LiveAction

LiveWire

User Guide

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

20230524-LWG2U_2311a

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

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	240 TB SAS storage, RAID 0 or optional RAID 6 **NOTE**: Optional external storage with LiveWire TeraVault — Up to 960 TB 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

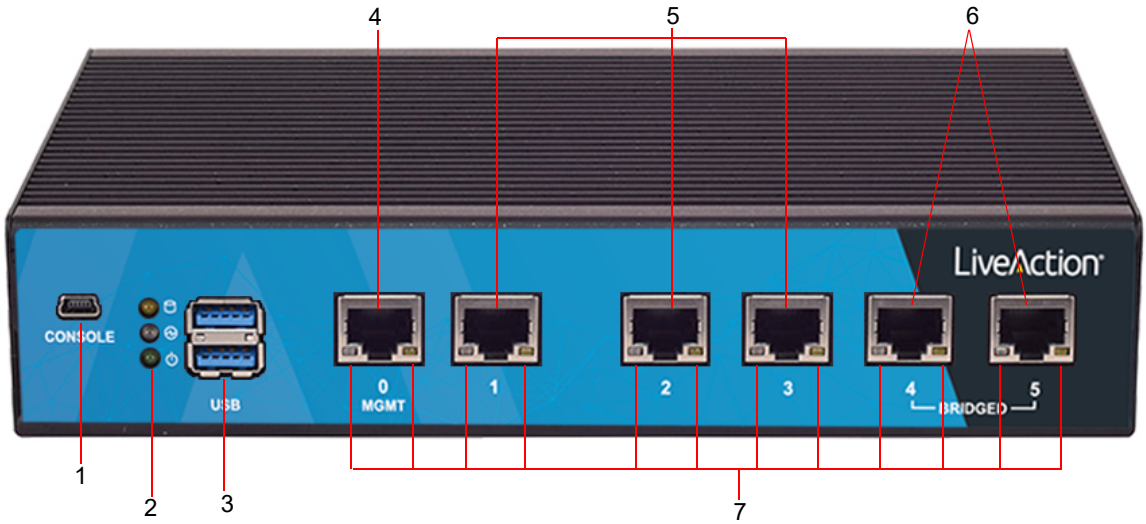
Front / rear panels

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 26.
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



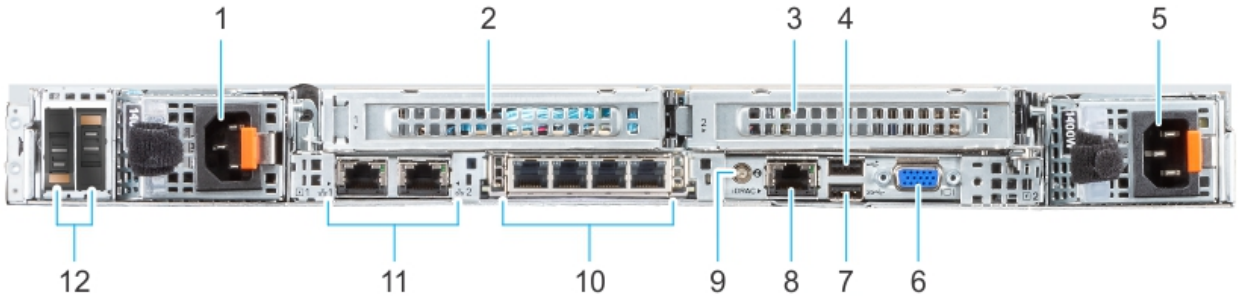
Item	Indicator, Button, or Connector	Description
1	Mini-USB Port	The Mini-USB port (console port) lets you connect to another computer terminal for advanced diagnostics or recovery access using a mini-USB console cable (not included with LiveWire Edge) connected from the USB port on your PC/laptop to the Mini-USB Port on the rear panel of LiveWire Edge. See 'Connecting to LiveWire through the serial port' on page 68.
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 26). 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.

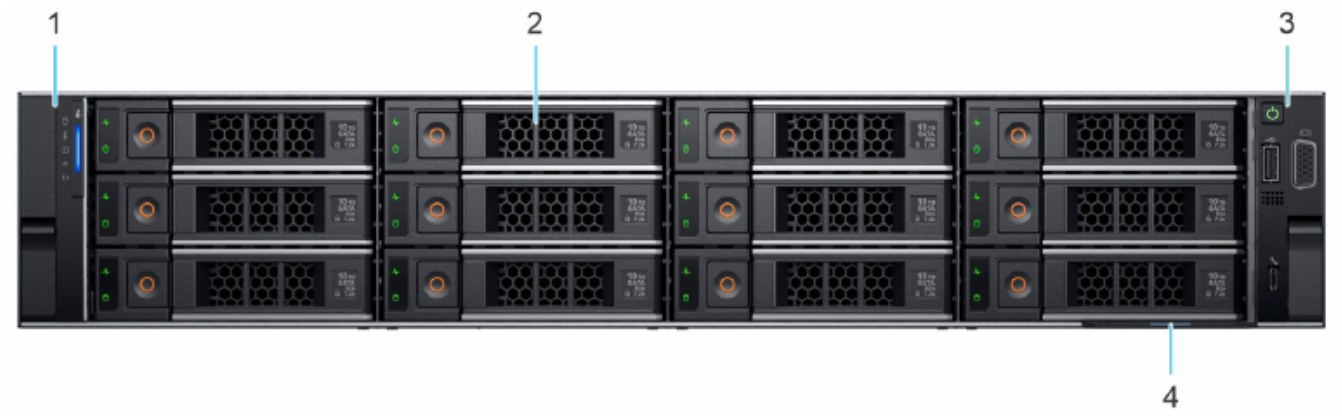
LiveWire Core back panel



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.

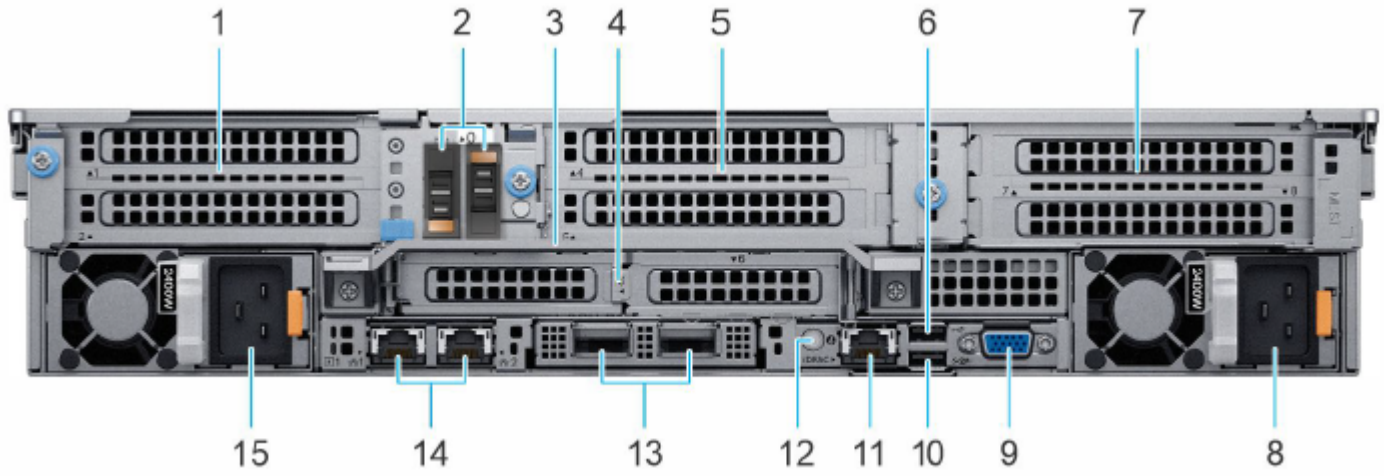
LiveWire PowerCore front panel



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

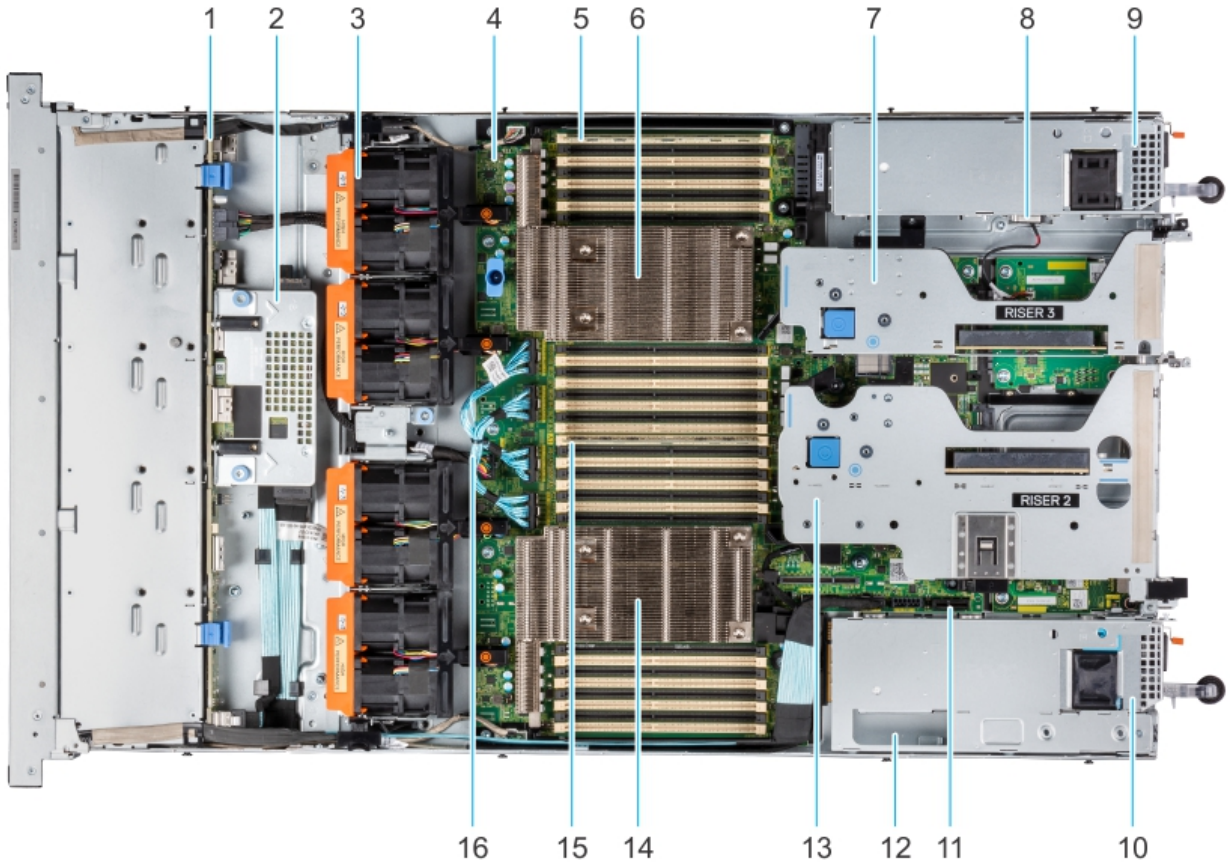


Item	Ports, Panels, or Slots	Description
1	PCIe expansion card riser 1 (slot 1 and slot 2)	The expansion card riser enables you to connect PCI Express expansion cards.
2	BOSS S2 card (optional)	This slot supports the BOSS S2 module.
3	Rear handle	To lift the system.
4	PCIe expansion card riser 2 (slot 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

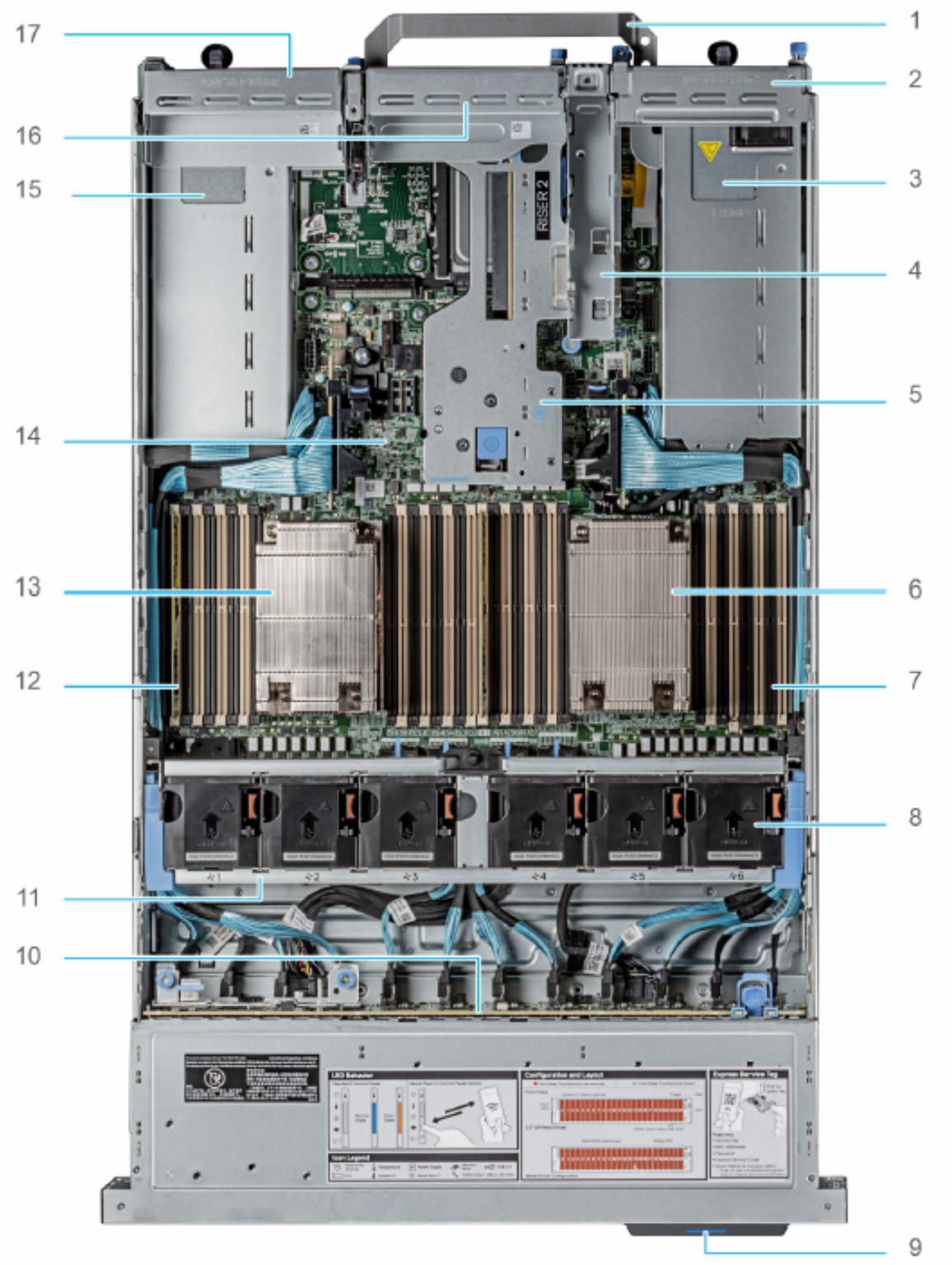


Item	Description
1	Drive backplane
2	Rear mounting front PERC module
3	Dual fan module (4)
4	System board
5	Memory DIMM socket for processor 2 (B1)
6	Heat sink for processor 2
7	Riser 3
8	Intrusion switch
9	Power supply unit (PSU 2)
10	Power supply unit (PSU 1)
11	IDSDM/Internal USB card port
12	BOSS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

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 70.

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

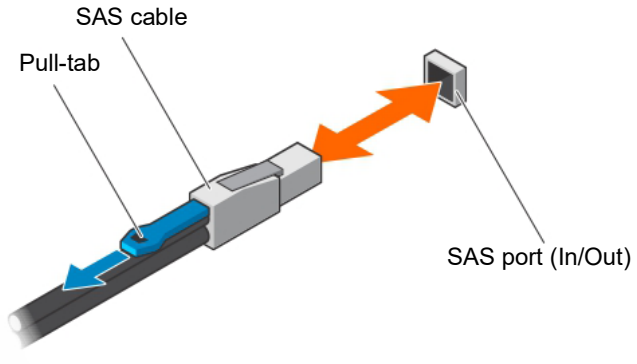
The storage capacity of any LiveWire PowerCore with 240 TB of total hard disk capacity can be increased through the addition of TeraVault for LiveWire PowerCore. TeraVault is available in a configuration of 240 TB. Up to four TeraVault units can be added for a total of up to 1200 TB. If you purchased 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.

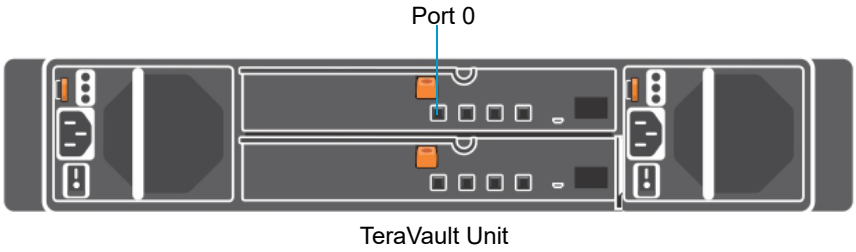
Note If you have multiple TeraVault boxes, and the system is disconnected for any reason, the cabling of the boxes needs to be exactly as it was before, otherwise the RAID won't be seen correctly. To assist you with the cabling, every TeraVault box is labeled with a number, and every TeraVault cable is labeled to the exact port it needs to get plugged into. See 'Connecting multiple TeraVault units' on page 15.

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.

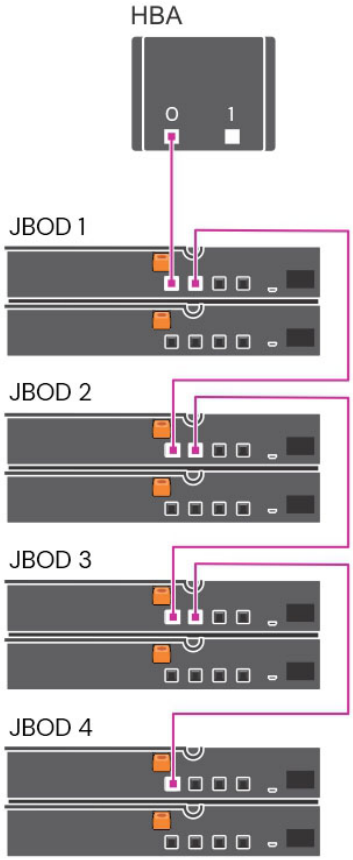
6. Turn on power to TeraVault by pressing the power button on the front of the chassis. You may see brief bursts of LED activity as the expander in TeraVault scans the drives.
7. Turn on the power to LiveWire PowerCore. The system is ready for use as soon as the LiveWire PowerCore boot sequence completes.

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:

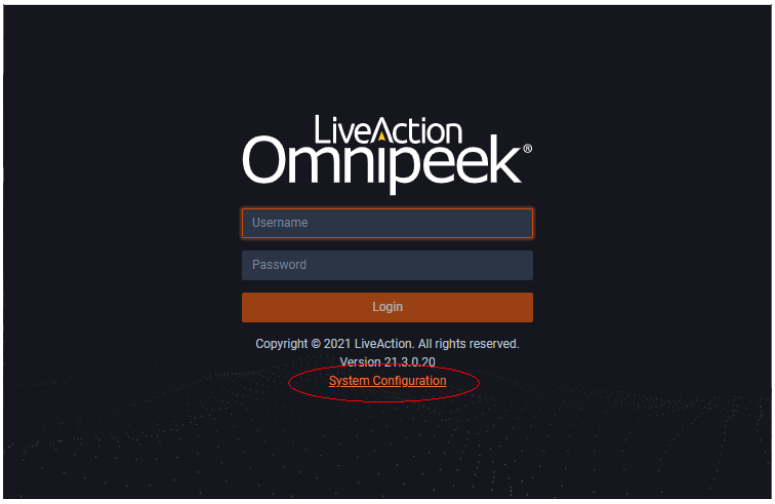
- IP address of LiveWire
- Product key
- User name
- Company name
- Email address
- Version number

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:

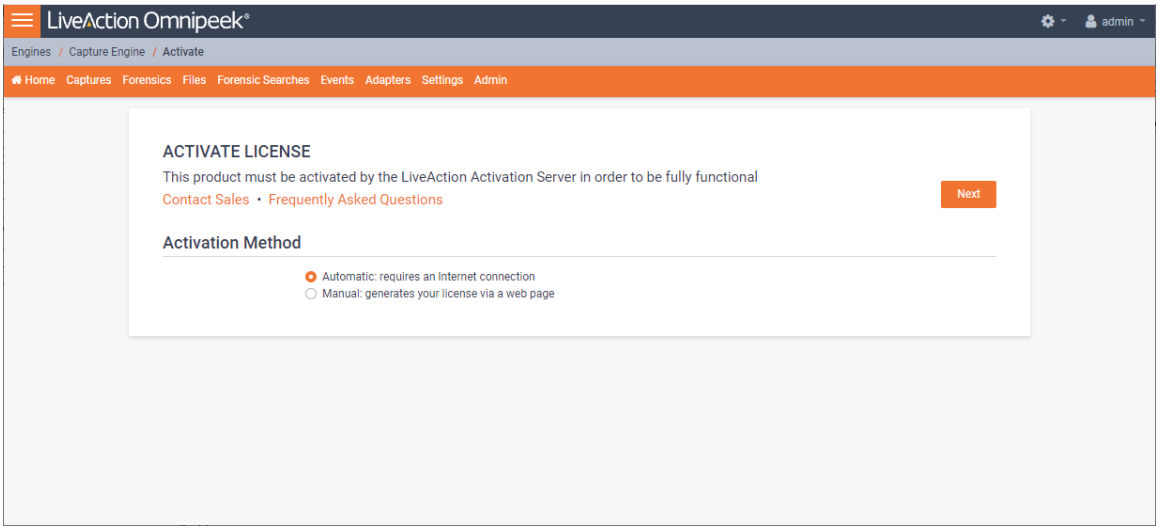
1. From your web browser, type the IP address of LiveWire into the URL field of the browser and press **Enter**. The Omnipeek login screen appears.



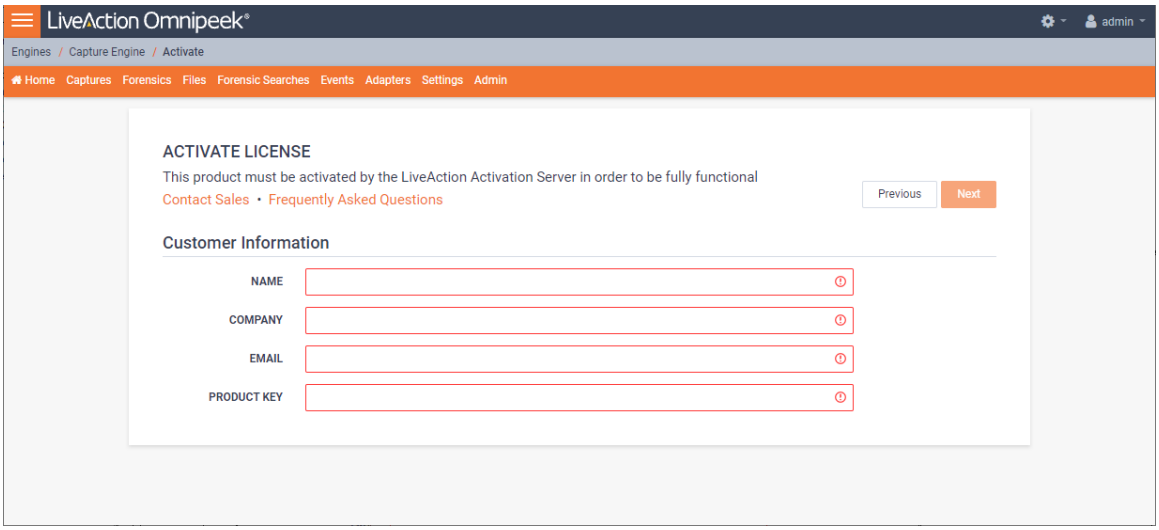
   - *Username*: Type the username for LiveWire. The default is *admin*.
   - *Password*: Type the password for LiveWire. The default is *admin*.

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

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



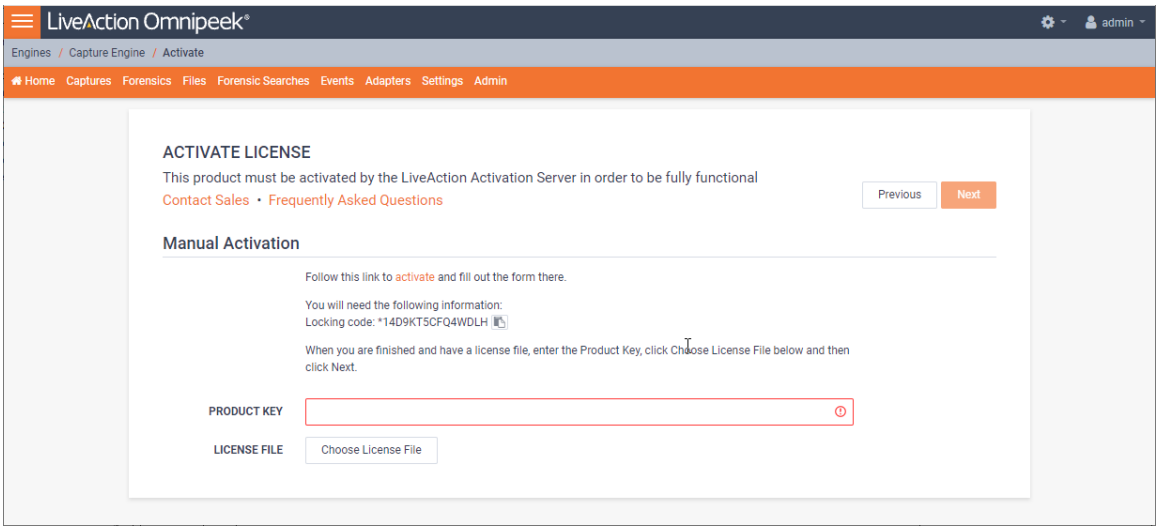
3. If your client has an active Internet connection, select *Automatic* and click **Next**. The **Customer Information** window appears. Continue with Step 4 below.



- *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.

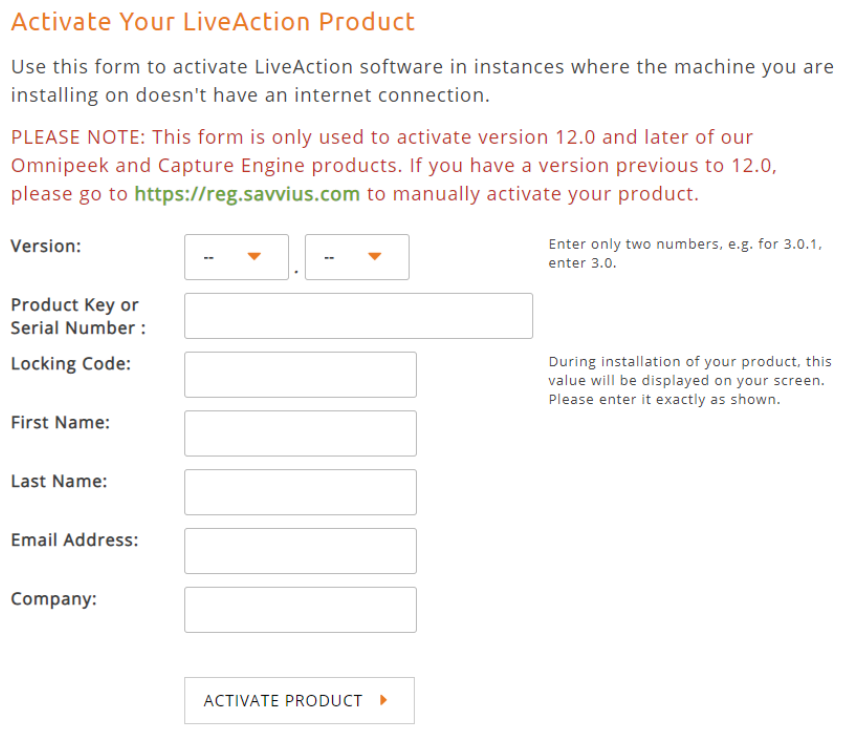


Note The *Locking code* displayed in the window above is required in Step 6 below. You can click the small icon next to the code to save it to the clipboard so you can paste it into the Locking Code field in Step 6 below.

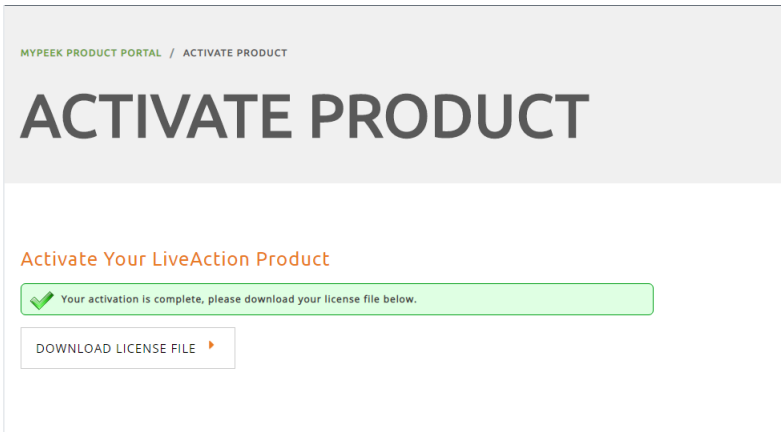
4. Complete the Customer Information window and click **Next**. LiveWire is now activated and you can begin using the product. The activation process is complete.

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.



