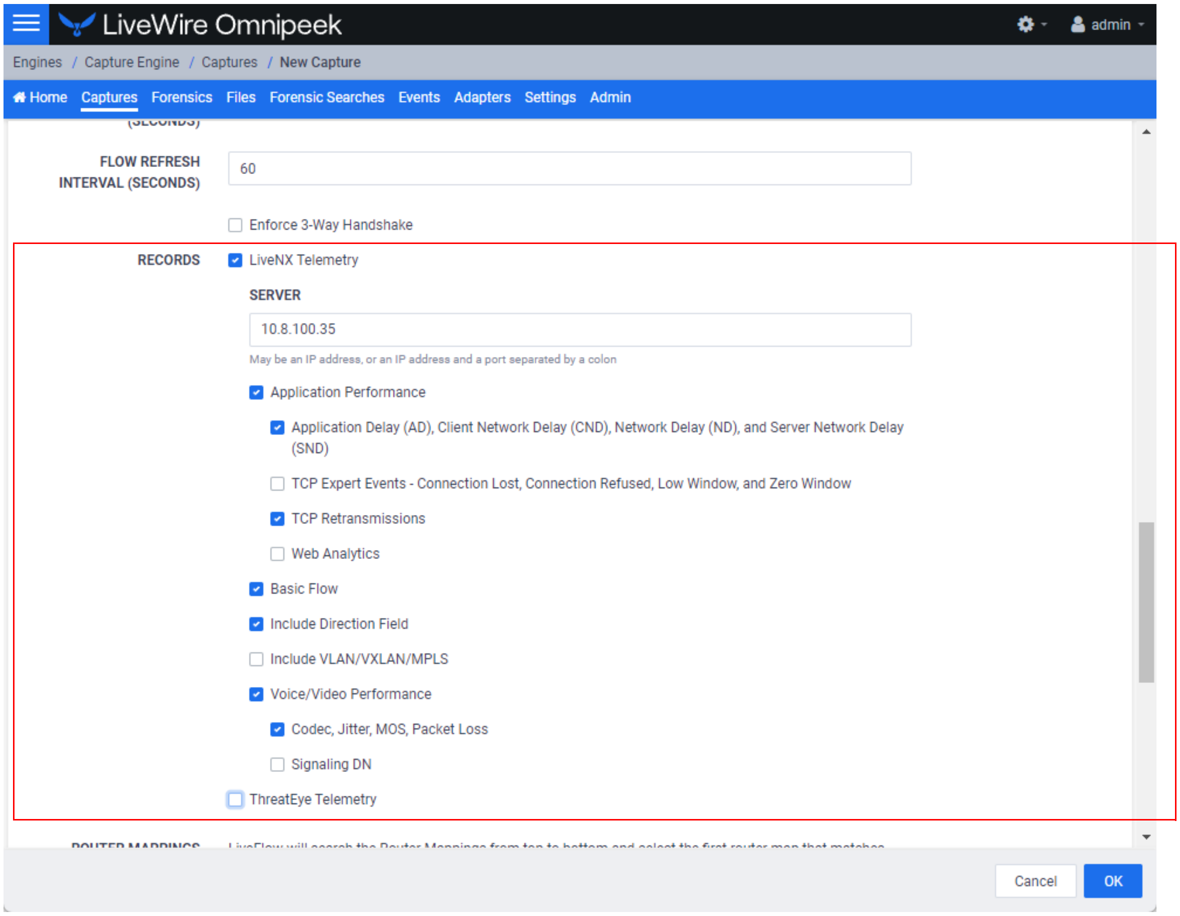
Note If you recently connected LiveWire to the network, it may take up to 600 seconds for LiveNX to see the LiveFlow data from LiveWire. You may want to adjust this setting to the desired intervals.

Flow Refresh Interval

- *Flow Refresh Interval (Seconds)*: Enter or select the number of seconds in which LiveWire generates and sends IPFIX data records to LiveNX. 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.
  - *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. If *ThreatEye Telemetry* is enabled below, then *Enforce 3-way Handshake* is automatically disabled.

Records

- *LiveNX Telemetry*: Select this option to send LiveFlow telemetry to a specific LiveNX server configured below.



(SECONDS)

FLOW REFRESH INTERVAL (SECONDS): 60

□ Enforce 3-Way Handshake

RECORDS ☑ LiveNX Telemetry

SERVER

10.8.100.35

May be an IP address, or an IP address and a port separated by a colon

☑ Application Performance

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

□ TCP Expert Events - Connection Lost, Connection Refused, Low Window, and Zero Window

☑ TCP Retransmissions

□ Web Analytics

☑ Basic Flow

☑ Include Direction Field

□ Include VLAN/VXLAN/MPLS

☑ Voice/Video Performance

☑ Codec, Jitter, MOS, Packet Loss

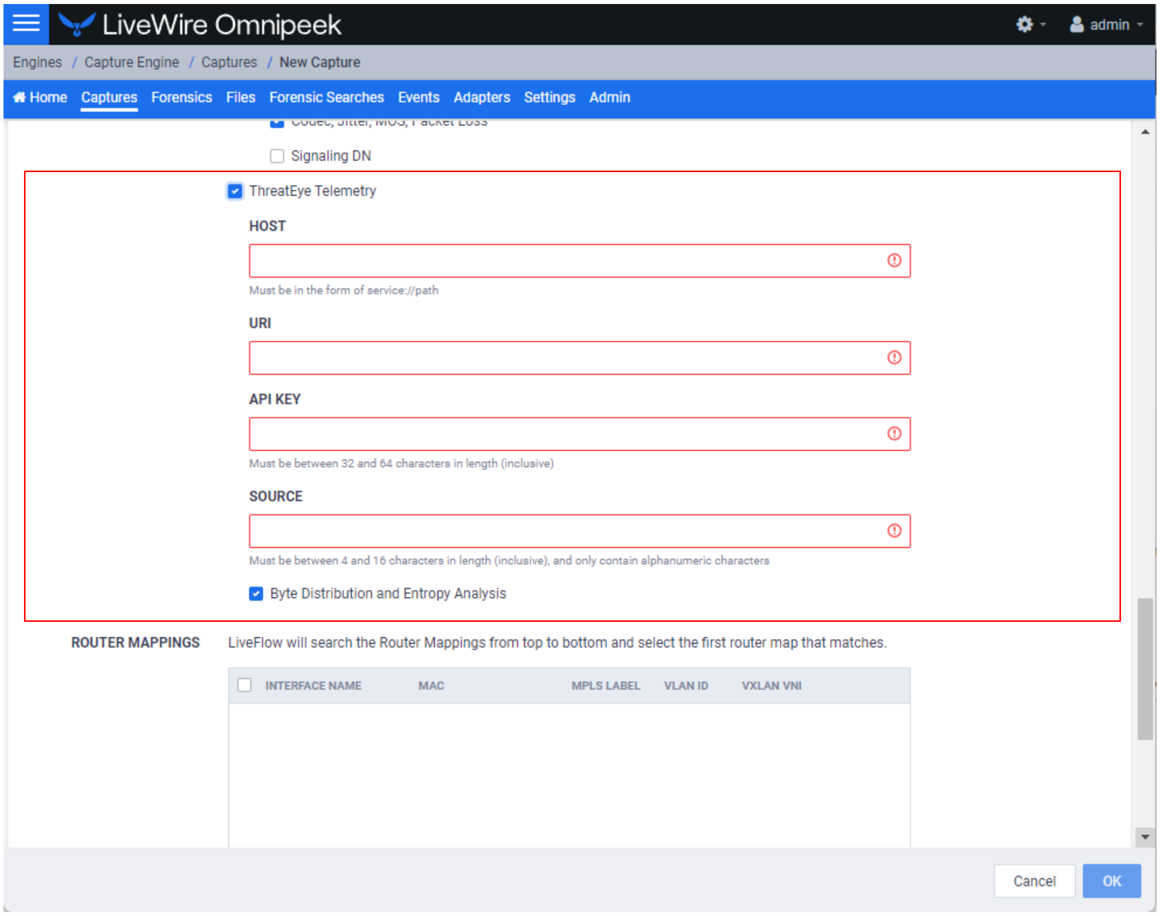
□ Signaling DN

□ ThreatEye Telemetry

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

  - *Server*: Displays the IP address of the LiveNX server receiving the LiveFlow data from LiveWire. To change the IP address, enter the IP address of the desired LiveNX server.
  - *Application Performance*: Select this option to generate AVC IPFIX records.
    - *Application Delay (AD), Client Network Delay (CND), Network Delay (ND), and Server Network Delay (SND)*: Select this option to perform and report latency analysis when AVC IPFIX records are generated.

    - *TCP Expert Events -Connection Lost, Connection Refused, Low Window, and Zero Window*: Select this option to perform TCP quality analysis (Expert) when AVC IPFIX records are generated.
    - *TCP Retransmissions*: Select this option to perform TCP retransmission analysis (Expert) when AVC IPFIX records are generated.
    - *Web Analytics*: Select this option to perform web analytics when AVC IPFIX records are generated.
      - *Decrypt Packets*: Select this option to perform decryption on HTTPS packets when *Web Analytics* is enabled.
  - *Basic Flow*: Select this option to generate FNF IPFIX records.
  - *Include Direction Field*: Select this option to send the 'flowDirection' key in unidirectional IPFIX records indicating the flow direction (0 for ingress, 1 for egress).
  - *Include VLAN/VXLAN/MPLS*: Select this option to perform MPLS, VLAN, and VXLAN analysis when AVC, FNF, or MediaNet IPFIX records are generated.
  - *Voice/Video Performance*: Select this option to generate MediaNet IPFIX records.
    - *Codec, Jitter, MOS, Packet Loss*: Select this option perform RTP analysis when MediaNet IPFIX records are generated.
    - *Signaling DN*: Select this option to generate Signaling DN IPFIX records when MediaNet IPFIX records are generated.
- *ThreatEye Telemetry*: Select this option to send LiveFlow telemetry to a specific ThreatEye host configured below.


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

☑ Codec, Jitter, MOS, Packet Loss

☐ Signaling DN

☑ ThreatEye Telemetry

HOST

Must be in the form of service://path

URI

API KEY

Must be between 32 and 64 characters in length (inclusive)

SOURCE

Must be between 4 and 16 characters in length (inclusive), and only contain alphanumeric characters

☑ Byte Distribution and Entropy Analysis

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

☐ INTERFACE NAME	MAC	MPLS LABEL	VLAN ID	VXLAN VNI

- *Host*: The *Host* (together with the *URI)* specifies the location of the ThreatEye analyzer and indicates where to send ThreatEye telemetry. The *Host* is provided by LiveAction and is made available as part of the licensing process. The *Host* must be configured if *ThreatEye Telemetry* is enabled.
- *URI*: The *URI* (together with the *Host)* specifies the location of the ThreatEye analyzer and indicates where to send ThreatEye telemetry. The *URI* is provided by LiveAction and is made available as part of the licensing process. The *URI* must be configured if *ThreatEye Telemetry* is enabled.
- *API KEY*: The *API Key* is an authentication key to access the ThreatEye server (represented by the Host and URI). The *API Key* must be between 32 and 64 characters in length.
- *SOURCE*: The *Source* is a user defined identifier that uniquely identifies data from LiveWire in the ThreatEye UI. The *Source* must be between 4 and 16 characters in length, and only contain alphanumeric characters.

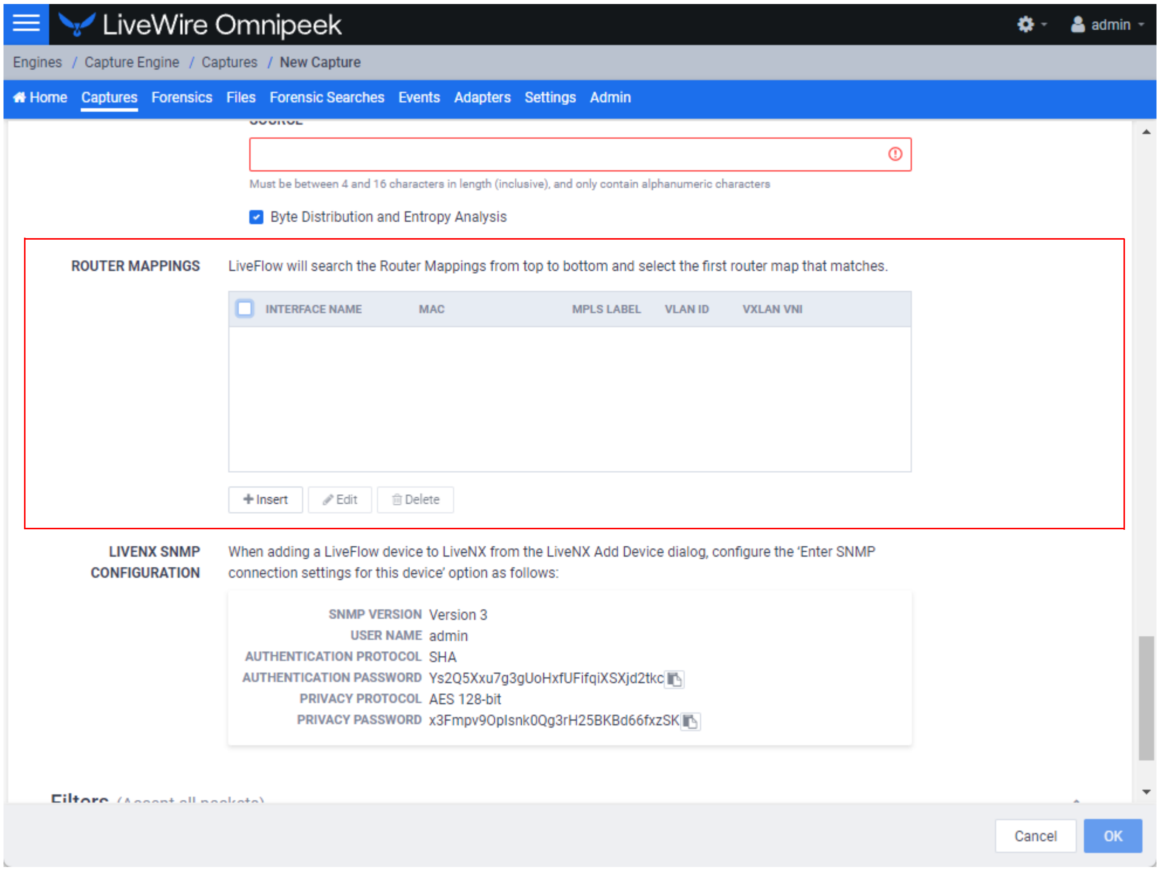
Tip A unique *Source* is recommended for each LiveWire so that they can be easily identified in ThreatEye.

- *Byte Distribution and Entropy Analysis*: Select this option to enable the collection of byte distribution and entropy analysis metadata for Encrypted Traffic Analysis (ETA). This data is used to identify malware communications in encrypted traffic.

Note You must enable a *LiveNX Telemetry* and/or *ThreatEye Telemetry* record type; otherwise, the **OK** button is disabled.

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.


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

Must be between 4 and 16 characters in length (inclusive), and only contain alphanumeric characters

☑ Byte Distribution and Entropy Analysis

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

□	INTERFACE NAME	MAC	MPLS LABEL	VLAN ID	VXLAN VNI

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	Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc
PRIVACY PROTOCOL	AES 128-bit
PRIVACY PASSWORD	x3Fmpv9OpIsnk0Qg3rH25BKBd66fxzSK

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 separated by a forward slash (e.g., *router_1/22:33:44:55:66:77*). 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.

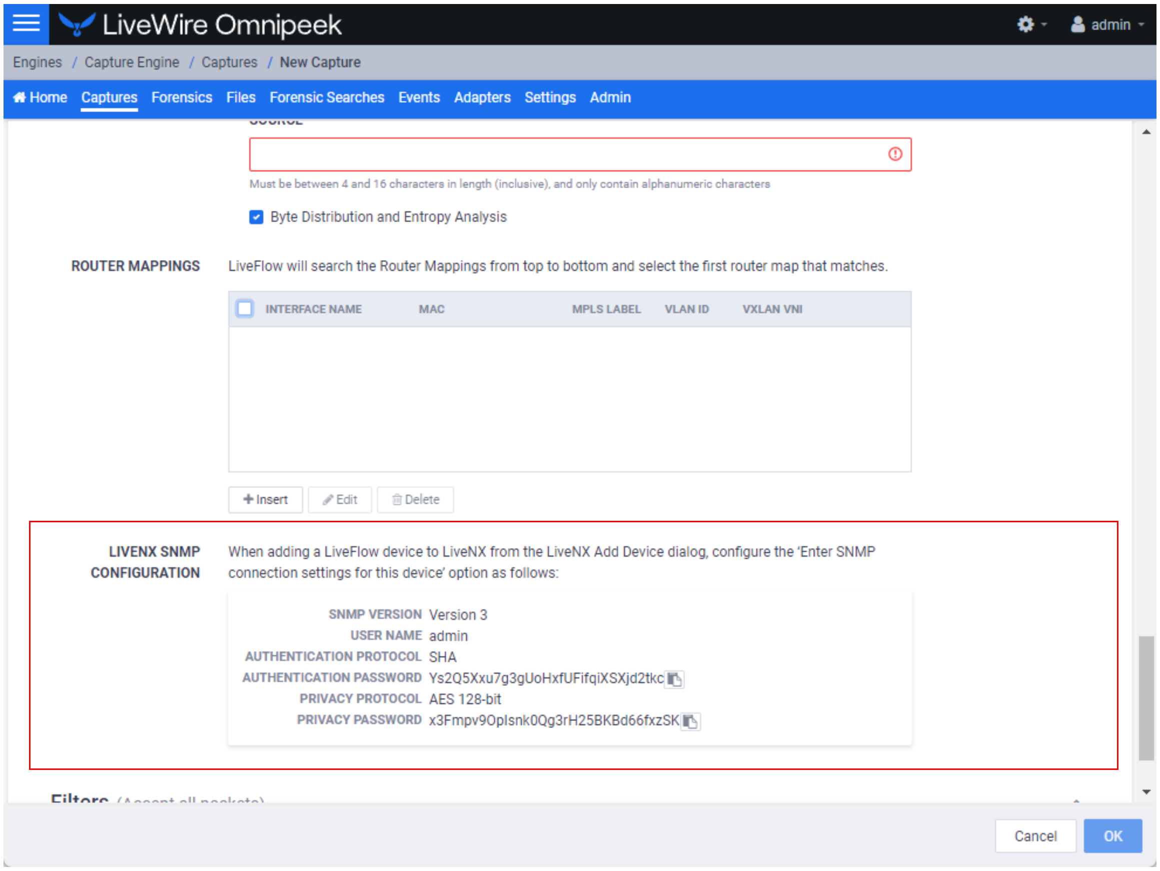
- *Interface Name:* Displays the interface name of the router. All interface names must be unique, must not be empty, must not be more than 15 characters long, and may only include the following characters: numbers, letters and an underscore (_).
- *MAC:* Displays the MAC address of the router. All MAC 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 mapping 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.


LiveWire Omnipeek
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
INTERFACE NAME
MAC
MPLS LABEL
VLAN ID
VXLAN VNI
Insert
Edit
Delete
Filters (Accept all packets)
Cancel
OK

Must be between 4 and 16 characters in length (inclusive), and only contain alphanumeric characters

☑ Byte Distribution and Entropy Analysis

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

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	Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc
PRIVACY PROTOCOL	AES 128-bit
PRIVACY PASSWORD	x3Fmpv9OpIsnk0Qg3rH25BKBd66fxzSK

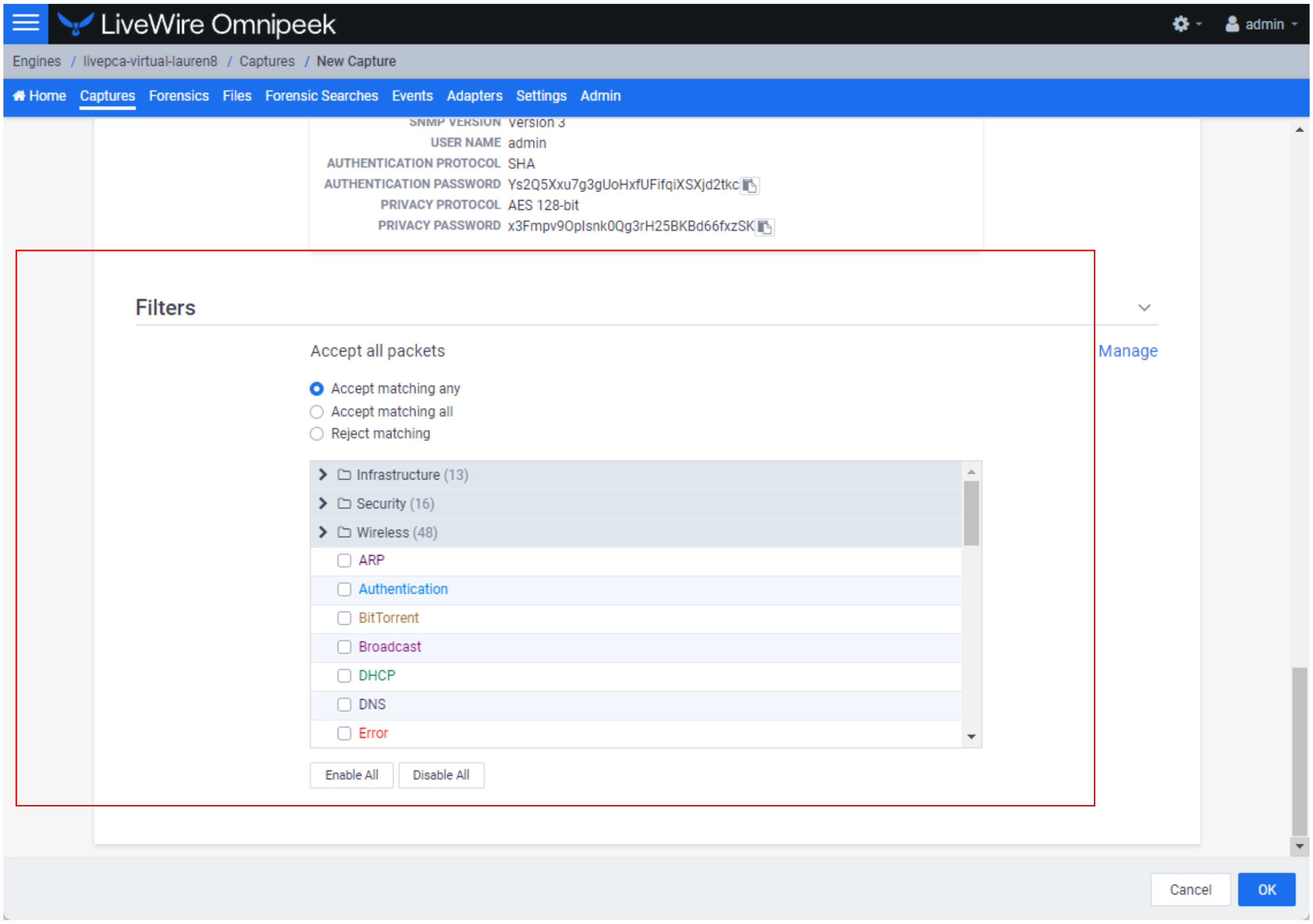
When configuring the '*Enter SNMP connection settings for this device*' option from the **Add Device** dialog in LiveNX client, configure the option as follows:

SNMP Version: **Version 3**
User Name: **admin**
Authentication Protocol: **SHA**
Authentication Password: **Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc**
Privacy Protocol: **AES 128-bit**
Privacy Password: **x3Fmpv9OpIsnk0Qg3rH25BKBd66fxzSK**

Note You can configure and change the *Authentication Password* and *Privacy Password*. See 'SNMP Credentials' in 'SNMP' on page 38.

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*.



SNMP VERSION Version 3
USER NAME admin
AUTHENTICATION PROTOCOL SHA
AUTHENTICATION PASSWORD Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc
PRIVACY PROTOCOL AES 128-bit
PRIVACY PASSWORD x3Fmpv9OpIsnk0Qg3rH25BKBd66fxzSK

Filters

Accept all packets

● Accept matching any
○ Accept matching all
○ Reject matching

- Infrastructure (13)
- Security (16)
- Wireless (48)
- □ ARP
- □ Authentication
- □ BitTorrent
- □ Broadcast
- □ DHCP
- □ DNS
- □ Error

- *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.

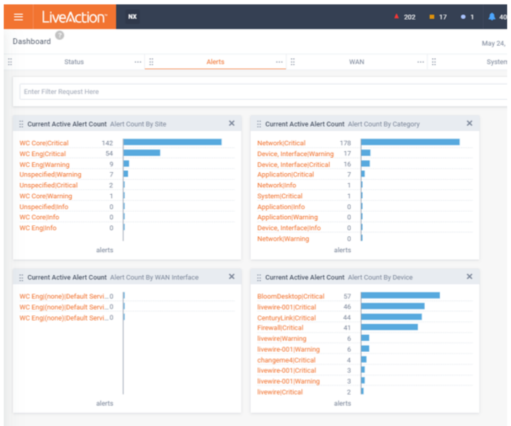
An example of using LiveWire, LiveNX, and Omnipeek

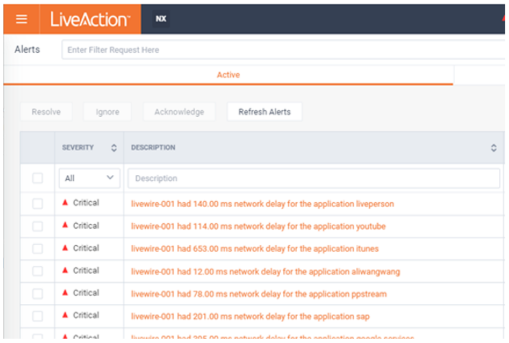
A web-based version of LiveAction's Omnipeek Network Analysis Software is available from LiveNX. You can easily start and use Omnipeek whenever you identify an interesting alert or flow in LiveNX that needs further investigation and you want to analyze the packet level details more closely in Omnipeek.

Note Omnipeek 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.

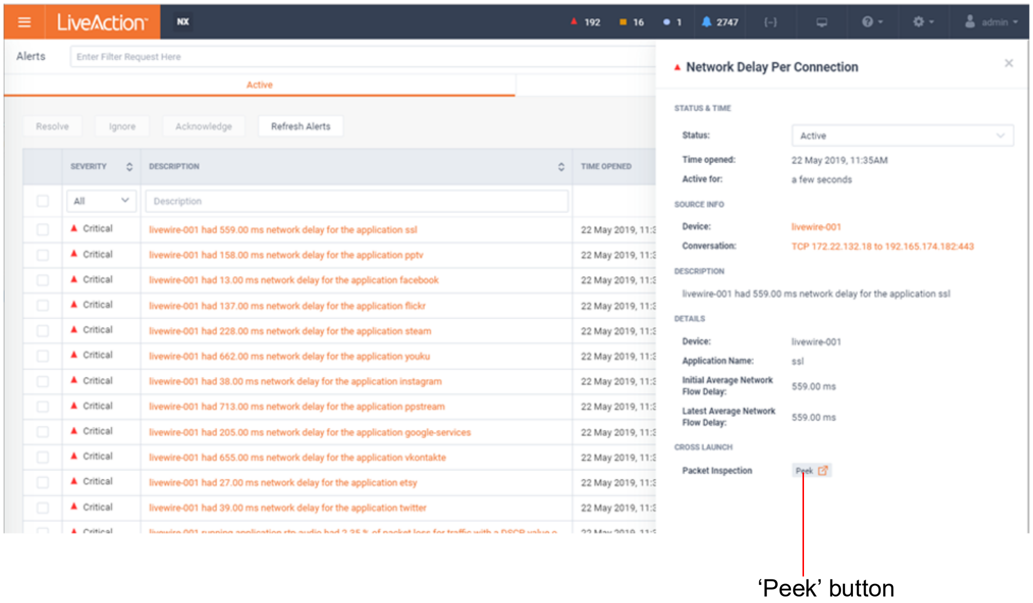
Since the user did not want to disrupt their meeting to report the issue, you find out after the call has ended that the user experienced problems. Based on the user's information, you can quickly find the flow in LiveNX and see critical metrics regarding the call, including jitter and latency. The screen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





	SEVERITY	DESCRIPTION
□	All	Description
□	▲ Critical	livewire-001 had 140.00 ms network delay for the application liveperson
□	▲ Critical	livewire-001 had 114.00 ms network delay for the application youtube
□	▲ Critical	livewire-001 had 653.00 ms network delay for the application itunes
□	▲ Critical	livewire-001 had 12.00 ms network delay for the application aliwangwang
□	▲ Critical	livewire-001 had 78.00 ms network delay for the application ppstream
□	▲ Critical	livewire-001 had 201.00 ms network delay for the application sap
□	▲ Critical	livewire-001 had 205.00 ms network delay for the application google-services

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.



	SEVERITY	DESCRIPTION	TIME OPENED
□	All	Description	
□	▲ Critical	livewire-001 had 559.00 ms network delay for the application ssl	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 158.00 ms network delay for the application pptv	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 13.00 ms network delay for the application facebook	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 137.00 ms network delay for the application flickr	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 228.00 ms network delay for the application steam	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 662.00 ms network delay for the application youku	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 38.00 ms network delay for the application instagram	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 713.00 ms network delay for the application ppstream	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 205.00 ms network delay for the application google-services	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 655.00 ms network delay for the application vkontakte	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 27.00 ms network delay for the application etsy	22 May 2019, 11:3
□	▲ Critical	livewire-001 had 39.00 ms network delay for the application twitter	22 May 2019, 11:3

▲ Network Delay Per Connection

STATUS & TIME

Status: Active

Time opened: 22 May 2019, 11:35AM

Active for: a few seconds

SOURCE INFO

Device: livewire-001

Conversation: TCP 172.22.132.18 to 192.165.174.182:443

DESCRIPTION

livewire-001 had 559.00 ms network delay for the application ssl

DETAILS

Device: livewire-001

Application Name: ssl

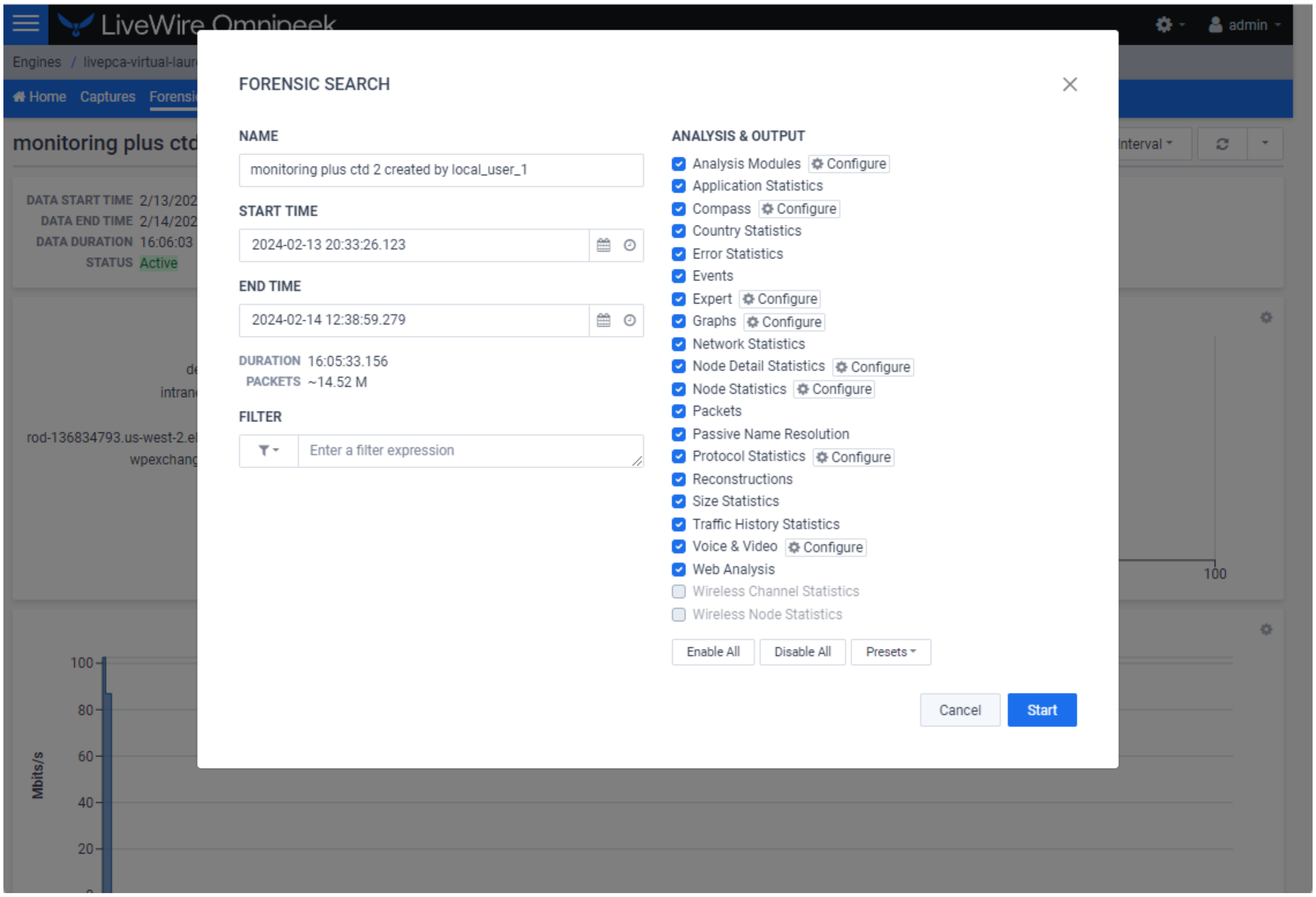
Initial Average Network Flow Delay: 559.00 ms

Latest Average Network Flow Delay: 559.00 ms

CROSS LAUNCH

Packet Inspection: Peek

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 Omnipeek and determine exactly when the jitter was bad, and correlate that with other activity on the network, to determine the root cause.



FORENSIC SEARCH

NAME

monitoring plus ctd 2 created by local_user_1

START TIME

2024-02-13 20:33:26.123

END TIME

2024-02-14 12:38:59.279

DURATION 16:05:33.156

PACKETS ~14.52 M

FILTER

Enter a filter expression

ANALYSIS & OUTPUT

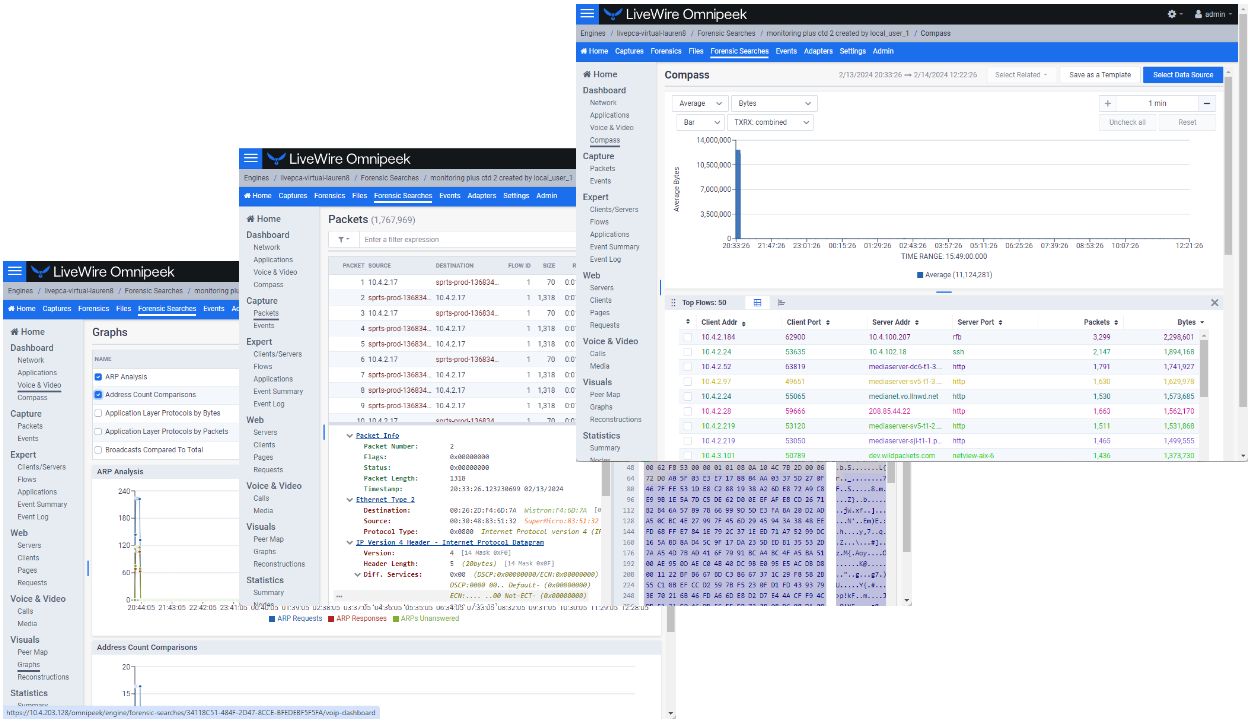
- ☑ Analysis Modules ⚙ Configure
- ☑ Application Statistics
- ☑ Compass ⚙ Configure
- ☑ Country Statistics
- ☑ Error Statistics
- ☑ Events
- ☑ Expert ⚙ Configure
- ☑ Graphs ⚙ Configure
- ☑ Network Statistics
- ☑ Node Detail Statistics ⚙ Configure
- ☑ Node Statistics ⚙ Configure
- ☑ Packets
- ☑ Passive Name Resolution
- ☑ Protocol Statistics ⚙ Configure
- ☑ Reconstructions
- ☑ Size Statistics
- ☑ Traffic History Statistics
- ☑ Voice & Video ⚙ Configure
- ☑ Web Analysis
- □ Wireless Channel Statistics
- □ Wireless Node Statistics

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 Omnipeek, 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 Omnipeek which are good places to start understanding the problem as well as drill-down to the packets view.