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



7. Click **DOWNLOAD LICENSE FILE** to save the license file to your computer. You will need the license file in the following steps.
8. Return back to the to the **Manual Activation** window, and click **Choose License File**.
9. Navigate to the license file downloaded above and click **Open**.

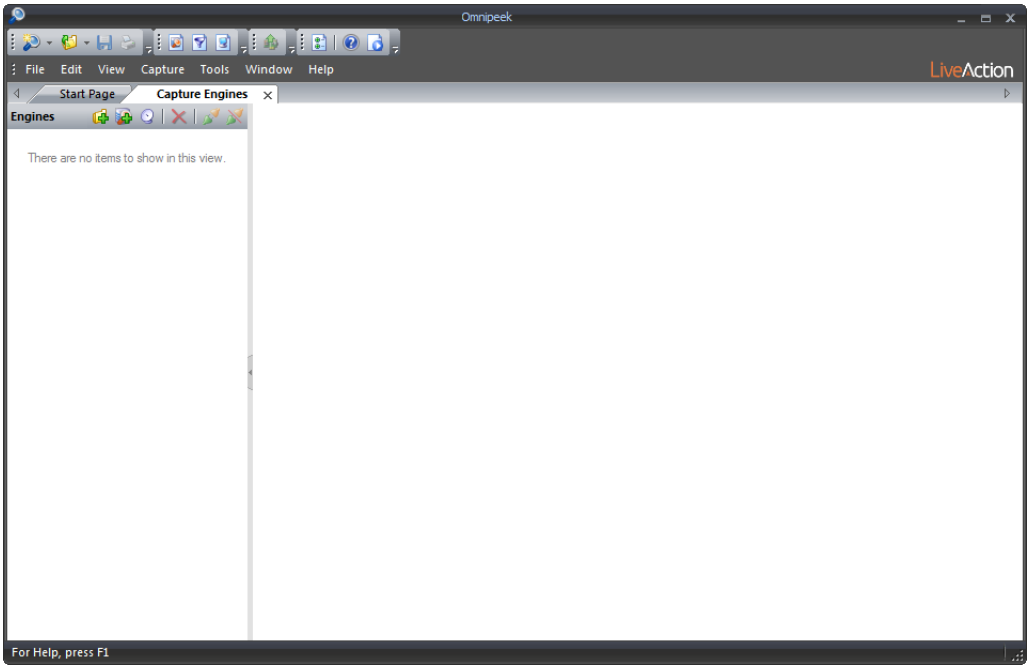
10. Click **Next** in the **Manual Activation** window. LiveWire is now activated and you can begin using the product. The activation process is complete.

Activation via Omnipeek

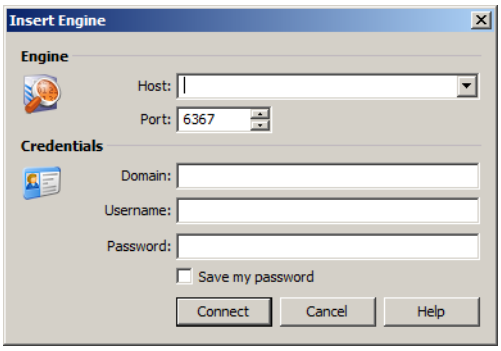
> **Note** Activation of LiveWire via Omnipeek is supported on Omnipeek version 13.1 or higher.

To activate LiveWire via Omnipeek:

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

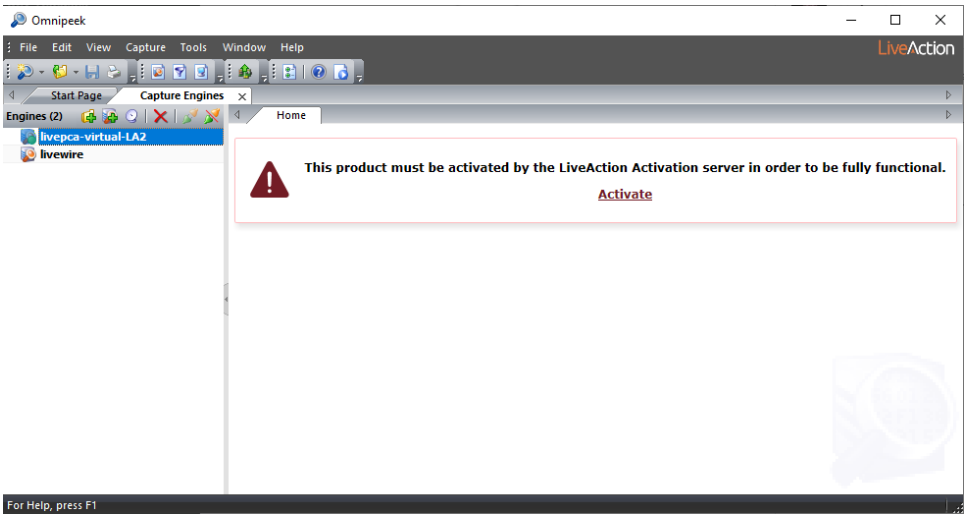


2. Click *Insert Engine* and complete the **Insert Engine** dialog.

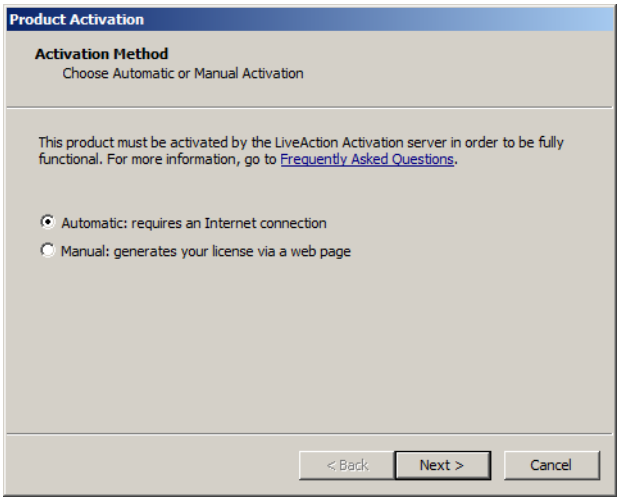


- *Host*: Enter the IP address of LiveWire.
- *Port*: Enter the TCP/IP port used for communications. Port 6367 is the default for LiveWire.
- *Domain*: Type the Domain for login to LiveWire. If LiveWire is not a member of any Domain, leave this field blank.
- *Username*: Type the username for LiveWire.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

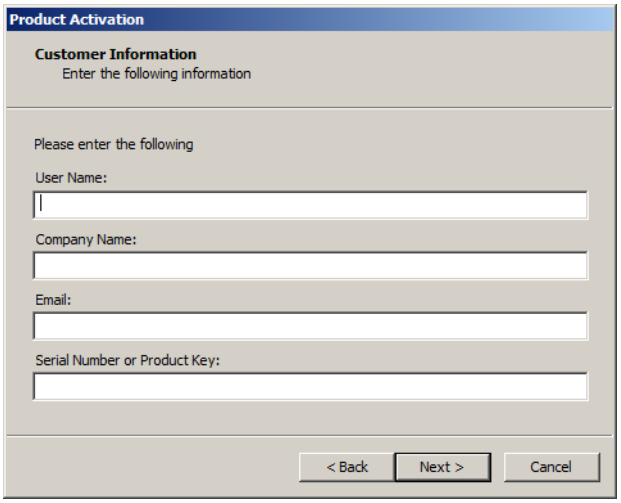
3. Click **Connect** to connect to LiveWire. If LiveWire has not yet been activated, the activation message appears in the **Capture Engines** window.



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



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



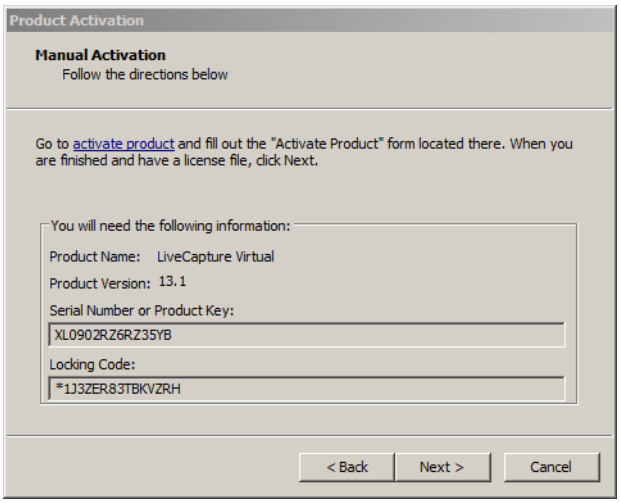
- *User Name*: Type the user name of the customer.

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

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

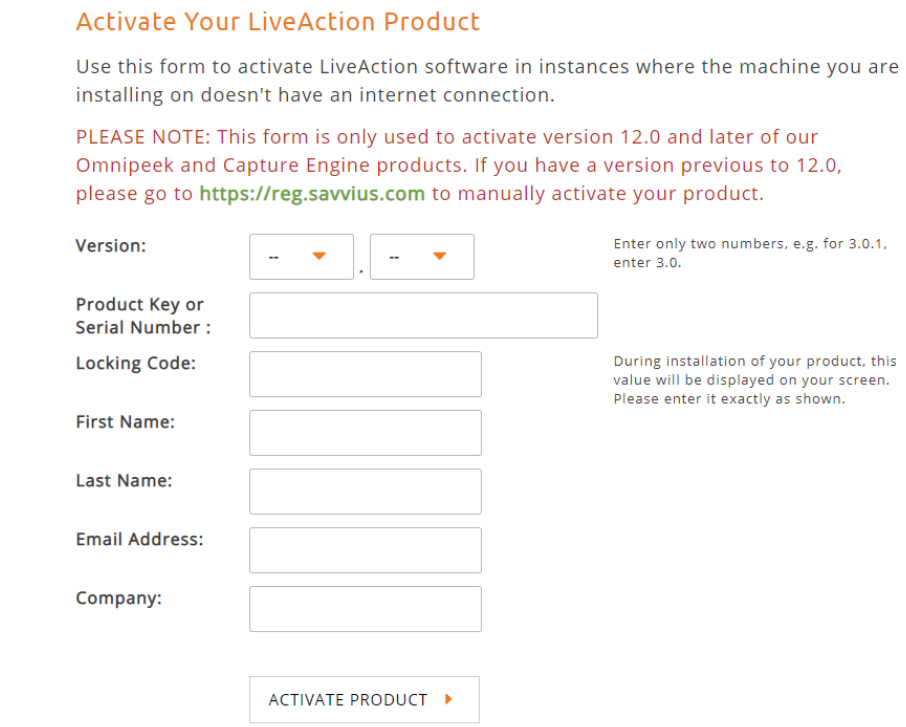
   If you selected the *Manual* activation, the **Manual Activation** dialog appears. You will need to continue with the remaining steps.

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

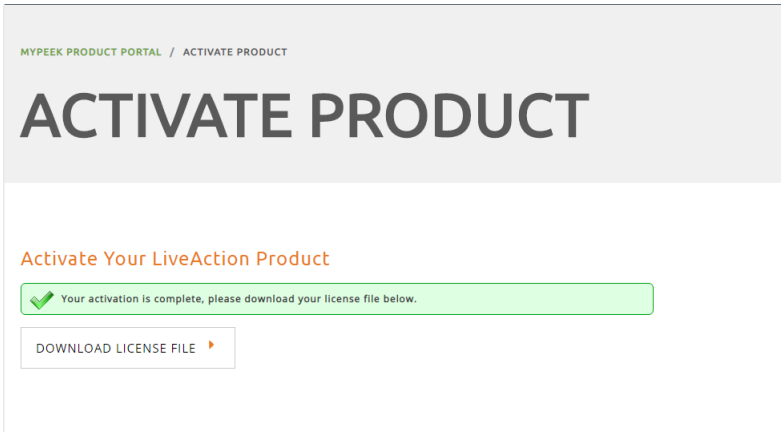


Note The *Product Key*, and also the *Locking Code* displayed in the **Manual Activation** dialog are required in the next step. You can cut and paste this information from the **Manual Activation** dialog when required in the next step.

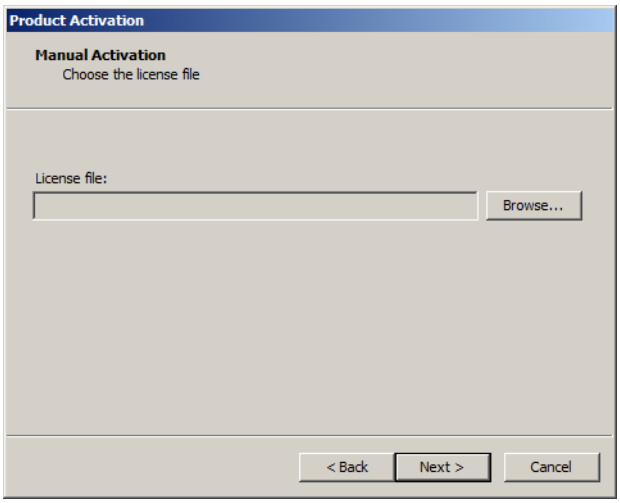
7. Click the *activate product* link (*https://mypeek.liveaction.com/activate_product.php*) in the dialog. A web browser page opens that allows you to activate your LiveAction product and to obtain and download a license file. The license file is required to complete the manual activation.



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



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



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

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 77.

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.

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*

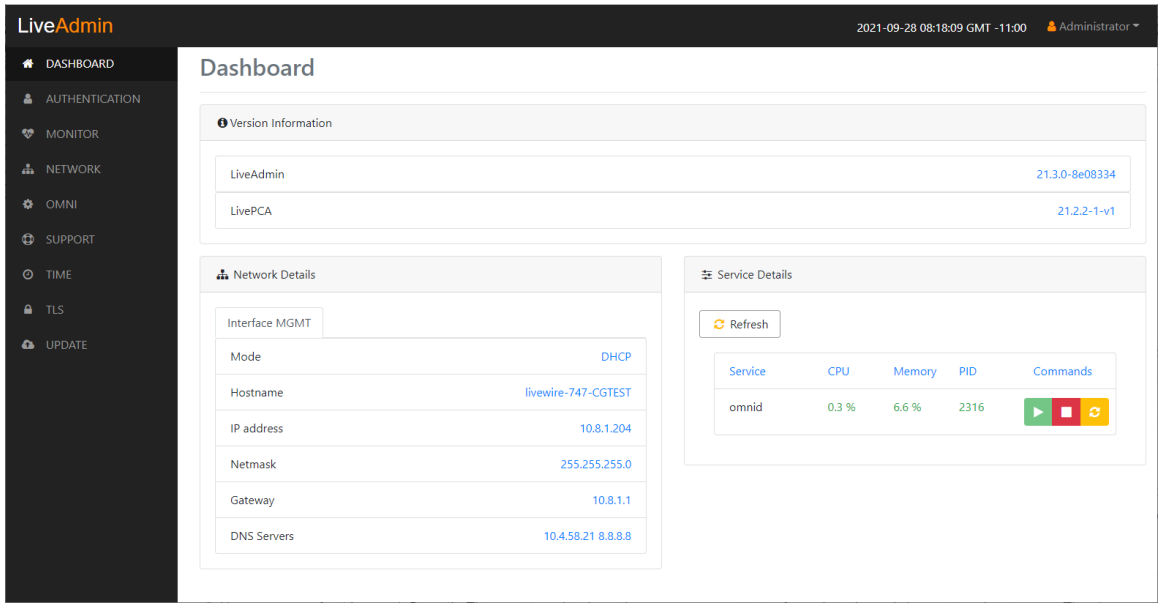
password: *admin*

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*: The *Dashboard* view provides you with some very basic information about the system. See 'Dashboard' on page 28.
- *Authentication*: The *Authentication* view lets you change the password for LiveWire. See 'Authentication' on page 29.
- *Monitor*: The *Monitor* view displays the health of the overall system. See 'Monitor' on page 30.
- *Network*: The *Network* view lets you configure the primary network interfaces network settings and the hostname of the system. See 'Network' on page 30.
- *Omni*: The *Omni* view lets you enable the Device Management Server (DMS) for the appliance. See 'Omni' on page 32.
- *Support*: The *Support* view let you download logs from the system that would be helpful in troubleshooting issues. See 'Support' on page 35.

- *Time*: The *Time* view lets you configure the system's Timezone and NTP servers. See 'Time' on page 36.
- *TLS*: The *TLS* view lets you change the self-signed certificates that LiveAdmin and Omnipeek use for HTTPS. See 'TLS' on page 37.
- *Update*: The *Update* view lets you update the appliance using a software update package. See 'Update' on page 37.
- *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 38.

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 the DMS as described in 'Using DMS to manage and configure LiveAction appliances' on page 38.

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.

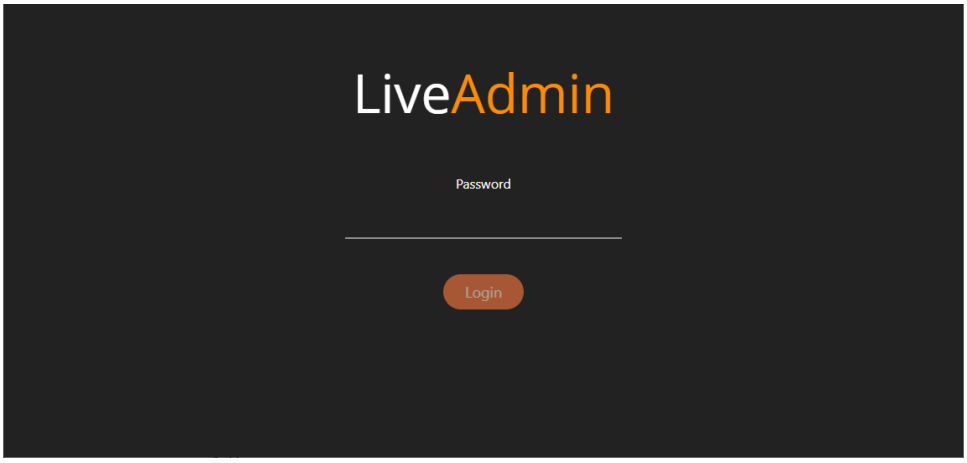
Login

To log into the LiveAdmin utility:

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

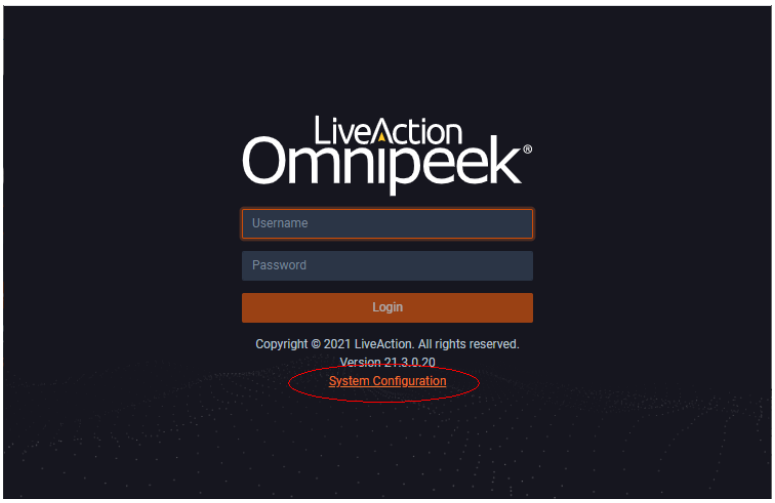
   LiveWire Edge: Connect the '0 MGMT' port on LiveWire Edge to your network router or switch with an Ethernet cable.

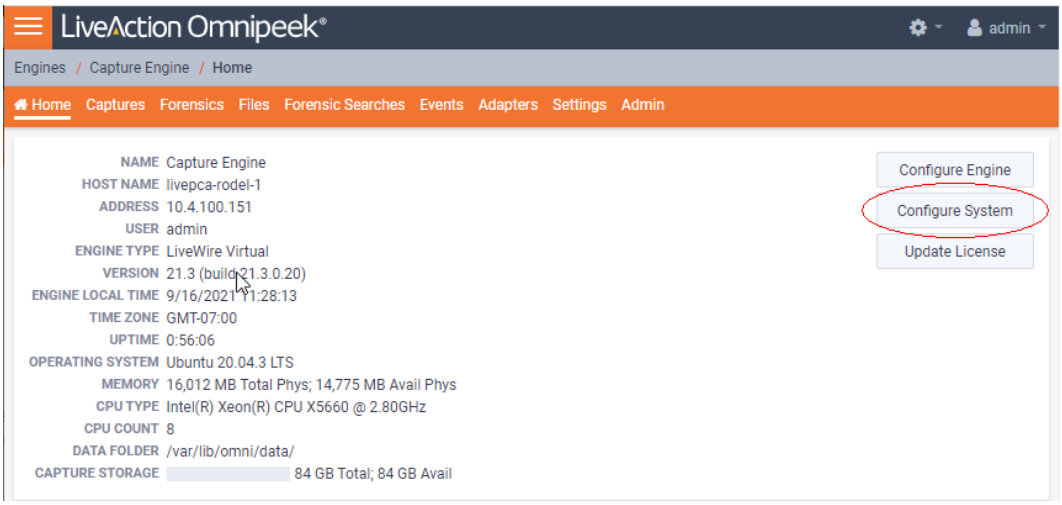
2. From a browser window on a computer connected to the same network as LiveWire, enter the IP address for LiveWire in the URL box as *<IP address>:8443* (e.g., 192.168.1.21:8443). The LiveAdmin Login screen appears.



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

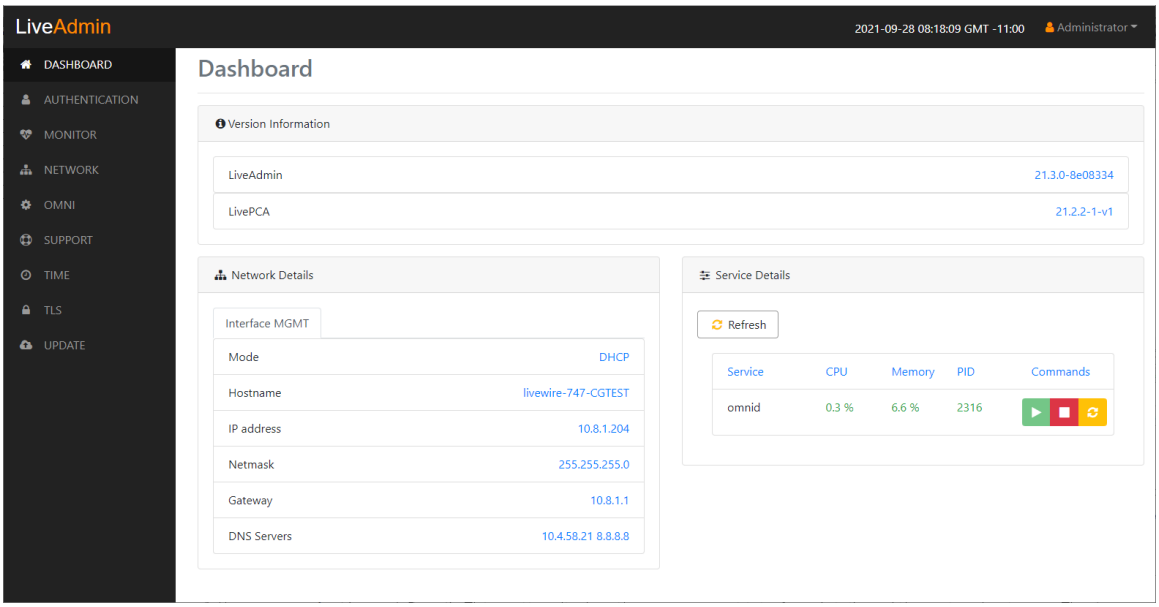
Note If you are using Omnipeek Web, you can also access the LiveAdmin Login screen by clicking *System Configuration* from either the Omnipeek Login screen, or by clicking *Configure System* from within Omnipeek itself.





Dashboard

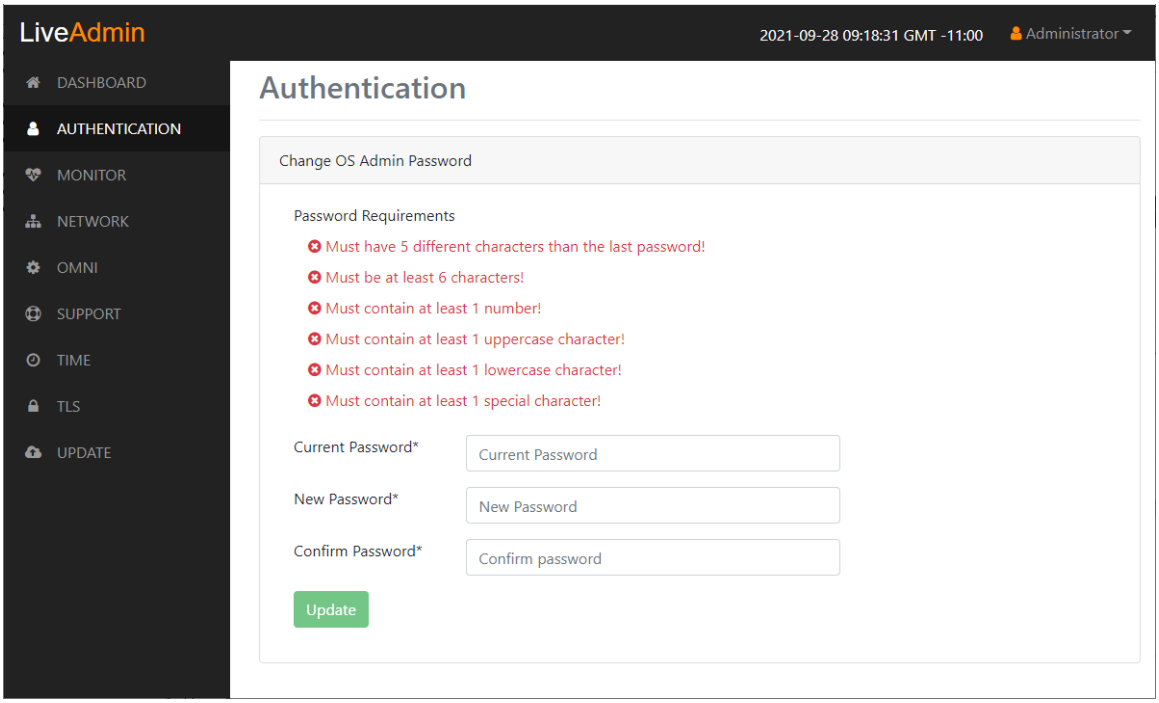
The Dashboard view provides you with some very basic information about the system.



- *Version Information*: This section displays the version numbers of the LiveAdmin utility and the software on the LiveAction appliance.
    - *LiveAdmin*: Displays the version number of the LiveAdmin utility
    - *LivePCA*: Displays the version number of the software installed on the LiveAction appliance.
- *Network Details*: This section displays the management interface details and the system hostname. The management interface is defined from the Network view in LiveAdmin. See 'Network' on page 30.
- *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.



- *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

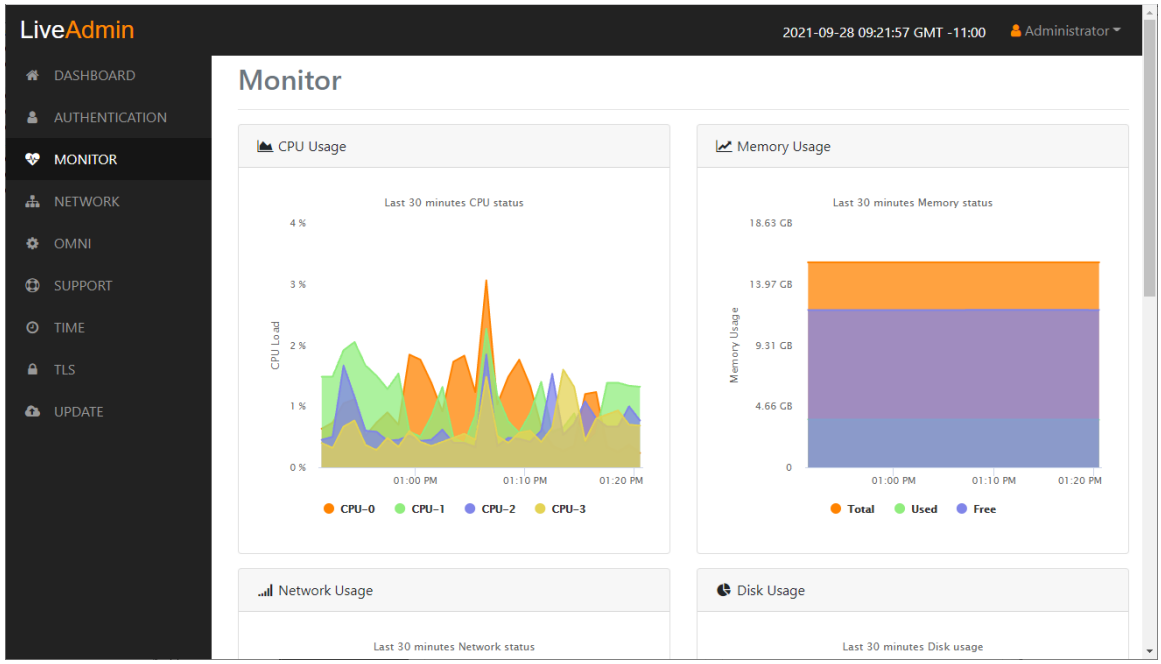
- Must contain at least 1 uppercase character.
- Must contain at least 1 lowercase character.
- Must contain at least 1 special character.

- *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.