Top Flows: 50

Client Addr	Client Port	Server Addr	Server Port	Packets	Bytes
10.4.2.184	62900	10.4.100.207	rfb	3,299	2,298,601
10.4.2.24	53635	10.4.102.18	ssh	2,147	1,894,168
10.4.2.52	63819	mediaserver-dc6-t1-3....	http	1,791	1,741,927
10.4.2.97	49651	mediaserver-sv5-t1-3....	http	1,630	1,629,978
10.4.2.24	55065	medianet.vo.llnwd.net	http	1,530	1,573,685
10.4.2.28	59666	208.85.44.22	http	1,663	1,562,170
10.4.2.219	53120	mediaserver-sv5-t1-2....	http	1,511	1,531,868
10.4.2.219	53050	mediaserver-sjl-t1-1.p...	http	1,465	1,499,555
10.4.3.101	50789	dev.wildpackets.com	netview-aix-6	1,436	1,373,730

Packets (1,767,969)

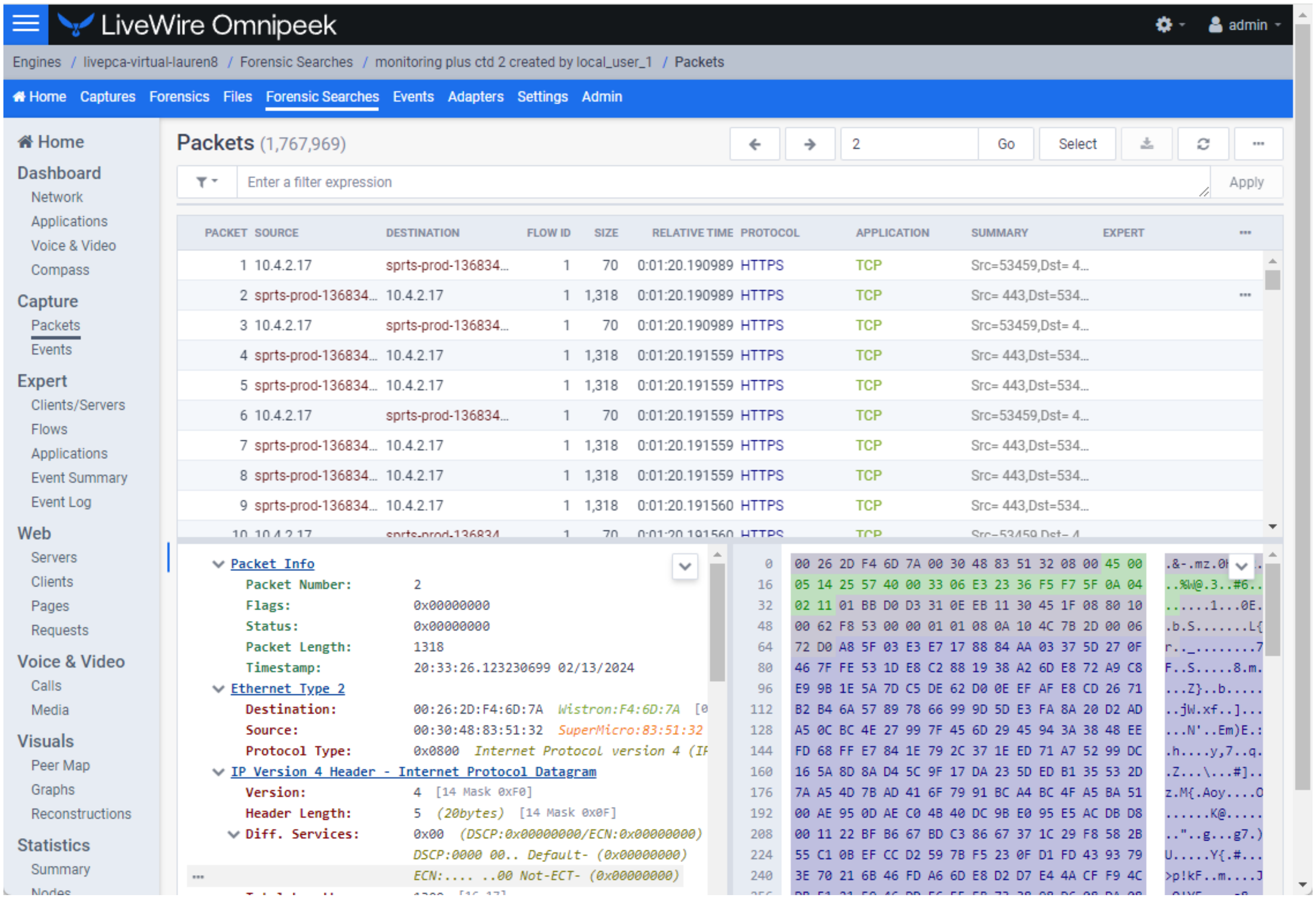
Enter a filter expression

PACKET	SOURCE	DESTINATION	FLOW ID	SIZE
1	10.4.2.17	sprts-prod-136834...	1	70
2	sprts-prod-136834...	10.4.2.17	1	1,318
3	10.4.2.17	sprts-prod-136834...	1	70
4	sprts-prod-136834...	10.4.2.17	1	1,318
5	sprts-prod-136834...	10.4.2.17	1	1,318
6	10.4.2.17	sprts-prod-136834...	1	70
7	sprts-prod-136834...	10.4.2.17	1	1,318
8	sprts-prod-136834...	10.4.2.17	1	1,318
9	sprts-prod-136834...	10.4.2.17	1	1,318

```
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
  Source:           00:30:48:83:51:32  SuperMicro:83:51:32
  Protocol Type:    0x0800  Internet Protocol version 4
IP Version 4 Header - Internet Protocol Datagram
  Version:          4
  Header Length:    5  (20bytes)
  Diff. Services:   0x00
```

https://10.4.203.128/omnipeek/engine/forensic-searches/34118C51-484F-2D47-8CCE-BFEDEBF5F5FA/voip-dashboard

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



Packets (1,767,969)

2

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 0x0F]
  Diff. Services:         0x00  (DSCP:0x00000000/ECN:0x00000000)
                          DSCP:0000 00.. Default- (0x00000000)
                          ECN:.... ..00 Not-ECT- (0x00000000)
```

```
  0  00 26 2D F4 6D 7A 00 30 48 83 51 32 08 00 45 00   .&-.mz.0
 16  05 14 25 57 40 00 33 06 E3 23 36 F5 F7 5F 0A 04   ..%W@.3..#6..
 32  02 11 01 BB D0 D3 31 0E EB 11 30 45 1F 08 80 10   ......1...0E.
 48  00 62 F8 53 00 00 01 01 08 0A 10 4C 7B 2D 00 06   .b.S.......L{
 64  72 D0 A8 5F 03 E3 E7 17 88 84 AA 03 37 5D 27 0F   r.._........7
 80  46 7F FE 53 1D E8 C2 88 19 38 A2 6D E8 72 A9 C8   F..S.....8.m.
 96  E9 9B 1E 5A 7D C5 DE 62 D0 0E EF AF E8 CD 26 71   ...Z}..b.....
112  B2 B4 6A 57 89 78 66 99 9D 5D E3 FA 8A 20 D2 AD   ..jW.xf..]...
128  A5 0C BC 4E 27 99 7F 45 6D 29 45 94 3A 38 48 EE   ...N'..Em)E.:
144  FD 68 FF E7 84 1E 79 2C 37 1E ED 71 A7 52 99 DC   .h....y,7..q.
160  16 5A 8D 8A D4 5C 9F 17 DA 23 5D ED B1 35 53 2D   .Z...\...#]..
176  7A A5 4D 7B AD 41 6F 79 91 BC A4 BC 4F A5 BA 51   z.M{.Aoy....O
192  00 AE 95 0D AE C0 4B 40 DC 9B E0 95 E5 AC DB D8   ......K@.....
208  00 11 22 BF B6 67 BD C3 86 67 37 1C 29 F8 58 2B   .."..g...g7.)
224  55 C1 0B EF CC D2 59 7B F5 23 0F D1 FD 43 93 79   U.....Y{.#...
240  3E 70 21 6B 46 FD A6 6D E8 D2 D7 E4 4A CF F9 4C   >p!kF..m....J
```

CHAPTER 4

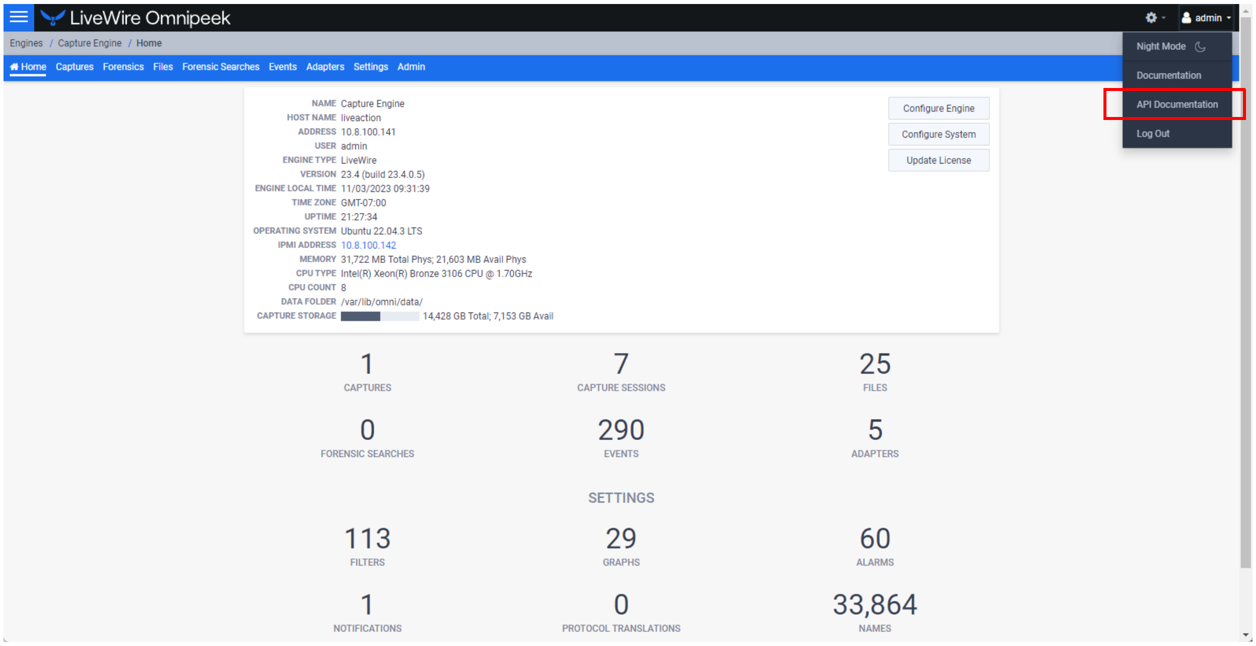
Creating and Managing API Tokens

In this chapter:

About API Tokens

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



NAME	Capture Engine
HOST NAME	liveaction
ADDRESS	10.8.100.141
USER	admin
ENGINE TYPE	LiveWire
VERSION	23.4 (build 23.4.0.5)
ENGINE LOCAL TIME	11/03/2023 09:31:39
TIME ZONE	GMT-07:00
UPTIME	21:27:34
OPERATING SYSTEM	Ubuntu 22.04.3 LTS
IPMI ADDRESS	10.8.100.142
MEMORY	31,722 MB Total Phys; 21,603 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; 7,153 GB Avail

1 CAPTURES	7 CAPTURE SESSIONS	25 FILES
0 FORENSIC SEARCHES	290 EVENTS	5 ADAPTERS

SETTINGS

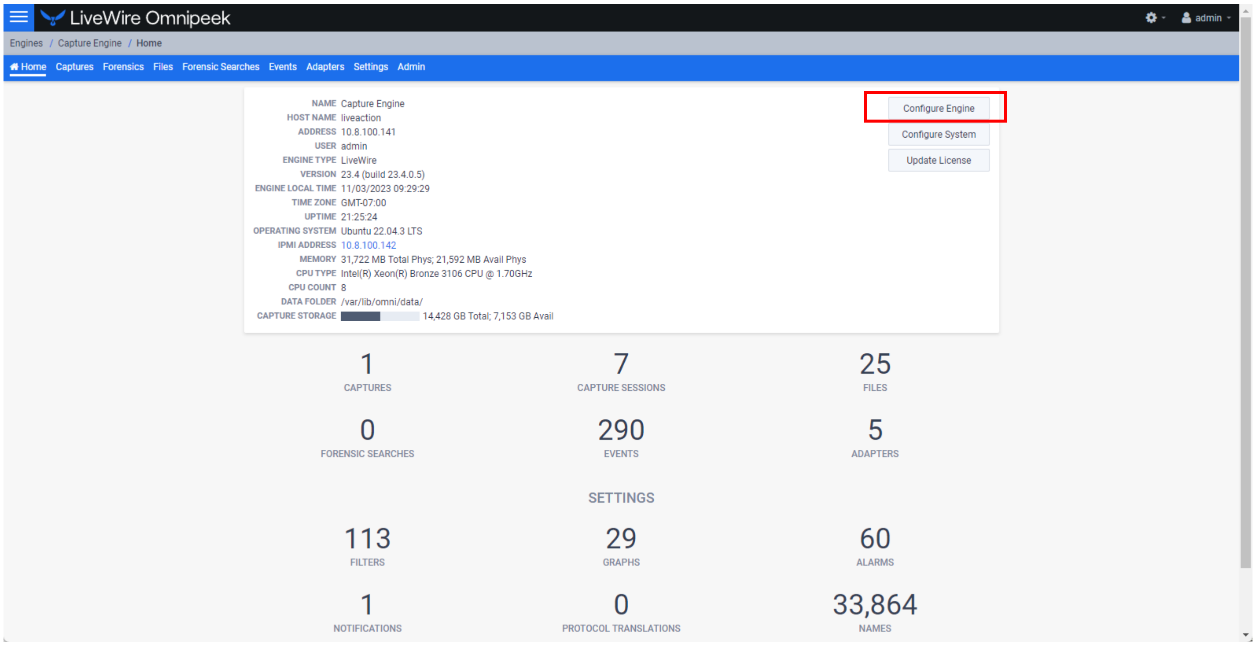
113 FILTERS	29 GRAPHS	60 ALARMS
1 NOTIFICATIONS	0 PROTOCOL TRANSLATIONS	33,864 NAMES

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. Use Omnipeek to view the *Home* page.


LiveWire Omnipeek
admin
Engines / Capture Engine / Home
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Configure Engine
Configure System
Update License

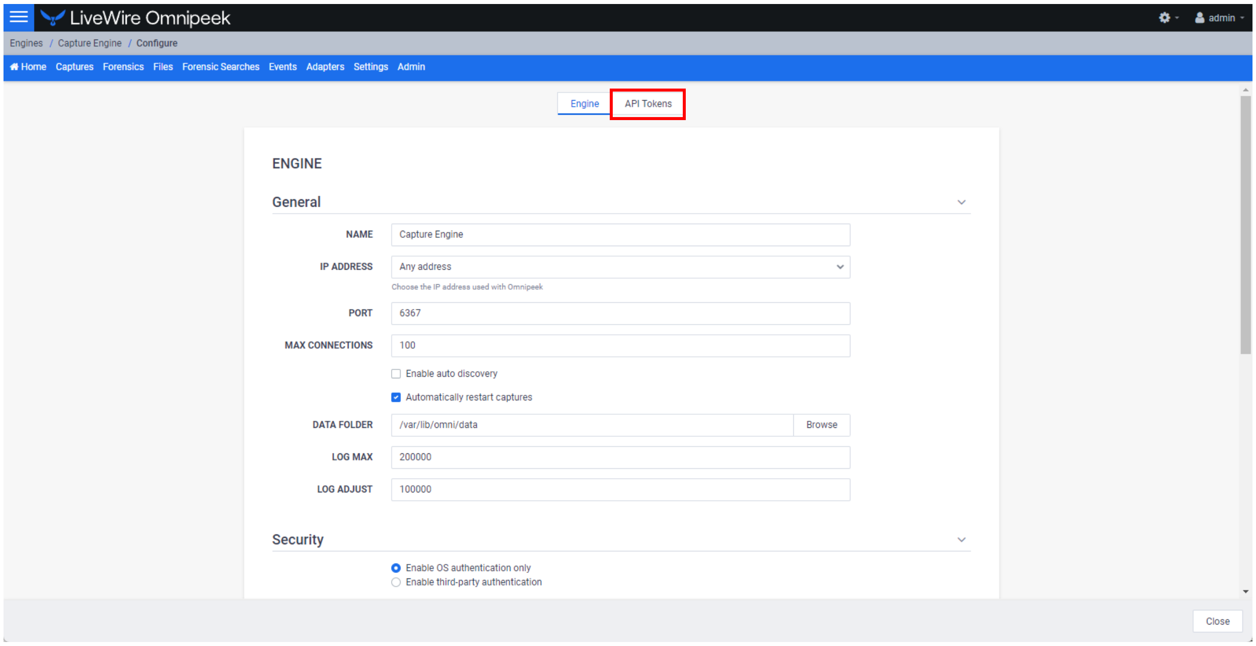
NAME Capture Engine
HOST NAME liveaction
ADDRESS 10.8.100.141
USER admin
ENGINE TYPE LiveWire
VERSION 23.4 (build 23.4.0.5)
ENGINE LOCAL TIME 11/03/2023 09:29:29
TIME ZONE GMT-07:00
UPTIME 21:25:24
OPERATING SYSTEM Ubuntu 22.04.3 LTS
IPMI ADDRESS 10.8.100.142
MEMORY 31,722 MB Total Phys; 21,592 MB Avail 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; 7,153 GB Avail

1 CAPTURES	7 CAPTURE SESSIONS	25 FILES
0 FORENSIC SEARCHES	290 EVENTS	5 ADAPTERS

SETTINGS

113 FILTERS	29 GRAPHS	60 ALARMS
1 NOTIFICATIONS	0 PROTOCOL TRANSLATIONS	33,864 NAMES

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


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
Browse
Close

ENGINE

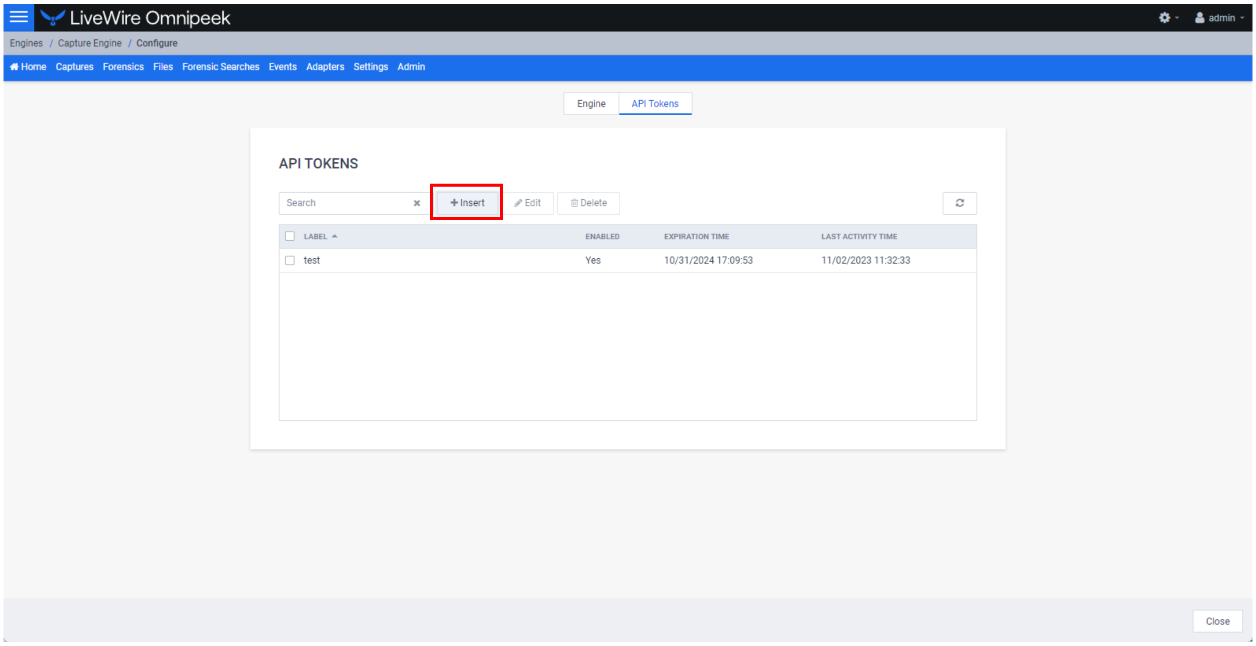
General

NAME Capture Engine
IP ADDRESS Any address
Choose the IP address used with Omnipeek
PORT 6367
MAX CONNECTIONS 100
☐ Enable auto discovery
☑ Automatically restart captures
DATA FOLDER /var/lib/omni/data
LOG MAX 200000
LOG ADJUST 100000

Security

● Enable OS authentication only
○ Enable third-party authentication

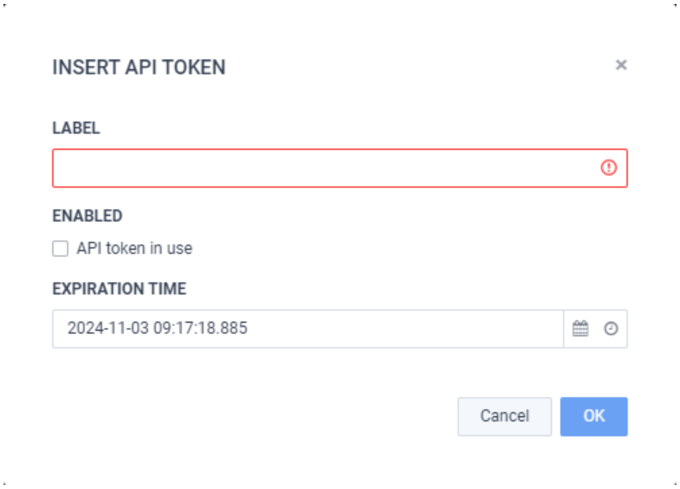
3. Click **API Tokens**. The *API Tokens* page appears.


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
Search
+ Insert
Edit
Delete
Close

API TOKENS

□	LABEL	ENABLED	EXPIRATION TIME	LAST ACTIVITY TIME
□	test	Yes	10/31/2024 17:09:53	11/02/2023 11:32:33

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



LABEL

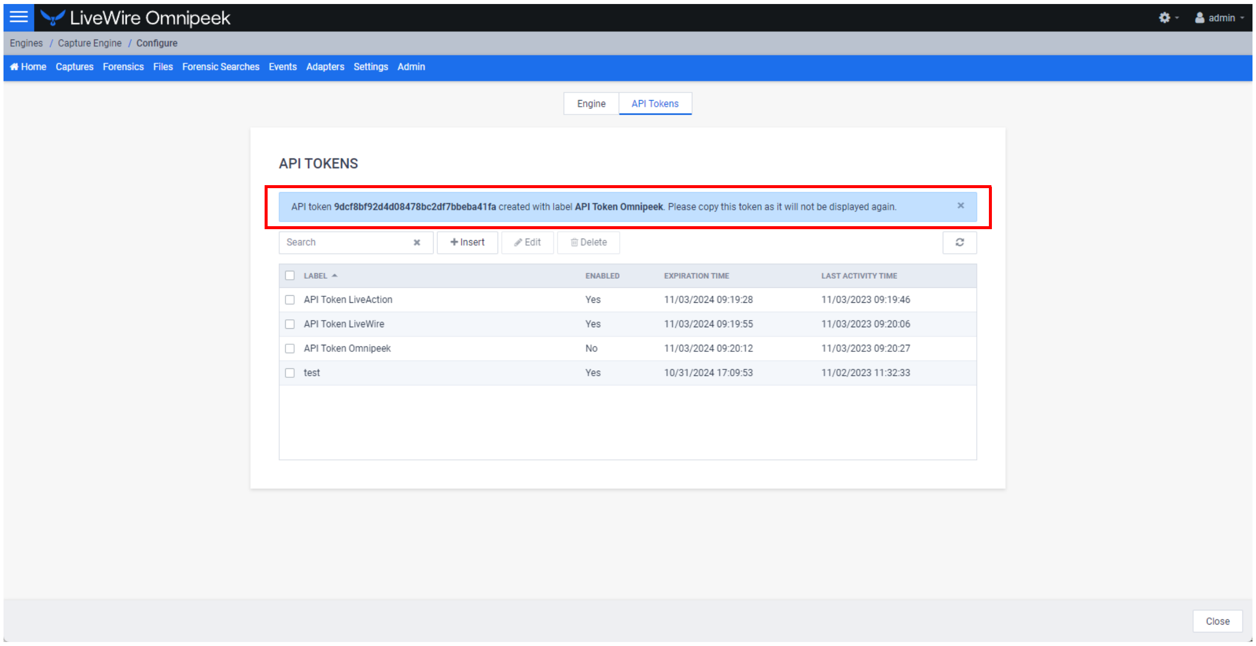
ENABLED

□ API token in use

EXPIRATION TIME

2024-11-03 09:17:18.885

5. 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.
6. 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.


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
Search
Insert
Edit
Delete
Close

API TOKENS

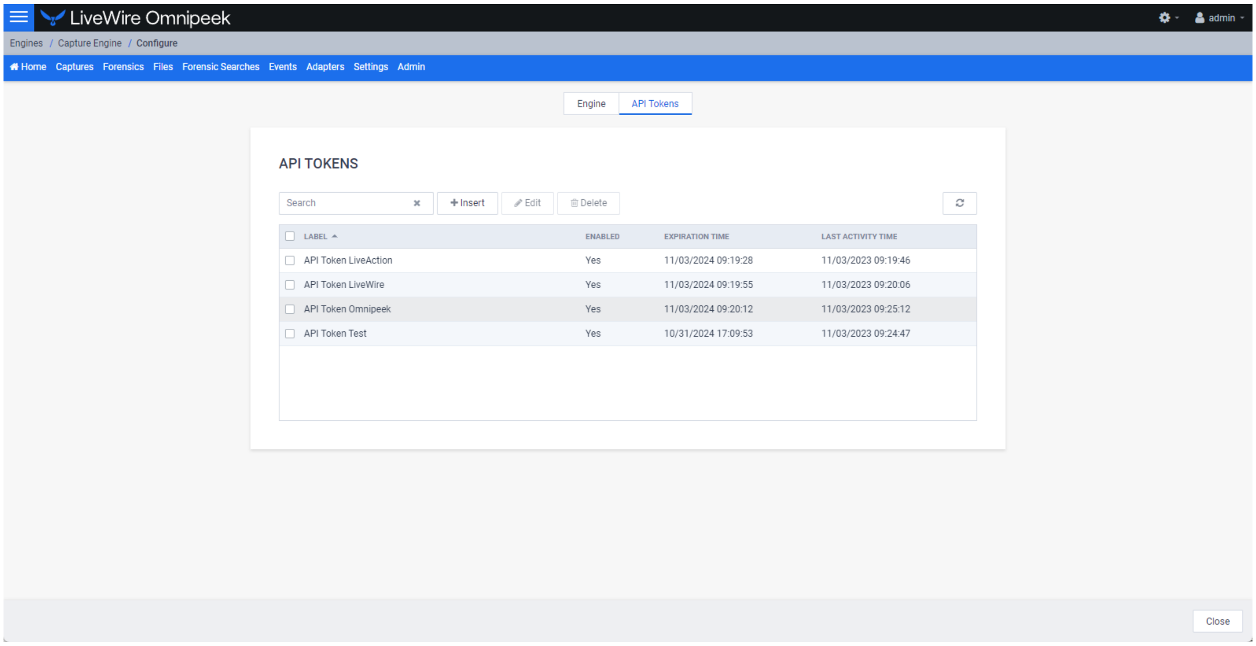
API token **9dcf8bf92d4d08478bc2df7bbeba41fa** created with label **API Token Omnipeek**. Please copy this token as it will not be displayed again.

□	LABEL	ENABLED	EXPIRATION TIME	LAST ACTIVITY TIME
□	API Token LiveAction	Yes	11/03/2024 09:19:28	11/03/2023 09:19:46
□	API Token LiveWire	Yes	11/03/2024 09:19:55	11/03/2023 09:20:06
□	API Token Omnipeek	No	11/03/2024 09:20:12	11/03/2023 09:20:27
□	test	Yes	10/31/2024 17:09:53	11/02/2023 11:32:33

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.


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
Search
Insert
Edit
Delete
Close

API TOKENS

□	LABEL	ENABLED	EXPIRATION TIME	LAST ACTIVITY TIME
□	API Token LiveAction	Yes	11/03/2024 09:19:28	11/03/2023 09:19:46
□	API Token LiveWire	Yes	11/03/2024 09:19:55	11/03/2023 09:20:06
□	API Token Omnipeek	Yes	11/03/2024 09:20:12	11/03/2023 09:25:12
□	API Token Test	Yes	10/31/2024 17:09:53	11/03/2023 09:24:47

- *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 108.
- *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

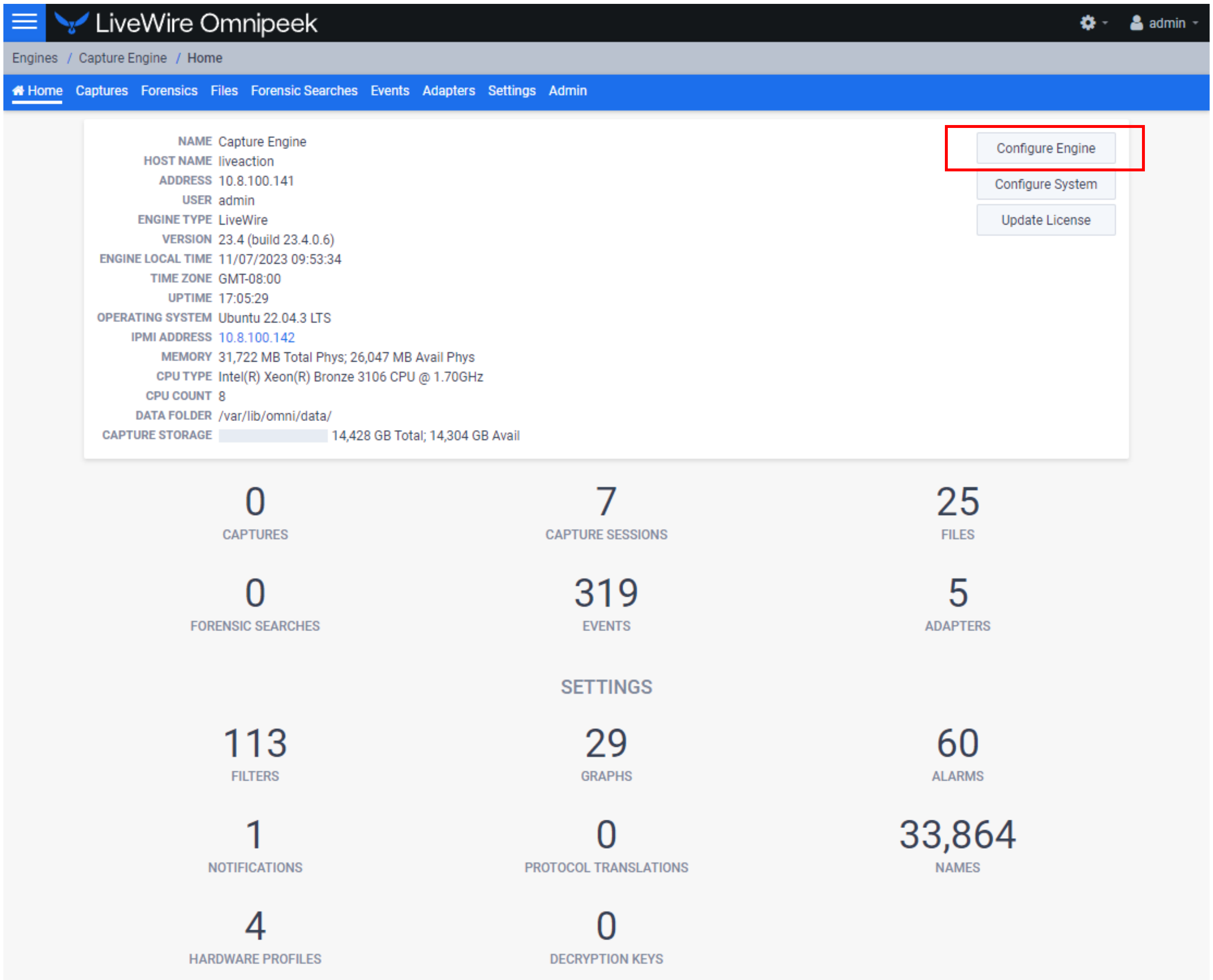
The Access Control List (ACL) feature in LiveWire provides the ability to restrict access of predefined actions to a particular set of roles and users. This allows users to be given different privileges for when they are using LiveWire. These predefined actions are called policies. A full list of these policies are described in 'Policy Descriptions' on page 120, To learn about roles, see 'About Roles' on page 118. To manage users and groups assigned to the roles, see 'Manage Users for Roles' on page 122 and 'Manage Groups for Roles' on page 123.

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.



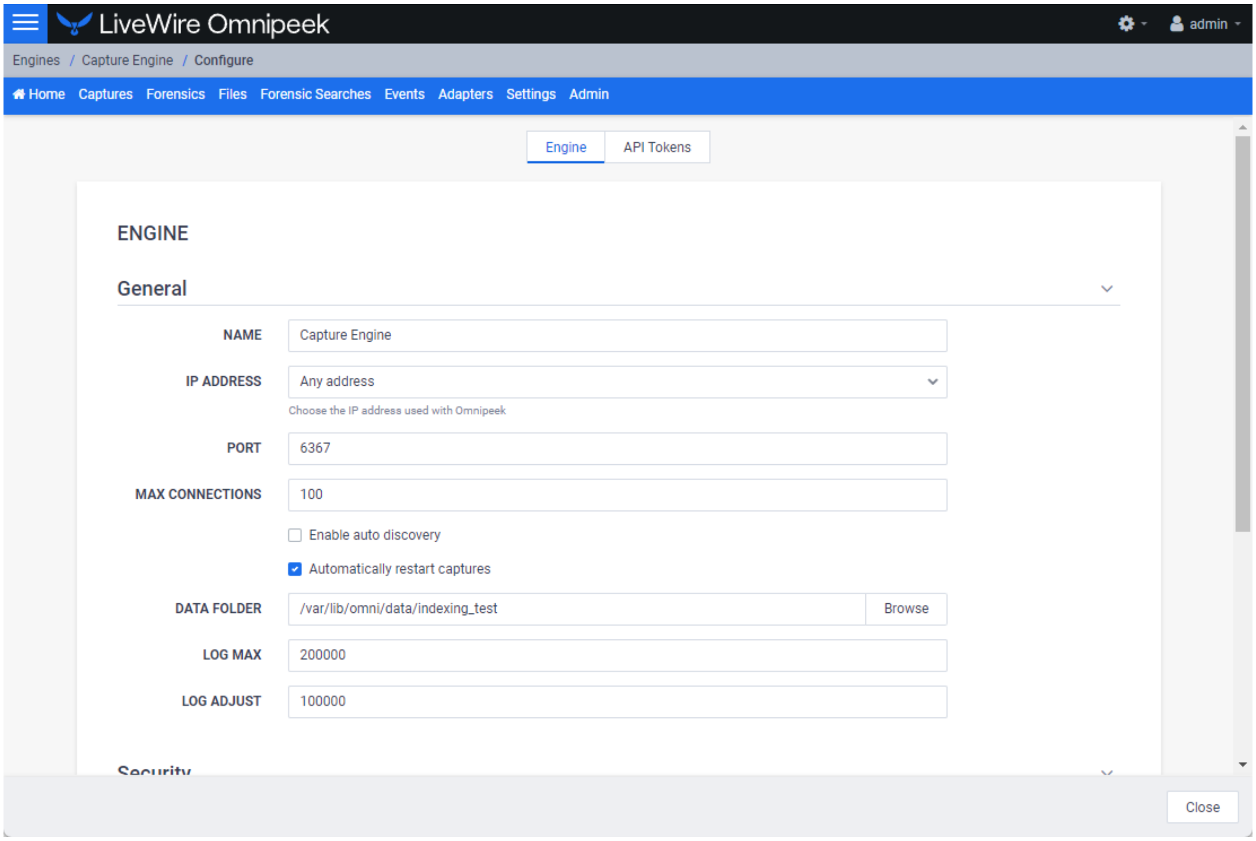
NAME Capture Engine
HOST NAME liveaction
ADDRESS 10.8.100.141
USER admin
ENGINE TYPE LiveWire
VERSION 23.4 (build 23.4.0.6)
ENGINE LOCAL TIME 11/07/2023 09:53:34
TIME ZONE GMT-08:00
UPTIME 17:05:29
OPERATING SYSTEM Ubuntu 22.04.3 LTS
IPMI ADDRESS 10.8.100.142