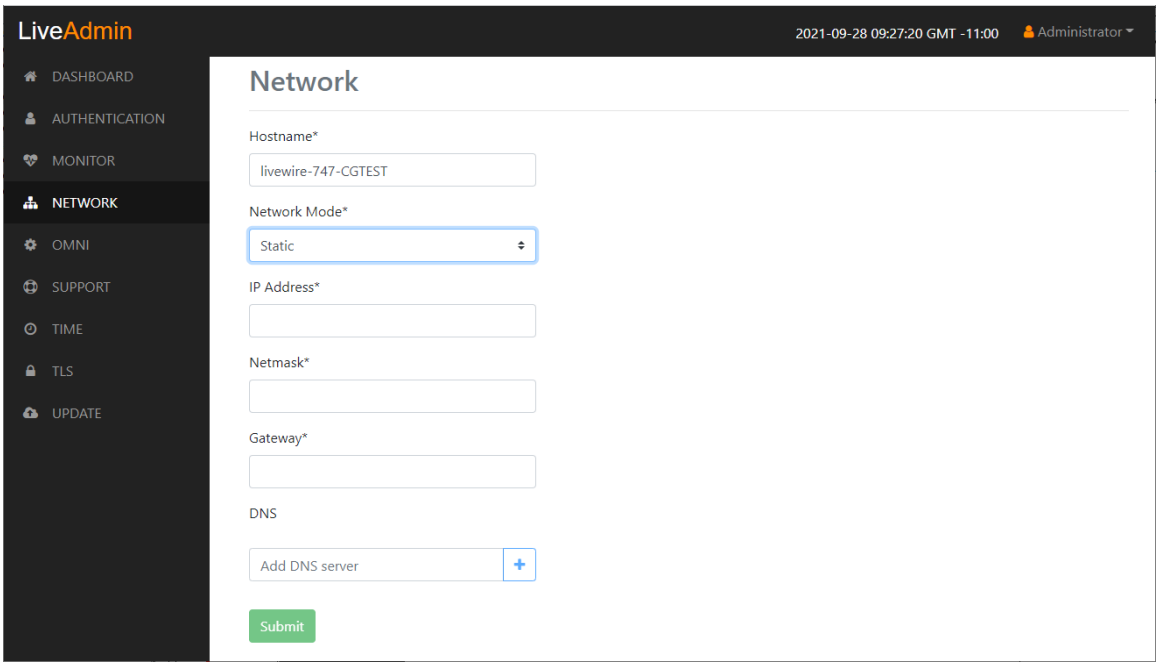


- *CPU Usage*: This chart displays the current usage of individual CPUs on the system. Click the CPU label in the legend to enable/disable its data displayed in the chart.
- *Memory Usage*: This chart displays the current amount of memory being consumed on the system. Click the *Total*, *Used*, or *Free*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



- *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

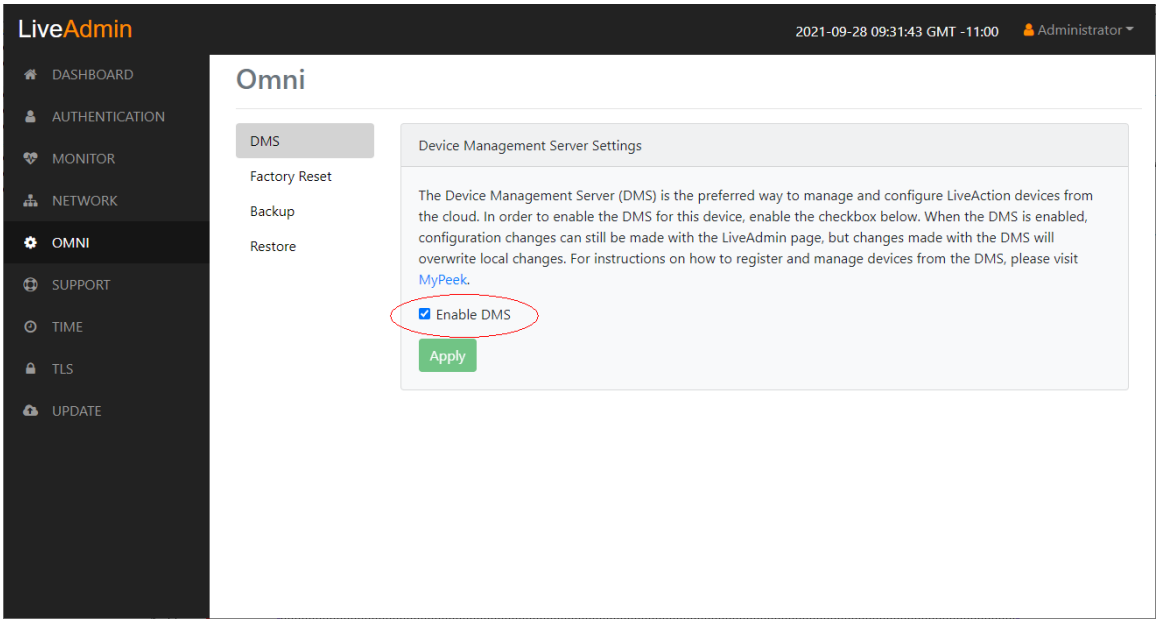
To configure a static IP address:

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

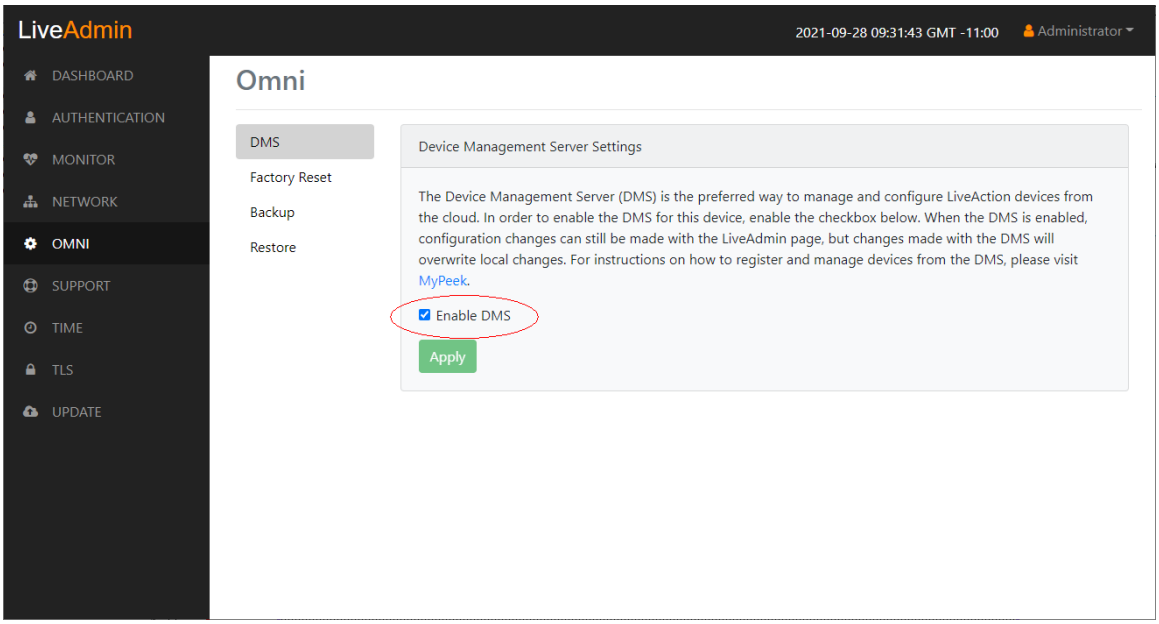
The *Omni* view lets you enable the Device Management Server (DMS) for the appliance, Factory Reset for LiveWire Edge, Backup, and Restore options.



DMS

The *DMS* (Device Management Server) is the preferred way to manage and configure LiveAction appliances from the cloud. In order to enable the DMS for LiveWire, enable the check box. When the DMS is enabled,

configuration changes can still be made with the LiveAdmin utility, but changes made with the DMS will overwrite local changes. For instructions on how to register and manage devices from the DMS, please visit *MyPeek*.



- *Enable DMS*: Select this check box to enable the DMS for LiveWire to manage and configure LiveWire from the cloud. See 'Using DMS to manage and configure LiveAction appliances' on page 38.

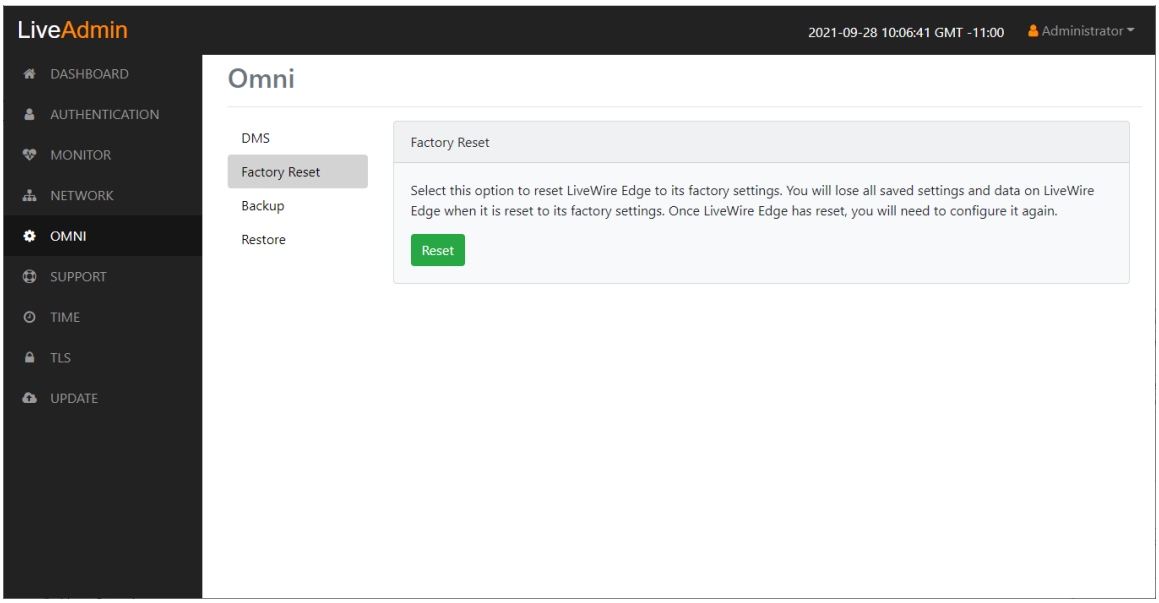
Note When DMS is enabled, you can make local changes to LiveWire using the LiveAdmin utility; however, changes made with the DMS will overwrite any local changes made with the LiveAdmin utility.

Factory reset

Factory reset (LiveWire Edge only) allows you to reset the LiveAction software to factory defaults on LiveWire Edge.

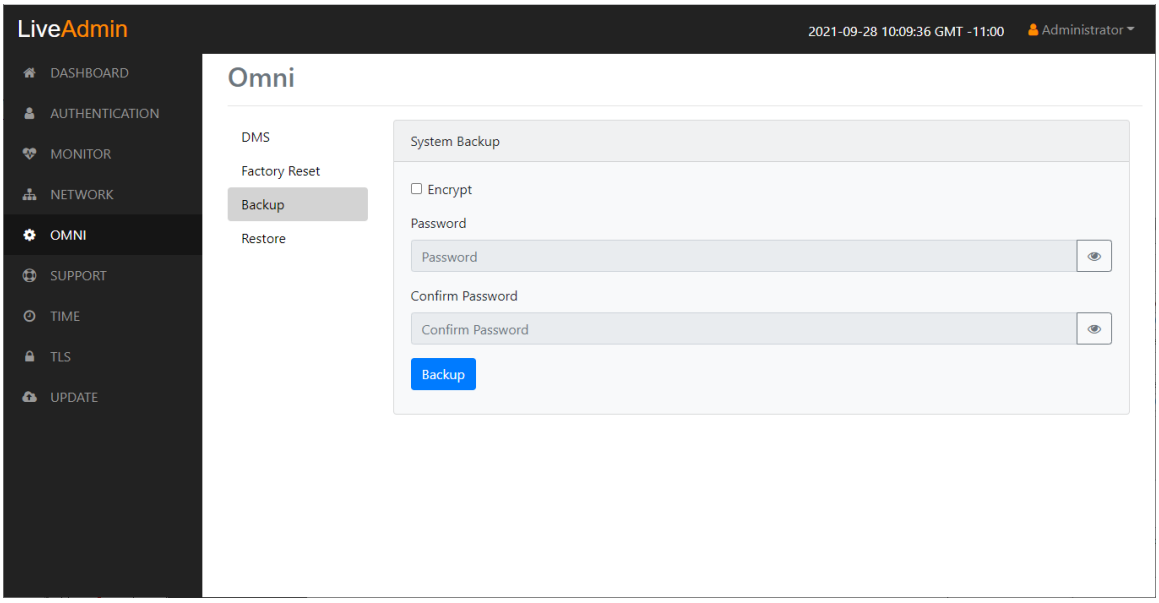
- *Factory Reset*: Click **Reset** to reset the LiveAction software.

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



Backup

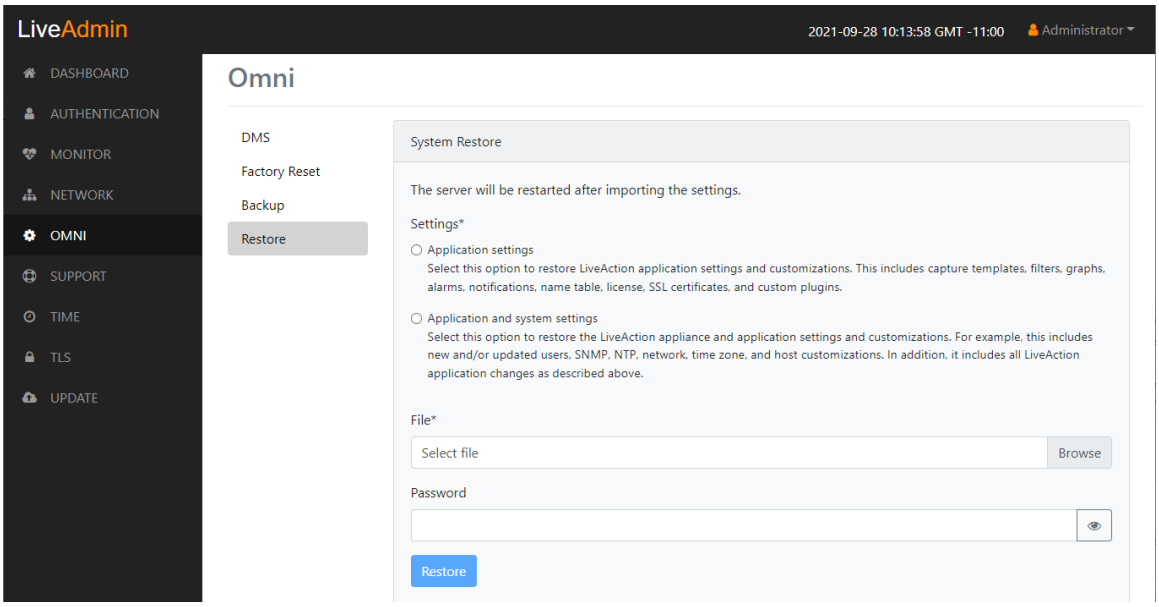
Backup allows you to back up all the system data on LiveWire to a back up file that you can restore at a later time.



- *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.

Restore

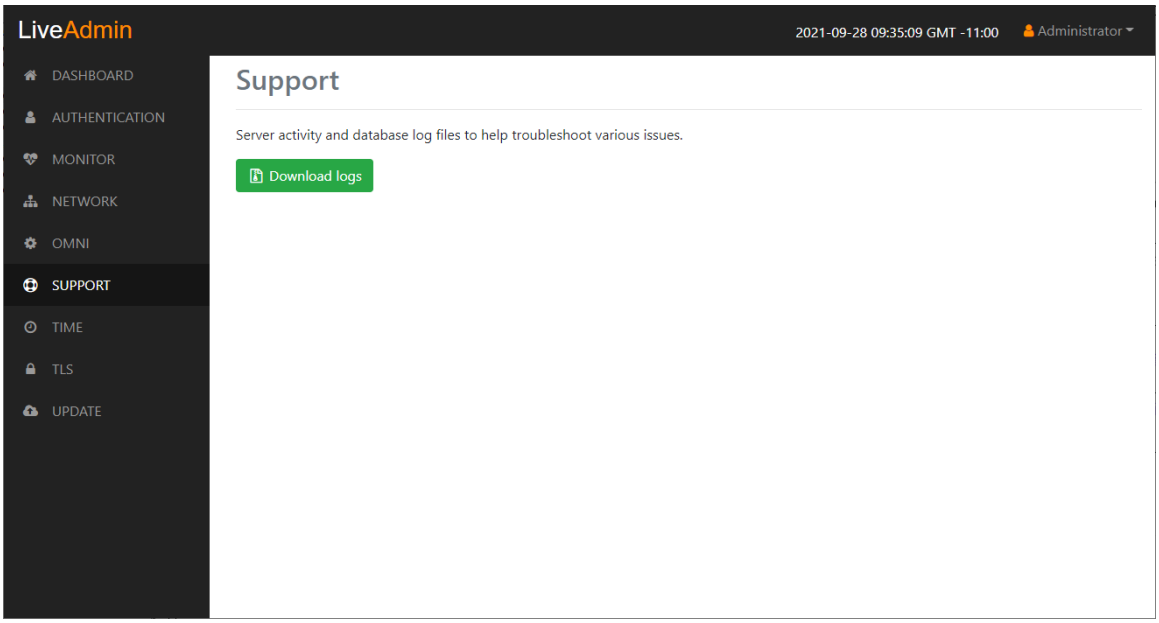
Restore allows you to restore to LiveWire a backup that was previously performed on LiveWire. To perform a restore, you will need the backup file you want to restore and any password associated with the backup.



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

Support

The Support view lets you download logs from LiveWire that would be helpful in troubleshooting issues.



- *Download logs*: Click to download the ***logs.tgz*** file to your default location.

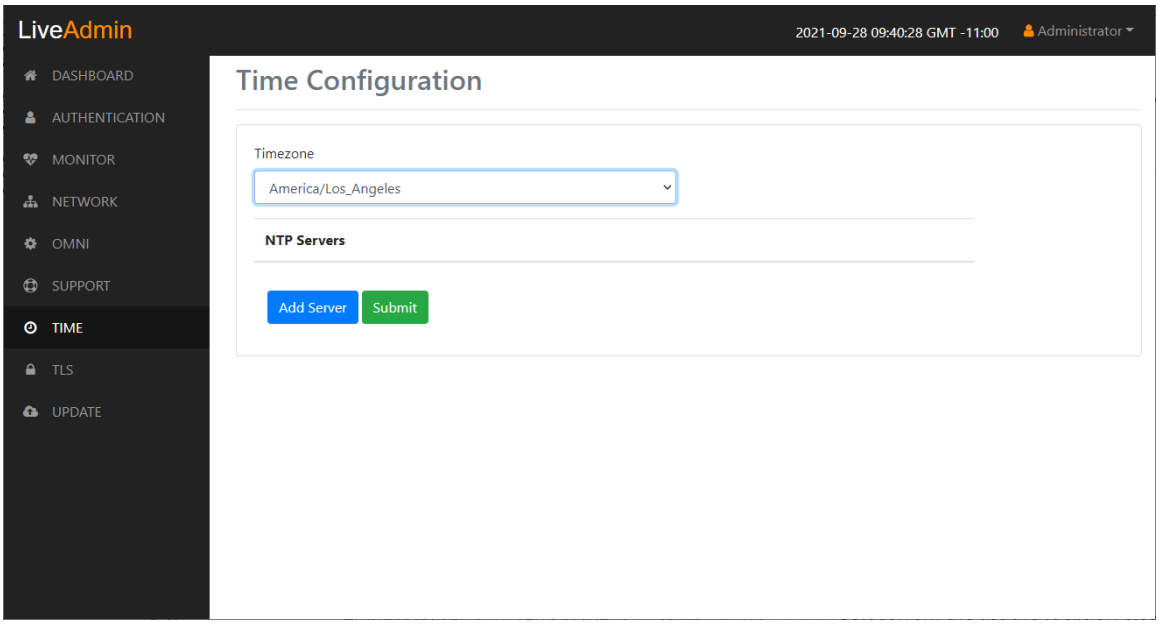
  The ***log.tgz*** file will consist of the following information and files:

  - */proc/mounts*

- */proc/meminfo*
- */proc/net/dev*
- */var/log/auth.log*
- */var/log/boot.log*
- */var/log/dmesg*
- */var/log/dms.log*
- */var/log/dmsd.log*
- */var/log/kern.log*
- */var/log/live*
- */var/log/liveflow*
- */var/log/nginx*
- */var/log/omniperf.log*
- */var/log/omnitrace.log*
- */var/log/routermap_to_interface.log*
- */var/log/syslog*

Time

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



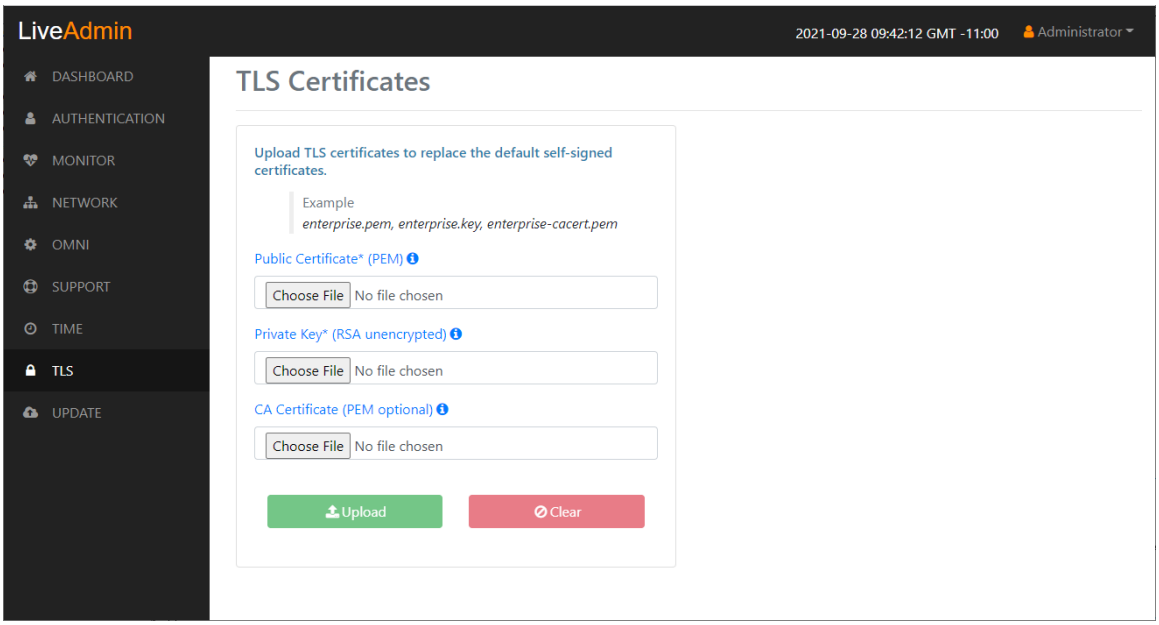
- *Timezone*: The Timezone setting lets you specify the physical location of LiveWire. Select from the list the location closest to your LiveWire.
- *NTP Servers*: The NTP (Network Time Protocol) server setting displays the NTP servers used to synchronize the clocks of computers over a network. Many features of LiveWire require accurate timestamps to properly analyze data.

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

- *Add Server*: Click to add a new NTP server to the list. Enter the IP address of the NTP server and click **Save** 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.

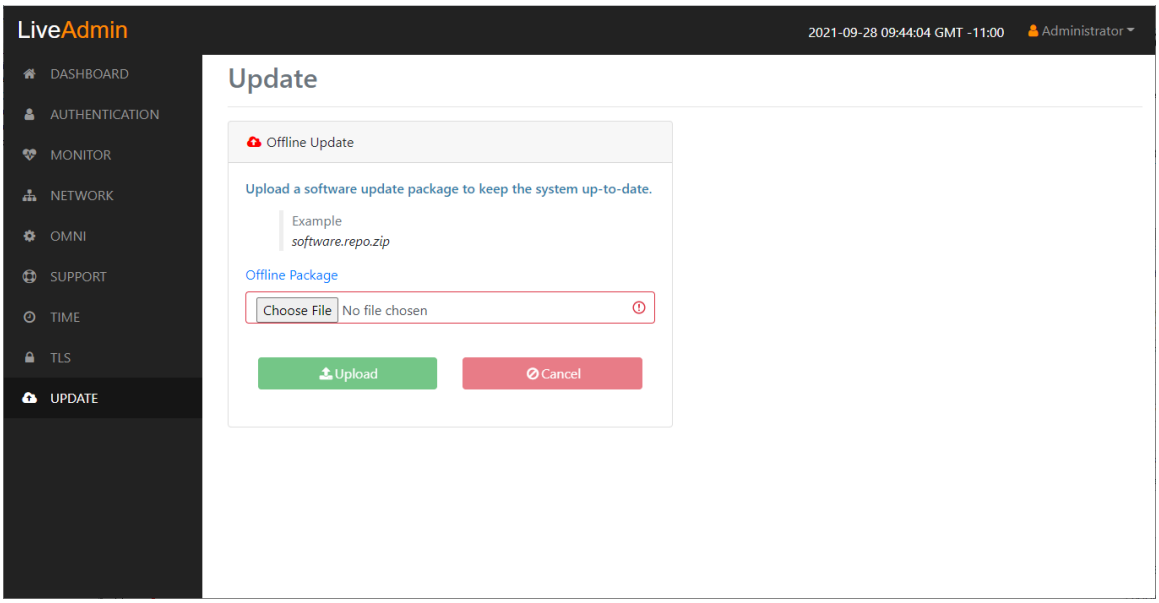


- *Public Certificate* (PEM)*: Click **Choose File** to browse and select your Public Certificate file. Click the information icon to display an example of the file.
- *Private Key* (RSA unencrypted)*: Click **Choose File** to browse and select your Private Key file. Click the information icon to display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

Update

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

Note Updating the software will cause the system to reboot.



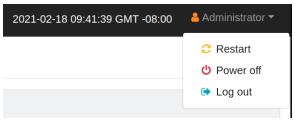
To update the software:

1. Download the latest software update package to your system.
2. Click **Choose File** and select the software update package.
3. Click **Upload** 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 DMS to manage and configure LiveAction appliances

If you have one or more LiveAction appliances, you can use the Device Management Server (DMS) to manage and configure these appliances from the cloud. In order to use the DMS server for the LiveAction appliance, you must first enable the *Enable DMS* option in the LiveAdmin utility as described in 'Omni' on page 32.

Note When DMS is enabled, you can make local changes to the LiveAction appliance using the LiveAdmin utility; however, changes made with the DMS will overwrite any local changes made with the utility.

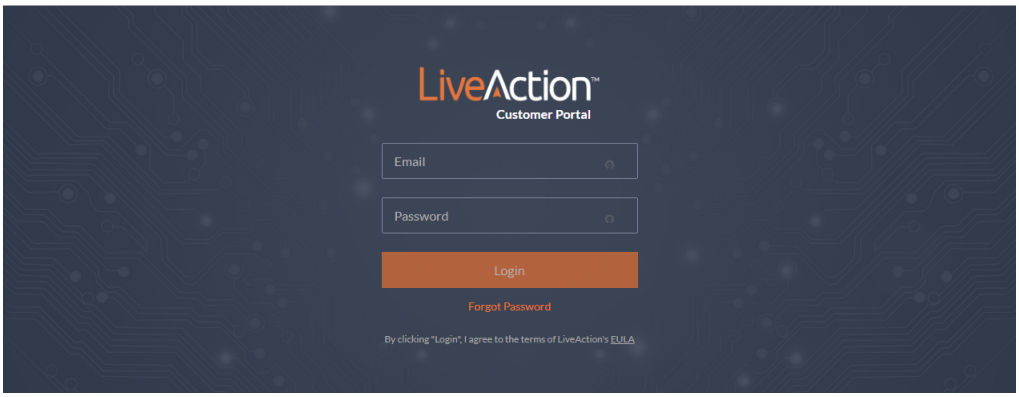
Note All DMS communications require that the LiveAction appliance has Internet access and is able to access various websites including *https://mypeek.liveaction.com* and *https://cloudkeys.liveaction.com* using TCP over port 443. If necessary, configure a DNS server to resolve the URLs above.

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

To use DMS to manage and configure LiveAction appliances:

1. Log into the LiveAction Customer Portal at *https://cloudkeys.liveaction.com/*.

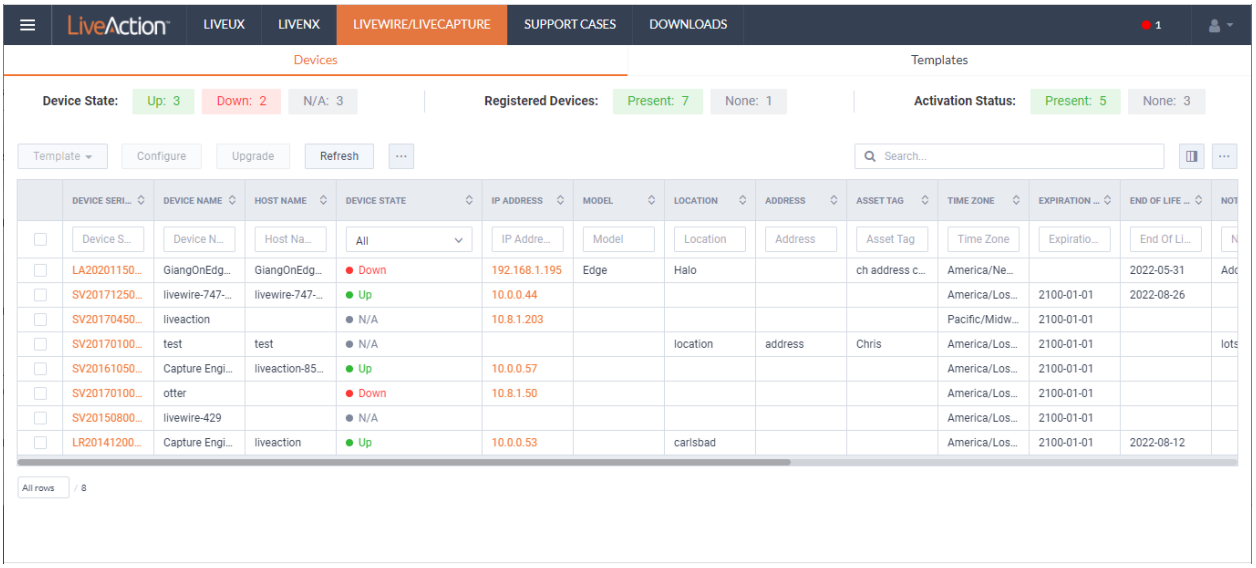
Note A link to the LiveAction Customer Portal and a temporary password is emailed to the customer whenever a LiveAction appliance is purchased. Use the customer email and temporary password to log into the customer portal. You will be required to change the temporary password upon first login.



2. Click the **LIVEWIRE/LIVECAPTURE** tab at the top of the portal to configure the appliances. The LiveAction appliances associated with the user account are displayed.

DMS Devices tab

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



Device State

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

- *Up*: Displays the number of devices that were able to connect the DMS portal.
- *Down*: Displays the number of devices the DMS portal 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 the DMS portal.

Registered Devices

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

- *Present*: Displays the number of devices that have registered with the DMS portal.
- *None*: Displays the number of devices that have not registered with the DMS portal.

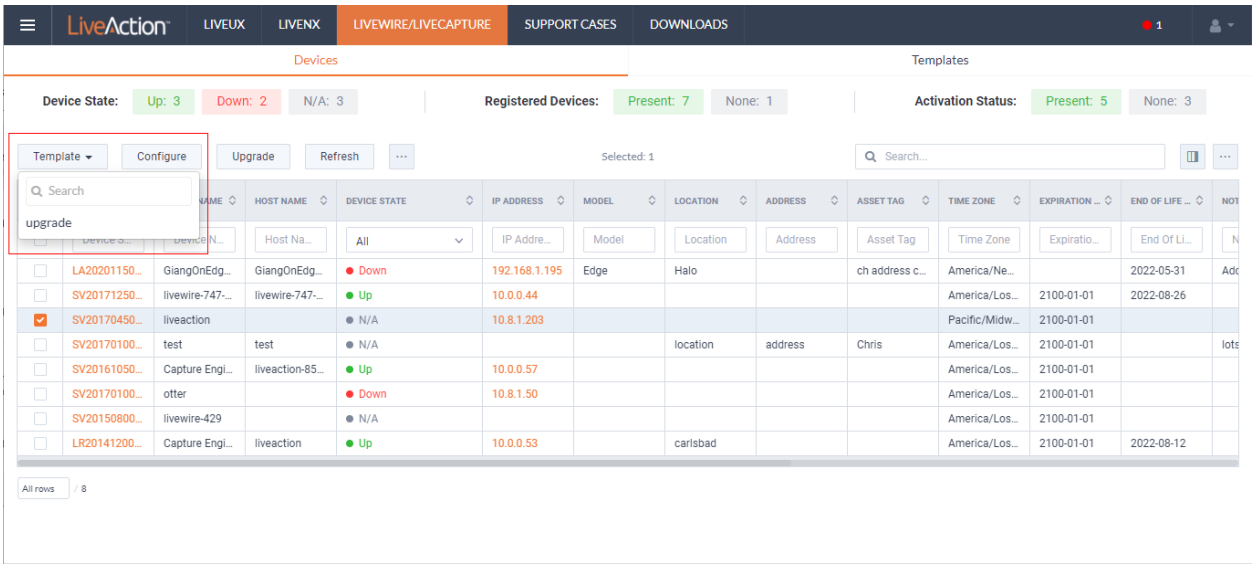
Activation Status

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

- *Present*: Displays the number of devices that have been activated with the DMS portal.
- *None*: Displays the number of devices that have not been activated with the DMS portal.

Template

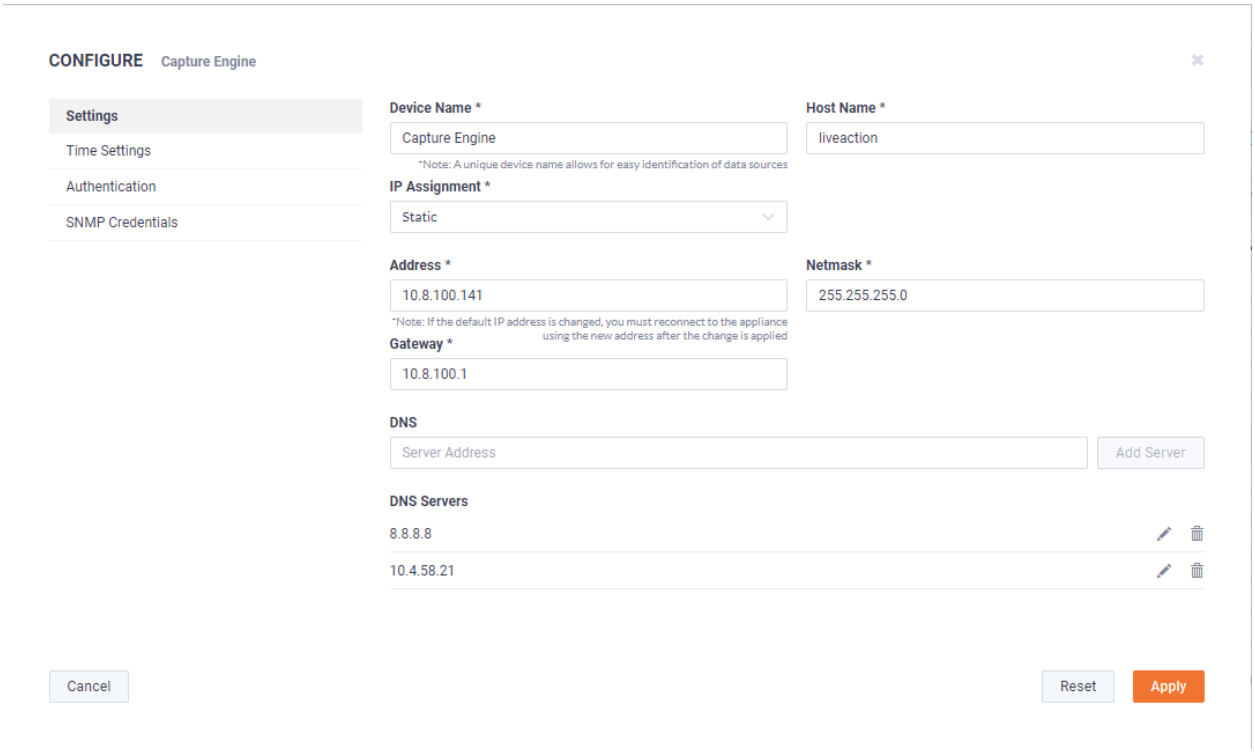
Click the **Template** button to select a template to apply to the selected devices. Templates allow you to apply version-specific settings to one or more devices. To create a template or modify an existing template, see 'DMS Templates tab' on page 55.



Configure

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*. There are tabs available for configuring *Settings*, *Time Settings*, and *Authentication*.

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.
- *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:

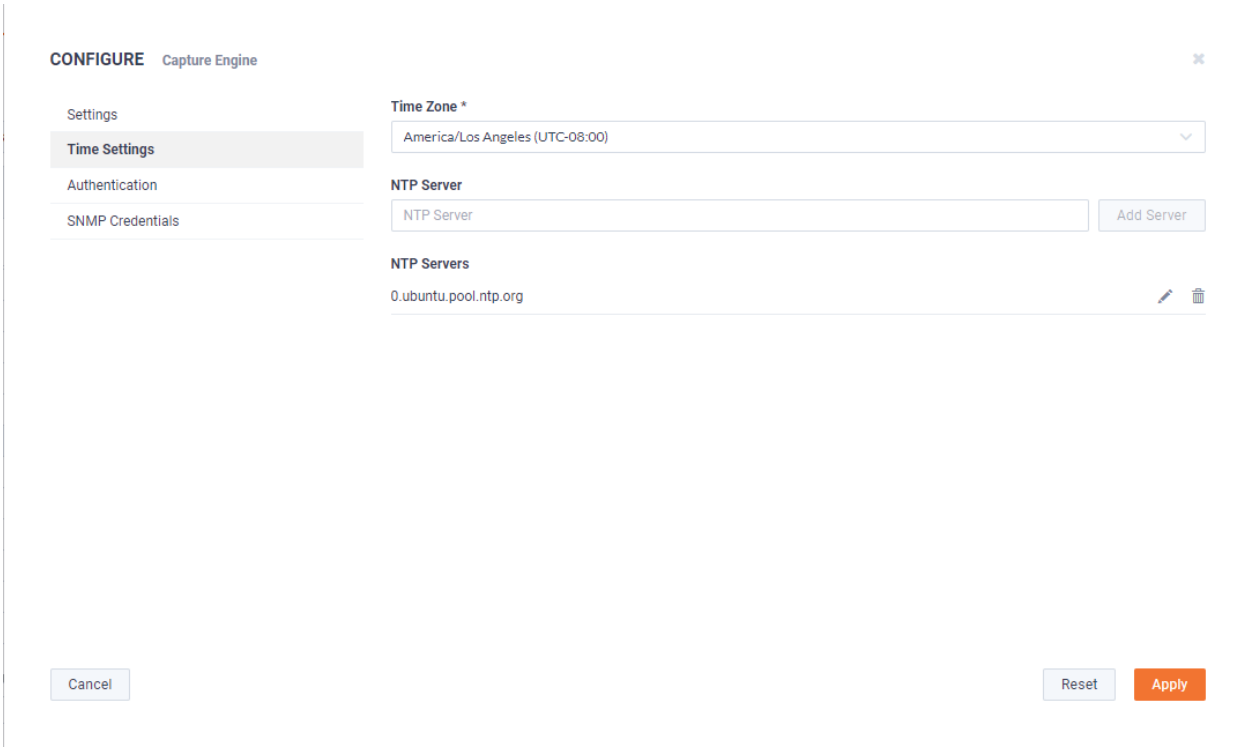
Important! LiveWire is pre-configured to obtain an IP address automatically from a DHCP server; however, we strongly recommend the use of a static IP address for LiveWire. If DHCP is selected as the *IP Assignment*, and if the address should change on a new DHCP lease, then the user must look up the 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, and click **Add Server**. Multiple DNS name servers can be defined. You can also edit or 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.

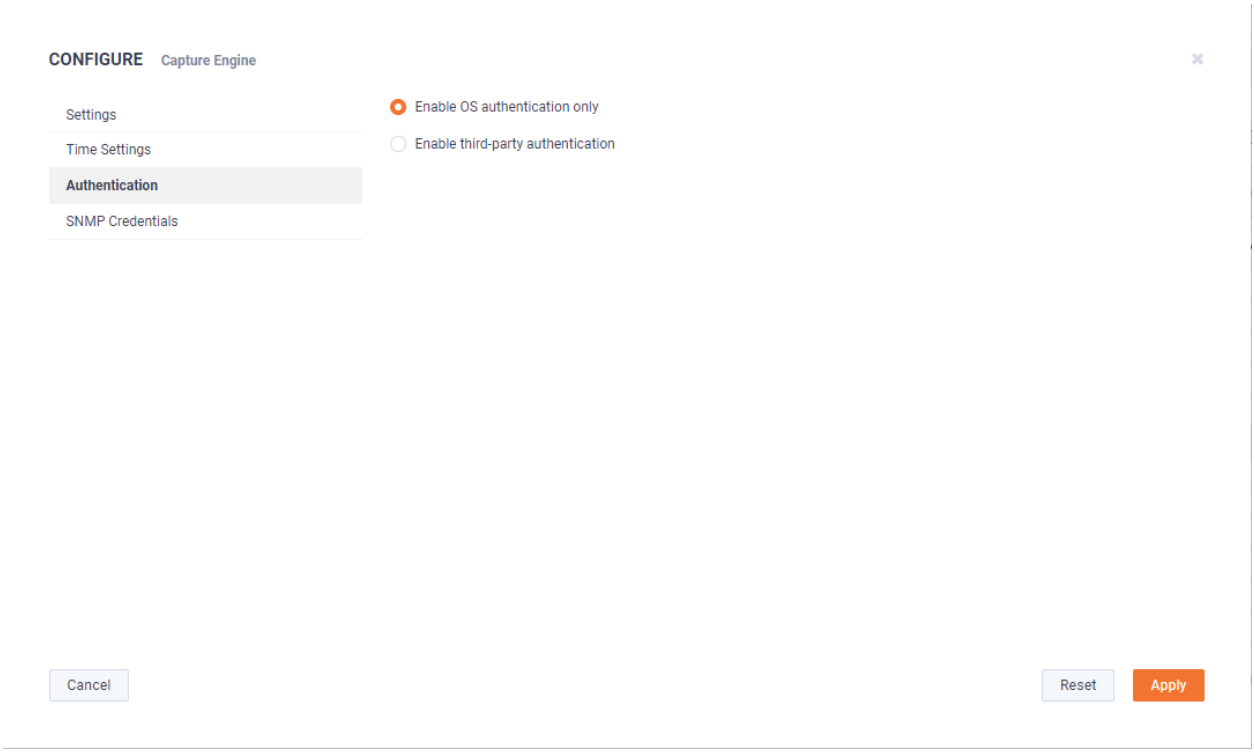
- *DHCP Timeout*: Displays the amount of time (in seconds) the device will wait for a DHCP address.

Time Settings



- *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*. You can click the **Edit** icon to edit an NTP server in the list, or click the **Trash** icon to remove an NTP server from the list.

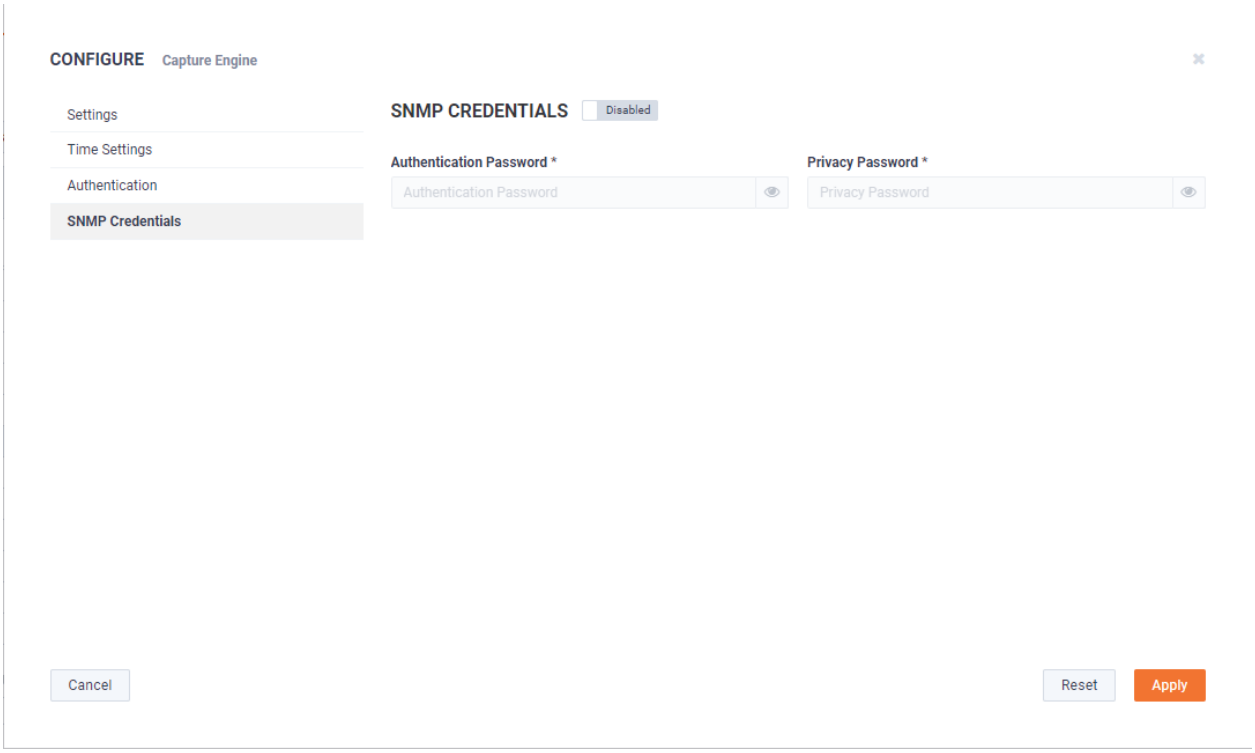
Authentication



- *Enable OS authentication only*: Select this option to use the local OS authentication.

- *Enable third-party authentication*: Select this option to use TACACS+ or RADIUS authentication. If this option is selected, click **Add** to configure the new authentication setting.
  - *Add*: Click to add a new authentication setting. You will need to configure the new authentication setting.
  - *Search*: Enter the text string to search the list of authentication settings.
  - *Name*: Displays the name of the authentication setting.
  - *Type*: Displays the type of authentication, which can be either 'RADIUS' or 'TACACS+.'
  - *Host*: Displays the host of the authentication setting.
  - *Port*: Displays the port of the authentication setting.
  - *Secret*: Displays the secret key of the authentication setting.
  - *In Use*: Displays whether or not the authentication setting is in use.
  - *Action*: Click the *Edit* icon to edit the authentication setting, or click the *Trash* icon to delete the authentication setting.
  - *Apply*: Click to save the authentication setting.

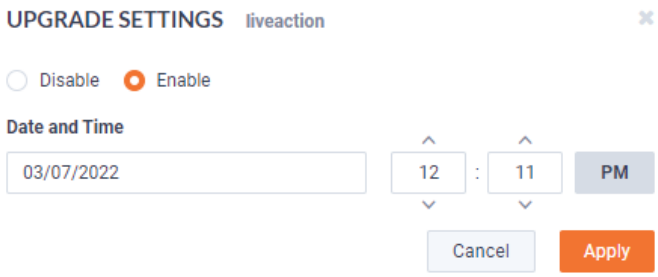
SNMP Credentials



- *Enabled/Disabled*: Select to enable or disable the *SNMP Credentials* configured below for the *Authentication Password* and *Privacy Password*.
- *Authentication Password*: Type a new *Authentication Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 85.
- *Privacy Password*: Type a new *Privacy Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 85.

Upgrade

Click the **Upgrade** button to upgrade the selected appliance remotely through the DMS. 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.



- *Disable*: Select to disable the upgrade on the selected devices.
- *Enable*: Select to enable the upgrade on the selected devices. If you enable the upgrade, you are presented with settings to specify the 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.
- *Apply*: Click to save the changes to the selected devices.

Refresh

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

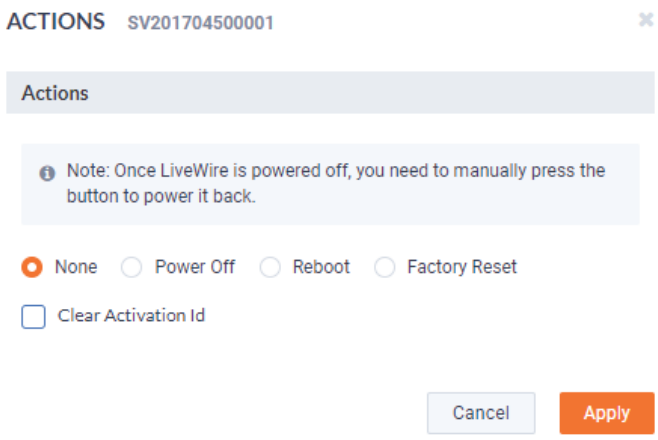
Elipsis (...)

Click the **Elipsis** (...) to view the following options:

- Power and Reset
- Change Password
- Edit Additional Info
- Backup Settings
- Restore Backup
- Share
- Create Template
- Compare Configurations
- iDRAC Settings

Power and Reset

Select the *Power and Reset* option to perform the actions below on the device.

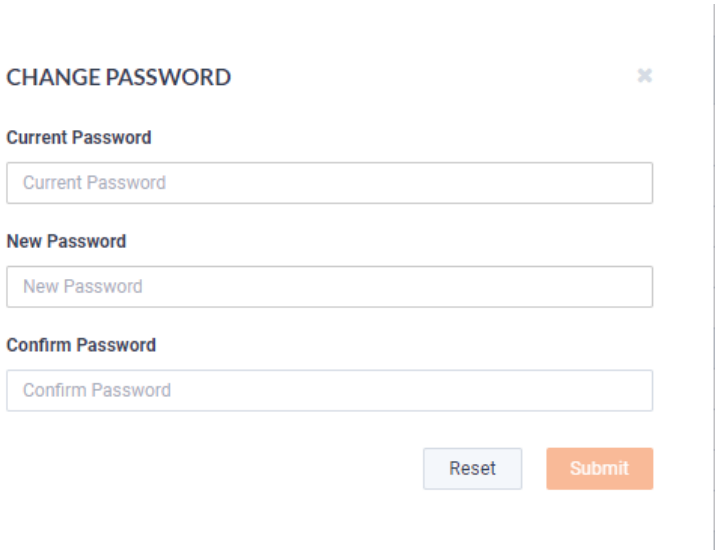


- *None*: Select to not perform an action on the selected appliances.
- *Power Off*: Select to power off the selected device. Once the device is powered off, you must manually press the power-on button on each of the devices to power them back on.
- *Reboot*: Select to reboot the selected appliances.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

Note If you select *Factory Reset* on a LiveWire Edge (or by hitting either the reset button or from the command line), then you will also need to select *Clear Activation ID* for that device in the DMS.

Change Password

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



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

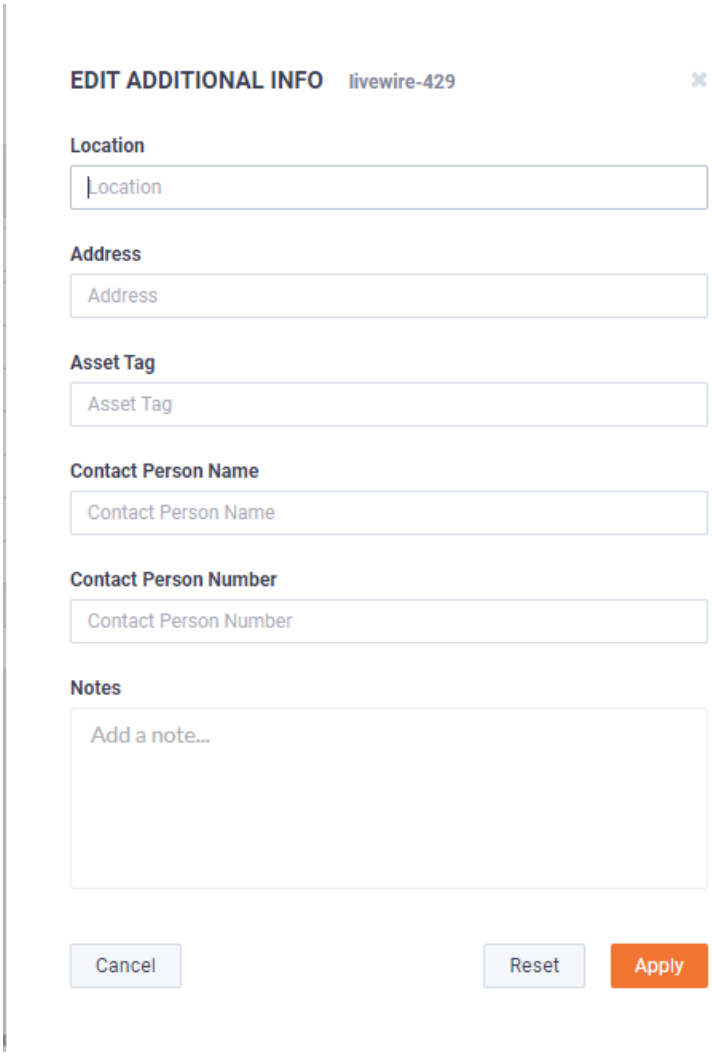
  Must have 5 different characters than the last password.
  Must be at least 6 characters.

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.

Edit Additional Info

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

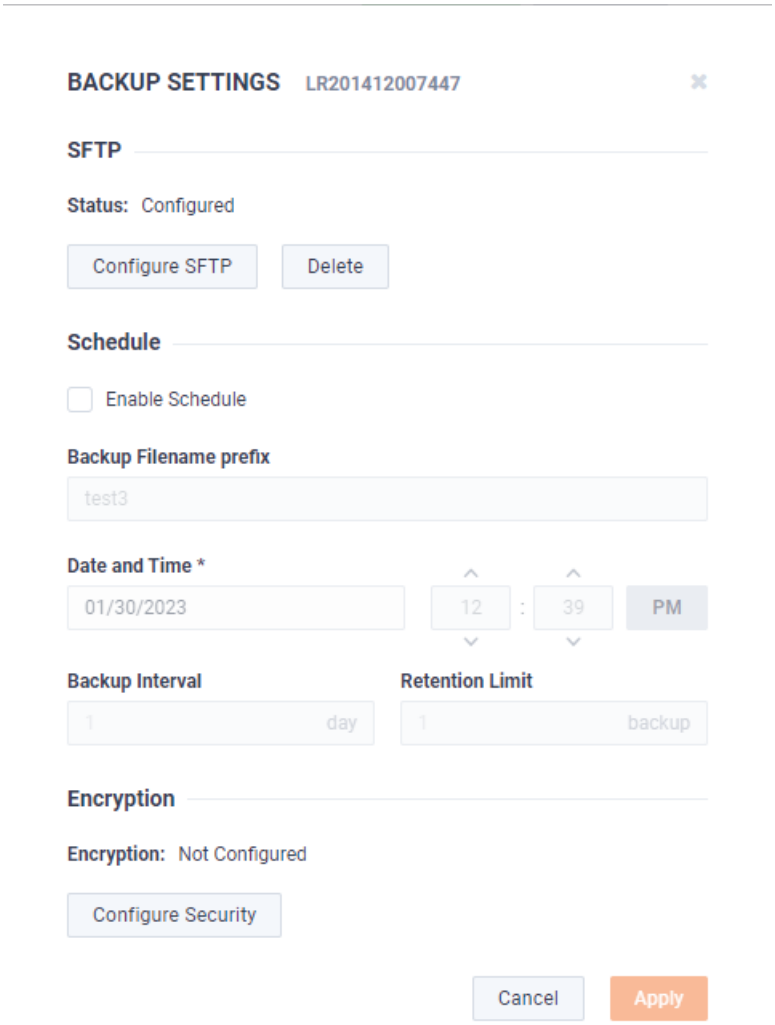


- *Location*: Displays the general location of the device. Type a new location to change the location. We suggest entering the physical location of the device for the organization. For example, 'Office.'
- *Address*: Displays the mailing address of the device. For example, 123 Main St., New York, NY. Type a new address to change the address.
- *Asset Tag*: Displays the asset tag of the device. Type a new asset tag to change the asset tag.
- *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.
- *Notes*: Displays any notes for the device. Type any new notes to update the notes.
- *Reset*: Click to clear the *Edit Additional Info* values.

- *Apply* Click to apply the additional info 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 63 for instructions on performing an actual backup.



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *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.

Schedule

- *Enable Schedule*: Click to enable scheduling for the backup.
- *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.

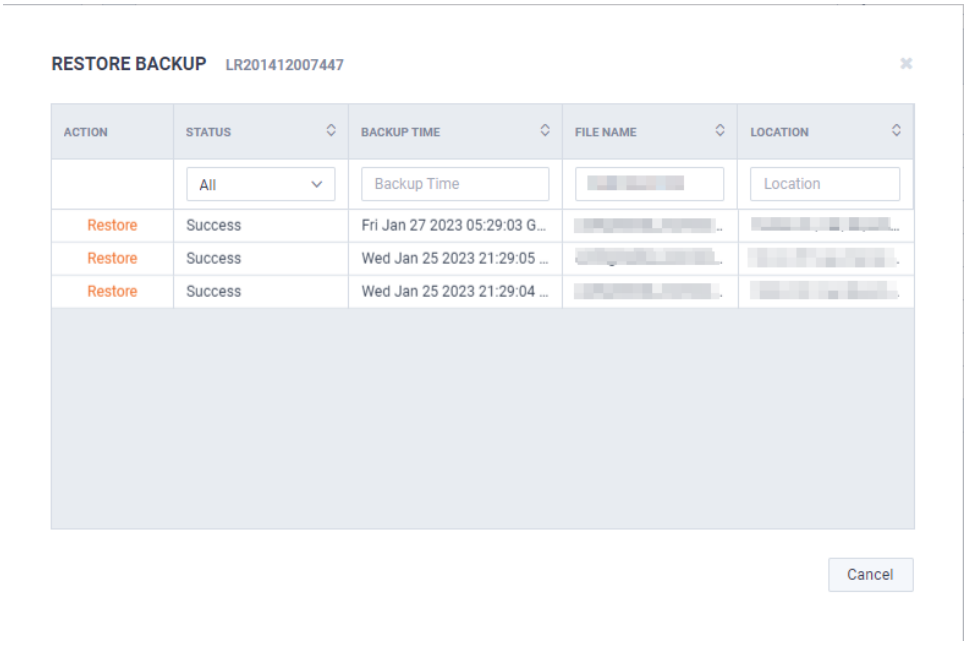
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between YADA.
- *Retention Limit*: Type the number backups to YADA.