MEMORY 31,722 MB Total Phys; 26,047 MB Avail 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

0 CAPTURES
7 CAPTURE SESSIONS
25 FILES
0 FORENSIC SEARCHES
319 EVENTS
5 ADAPTERS

SETTINGS

113 FILTERS
29 GRAPHS
60 ALARMS
1 NOTIFICATIONS
0 PROTOCOL TRANSLATIONS
33,864 NAMES
4 HARDWARE PROFILES
0 DECRYPTION KEYS

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


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
Browse
Close

ENGINE

General

NAME: Capture Engine

IP ADDRESS: Any address

Choose the IP address used with Omnipeek

PORT: 6367

MAX CONNECTIONS: 100

☐ Enable auto discovery

☑ Automatically restart captures

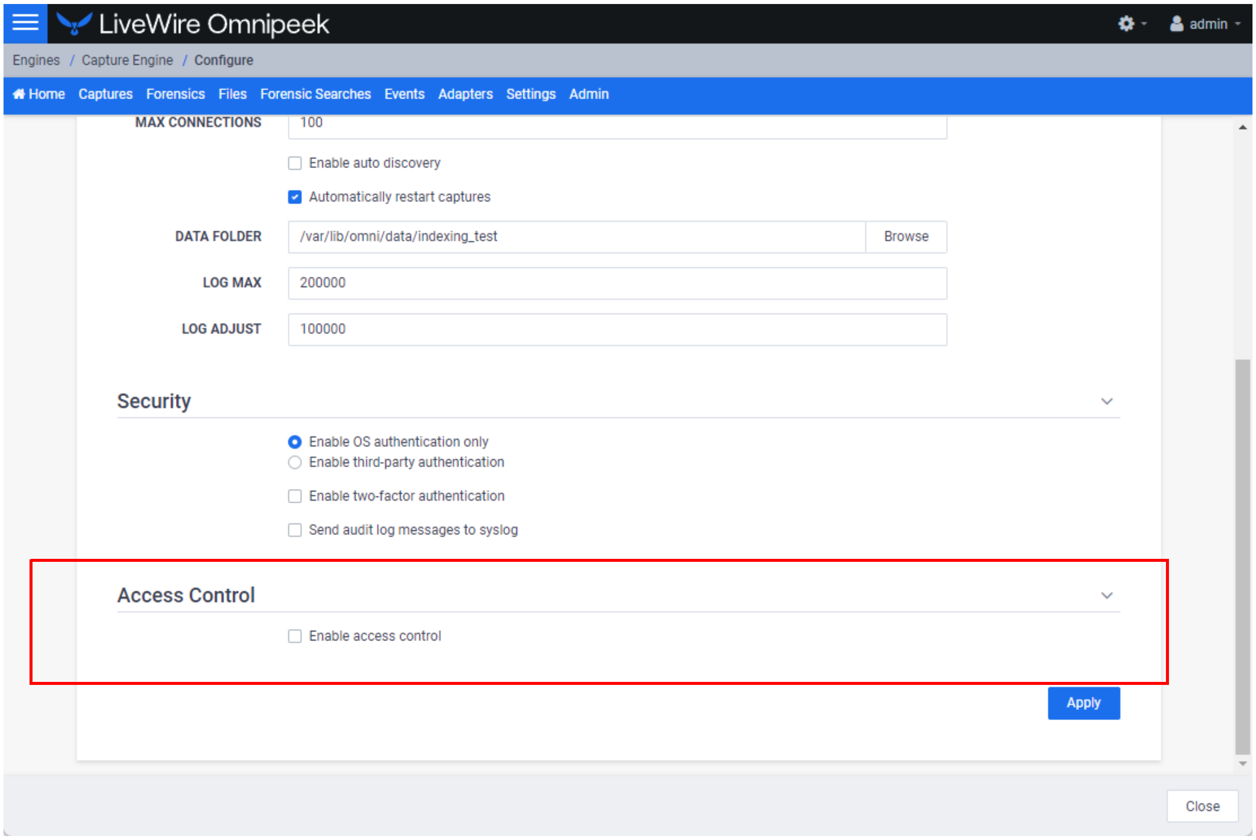
DATA FOLDER: /var/lib/omni/data/indexing_test

LOG MAX: 200000

LOG ADJUST: 100000

Security

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


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Browse
Apply
Close

MAX CONNECTIONS: 100

☐ Enable auto discovery

☑ Automatically restart captures

DATA FOLDER: /var/lib/omni/data/indexing_test

LOG MAX: 200000

LOG ADJUST: 100000

Security

● Enable OS authentication only
○ Enable third-party authentication

☐ Enable two-factor authentication

☐ Send audit log messages to syslog

Access Control

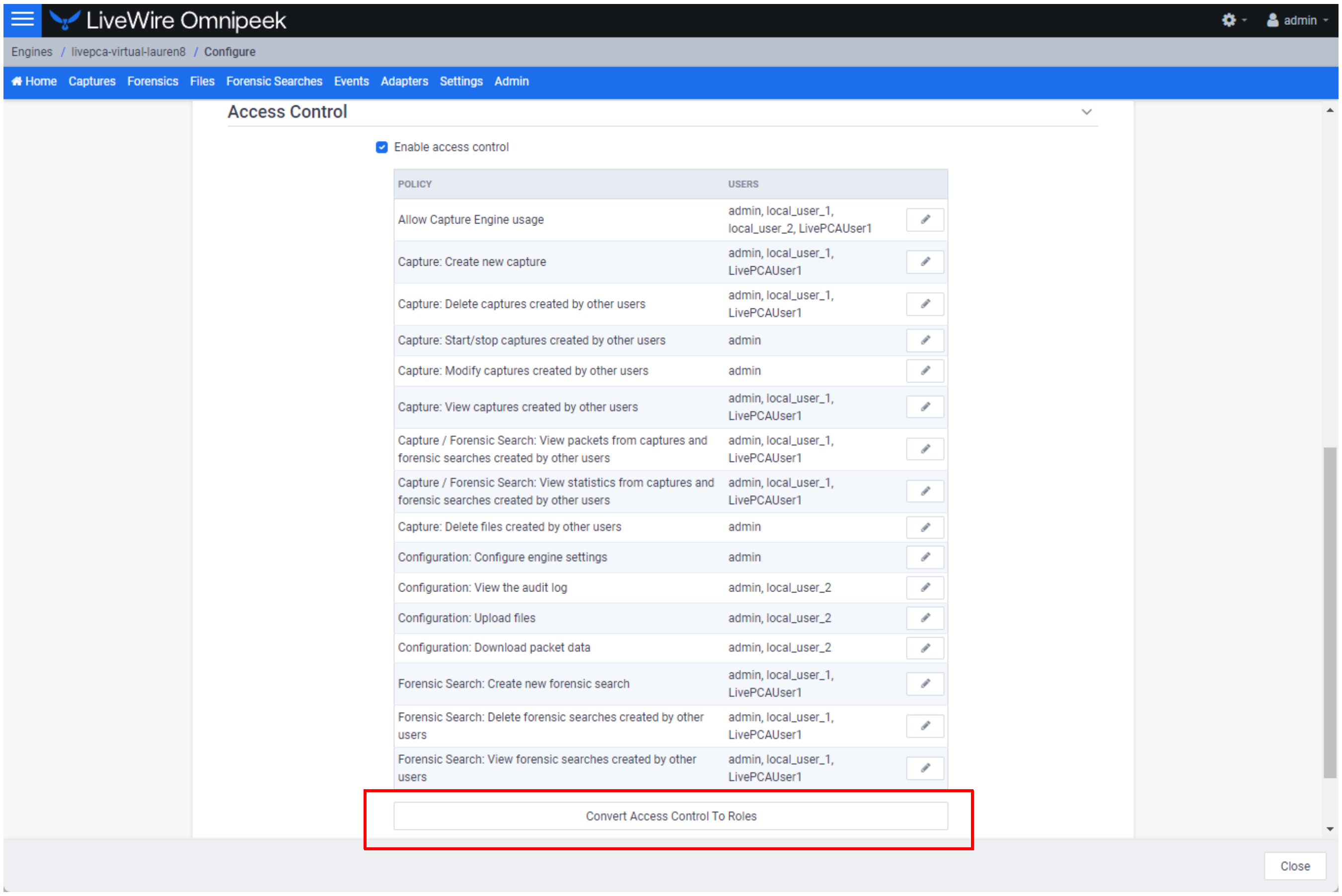
☐ Enable access control

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:

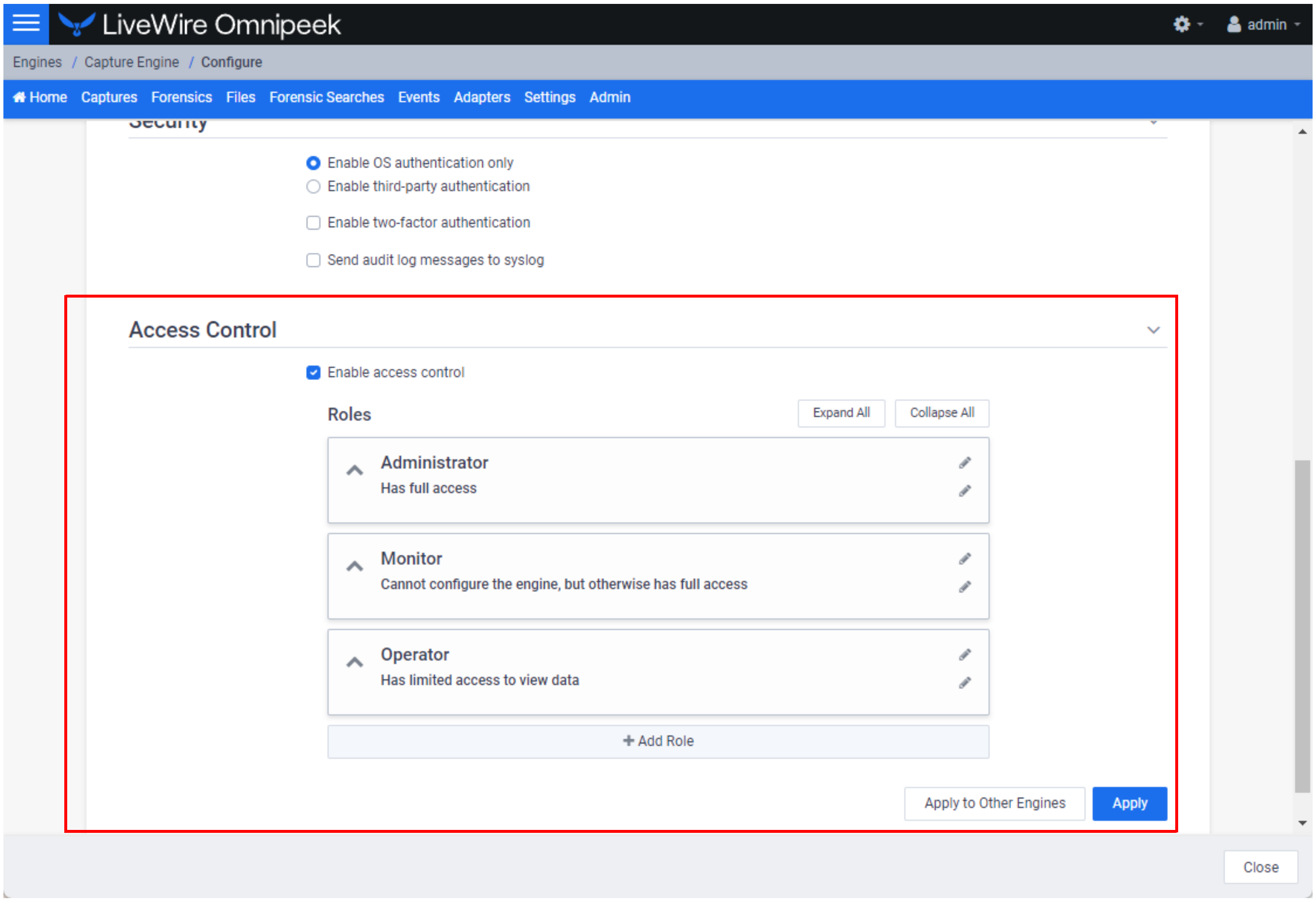

LiveWire Omnipeek
admin
Engines / livepca-virtual-lauren8 / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin

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

Role-based access control settings:



● 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

- *Enable access control*: Select this setting to enable access control.
- *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.
- *Add Role*: Click to add a new role to the list of roles. You will need to provide a unique name for the role.

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

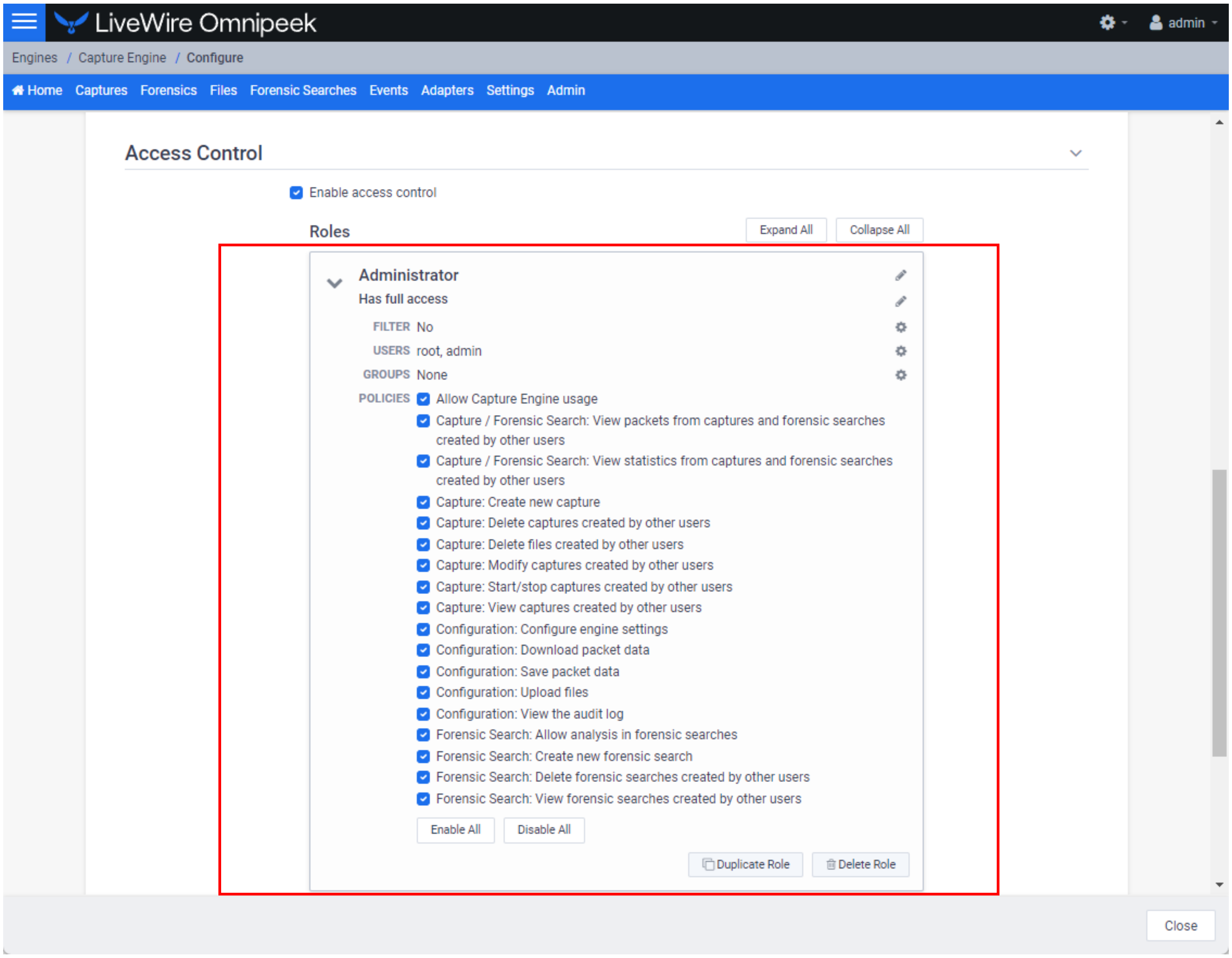
Roles are a collection of pre-defined policies for specific actions within LiveWire. For each role, one or more Polices are selected, and users or Active Directory groups are assigned. LiveWire includes a default set of roles (*Administrator*, *Monitor*, and *Operator*), with each providing a unique 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 121.
- *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 123.
- *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 120.

Configuring Roles

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


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Expand All
Collapse All
Enable All
Disable All
Duplicate Role
Delete Role
Close

Access Control

☑ Enable access control

Roles

Administrator

Has full access

FILTER No

USERS root, admin

GROUPS None

POLICIES
- ☑ Allow Capture Engine usage
- ☑ Capture / Forensic Search: View packets from captures and forensic searches created by other users
- ☑ Capture / Forensic Search: View statistics from captures and forensic searches created by other users
- ☑ Capture: Create new capture
- ☑ Capture: Delete captures created by other users
- ☑ Capture: Delete files created by other users
- ☑ Capture: Modify captures created by other users
- ☑ Capture: Start/stop captures created by other users
- ☑ Capture: View captures created by other users
- ☑ Configuration: Configure engine settings
- ☑ Configuration: Download packet data
- ☑ Configuration: Save packet data
- ☑ Configuration: Upload files
- ☑ Configuration: View the audit log
- ☑ Forensic Search: Allow analysis in forensic searches
- ☑ Forensic Search: Create new forensic search
- ☑ Forensic Search: Delete forensic searches created by other users
- ☑ Forensic Search: View forensic searches created by other users

- *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 121. 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 122.
- *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 123.
- *Policies*: Select one or more policies associated with a role. See also 'Policy Descriptions' on page 120.
- *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 polices 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 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 122.

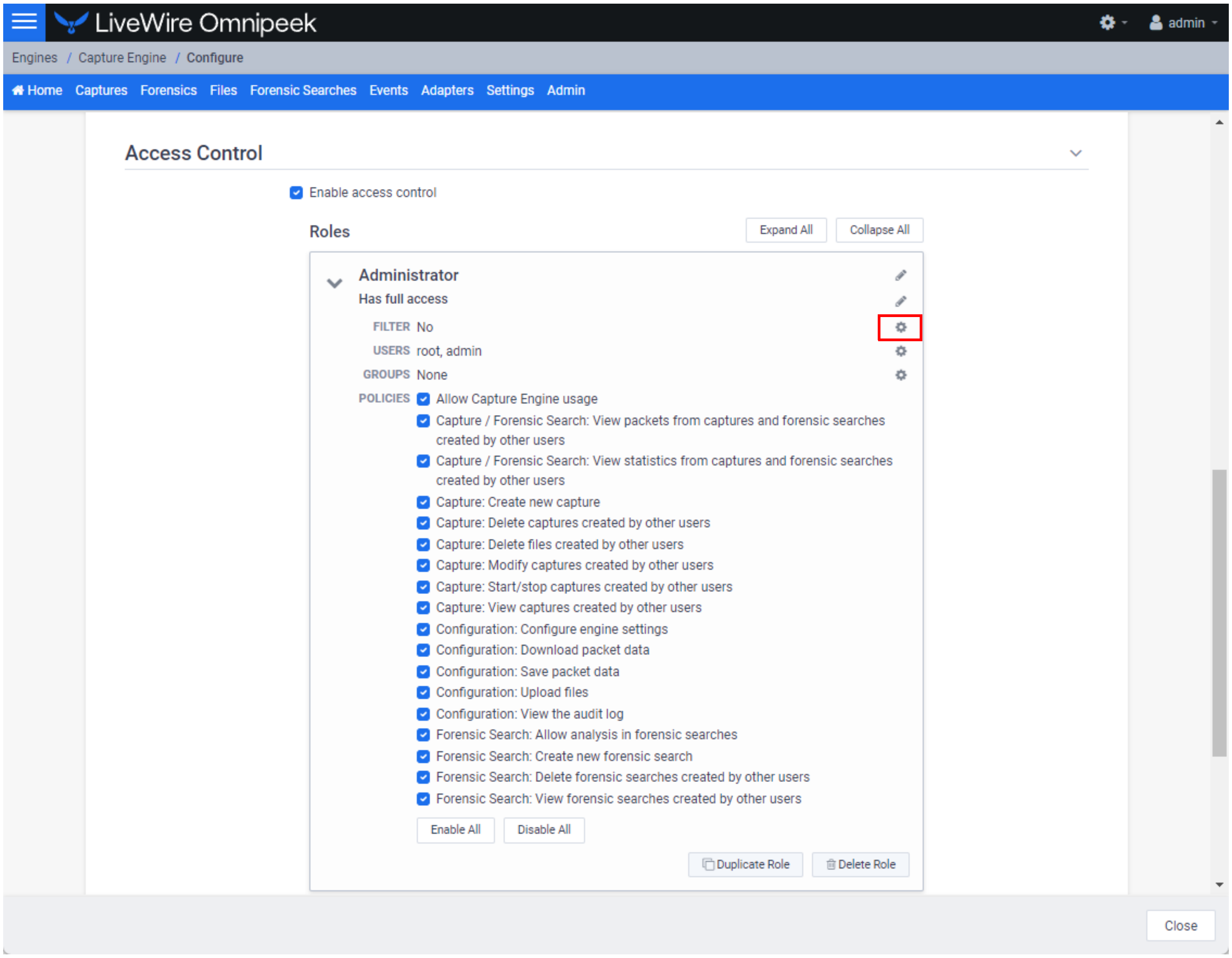
Configuring Filters for Roles

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.



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

Access Control

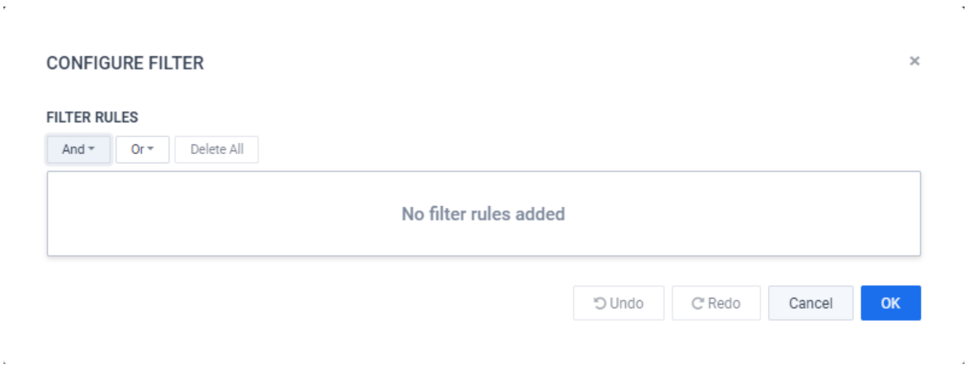
☑ Enable access control

Roles

Administrator
Has full access

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

2. Configure the filter.



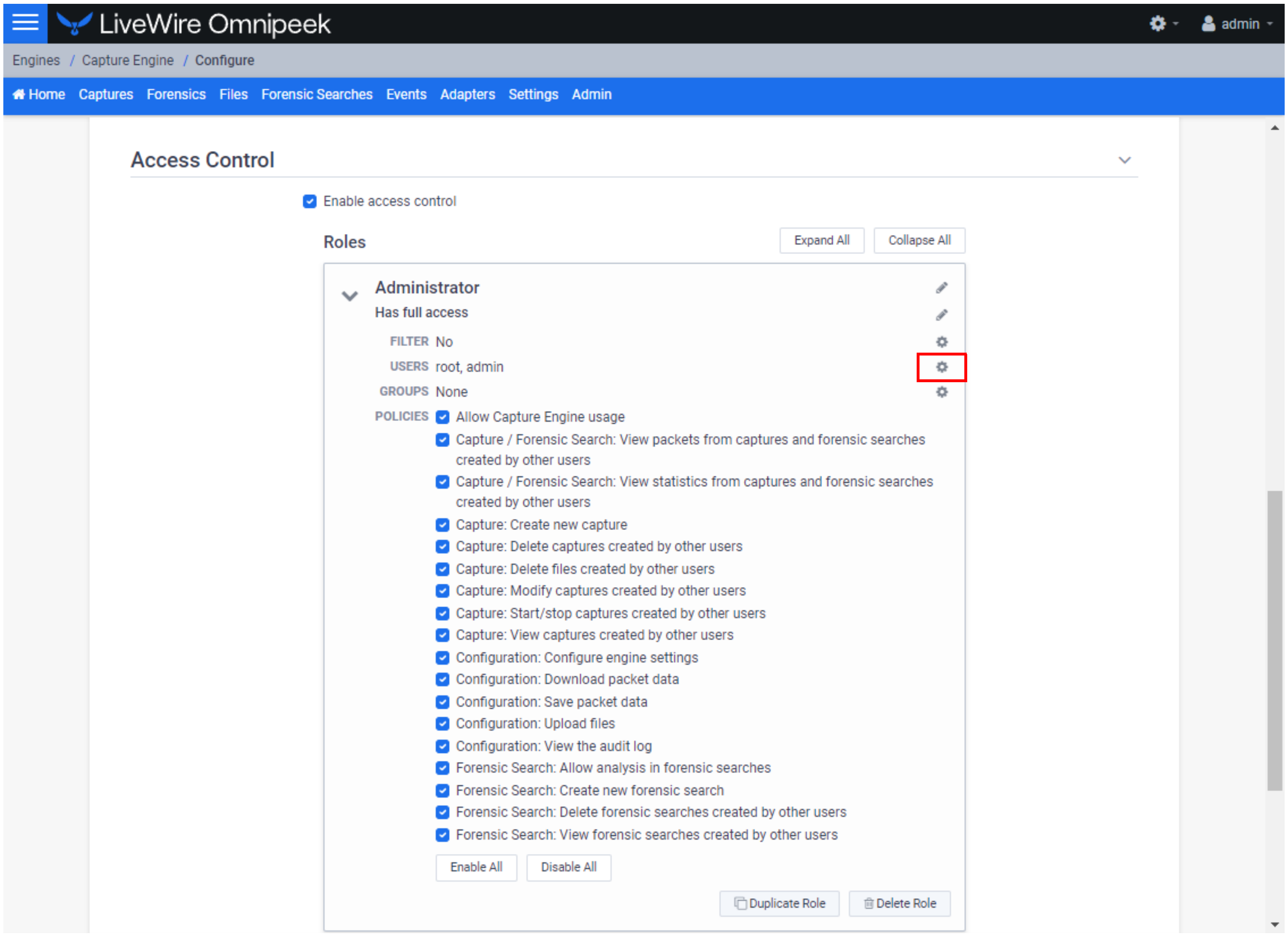
No filter rules added

- *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.

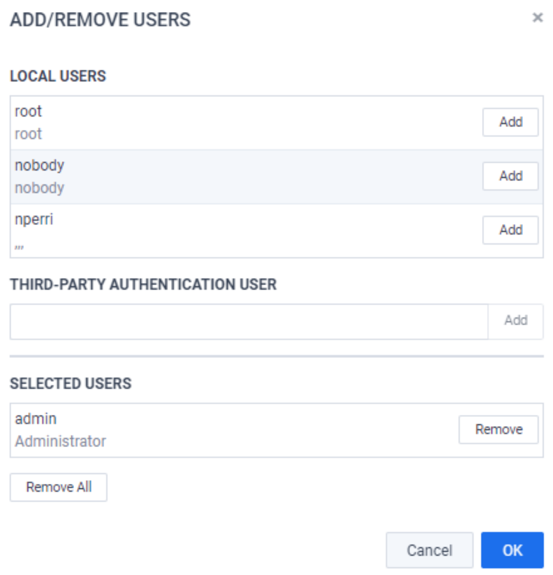


☑ Enable access control

Administrator
Has full access

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

2. Configure the users.



ADD/REMOVE USERS

LOCAL USERS

root
root

nobody
nobody

nperri
""

THIRD-PARTY AUTHENTICATION USER

SELECTED USERS

admin
Administrator

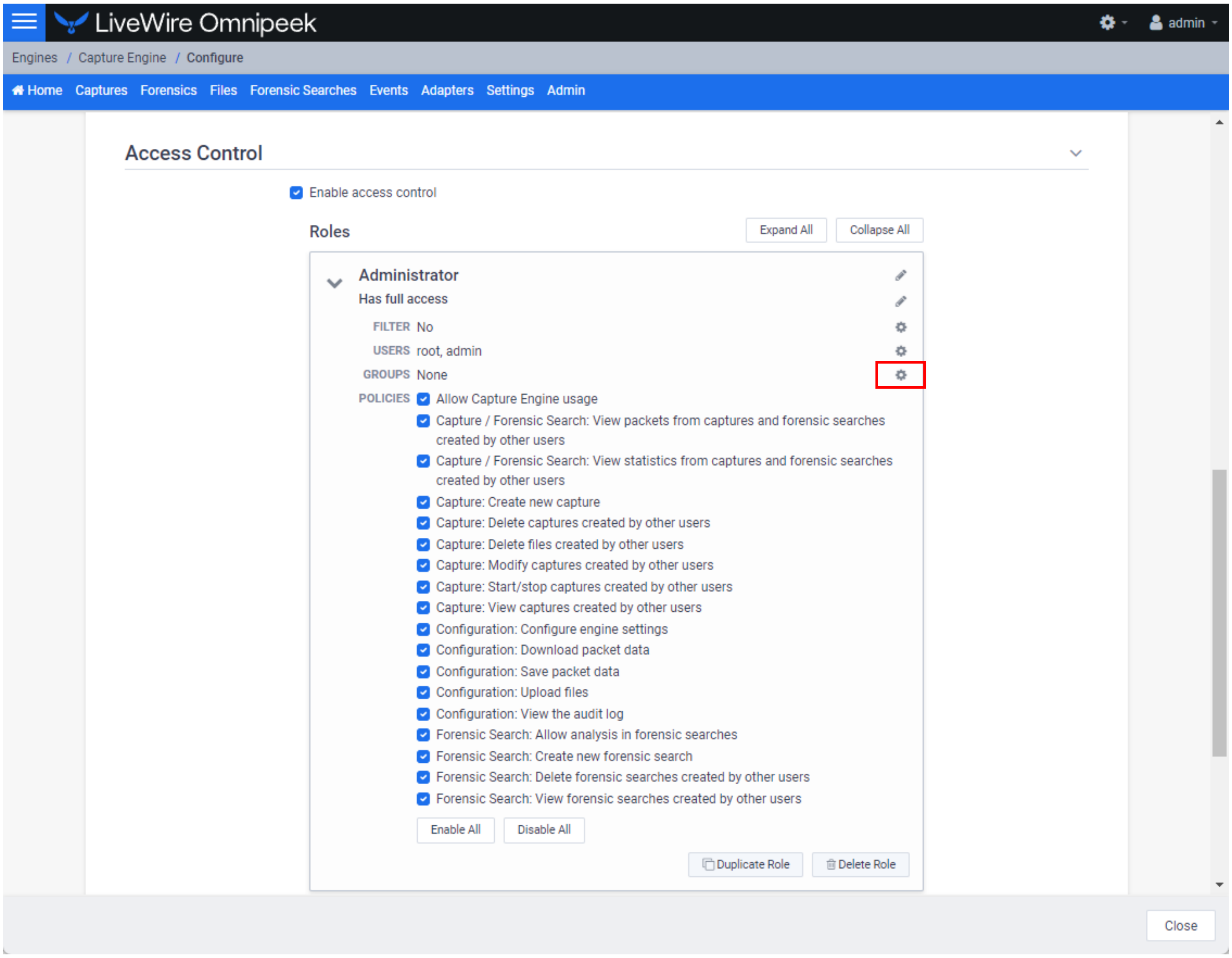
- *Local Users*: Displays the local users that can be added to a role. Click *Add* to add a user to the *Selected Users* list.
- *Third-Party Authentication User*: Allows users to type in third-party users from third-party authentication servers. Click *Add* to add a user to the *Selected Users* list.
- *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 126. 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.


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

Access Control

☑ Enable access control

Roles

Administrator

Has full access

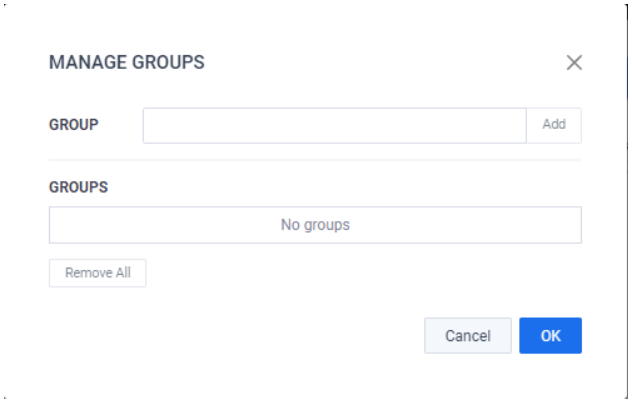
FILTER No

USERS root, admin

GROUPS None

POLICIES
☑ Allow Capture Engine usage
☑ Capture / Forensic Search: View packets from captures and forensic searches created by other users