Encryption

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

Restore Backup

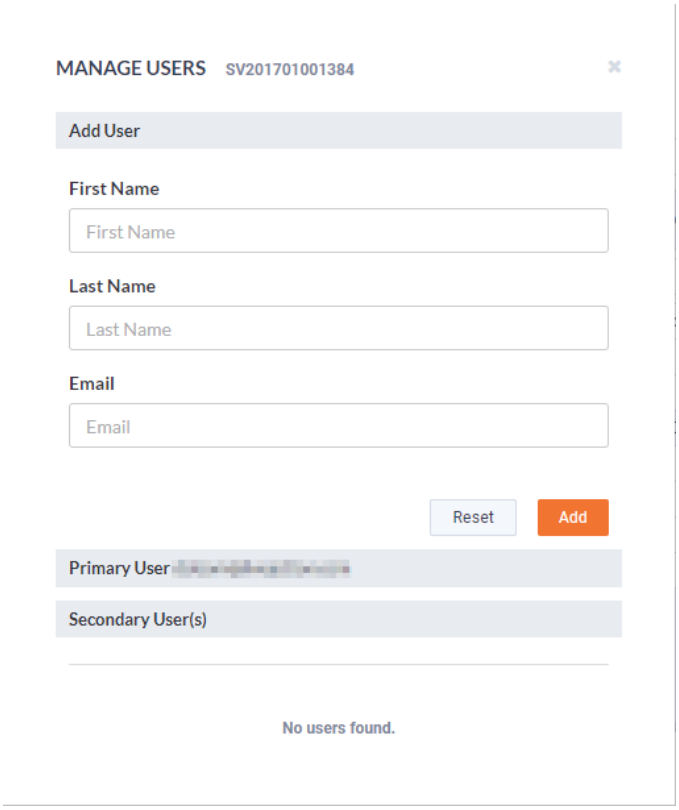
Select *Restore Backup* to restore a backup from an earlier backup. See 'Backup and restore' on page 63 for instructions on performing an actual restore.



  - *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.
  - *Backup TIme*: Displays the date and time the backup was completed
  - *File Name*: Displays the name of the backup.
  - *Location*: Displays the location of the backup.

Share

Select the *Share* option to share the selected devices with other users who manage and configure appliances. You will need to add a user by completing the *Manage Users* dialog.



- *First Name*: Type the first name of the user.
- *Last Name*: Type the last name of the user.
- *Email*: Type the email address of the user.
- *Reset*: Click to clear the *Add User* values.
- *Add*: Click to add the user to the list of secondary users.
- *Primary User*: Displays the primary user of the device when the device was registered with LiveAction. If multiple appliances are selected in the list of devices, the *Primary User* is not displayed.
- *Secondary User(s)*: Displays any secondary users assigned to the device. If multiple appliances are selected in the list of devices, the *Secondary User(s)* are not displayed.

Create Template

Select the *Create Template* option to create a template based on the configuration of the selected device. Once created, the template can be selected when you click the **Template** button. See also 'Template' on page 40 and 'DMS Templates tab' on page 55.

Compare Configurations

Select the *Compare Configurations* option to compare details between two selected devices. This option is available only when two devices are selected.

iDRAC Settings

Select the *iDRAC Settings* option 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 70.

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

- *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 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.

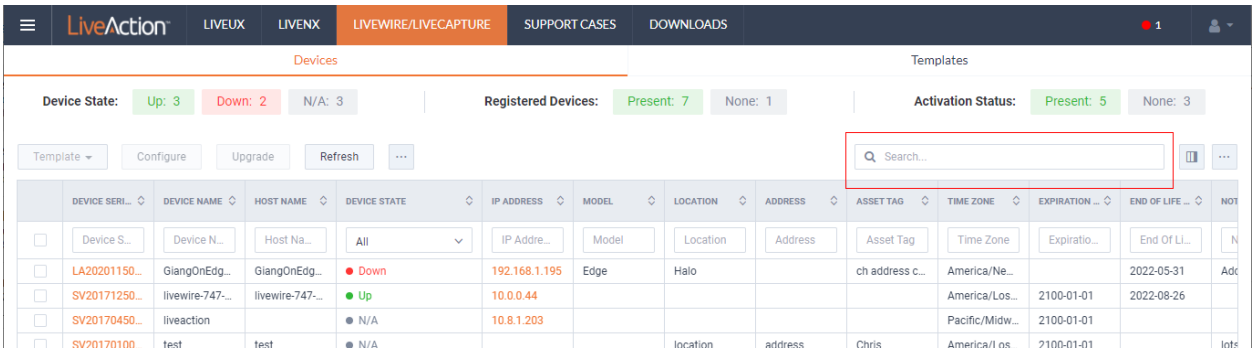
Event Filters:

- *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]

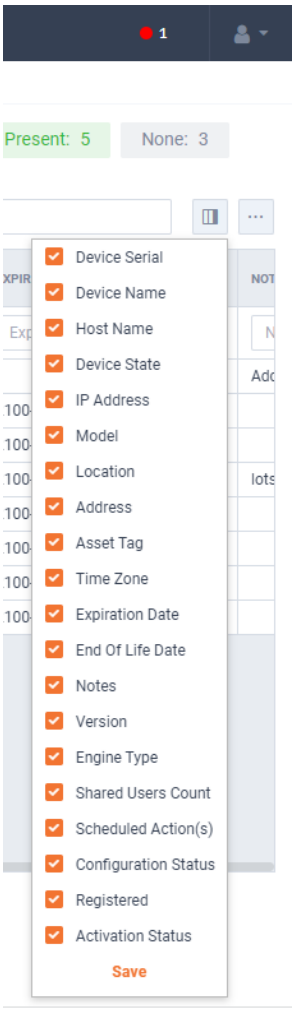
Search

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.



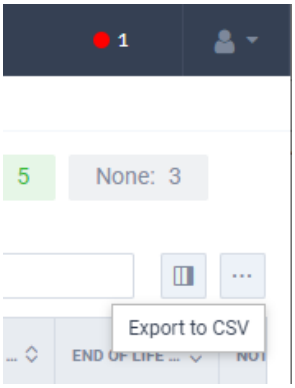
Display Columns

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



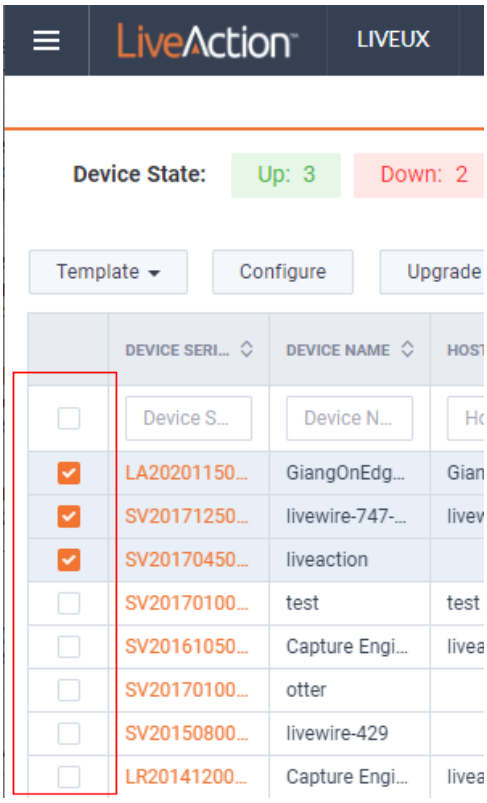
Export to CSV

Click the **Export to CSV** icon (...) to display an option for exporting the list of devices to a *.csv* file.



Check Box

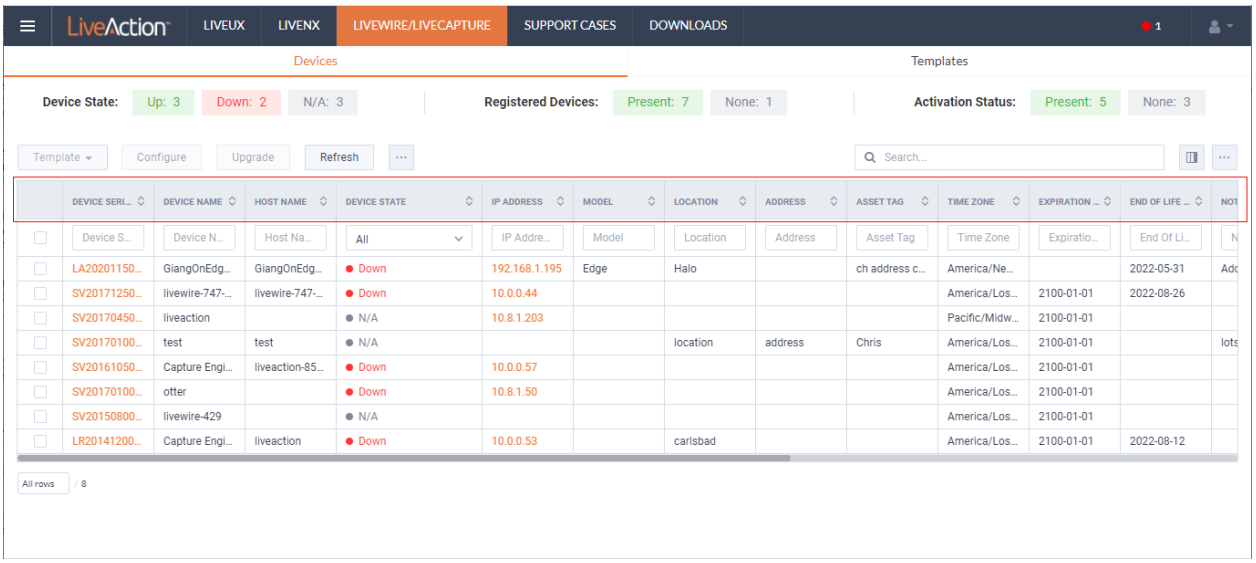
To select a device in the list of devices, select the check box of the desired devices. Selecting the check box at the top of the column allows you to select or clear the check boxes of all devices in the list of devices.



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.

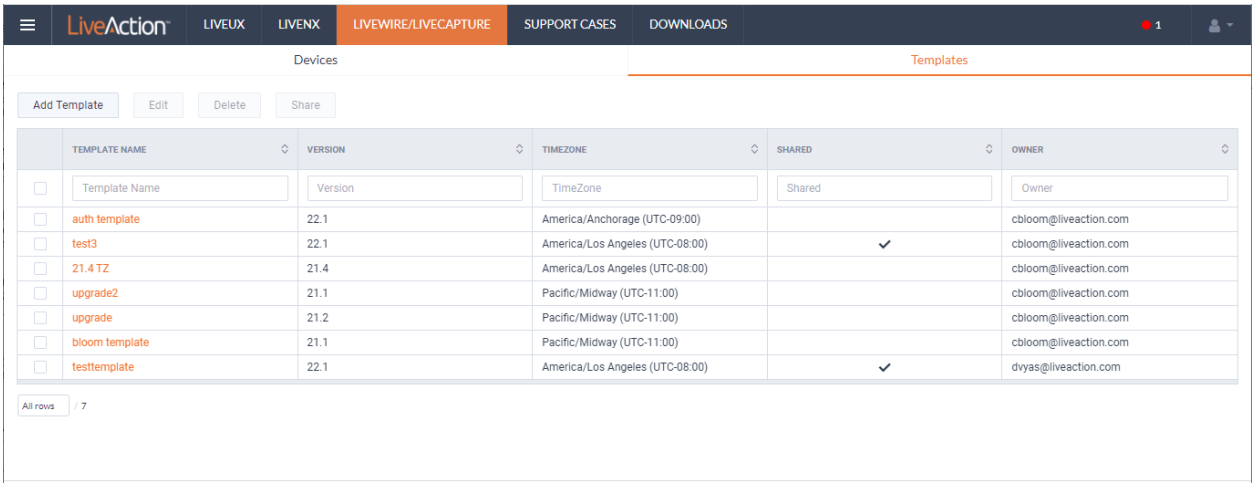


- *Device Serial*: Displays the serial number of the device.
- *Device Name*: Displays the name of the device.
- *Host Name*: Displays the host name of the device used by DNS.

- *Device State*: Displays whether the device is *Up* or *Down*. A device is up if it has contacted the DMS in the last 25 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 DMS 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 the DMS portal will reflect that.
- *Model*: Displays the model of the device (*Edge*, *1100*, *3100*, 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.
- *Expiration Date*: Displays the date that the maintenance on the device will expire. Once the expiration date has passed, you can still access the DMS 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*.
- *Shared Users 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.

DMS Templates tab

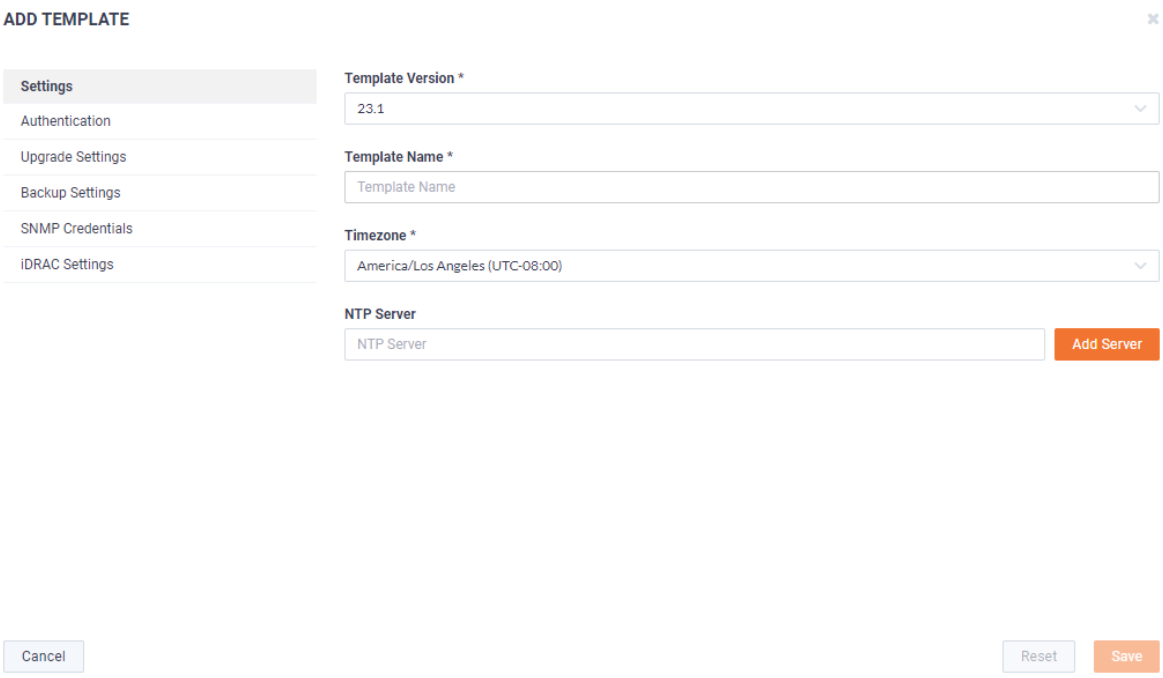
The DMS *Templates* tab displays the templates associated with your account. Templates allow you to configure settings independent of a particular device, and then apply the template, and thus the settings, to a device, or multiple devices in bulk at the same time. A description of each of the available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



Add Template

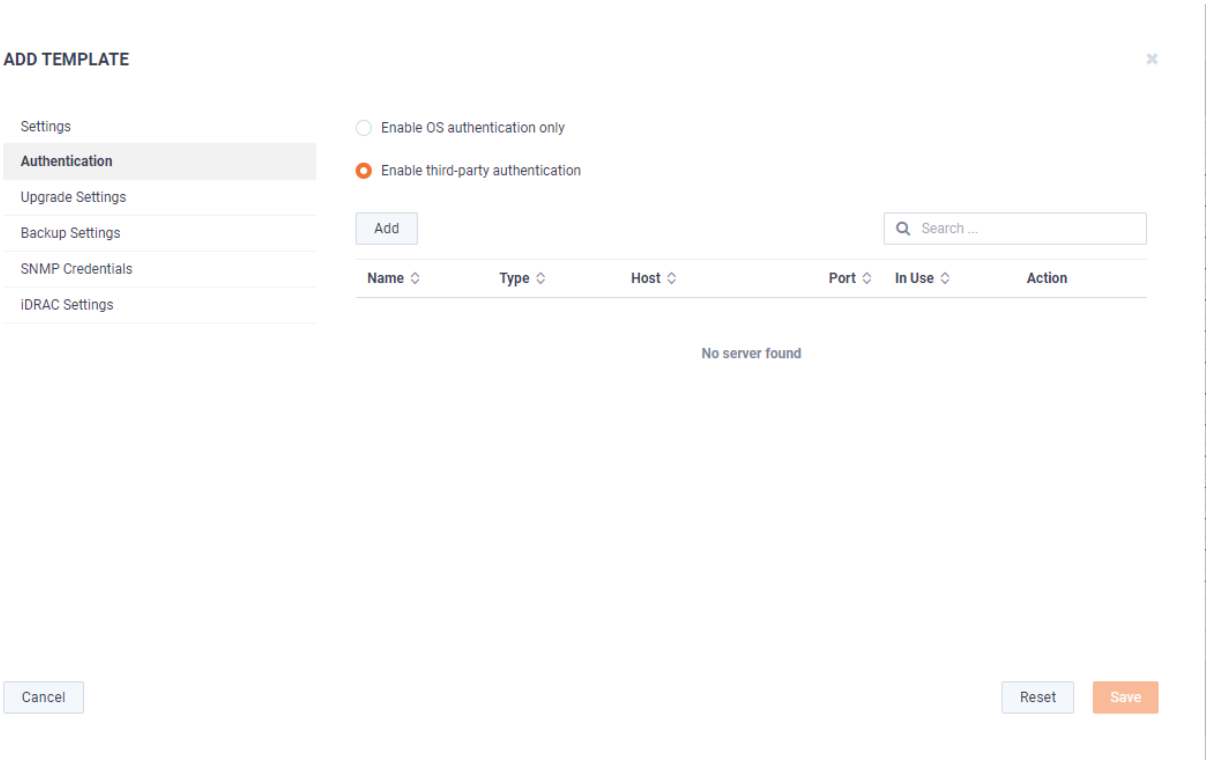
Click the **Add Template** button to display the *ADD TEMPLATE* dialog to add a new template to the configuration.

Settings



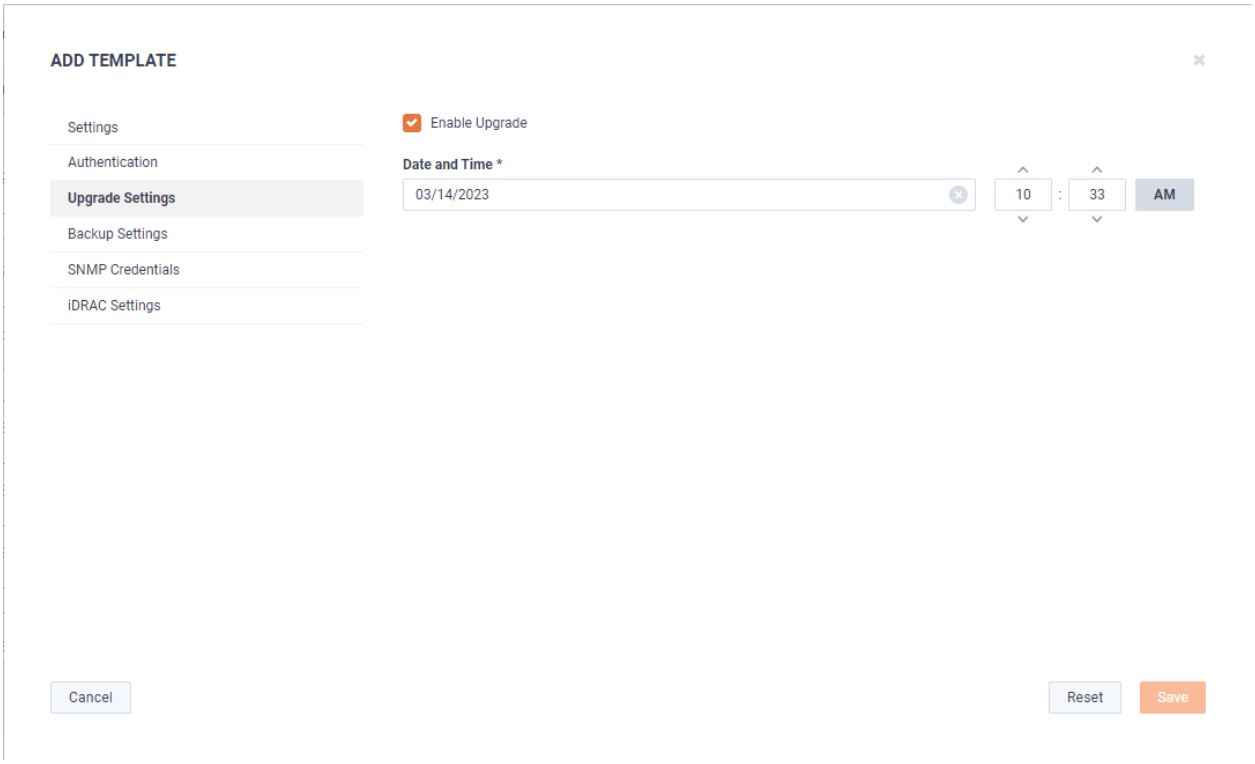
- *Template Version*: Click to select the version of the template you are configuring.
- *Template Name*: Type a name for the template.
- *Timezone*: Click to select the timezone for the template.
- *NTP Server*: Enter the address of any NTP servers to add to the configuration, and then click **Add Server**.
- *NTP Servers*: Displays the list of NTP servers added to *Settings*. You can click the **Edit** icon to edit an NTP server in the list, or click the **Trash** icon to remove an NTP server from the list.

Authentication



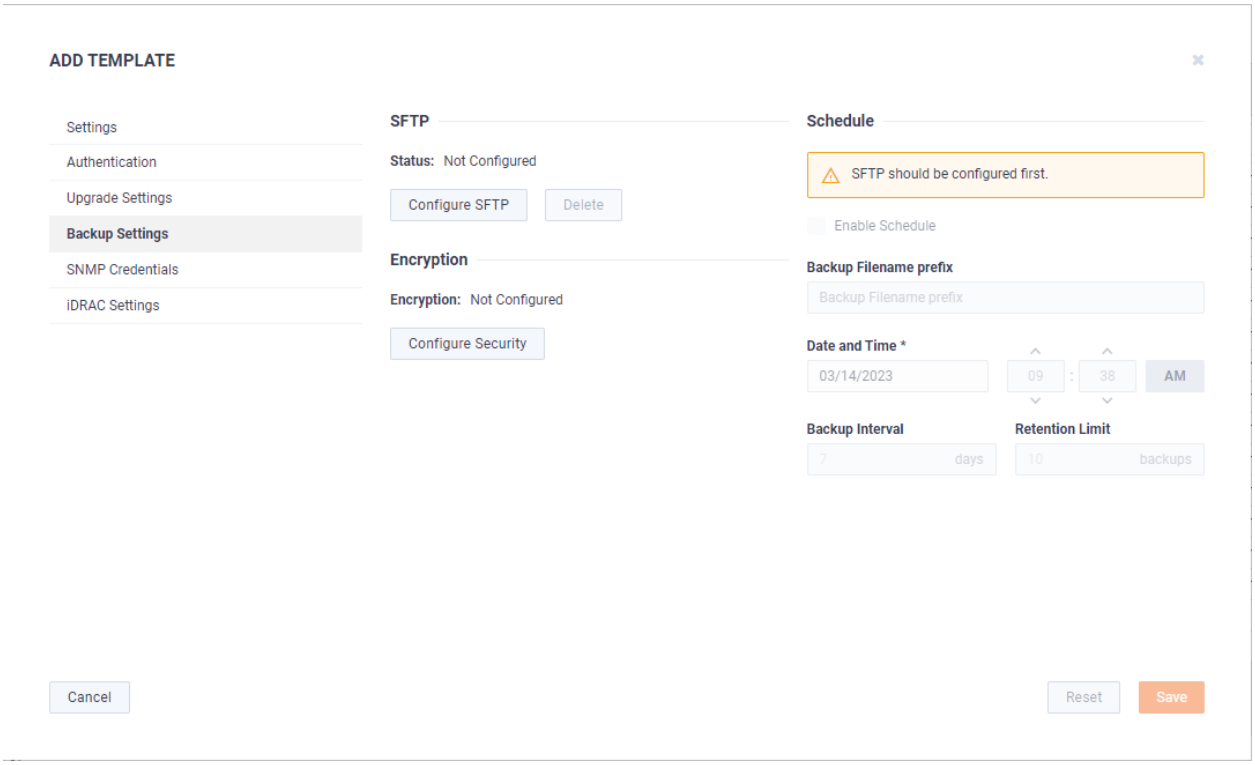
- *Enable OS authentication only*: Select this option to use the local OS authentication.
- *Enable third-party authentication*: Select this option to use TACACS+ or RADIUS authentication. If this option is selected, click **Add** to configure the new authentication setting.
  - *Add*: Click to add a new authentication setting. You will need to configure the new authentication setting.
    - *Name*: Displays the name of the authentication setting.
    - *Type*: Displays the type of authentication, which can be either 'RADIUS' or 'TACACS+.'
    - *Host*: Displays the host of the authentication setting.
    - *Port*: Displays the port of the authentication setting.
    - *Secret*: Displays the secret key of the authentication setting.
    - *Use*: Displays whether or not the authentication setting is in use.
    - *Save*: Click to save the authentication setting.
  - *Search*: yadayada.

Upgrade Settings



- *Enable Upgrade*: Select to enable the upgrade on the selected templates. If you enable the upgrade, you are presented with settings to specify the date and time the upgrade should take place.

Backup Settings



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *Hostname*: Type the IP address of the SFTP server.

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

- *Delete*: Click to delete the configured SFTP server for the backup.

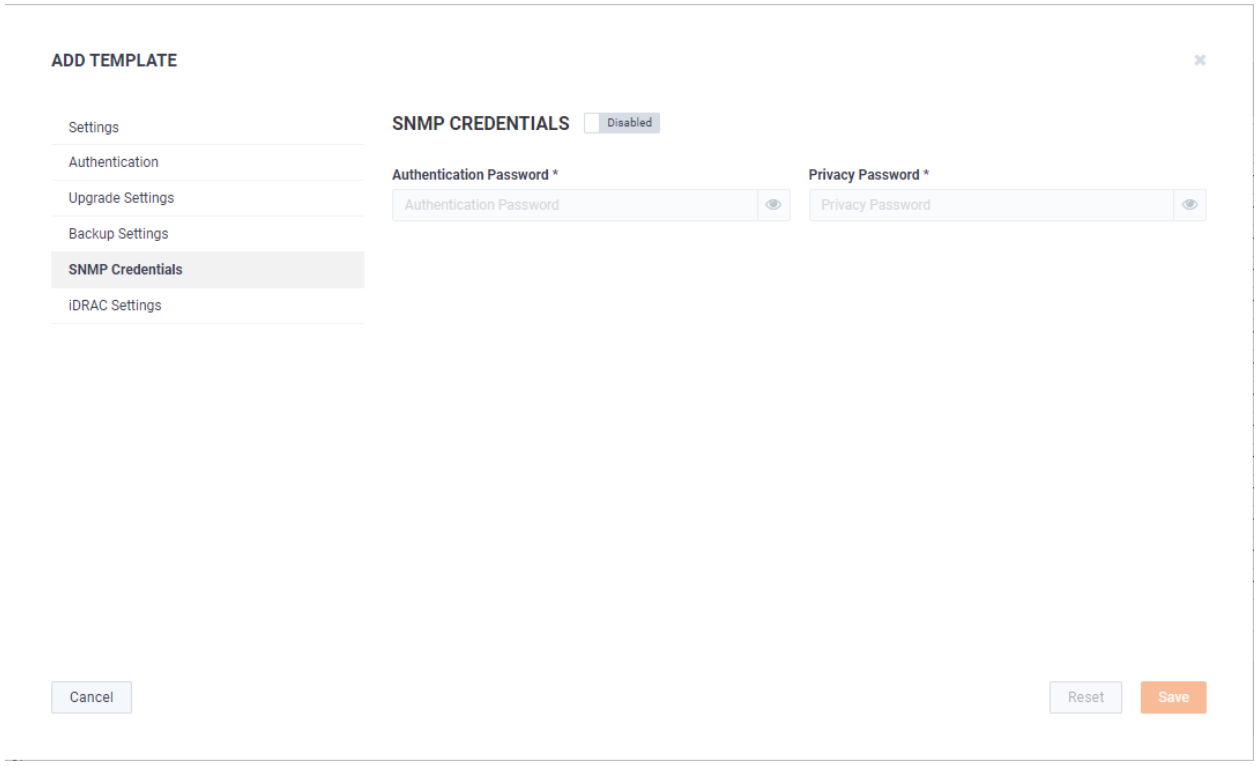
Schedule

- *Enable Schedule*: Click to enable scheduling for the backup.
- *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.
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between YADA.
- *Retention Limit*: Type the number backups to YADA.

Encryption

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

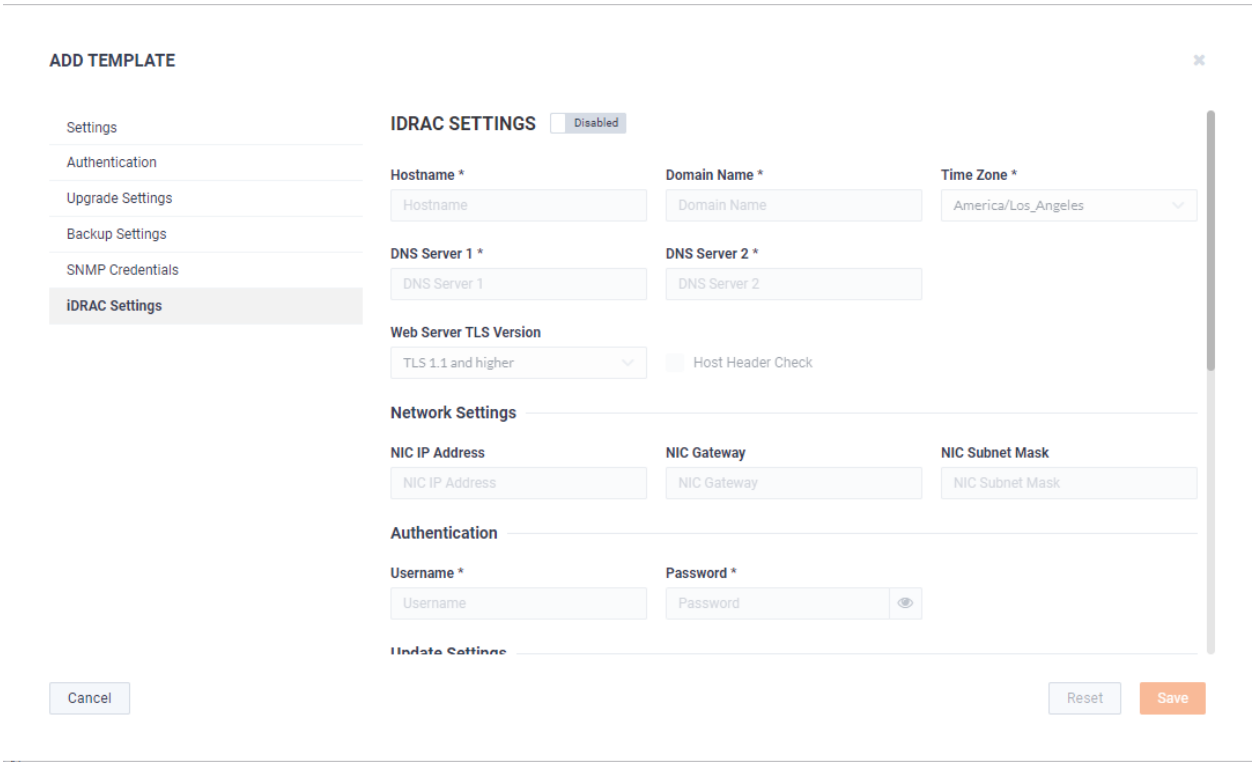
SNMP Credentials



- *Enabled/Disabled*: Select to enable or disable the *SNMP Credentials* configured below for the *Authentication Password* and *Privacy Password*.
- *Authentication Password*: Type a new *Authentication Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 85.

- *Privacy Password*: Type a new *Privacy Password* to change it from the default Authentication Password displayed in 'LiveNX SNMP Configuration' in 'LiveFlow' on page 85.

iDRAC Settings



Note Only selected options available from the iDRAC utility are available and configurable below. See also 'Integrated Remote Access Controller (iDRAC)' on page 70.

- *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 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]

Edit

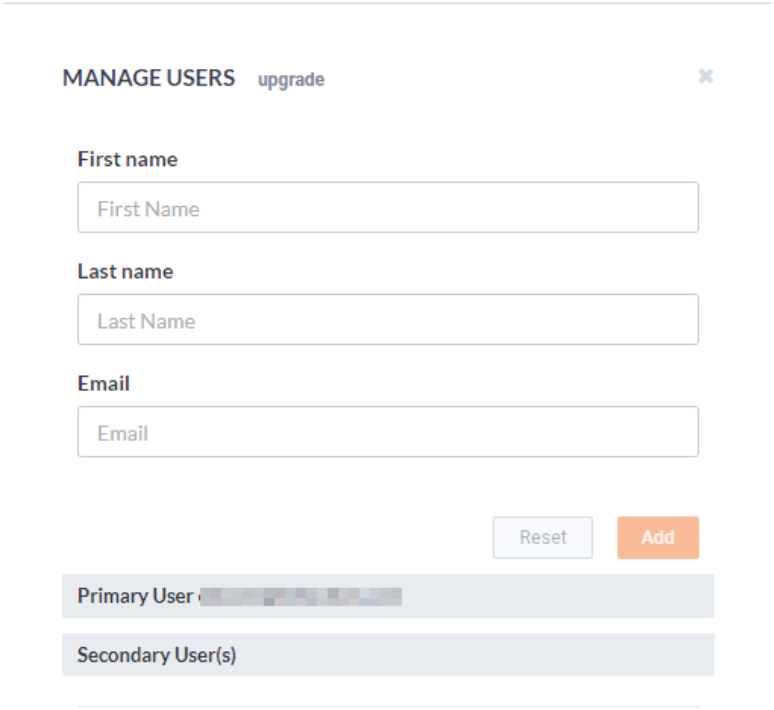
Click the **Edit** button to edit the selected template. See also 'Add Template' on page 56.

Delete

Click the **Delete** button to delete the selected template.

Share

Click the **Share** button to share the selected template with other users who manage and configure appliances. You will need to add a user by completing the *Manage Users* dialog.

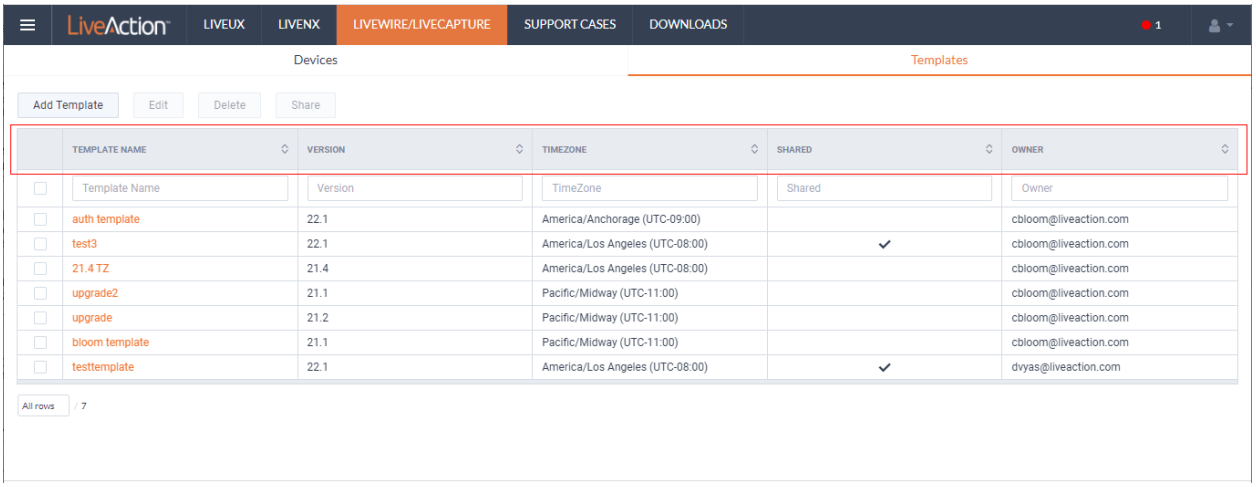


- *First Name*: Type the first name of the user.
- *Last Name*: Type the last name of the user.
- *Email*: Type the email address of the user.
- *Reset*: Click to clear the *Manage User* values.
- *Add*: Click to add the user to the list of secondary users.
- *Primary User*: Displays the primary user of the device when the device was registered with LiveAction. If multiple appliances are selected in the list of devices, the *Primary User* is not displayed.
- *Secondary User(s)*: Displays any secondary users assigned to the device. If multiple appliances are selected in the list of devices, the *Secondary User(s)* are not displayed.

Template column headings

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

Tip Below each of the column headings is a text box you can use to filter the templates displayed in the list of templates. To filter using the text box, simply enter a text string to display the templates that match the text string.



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

Backup and restore

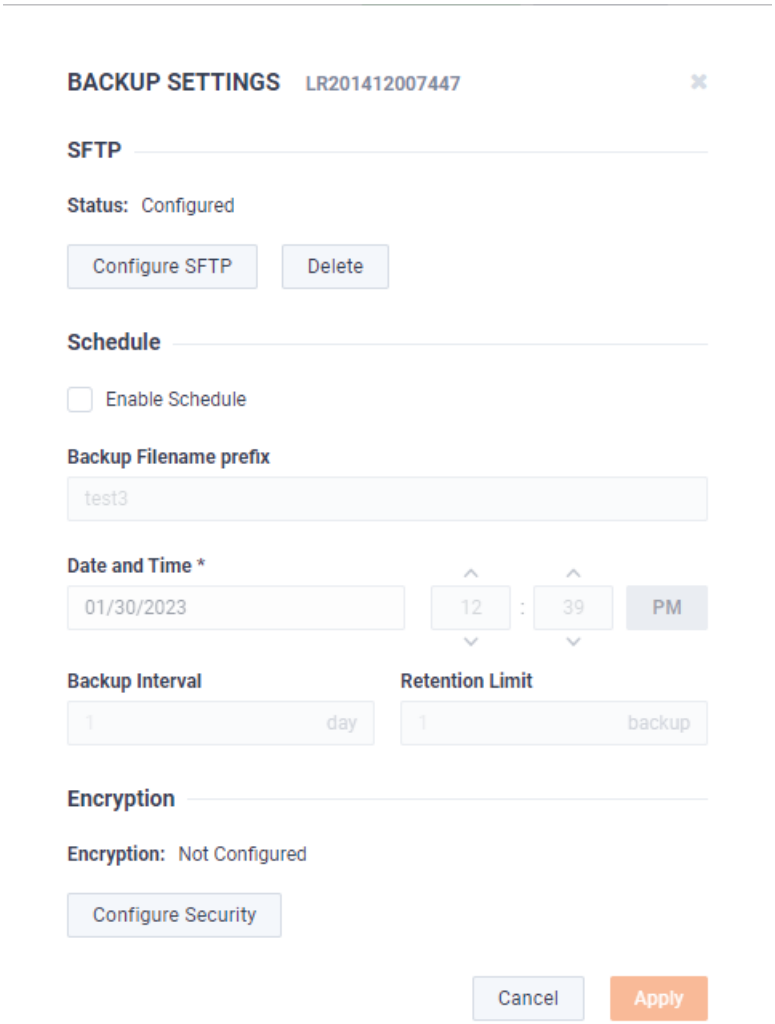
The *Backup Settings* in DMS lets you configure and designate an SFTP (Secure FTP) server for backing up the application and system settings on the LiveWire device. Once a backup is created, you can use the *Restore Backup* settings to restore either the application settings, or both the application 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 DMS and select *Backup Settings*. The *Backup Settings* dialog appears. See 'Backup Settings' on page 48 for a description of each of the settings.



SFTP

- *Configure SFTP*: Click to configure the SFTP (Secure FTP) server for the backup.
  - *Hostname*: Type the IP address of the SFTP server.
  - *Port*: Type the port used for the SFTP server.
  - *Username*: Type a username for the SFTP server.
  - *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.

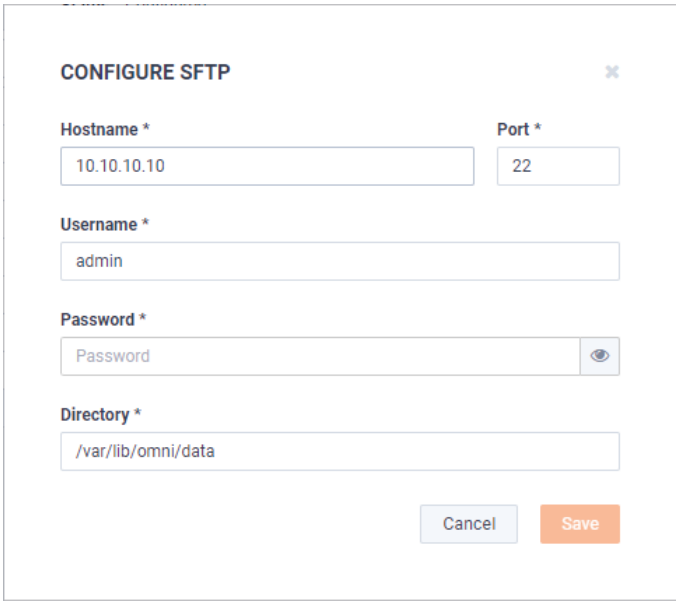
Schedule

- *Enable Schedule*: Click to enable scheduling for the backup.
- *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.
- *Date and Time*: Click to configure the date and time the backup will complete.
- *Backup Interval*: Type the number of days between when backups are performed.
- *Retention Limit*: Type the number backups to save before a backup is deleted.

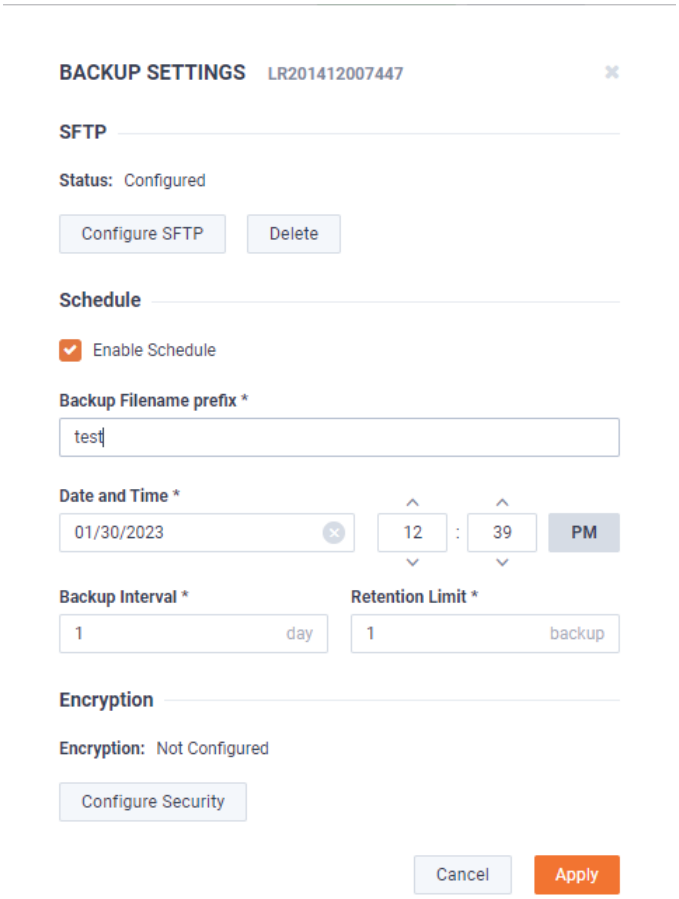
Encryption

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

2. Click **Configure SFTP** to configure the SFTP (Secure FTP) server for the backup.The *Configure SFTP* dialog appears.

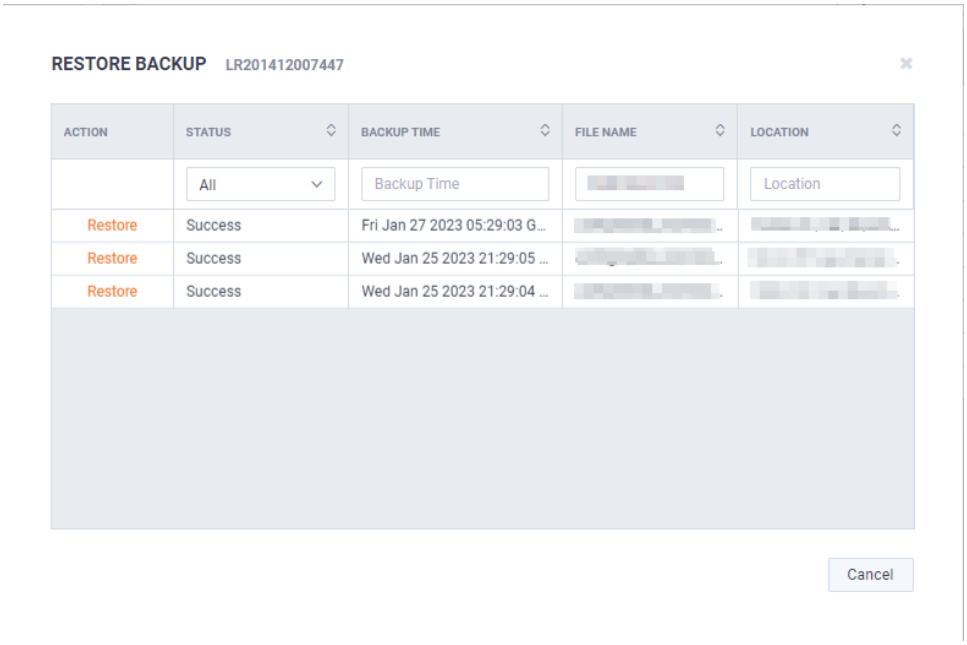


3. Configure the SFTP server you want to use as the backup server. You will need to configure the *Hostname*, *Port*, *Username*, *Password*, *Directory*, and click **Save**.
4. On the *Backup Settings* dialog, select the *Enable Schedule* check box. You will need to configure the *Backup Filename Prefix*, *Date and Time*, *Backup Interval*, *Retention Limit*, *Encryption*, and click **Apply**.

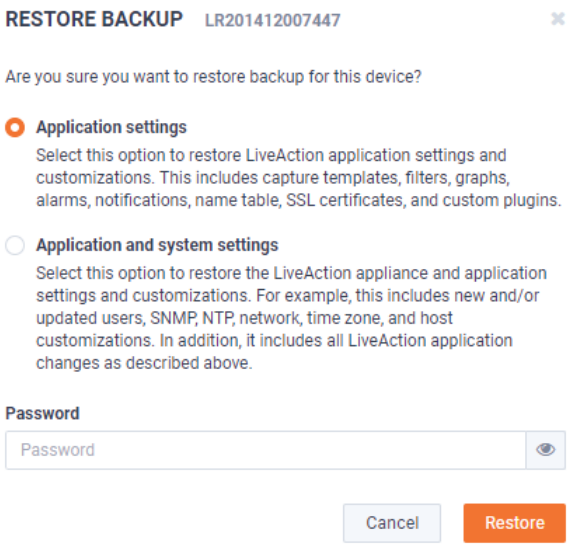


Restoring a backup

1. Click the **Elipsis** (...) in DMS and select **Restore Backup**. The *Restore Backup* dialog appears.



2. In the *Action* column, select the backup you want to restore. The second *Restore Backup* dialog appears.



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 67. Additionally, please configure an NTP server as described in 'Time' on page 36.

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 120, 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 72.
- **Encrypt Traffic**: Enable encryption on iDRAC, if possible. For example, use HTTPS in your web browser's URL location field when connecting to iDRAC (e.g., 'https://xxx.xxx.xxx.xxx').

Setting the IP address for iDRAC

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

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

Access BIOS setting to configure IP address

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

To initially set the iDRAC IP address:

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

Connecting to iDRAC on LiveWire

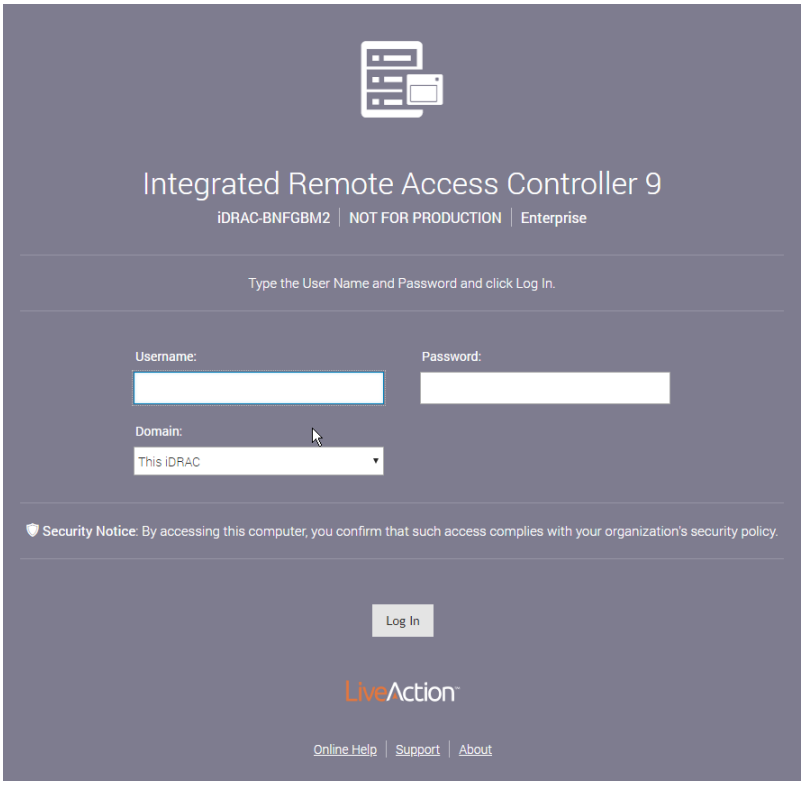
You can use an Internet browser window to connect to iDRAC on LiveWire. Additionally, you must make sure the following ports are accessible through any firewall:

- Port 80 (TCP)
- Port 443 (Web HTTP SSL)
- Port 623 (UDP)

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

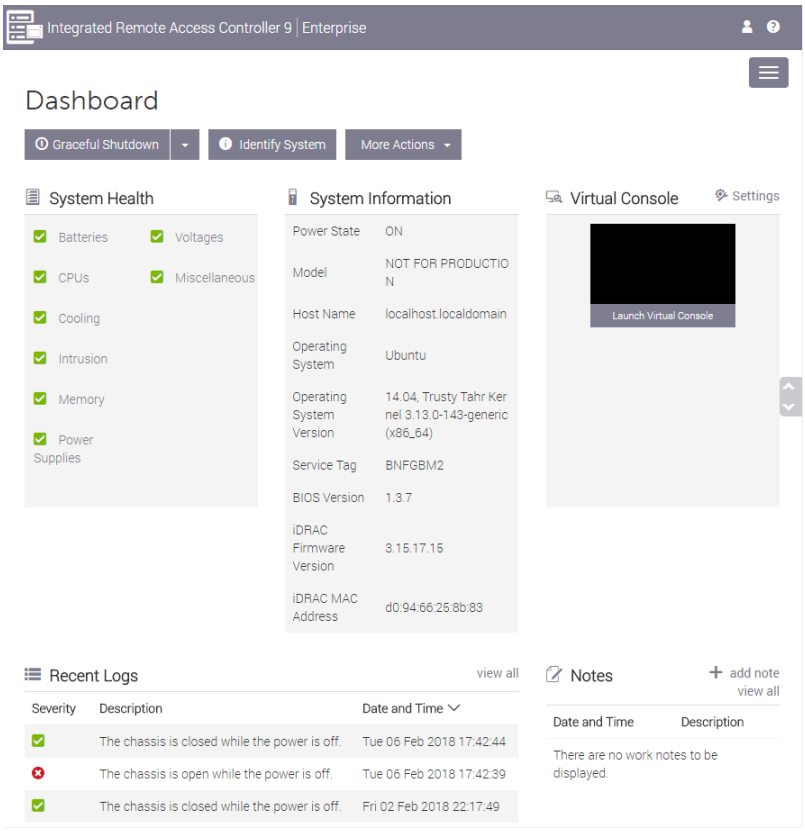
To connect to iDRAC on LiveWire using your browser:

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



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

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



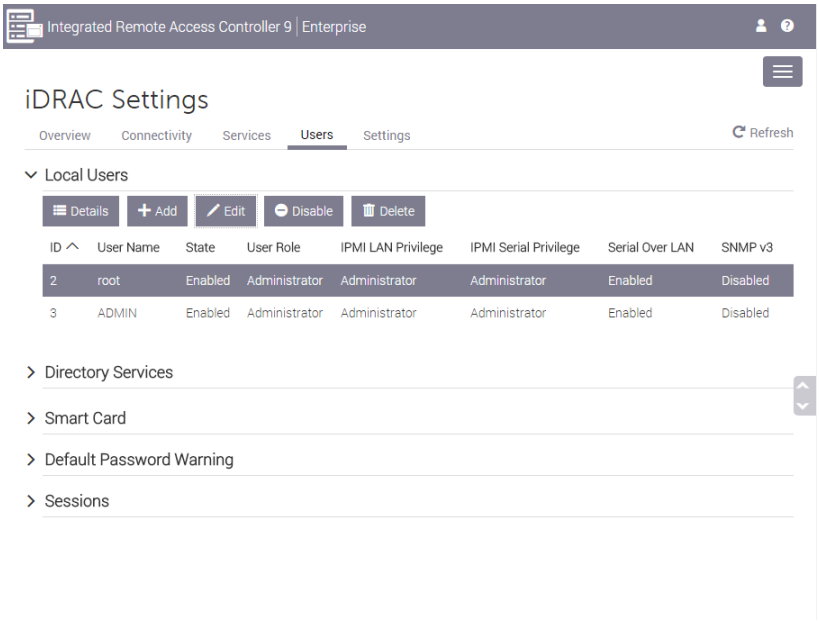
5. View the remaining instructions in this section for instructions on using iDRAC to perform tasks such as changing the default password, accessing a remote console, reimaging, rebooting, starting, and shutting down LiveWire.

Changing the default password

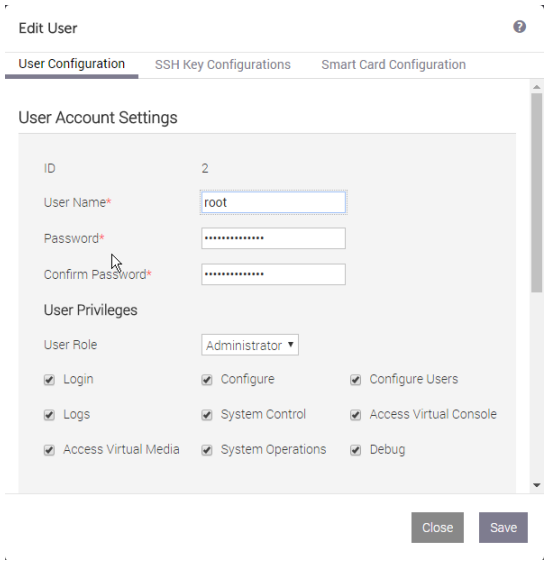
For security reasons, we strongly recommend changing both the default username and password to iDRAC.

To change the default password:

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



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.



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

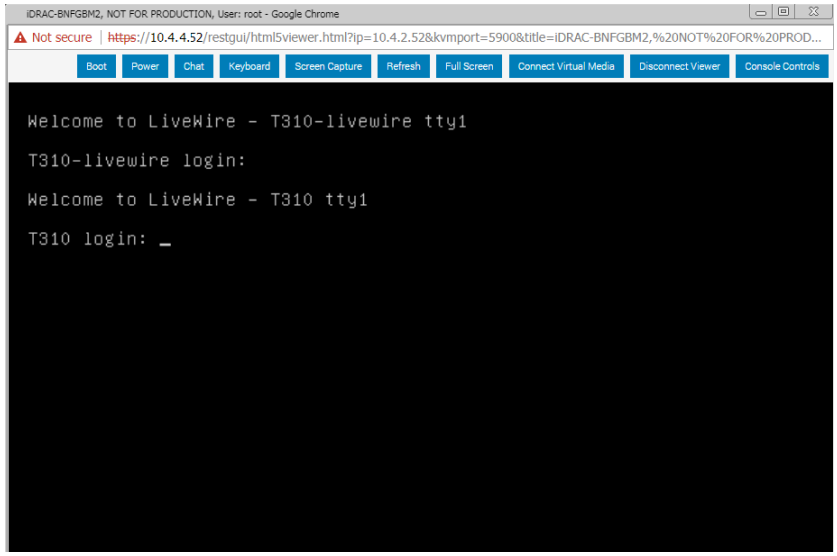
Accessing a remote console

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

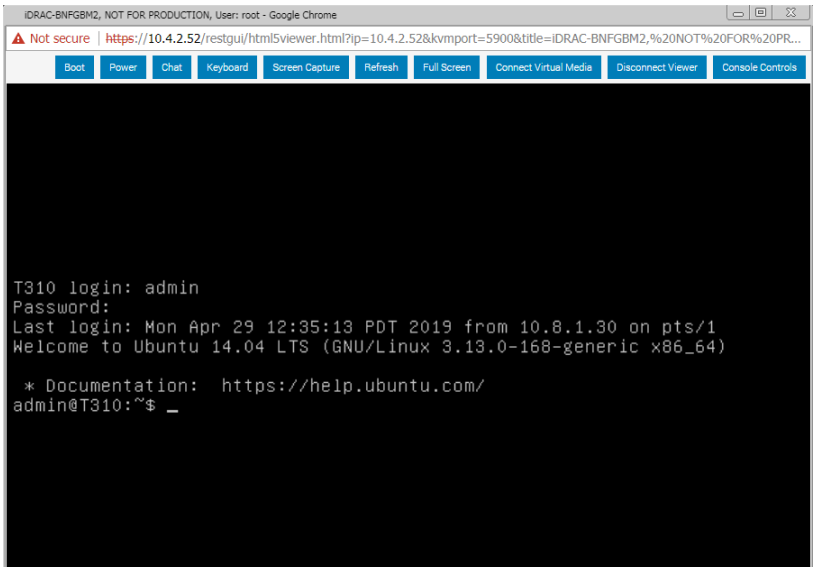
To open a remote console:

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

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



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

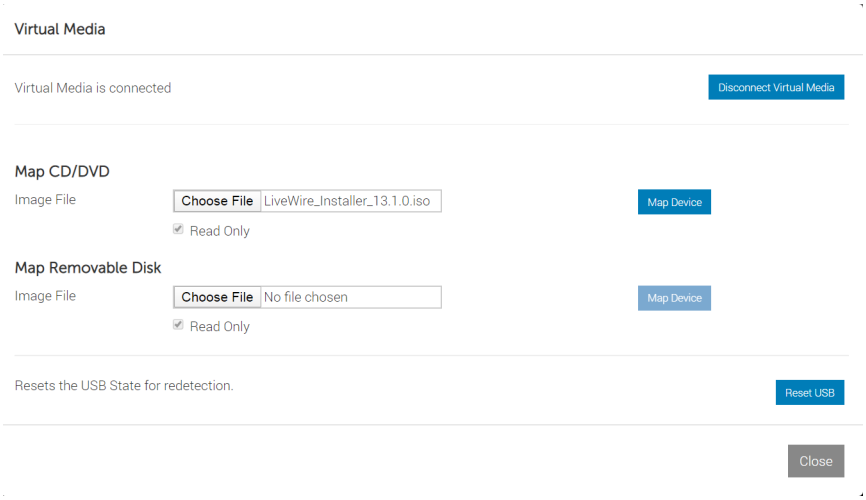


Reimaging LiveWire with an ISO image

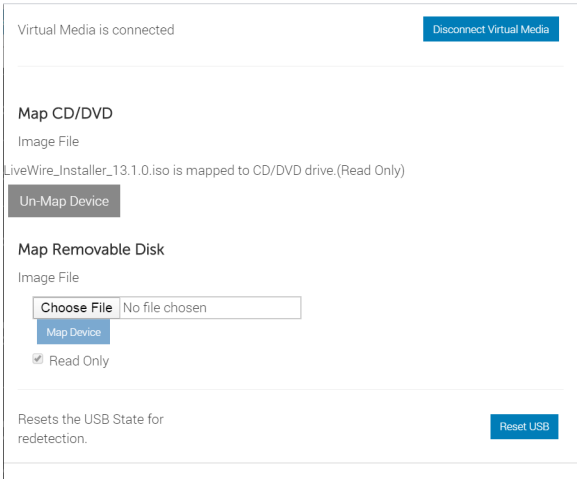
You can reimage LiveWire remotely using iDRAC and an ISO image available from LiveAction technical support. See 'Contacting LiveAction support' on page 24.