☑ Capture / Forensic Search: View statistics from captures and forensic searches created by other users
☑ Capture: Create new capture
☑ Capture: Delete captures created by other users
☑ Capture: Delete files created by other users
☑ Capture: Modify captures created by other users
☑ Capture: Start/stop captures created by other users
☑ Capture: View captures created by other users
☑ Configuration: Configure engine settings
☑ Configuration: Download packet data
☑ Configuration: Save packet data
☑ Configuration: Upload files
☑ Configuration: View the audit log
☑ Forensic Search: Allow analysis in forensic searches
☑ Forensic Search: Create new forensic search
☑ Forensic Search: Delete forensic searches created by other users
☑ Forensic Search: View forensic searches created by other users

2. Configure the groups.


MANAGE GROUPS

GROUP

GROUPS

No 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.

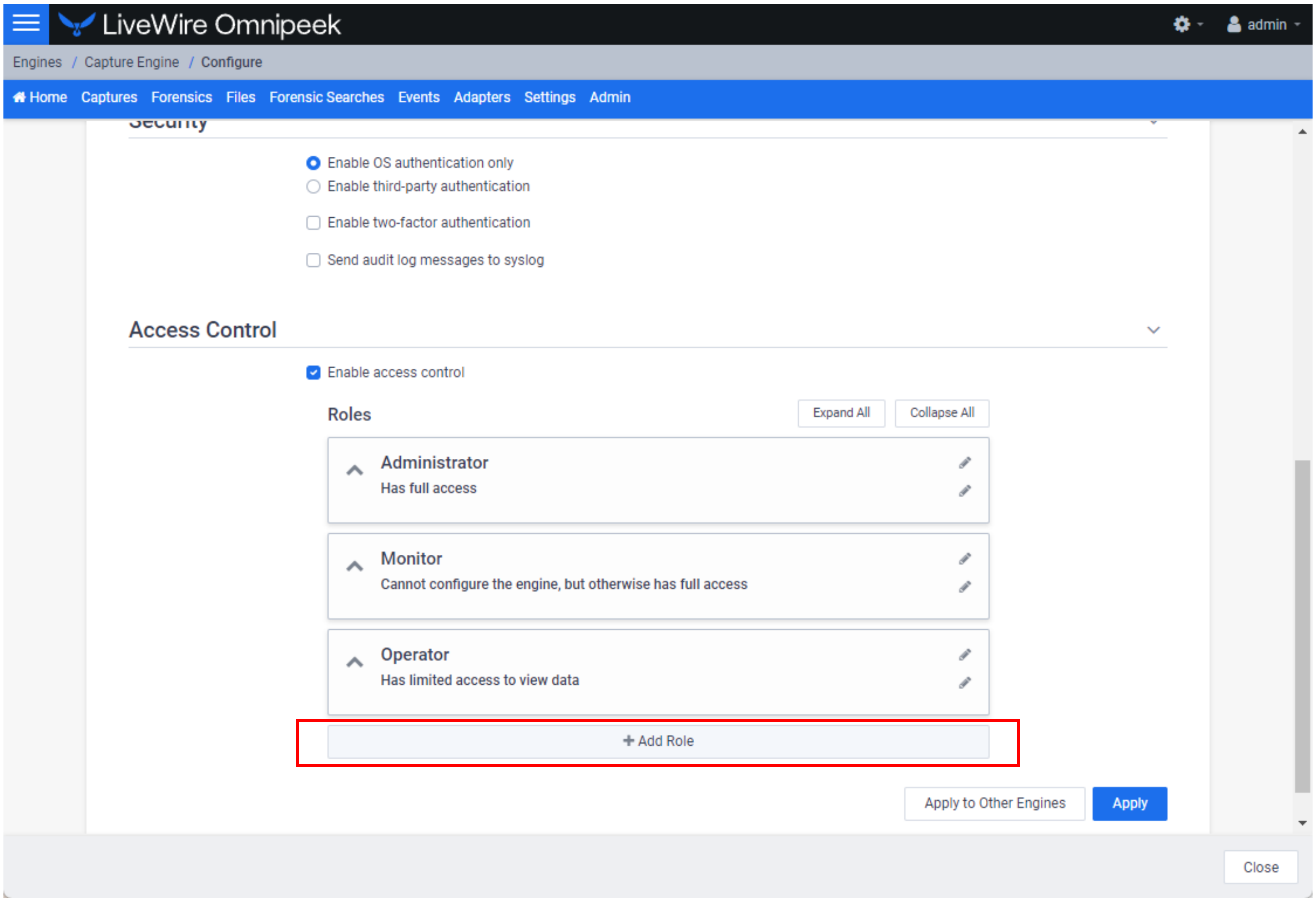
Adding a Role

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 118.


LiveWire Omnipeek
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Expand All
Collapse All
+ Add Role
Apply to Other Engines
Apply
Close

Security

● Enable OS authentication only
○ Enable third-party authentication

□ Enable two-factor authentication

□ Send audit log messages to syslog

Access Control

☑ Enable access control

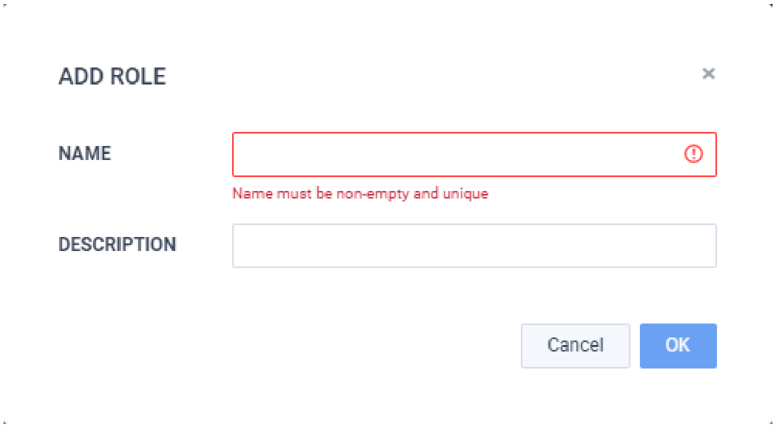
Roles

Administrator
Has full access

Monitor
Cannot configure the engine, but otherwise has full access

Operator
Has limited access to view data

2. Configure the dialog.



ADD ROLE

NAME

Name must be non-empty and unique

DESCRIPTION

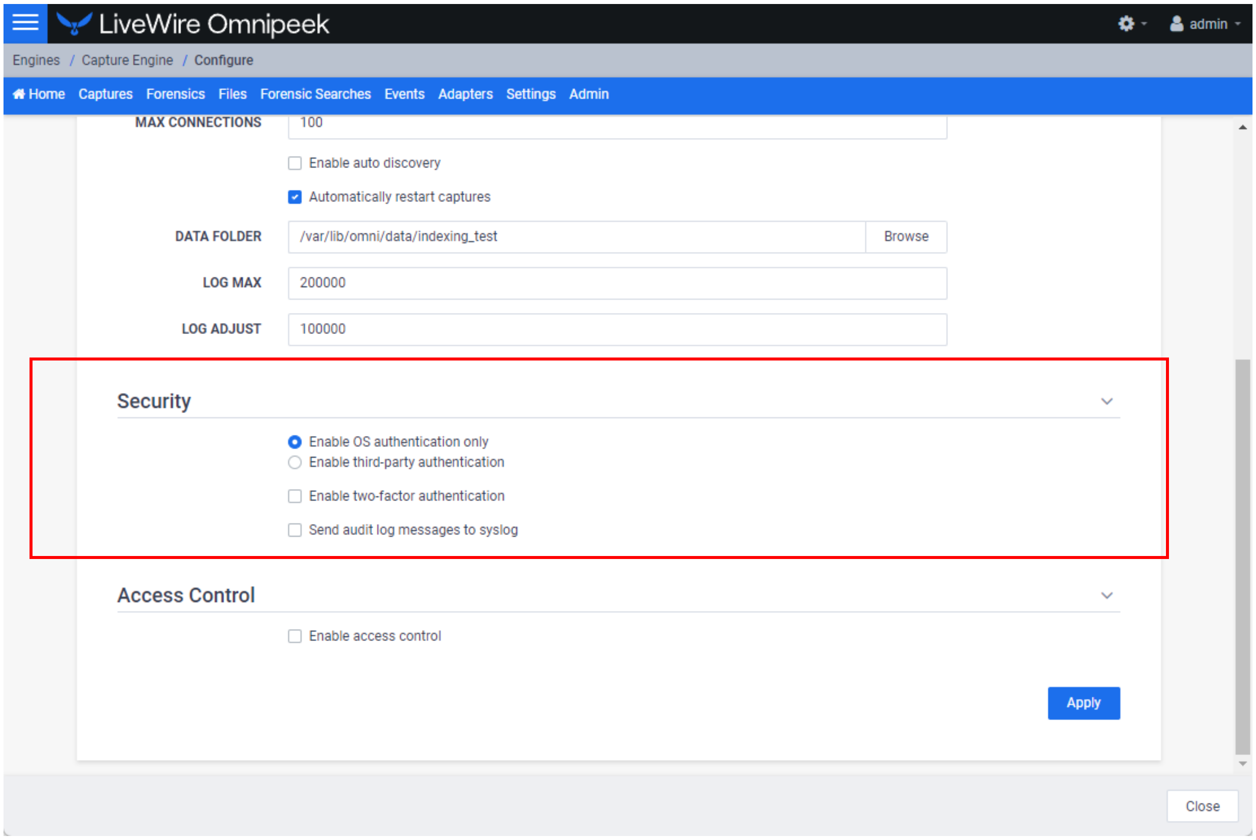
- *Name*: Type a unique name for the role.
- *Description*: Type a description for the role.
- *OK*: Click to save the role and add it to list of roles.

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.



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

MAX CONNECTIONS 100

□ Enable auto discovery

☑ Automatically restart captures

DATA FOLDER /var/lib/omni/data/indexing_test

LOG MAX 200000

LOG ADJUST 100000

Security

● Enable OS authentication only

○ Enable third-party authentication

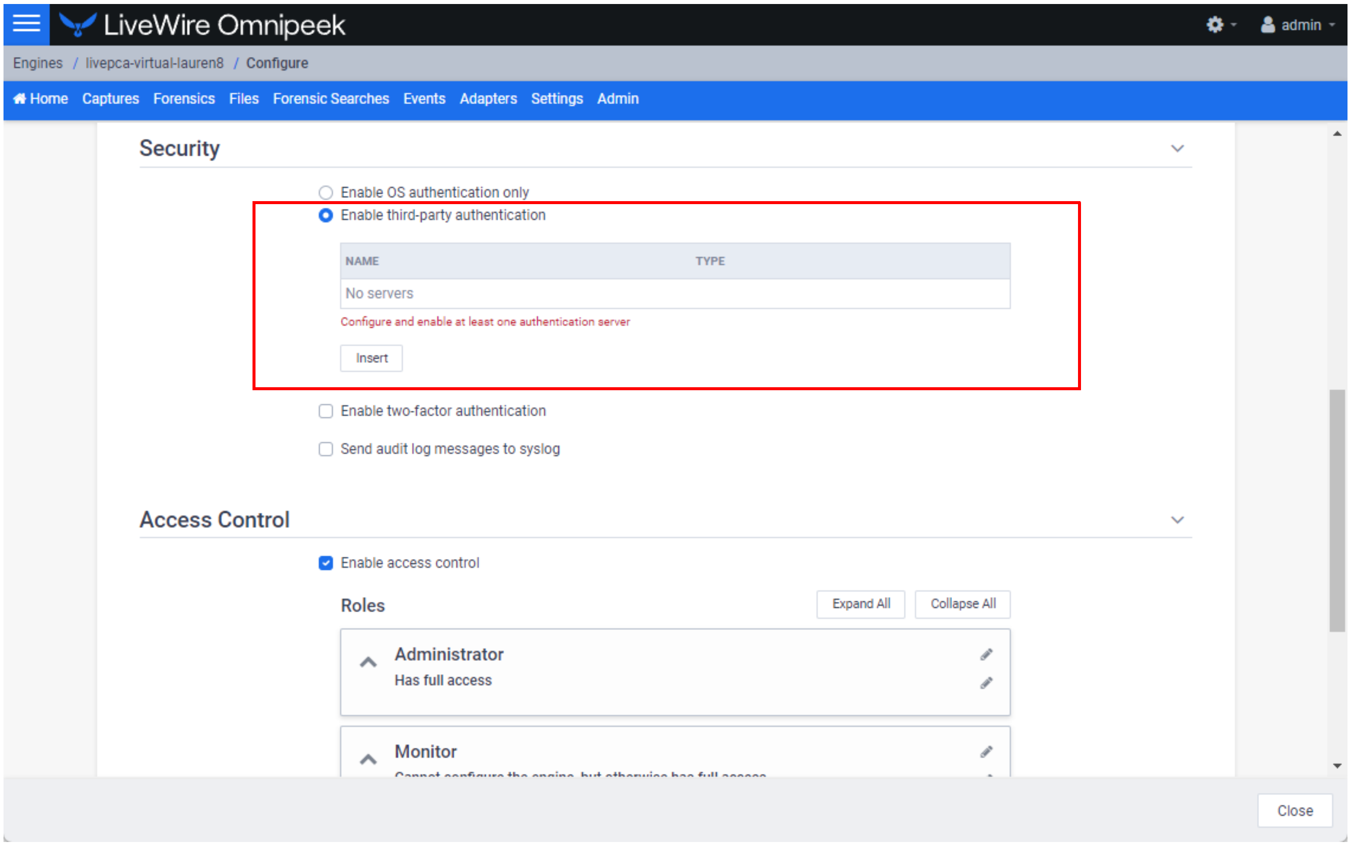
□ Enable two-factor authentication

□ Send audit log messages to syslog

Access Control

□ Enable access control

2. Select *Enable third-party authentication*.


LiveWire Omnipeek
admin
Engines / livepca-virtual-lauren8 / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Insert
Expand All
Collapse All
Close

Security

○ Enable OS authentication only

● Enable third-party authentication

NAME	TYPE
No servers	

Configure and enable at least one authentication server

□ Enable two-factor authentication

□ Send audit log messages to syslog

Access Control

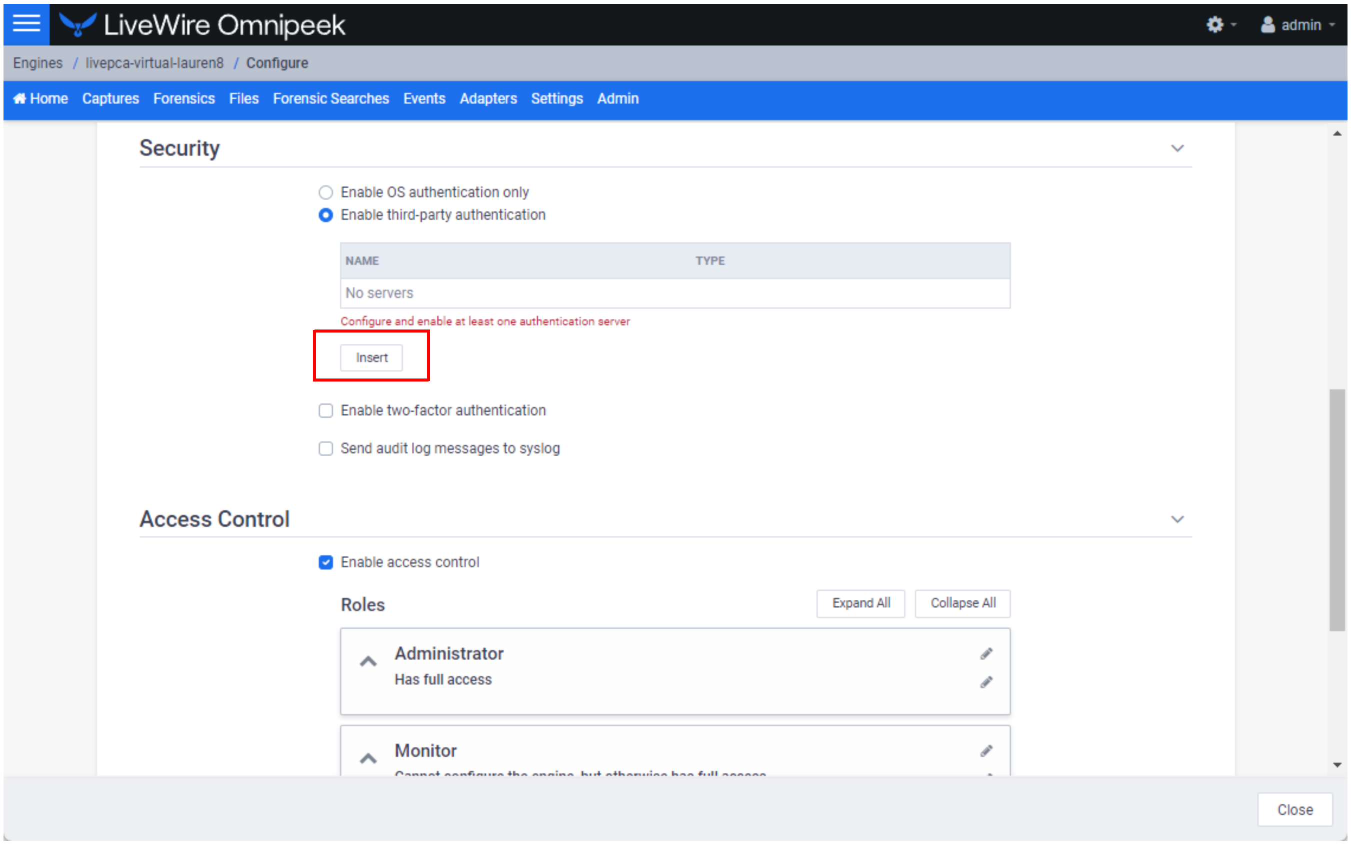
☑ Enable access control

Roles

Administrator
Has full access

Monitor
Cannot configure the engine, but otherwise has full access

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


LiveWire Omnipeek
admin
Engines / livepca-virtual-lauren8 / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Insert
Expand All
Collapse All
Close

Security

○ Enable OS authentication only

● Enable third-party authentication

NAME	TYPE
No servers	

Configure and enable at least one authentication server

□ Enable two-factor authentication

□ Send audit log messages to syslog

Access Control

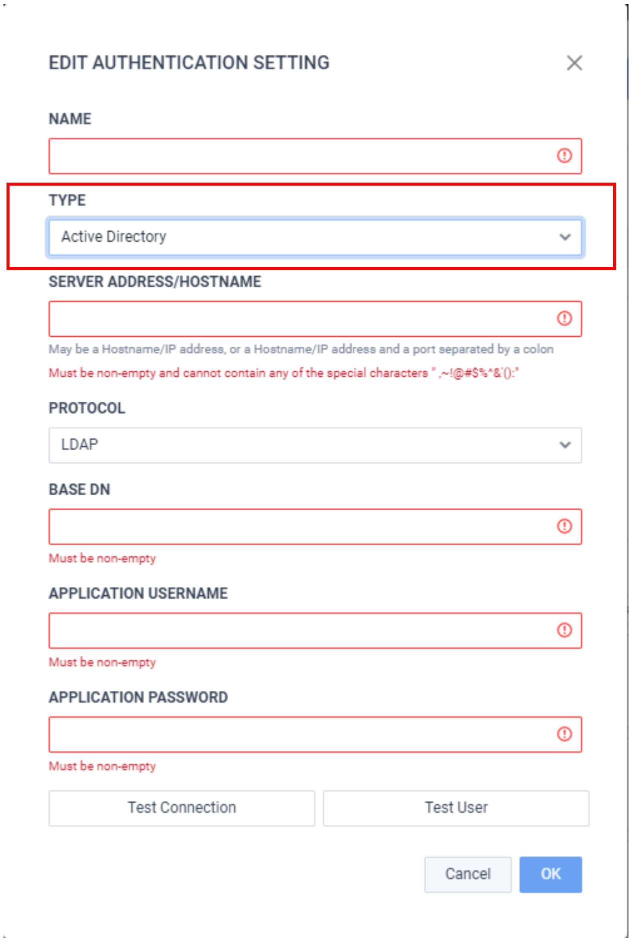
☑ Enable access control

Roles

Administrator
Has full access

Monitor
Cannot configure the engine, but otherwise has full access

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

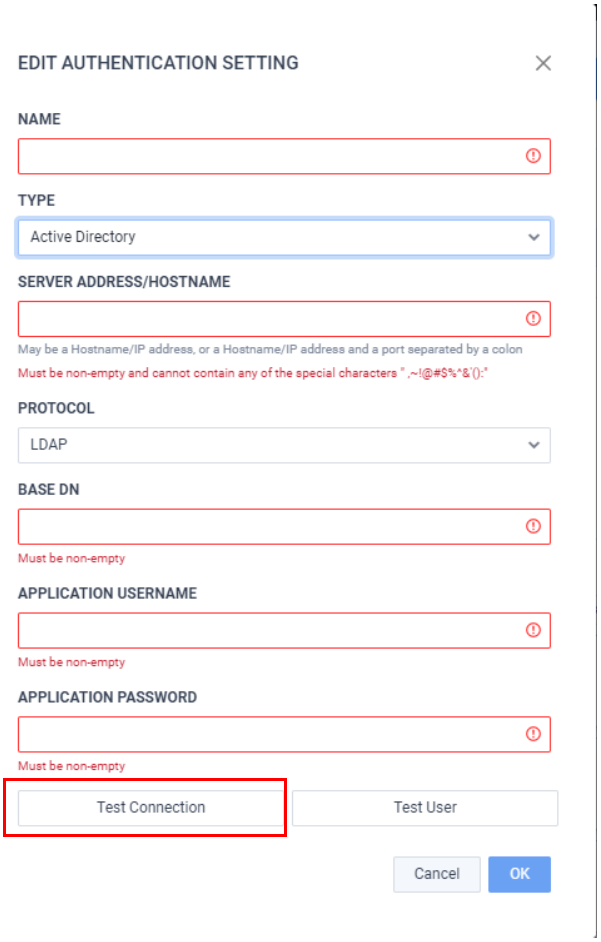
APPLICATION USERNAME

Must be non-empty

APPLICATION PASSWORD

Must be non-empty

5. 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

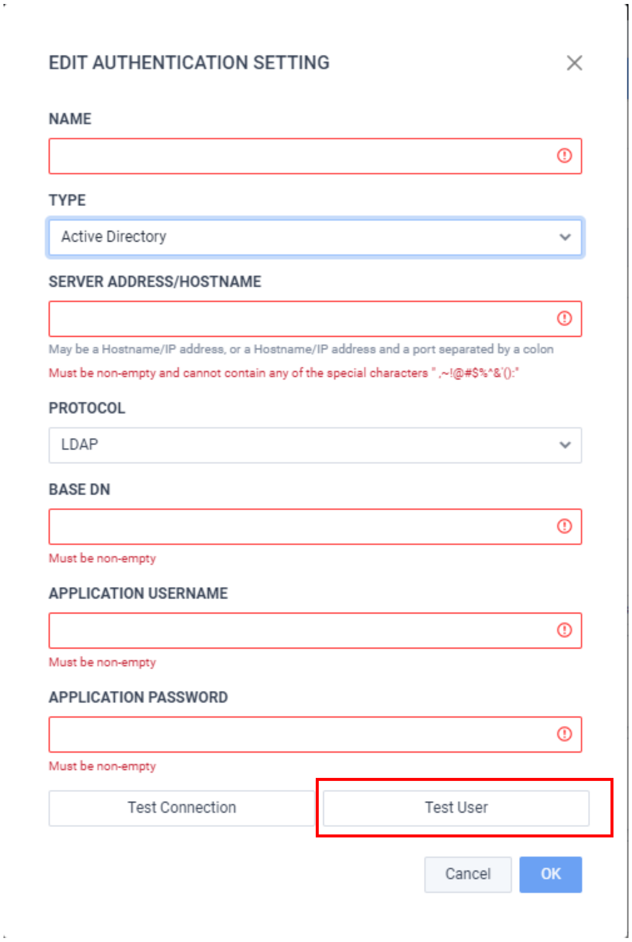
APPLICATION USERNAME

Must be non-empty

APPLICATION PASSWORD

Must be non-empty

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



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

7. Click **OK**.

When Upgrading From LiveWire v23.3.1 or Earlier

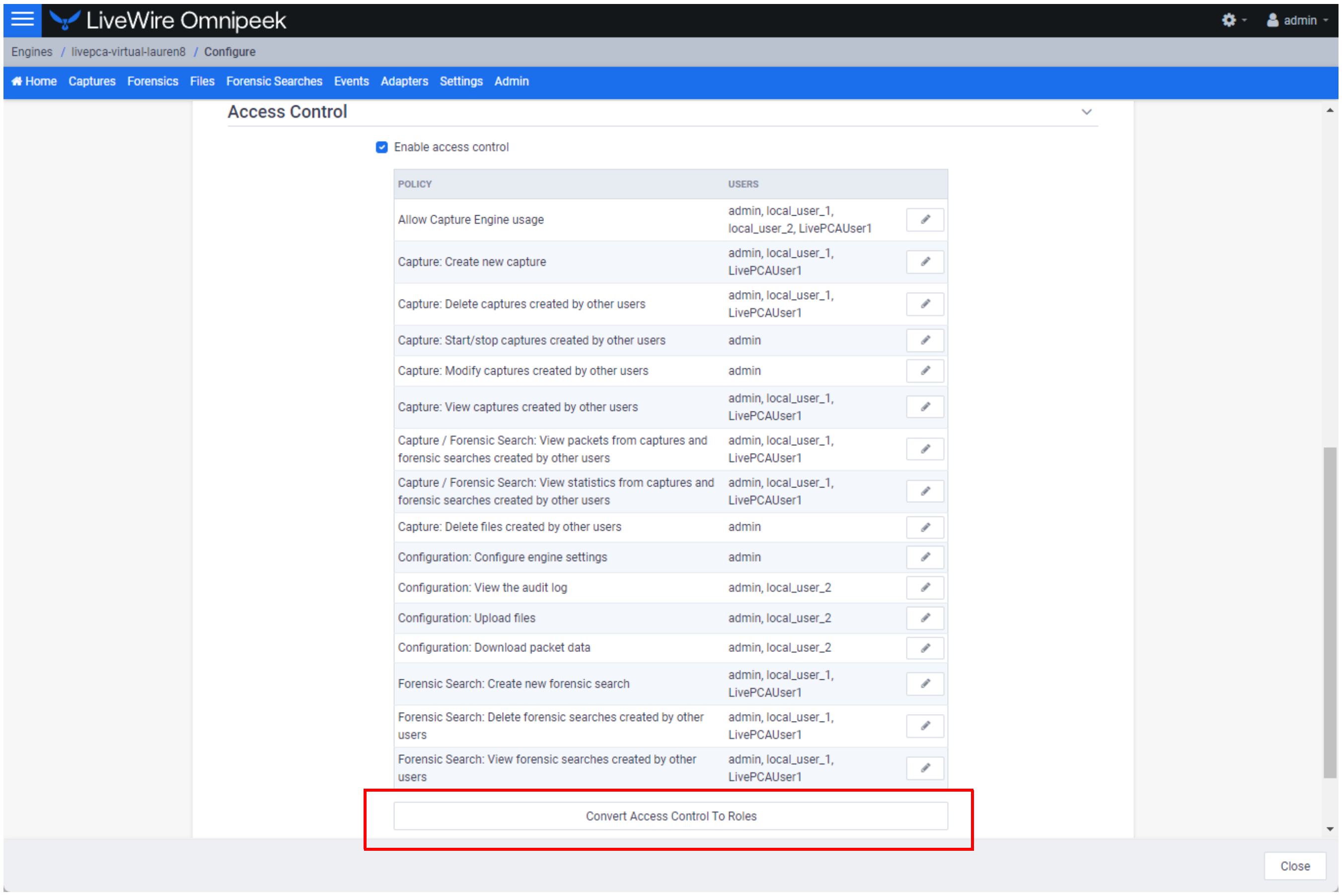
When upgrading from LiveWire v23.3.1 or earlier to LiveWire v23.4.0 or later, there are two possible upgrade scenarios that affect the Access Control List (ACL):

- 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:

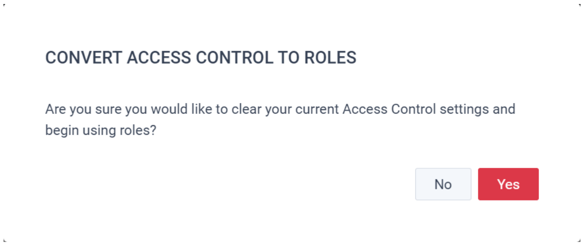
  In this case, upon upgrading to v23.4.0 or later, LiveWire keeps the policy-based approach. You will need to manually opt-in to the role-based approach. If you decide to upgrade to a role-based approach, and upon your confirmation, LiveWire completely clears the current ACL settings and forces you to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


LiveWire Omnipeek
admin
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

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

CHAPTER 6

Capture Adapters for LiveWire

In this chapter:

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 133)
- 10G capture adapter—Two or four port 10 Gigabit adapter (see '10G capture adapter' on page 134)
- 40G capture adapter—Two port 40 Gigabit adapter (see '40G capture adapter' on page 136)
- 100G capture adapter—Two port 100 Gigabit adapter (see '100G capture adapter' on page 137)

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*.

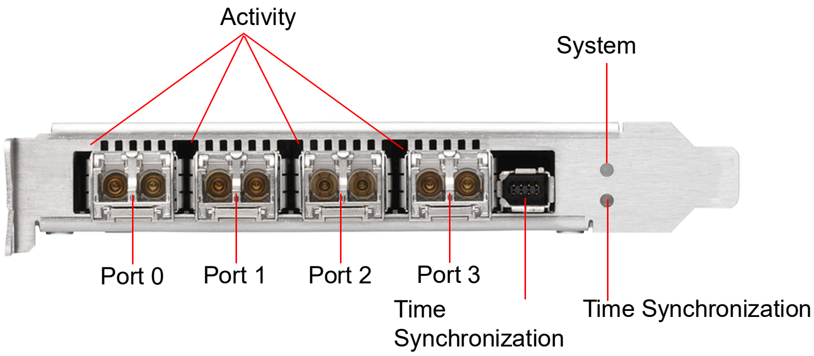
1G capture adapter

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.

LED	State and Color	Condition
	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: • 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: • 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:

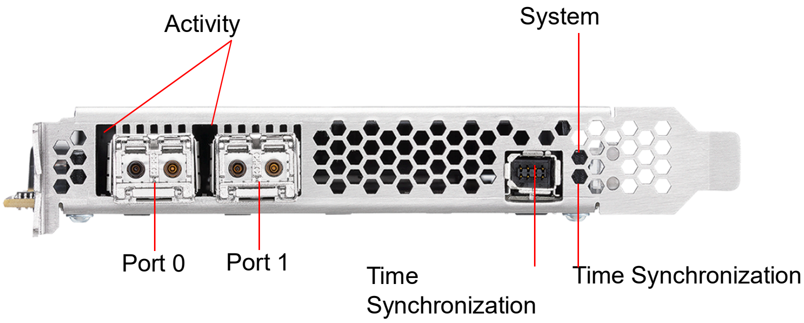
- Two or four 850nm MMF SFP+ optical transceivers with LC connectors
- Two or four 1310nm SMF SFP+ optical transceivers with LC connectors

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
```

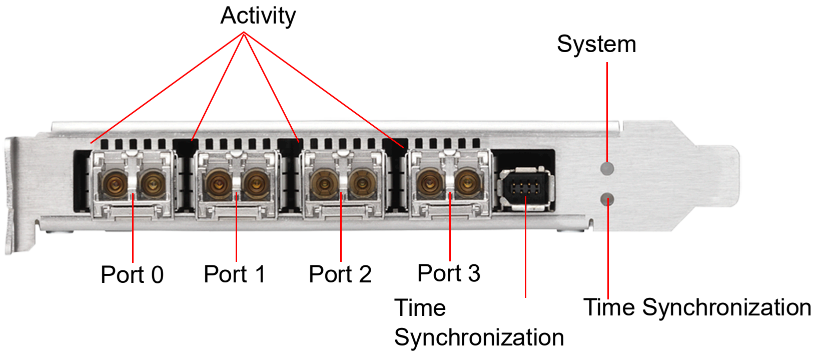
10G capture adapter (2-port) I/O bracket

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
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.

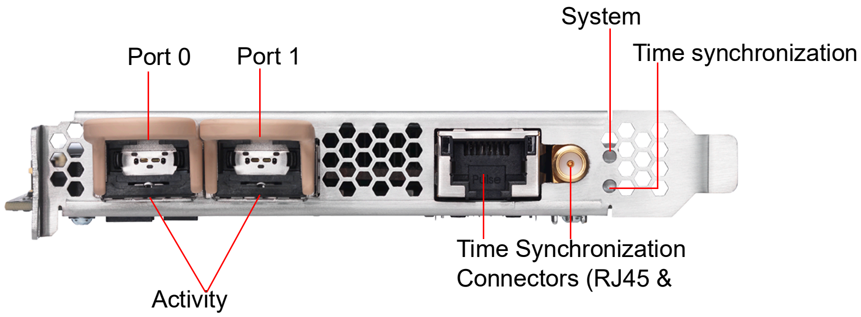
LED	State and Color	Condition
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the PTP port is down and the following condition is fulfilled: When the SMA port of the external time synchronization connector is configured as a: • PPS or NT-TS input connector: A driver is loaded, 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: • 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 timestamping. 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.
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.
	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 externalRJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: • 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 externalRJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: • 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.