To reimage LiveWire:

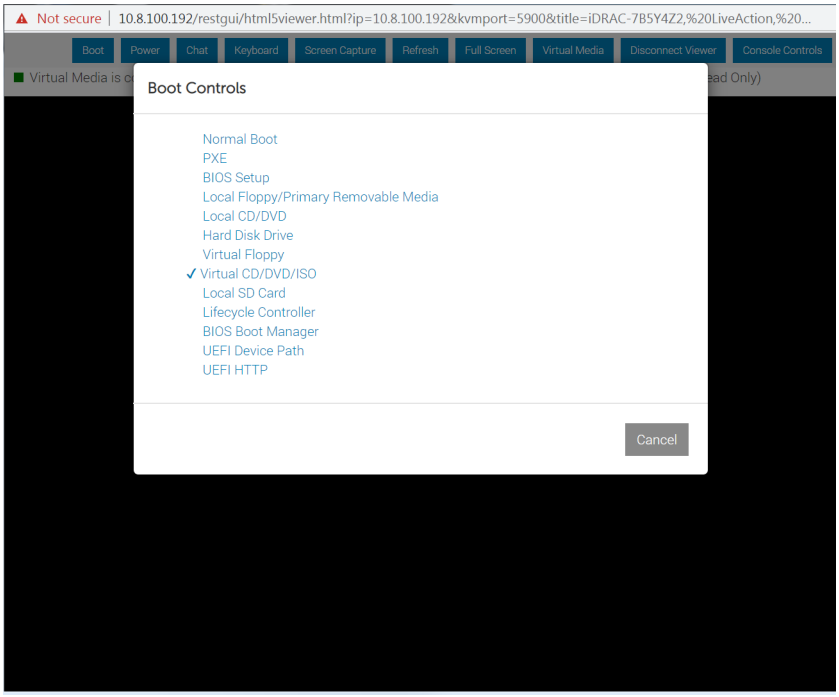
1. From the remote console, click **Connect Virtual Media**. The **Virtual Media** dialog appears.



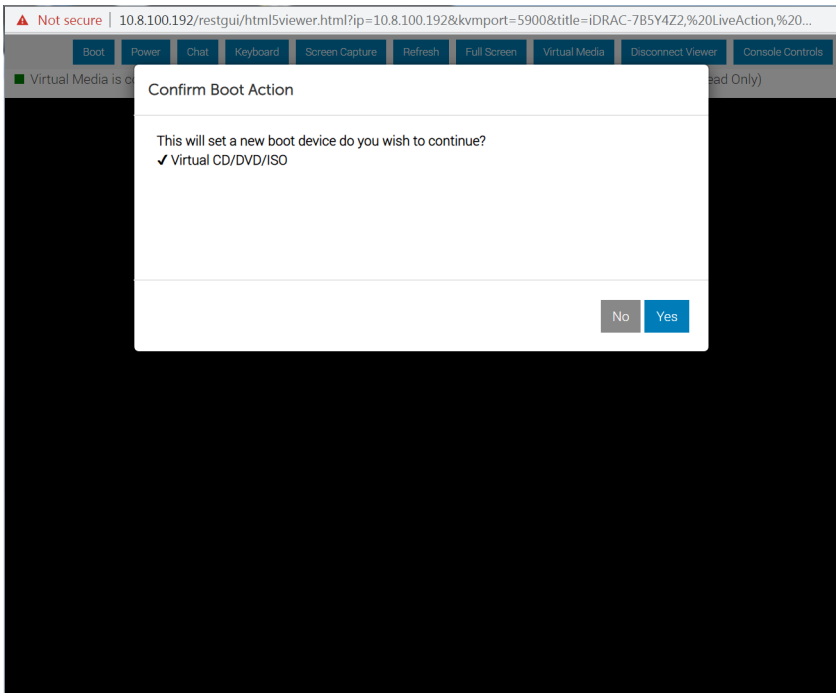
2. Click **Choose File** under *Map CD/DVD* to select the ISO file (e.g., *omni-20.1.0-x.iso*), and then click **Map Device**. The ISO image is mapped to the CD/DVD drive.



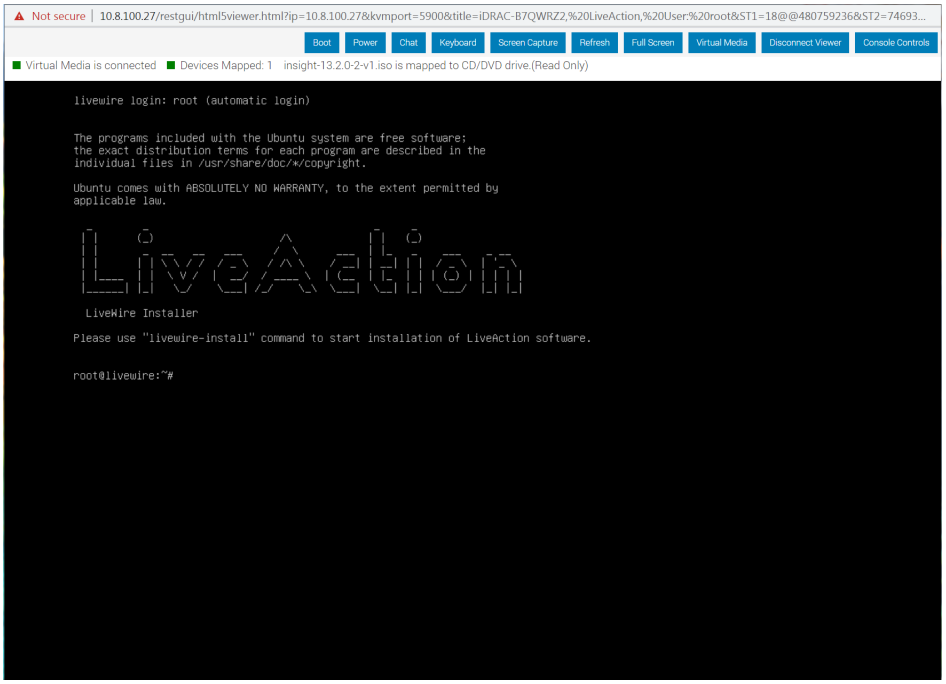
3. Click **Close** to close the dialog.
4. From the remote console, click **Boot** and select *Virtual CD/DVD/ISO* from the boot controls. The **Confirm Boot Action** dialog appears.



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



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



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

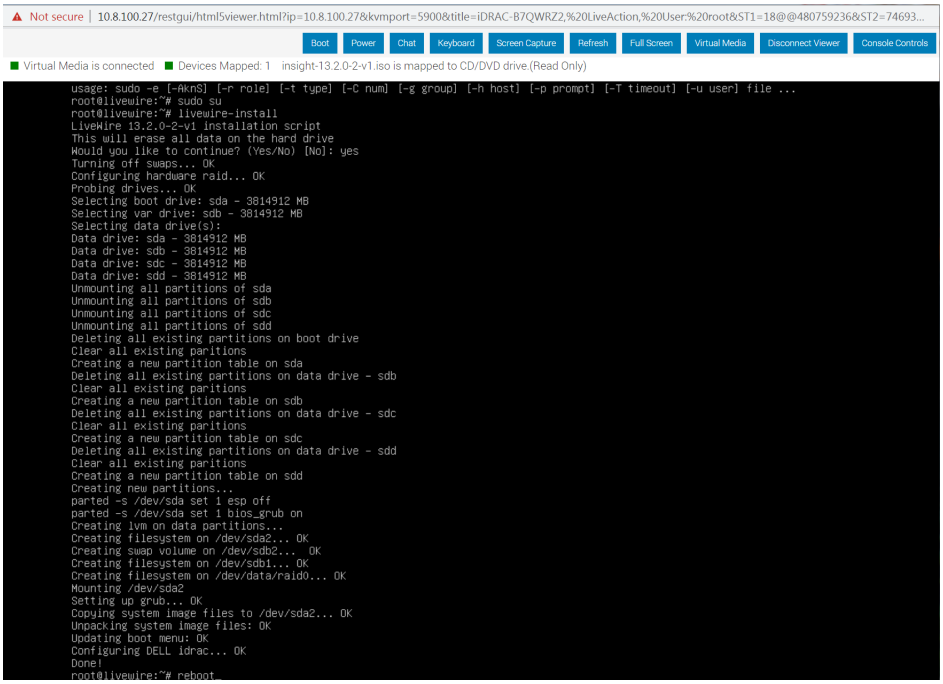
Note When running the *livewire-install* script though the remote console, do not close the console until the script completes. Closing the console prematurely causes the reimaging process to fail.

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.



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.

Sending Telemetry to LiveNX and ThreatEye

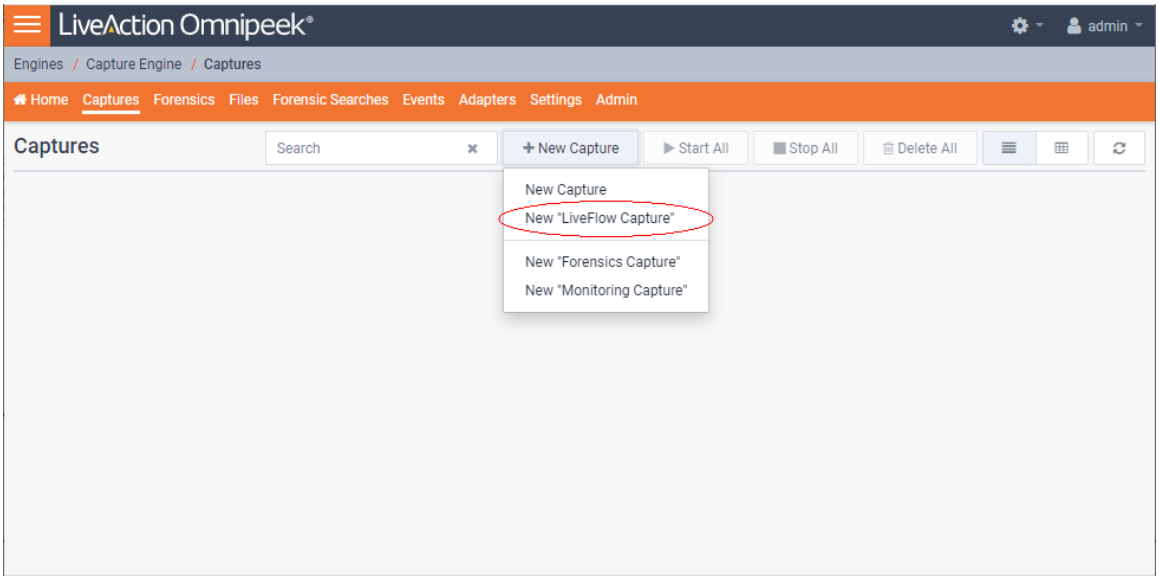
In this chapter:

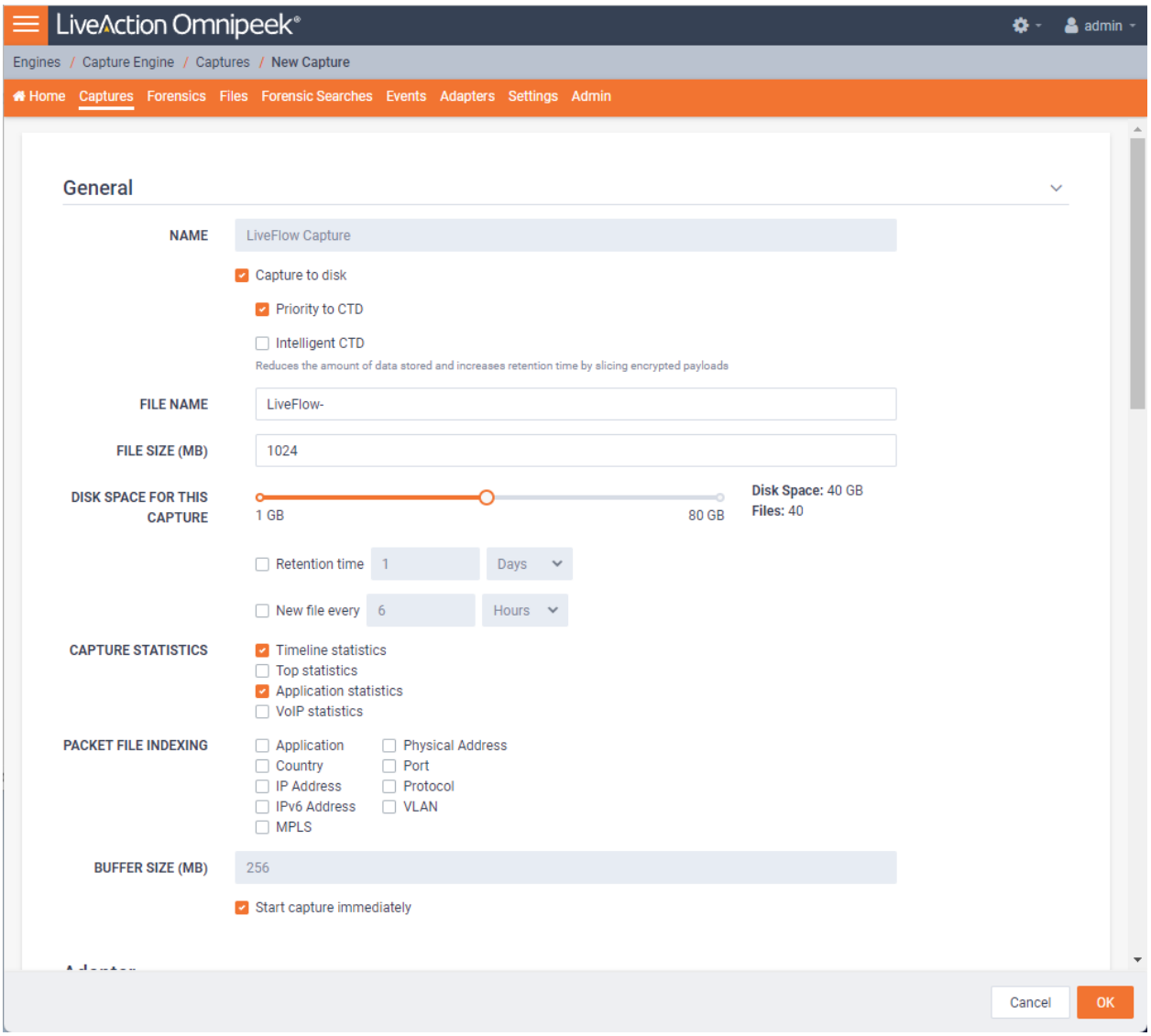
About sending telemetry to LiveNX and ThreatEye

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.

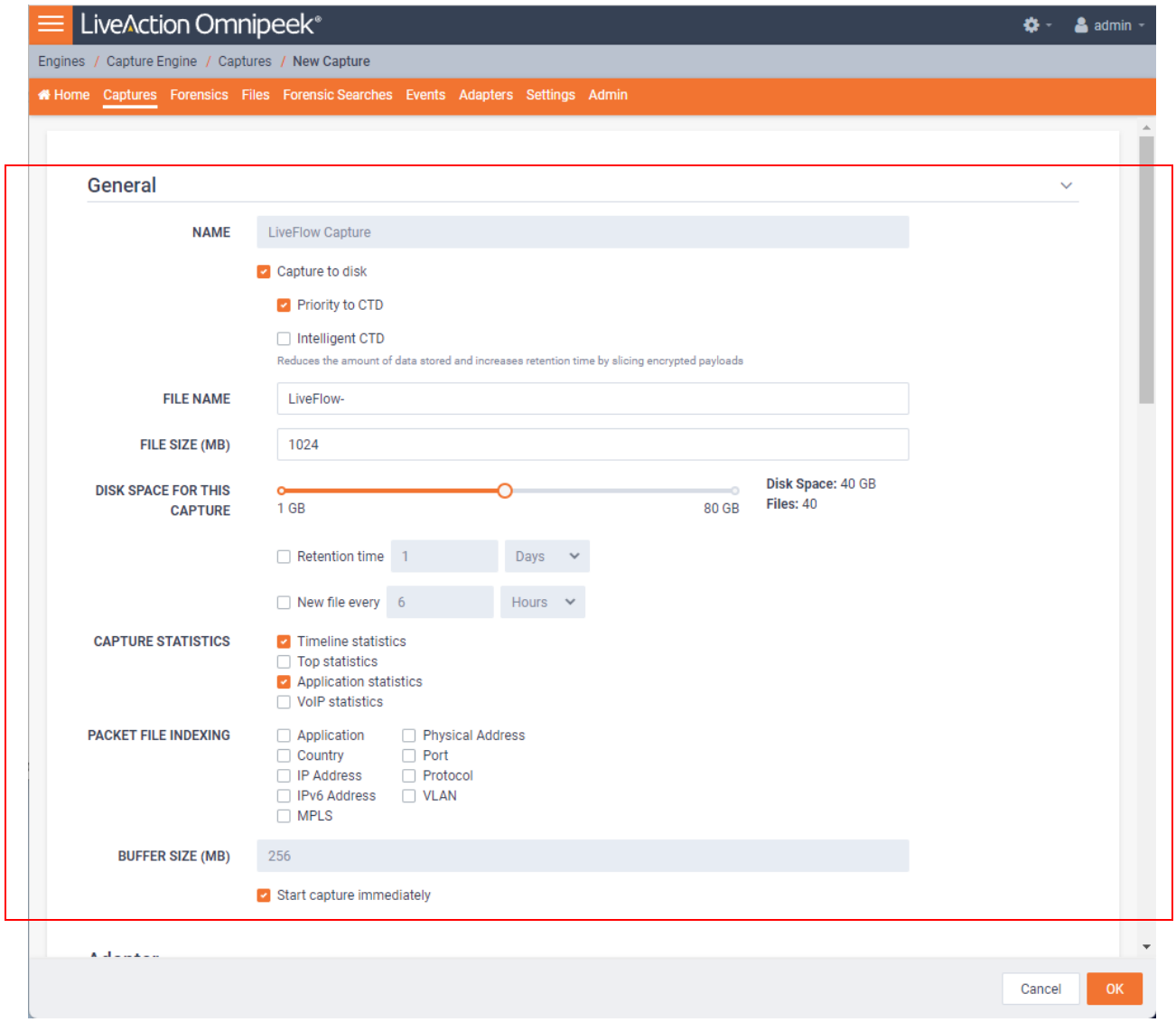




Note Scroll down in the capture options to see LiveFlow settings for *Template Refresh Interval* and *Options Template Refresh Interval*. These settings let you configure the amount of time (in seconds) LiveWire sends template information to LiveNX. The templates provide the instructions to LiveNX on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



- *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.

- *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.

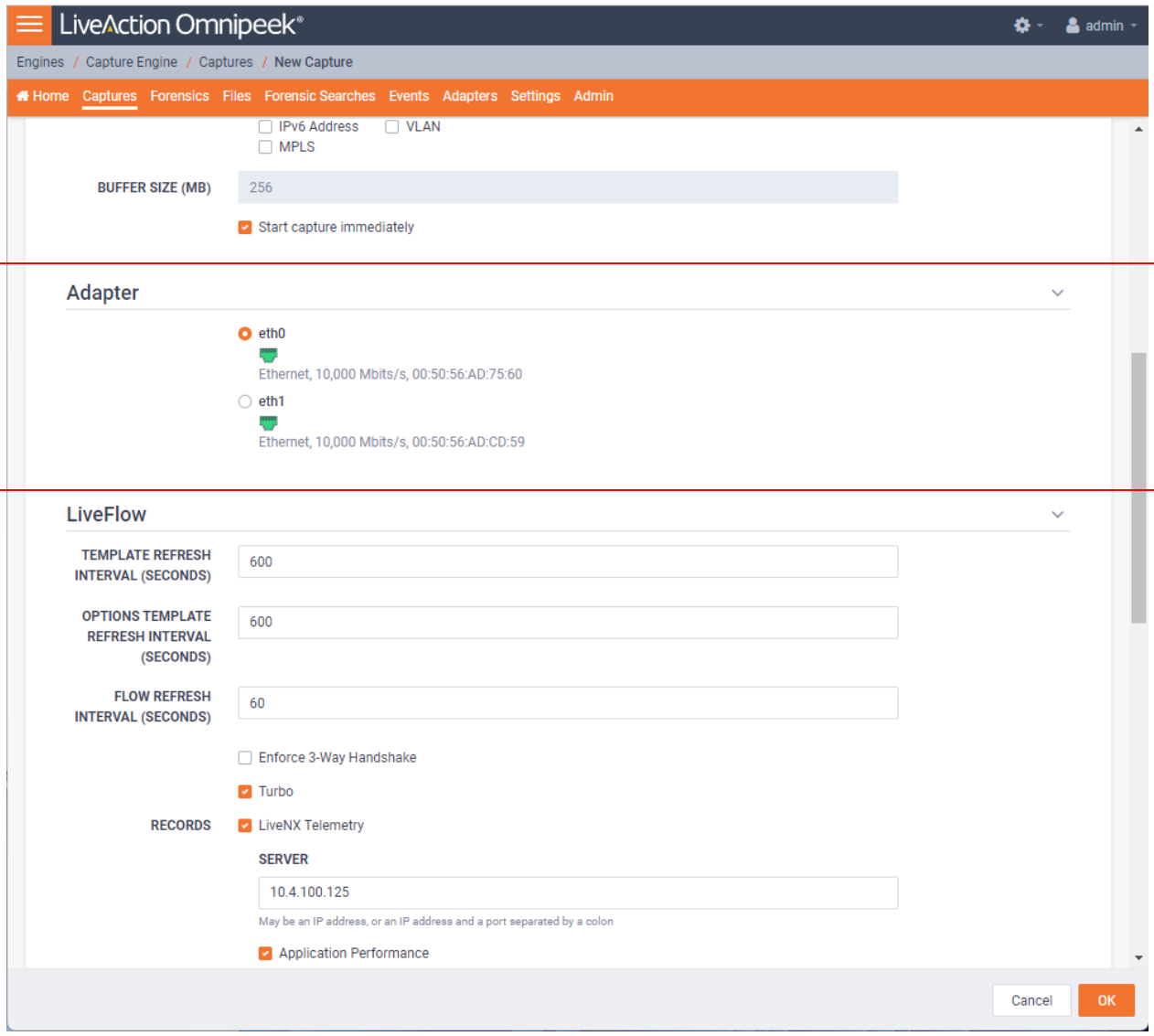
Note Selecting the *VoIP Statistics* option may affect capture performance, especially when there are more than 2000 simultaneous calls on the network. Selecting the *Top Statistics* option may

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**.

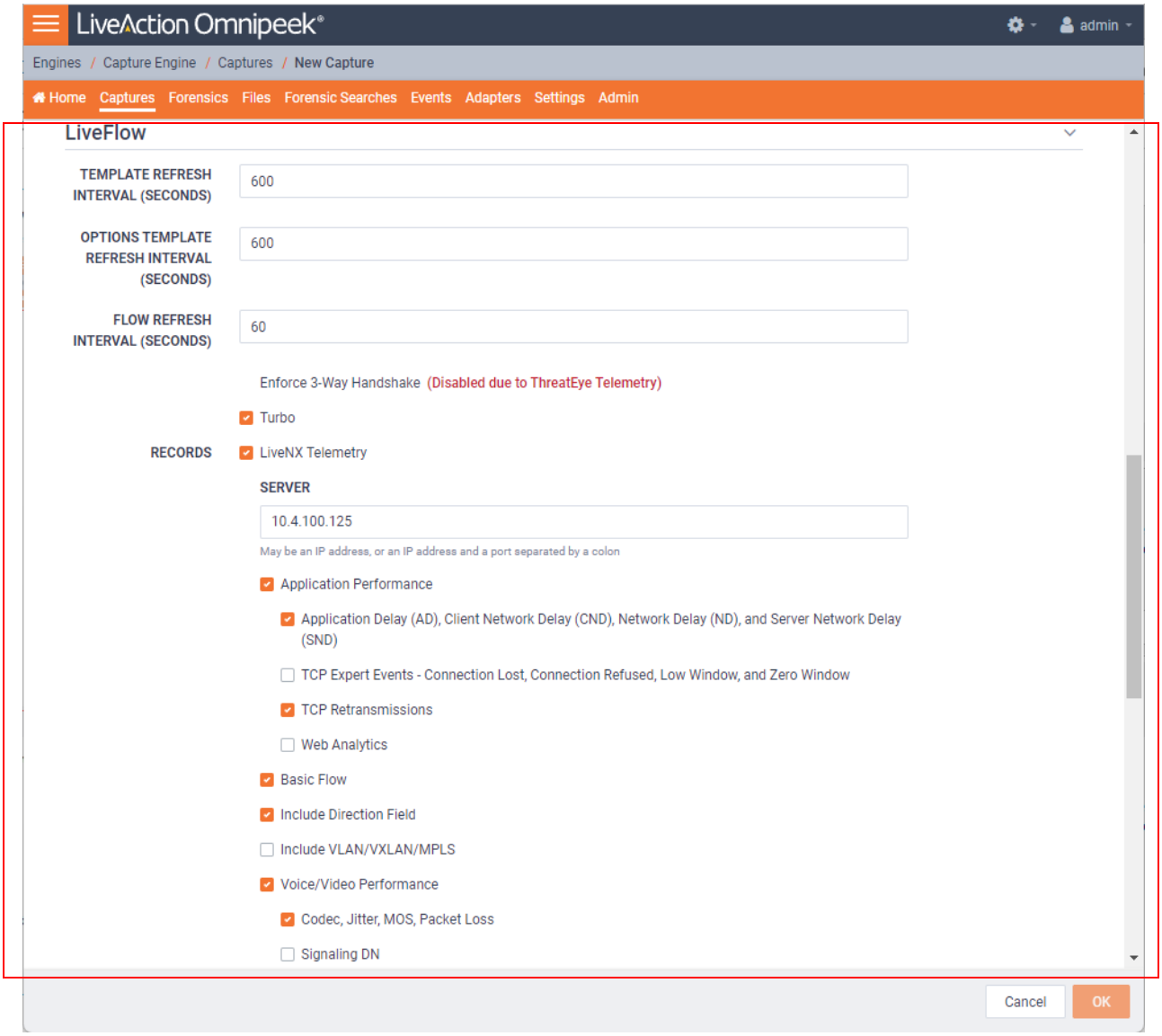
Adapter

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


LiveAction Omnipeek
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
IPv6 Address
VLAN
MPLS
BUFFER SIZE (MB)
256
Start capture immediately
Adapter
eth0
Ethernet, 10,000 Mbits/s, 00:50:56:AD:75:60
eth1
Ethernet, 10,000 Mbits/s, 00:50:56:AD:CD:59
LiveFlow
TEMPLATE REFRESH INTERVAL (SECONDS)
600
OPTIONS TEMPLATE REFRESH INTERVAL (SECONDS)
600
FLOW REFRESH INTERVAL (SECONDS)
60
Enforce 3-Way Handshake
Turbo
RECORDS
LiveNX Telemetry
SERVER
10.4.100.125
May be an IP address, or an IP address and a port separated by a colon
Application Performance
Cancel
OK

LiveFlow

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



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.