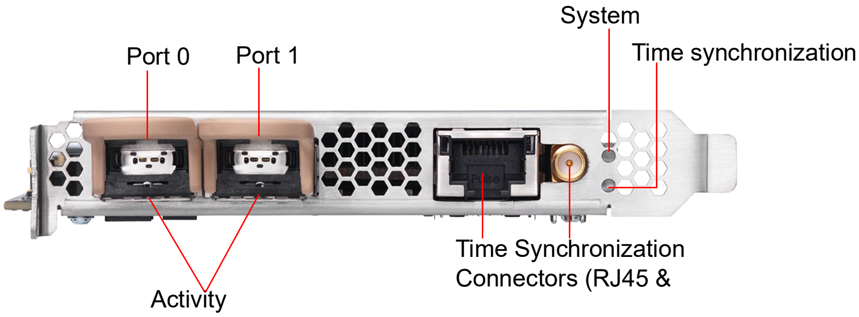
100G capture adapter

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 timestamping. 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.

LED	State and Color	Condition
	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 externalRJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: • 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 externalRJ45 time synchronization connector is down, and the following condition is fulfilled: When the external SMA time synchronization connector is configured as a: • 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 140.

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 ntcard_setup script to update the configuration file with the PTP settings.
    - service ntcard_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 *PtpIpAddr*, *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	PtpIpAddr	Specifies a static IP address for the PTP port.	Any valid IPv4 address (e.g. 192.168.1.10)	Not set
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

Section	Parameters	Description	Values	Default Value
AdapterN	PtpUnicastMasterAddre<1...10>	Adds an IP address of a PTP master to the unicast master table. Up to 10 IP addresses can be added. The order of the addresses is not important.	Any valid IPv4 address (e.g. 192.168.1.10)	Not set
AdapterN	TimeSyncReferencePriority	Comma separated list of clock sources. In order to enable PTP, PTP must be the first item in the list. The last item in the list must be either FreeRun or OSTime.	PTP - Ext1 - FreeRun - OSTime	OSTime

Example of /etc/omni/ntoverrides.ini:

```
## This file is used to specify overrides for the ntservice 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 timestamps 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 'ntpdate' 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).

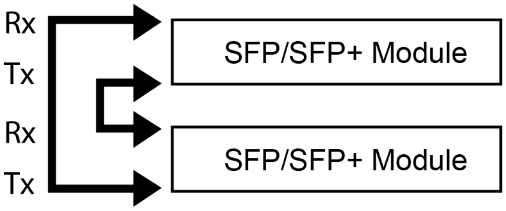
Note For instructions on manually enabling PTP support on your Capture Engine, see 'Enabling PTP support for capture adapters' on page 138.

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:



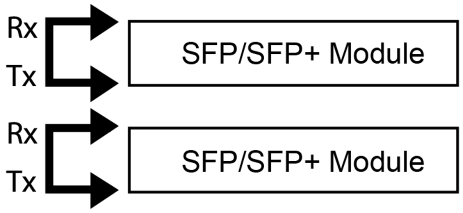
2. If the two links are established, this will indicate that both channels, including the SFP/SFP+ modules, are functional. An external connection issue should then be investigated.

   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.

CHAPTER 7

Network Port Requirements

In this appendix:

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		

Hardware Specifications

In this appendix:

LiveWire technical specifications

LiveWire Edge

Specification	Description
Processor Base Frequency Cores	Intel® Atom® C3758 2.2 GHz 8
Memory	16 GB DDR4 2400 MHz ECC DIMM
Storage	1 x 1 TB SSD
I/O	(4) RJ45 LAN (GbE) (2) RJ45 Inline bypass ports (GbE) (2) USB 3.0 ports (1) Console port (Mini USB) (1) On/Off switch (1) Reset button (3) Status LEDs
Physical Dimensions: Unit Weight: Shipping Weight:	 8.54-by-1.7-by-5.7-inches (217-by-44-by-145.5-millimeters) 2.64 lbs (1.2 kg) 6.61 lbs (3 kg)
System Cooling Processor: System:	 Passive CPU Heat sink Fanless **NOTE**: Do not place anything on top of or directly next to LiveWire Edge. Any obstructions to the heat sink located on top of LiveWire Edge can cause the unit to overheat.
Power Supply	60 W Power adapter 100-240 V @50-60 Hz
Operating Environment Operating Temperature: Storage Temperature: Relative Humidity: Storage Humidity:	 32° to 104° F (0° to 40° C) -4° to 158° F (-20° to 70° C) 5% to 90% (non condensing) 5% to 95% (non condensing)
Regulations	EMC CE Class B FCC Class B RoHS UL

LiveWire Core

Specification	Description
Processor Base Frequency Cores Thread	AMD® 1x7313 3.0 GHz 16 32
Memory	64 GB RAM
Expansion Slots	1 x 16 full-height PCI Express 3.0 slot **NOTE**: A total of one capture adapter can be added to the LiveWire Core.
Integrated Network Interfaces	4 x 1GBASE-T iDRAC
Storage-OS	Included as part of Storage-Data
Storage-Data	Available with 32 TB SAS ISE storage, RAID 0 with optional RAID 10
Chassis Dimensions (WxHxD): Weight:	1U Rackmount 17.08 x 1.68 x 28.98-inches (433.8 x 42.7 x 736.3-millimeters) 48.1 lbs (21.8 kg) maximum
System Cooling	Five chassis cooling fans (hot-pluggable)
System Input Requirements AC Input Voltage: Rated Input Current: Rated Input Frequency:	 100-240 V AC 7.4 A-3.7 A 50-60 Hz
Power Supply (2 units) Rated Output Power:	 800 W
Operating Environment Operating Temperature: Non-operating Temperature: Operating Relative Humidity: Non-operating Relative Humidity: Heat dissipation (maximum):	 50° to 95° F (10° to 35° C) -40° to 149° F (-40° to 65° C) 10% to 80% (non condensing) 5% to 95% (non condensing) 3000 BTU/Hours

LiveWire PowerCore

Specification	Description
Processor	AMD® 2x EPYC 73F3
Base Frequency Cores Thread	3.5 GHz 32 64
Memory	256 GB RAM
Expansion Slots	Eight available PCI Express 3.0 slots to support up to three high speed capture adapters
Integrated Network Interfaces	4 x 1GBASE-T iDRAC
Storage-OS	Two 2 TB SSD SAS ISE drives for OS
Storage-Data	200 TB SAS storage, RAID 6 (240 TB, optional RAID 0) **NOTE**: Optional external storage with LiveWire TeraVault — Up to 800 TB, RAID 6 (960 TB, optional RAID 0) of additional storage (4x 2U TeraVaults)
Chassis Dimensions (WxHxD): Weight:	Rack-mount 2U appliance 17.09 x 3.42 x 28.99 in. (434 x 86.8 x 715.5 mm) Up to 80 lb (36.3 kg) maximum
System Input Requirements AC Input Voltage: Rated Input Frequency:	 100-240 V AC, autoranging 50/60 Hz
Power Supply (2 units) Rated Output Power:	 1100 W
Operating Environment Operating Temperature: Non-operating Temperature: Operating Relative Humidity: Non-operating Relative Humidity: Heat dissipation (maximum):	 50° to 95° F (10° to 35° C) -40° to 149° F (-40° to 65° C) 10% to 80% (non condensing) 5% to 95% (non condensing) 4100 BTU/Hour

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.

Capture adapter technical specifications

1G capture adapter specifications

Specification	Description
Network Interfaces Standard: Physical interface:	 IEEE 802.3 1 Gbps Ethernet support 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: Operating temperature: Operating humidity:	 23.3 Watts including SFP SX modules 32° F to 113° F (0° to 45° C) 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: Physical interface:	 IIEEE 802.3 10 Gbps Ethernet LAN 2 x SFP or SFP+ ports
Supported SFP modules: Supported SFP+ modules: Supported dual-rate modules:	Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T Multi-mode SR, single-mode LR and ER, 10GBASE-CR Multi-mode SR and single-mode LR
Environment Operating temperature: Operating humidity:	 32°F to 113°F (0° to 45°C) 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: Physical interface:	 IIEEE 802.3 10 Gbps Ethernet LAN 4x SFP or SFP+ ports
Supported SFP modules: Supported SFP+ modules: Supported dual-rate modules:	Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T Multi-mode SR, single-mode LR and ER, 10GBASE-CR Multi-mode SR and single-mode LR
Environment Power consumption: Operating temperature: Operating humidity:	 27 Watts including SFP+ SR modules 32° F to 113° F (0° C to 45° C) 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: Physical interface:	 IEEE 802.3 40 Gbps Ethernet LAN 2x QSFP+ ports
Supported optical transceivers: Supported QSFP+ modules: Supported QSFP28 modules:	 40GBASE-SR4, 40GBASELR4, and 40GBASE-SR-BiDi 100GBASE-SR4 and 100GBASE-LR4
Environment Operating temperature: Operating humidity:	 32°F to 113°F (0° to 45°C) 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: Physical interface:	 IEEE 802.3 40 Gbps Ethernet LAN 2x QSFP+ ports
Supported optical transceivers: Supported QSFP+ modules: Supported QSFP28 modules:	 40GBASE-SR4, 40GBASELR4, and 40GBASE-SR-BiDi 100GBASE-SR4 and 100GBASE-LR4
Environment Operating temperature: Operating humidity:	 32°F to 113°F (0° to 45°C) 20% to 80%
Regulatory approvals and compliances	PCI-SIG® NEBS level 3 CE CB RoHS REACH cURus (UL) FCC ICES VCCI C-TICK