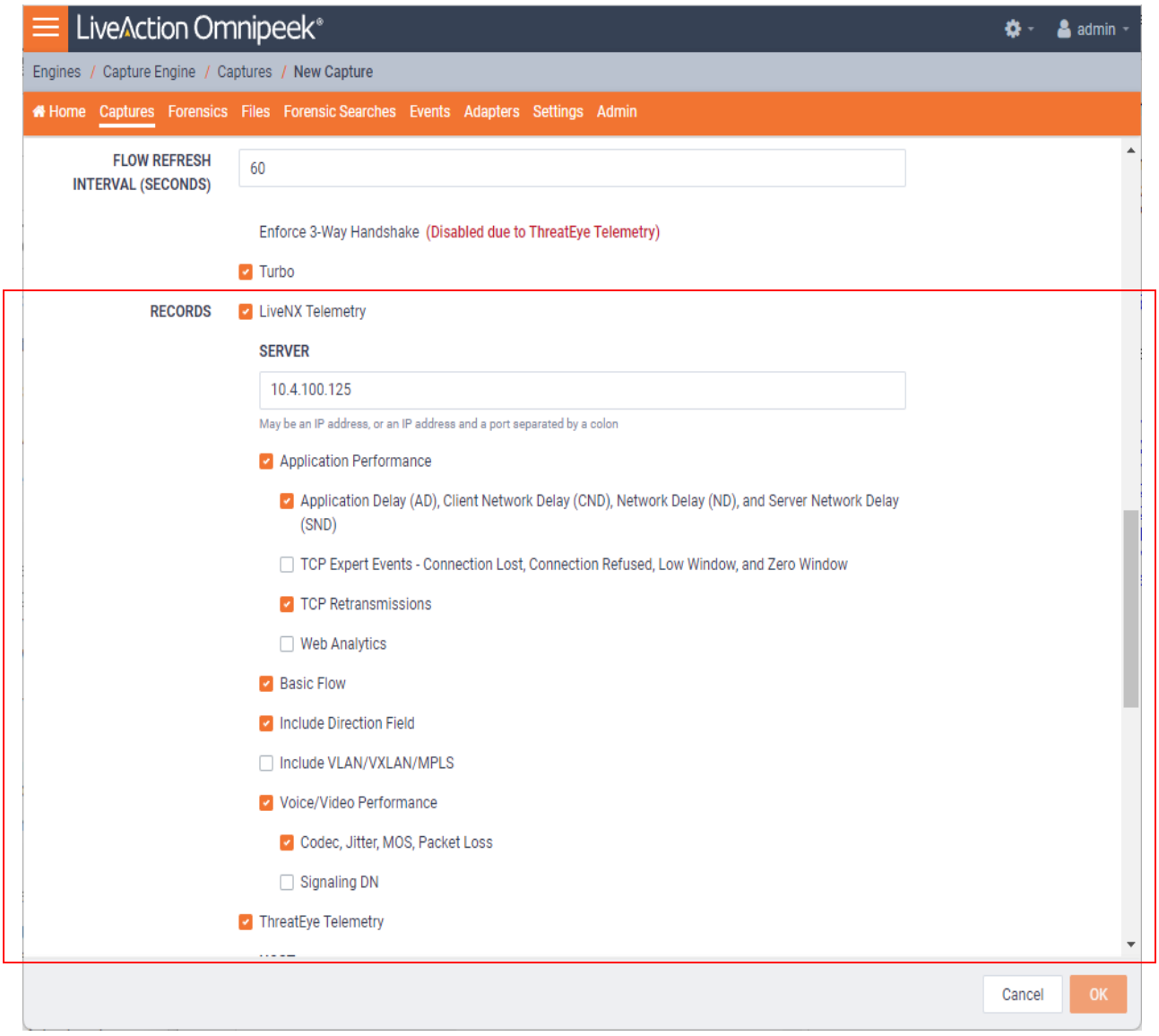
Note If you recently connected LiveWire to the network, it may take up to 600 seconds for LiveNX to see the LiveFlow data from LiveWire. You may want to adjust this setting to the desired intervals.

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.
  - *Turbo*: Select this option to enable multi-stream CTD (also called Turbo mode) which is done in the capture template. This option will only be configurable (and enabled by default) for virtual capture engines with the *Large* or *Unlimited LiveFlow* activation feature.

Records

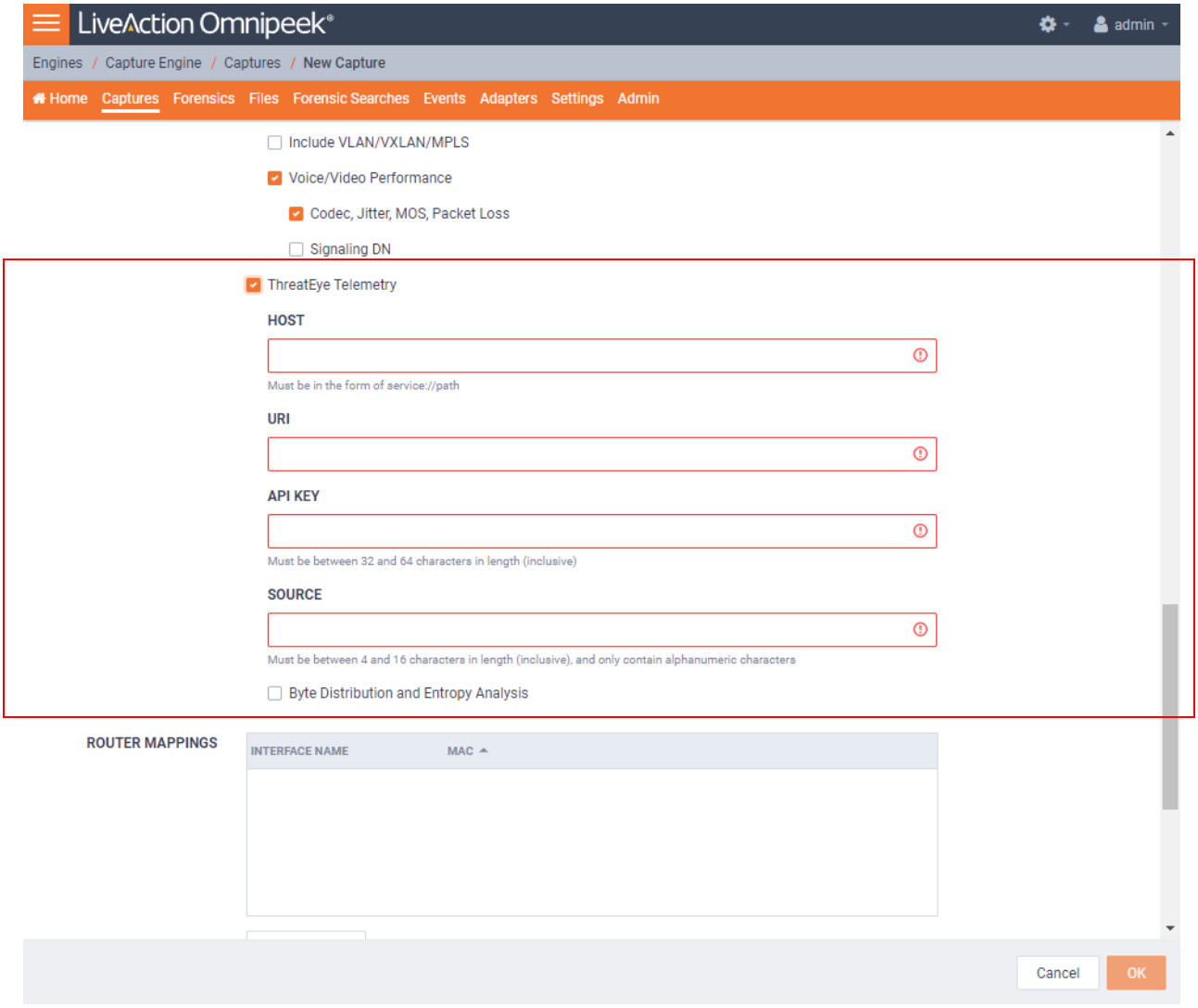
- *LiveNX Telemetry*: Select this option to send LiveFlow telemetry to a specific LiveNX server configured below.



- *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.



- *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.

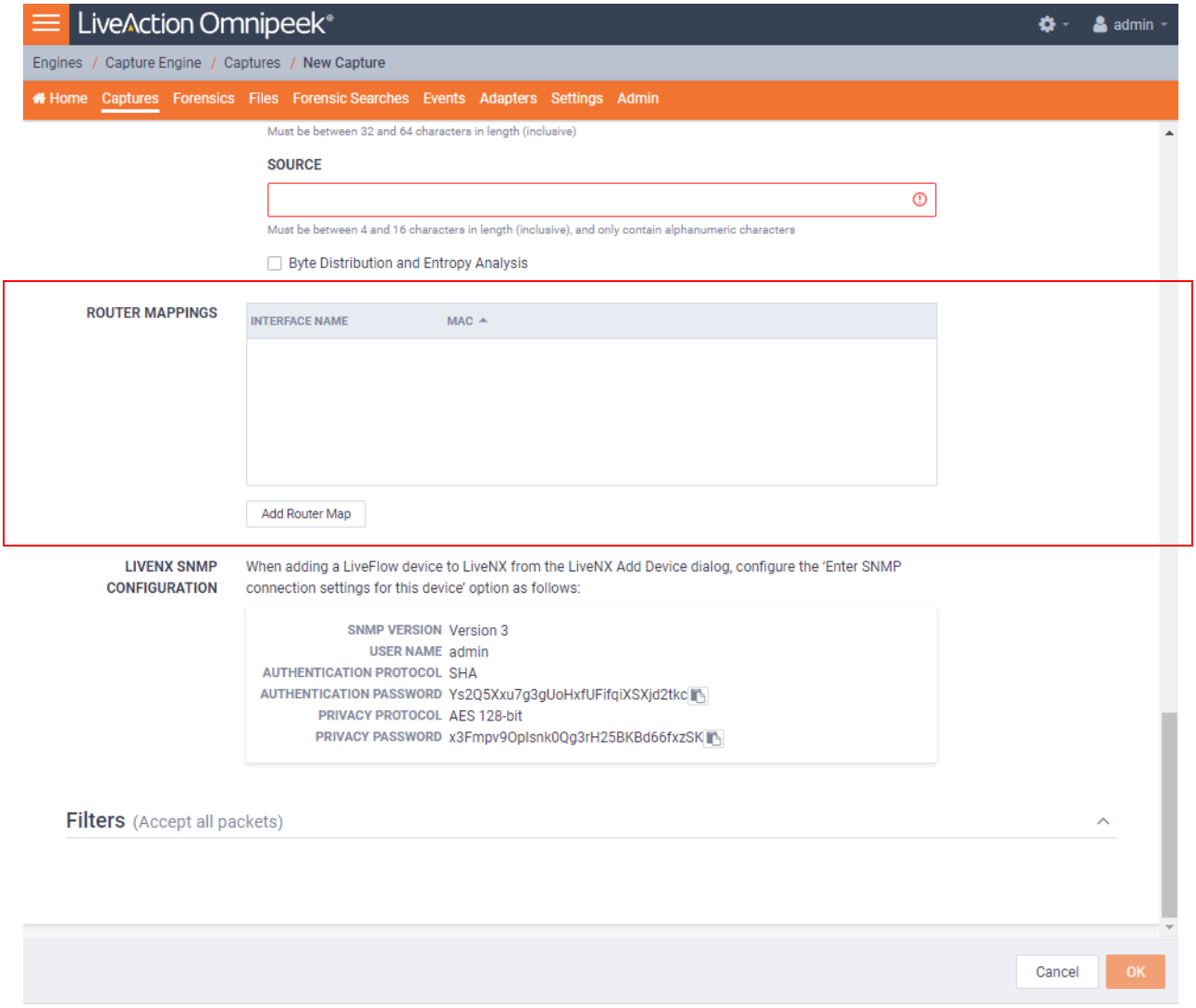
> **Tip** A unique *Source* is recommended for each LiveWire so that they can be easily identified in ThreatEye.

- *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.



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.

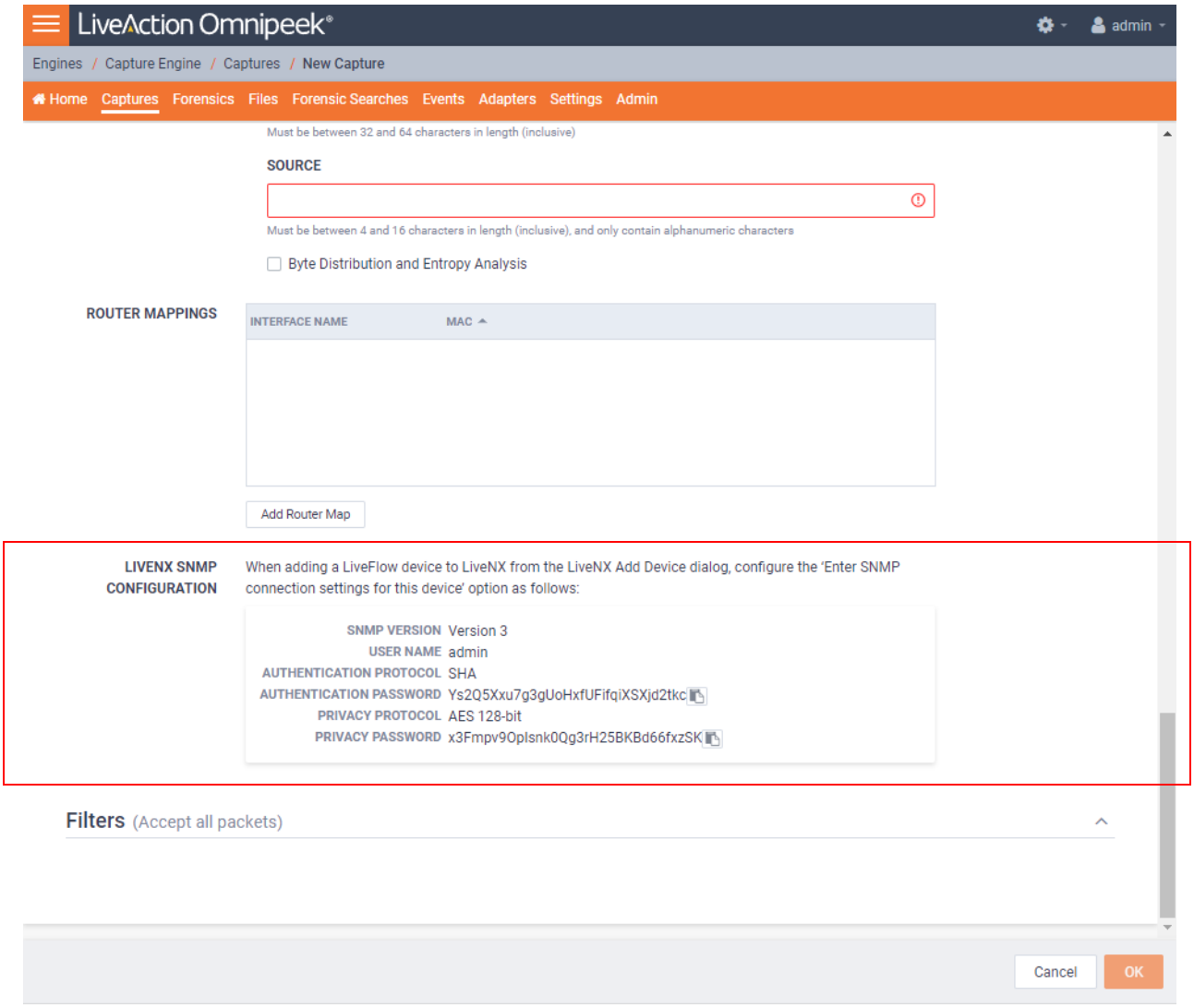
To find the MAC address of the gateway or router, the CLI can be used; otherwise, capture some traffic, or do a Forensics search and look at the *Nodes* view in hierarchical mode. The top level addresses should be the MAC addresses of the gateways and routers for each segment being captured.

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 unique and must be a valid MAC address.
- *Add Router Map:* Click to add a new router mapping. You can add an unlimited number of router mappings.

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.



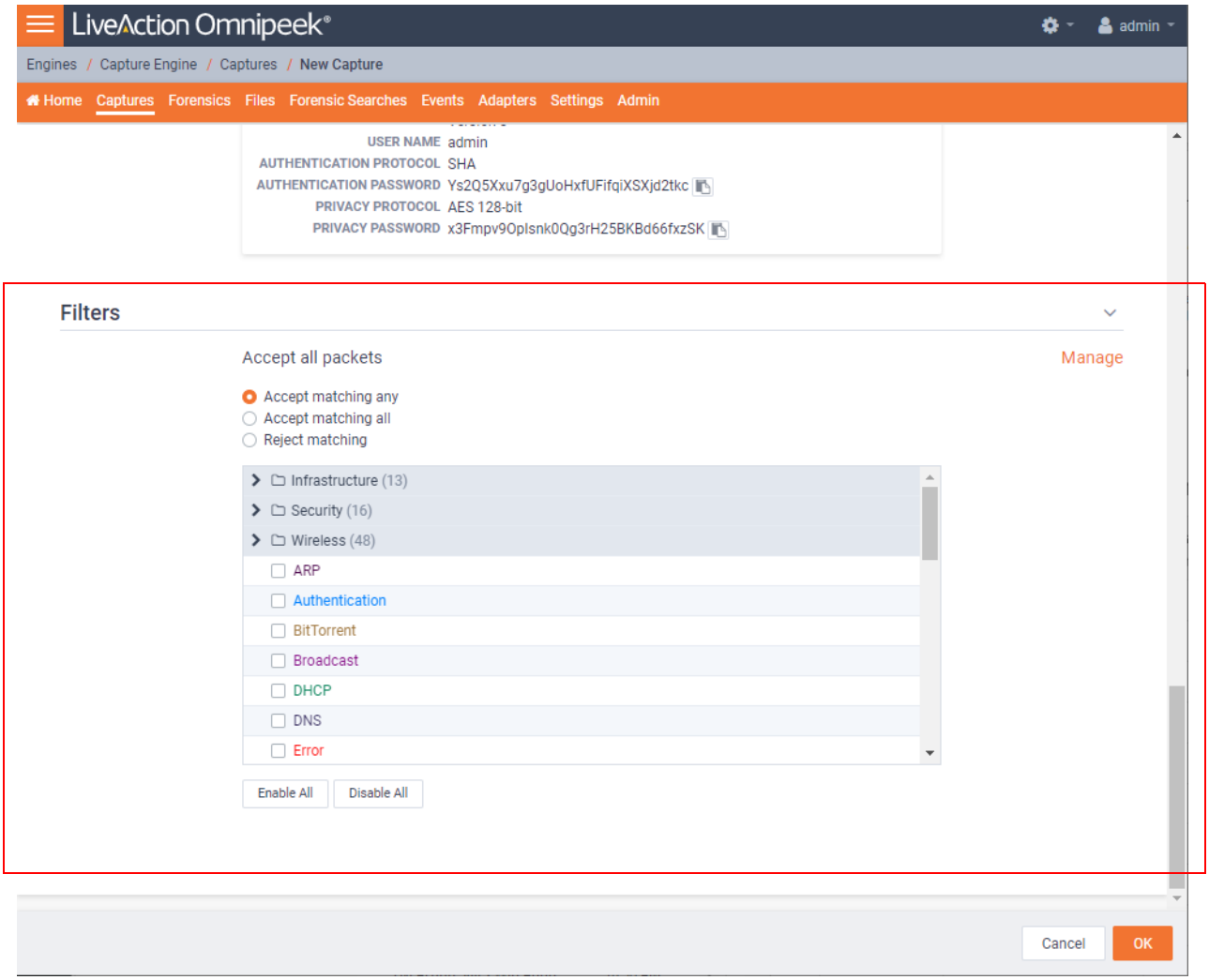
When configuring the '*Enter SNMP connection settings for this device*' option from the **Add Device** dialog in LiveNX client, configure the option as follows:

SNMP Version: **Version 3**
User Name: **admin**
Authentication Protocol: **SHA**
Authentication Password: **Ys2Q5Xxu7g3gUoHxfUFifqiXSXjd2tkc**
Privacy Protocol: **AES 128-bit**
Privacy Password: **x3Fmpv9Oplsnk0Qg3rH25BKBd66fxzSK**

Note You can configure and change the *Authentication Password* and *Privacy Password*. See 'SNMP Credentials' in 'Configure' on page 41.

Filters

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



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

Recommendations for better performance at higher data rates

- At high data rates the capture file can roll over multiple times every second. For higher data rates, the File Size should be increased. This will decrease how often the capture file has to be rolled over, and indirectly increase the performance.

- Forensic Searches use the same partition as the capture files, so leave some disk space available for the Forensic Search. Typically, 10-20 GB is sufficient, but the right setting will depend on the size of the forensic searches, and how many there are.
- Packet File Indexing is used to potentially increase Forensic Search performance when relevant filters are used. However, packet file indexing also decreases capture performance and can take a considerable amount of disk space.
- The file size and file indexes are related in that the smaller the file size the more packet indexes there will be. When there are more addresses, this can lead to large index files. A larger file size will generate fewer indexes.

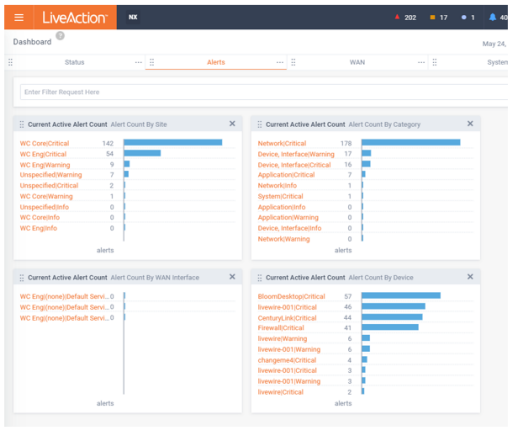
An example of using LiveWire, LiveNX, and Omnipeek

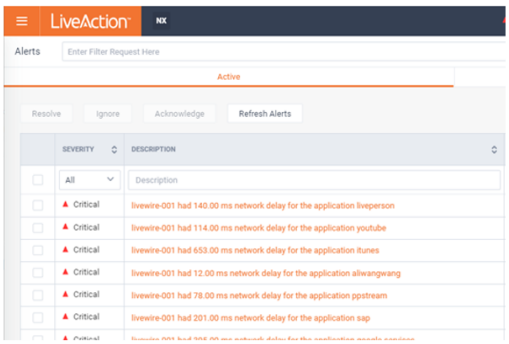
A web-based version of LiveAction's Omnipeek Network Analysis Software is available from LiveNX. You can easily start and use Omnipeek whenever you identify an interesting alert or flow in LiveNX that needs further investigation and you want to analyze the packet level details more closely in Omnipeek.

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.

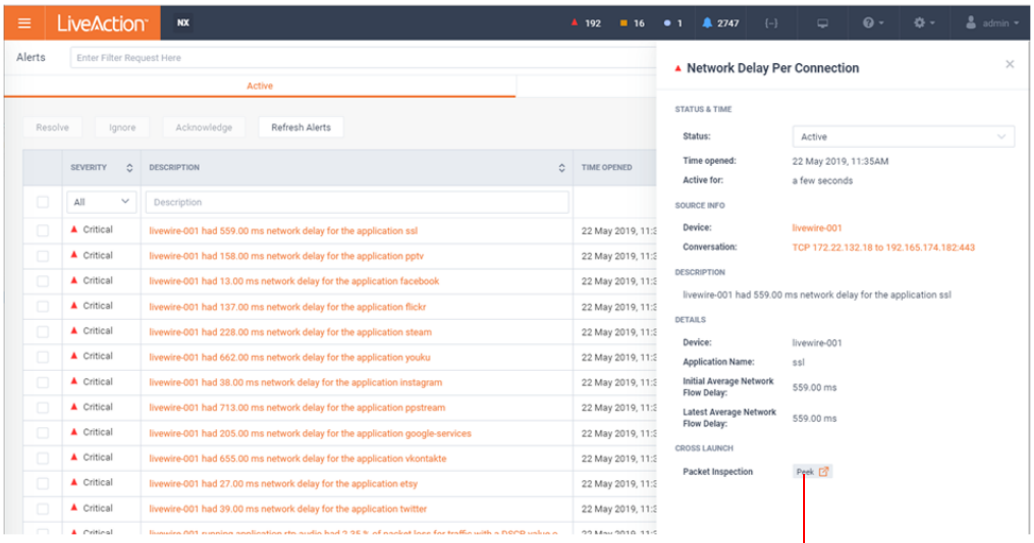
For example, a user on your network experiences poor call quality during a portion of their teleconference meeting. Since you have LiveNX and are populating it with both NetFlow from infrastructure routers as well as LiveFlow from LiveWire appliance, you can visualize any flow, including this teleconference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

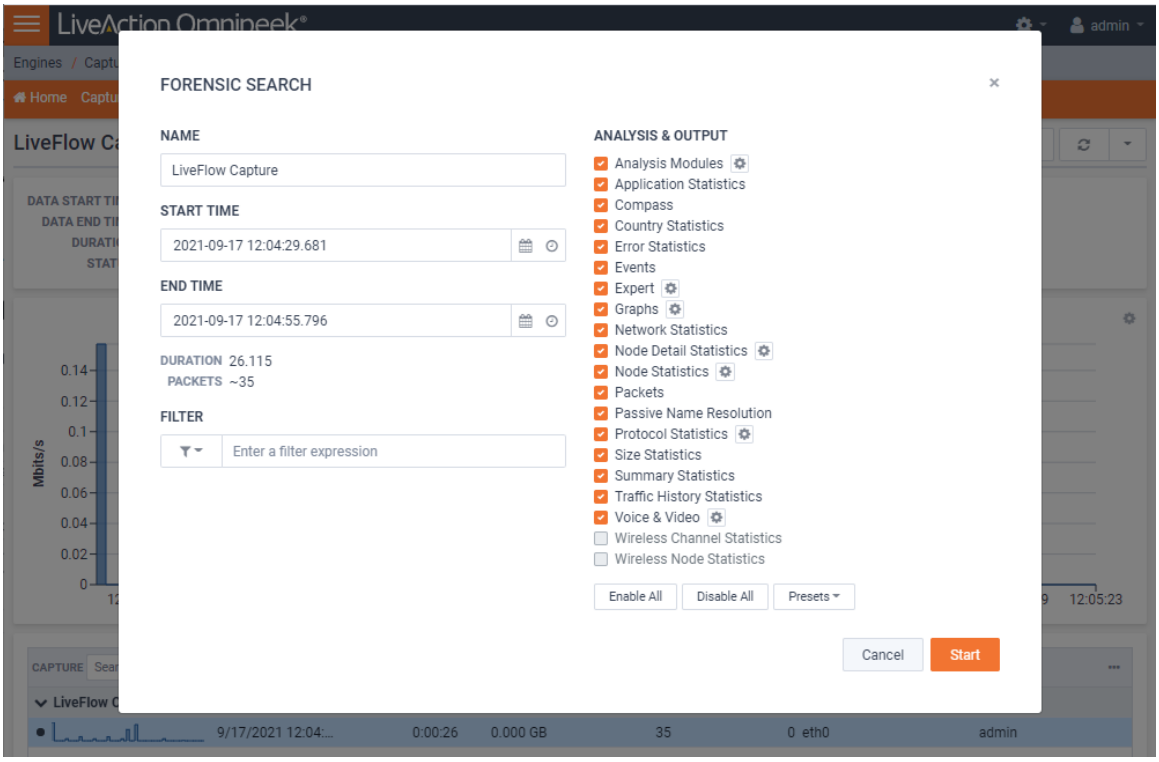




You also notice that an alert was triggered for excessive delay. This alert confirms the user's report, but you'd like to dig in even deeper to perform a root cause analysis of the issue. The best way to do this is with the network packets themselves, and since this call was captured by a LiveWire appliance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



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.

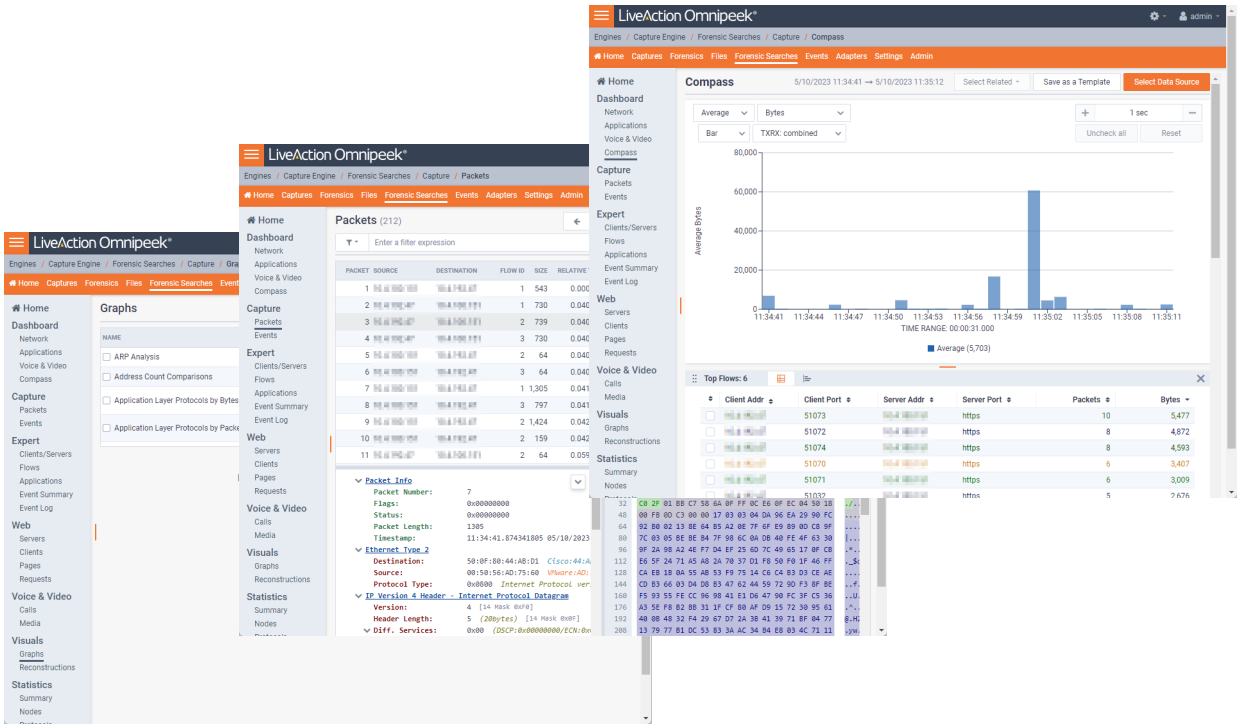


The default filter in the Forensic Search dialog includes the source and destination IP addresses of the flow. The filter can be changed to include more packets in the result, providing insight into what other traffic may be related or affecting the quality of the flow in question.

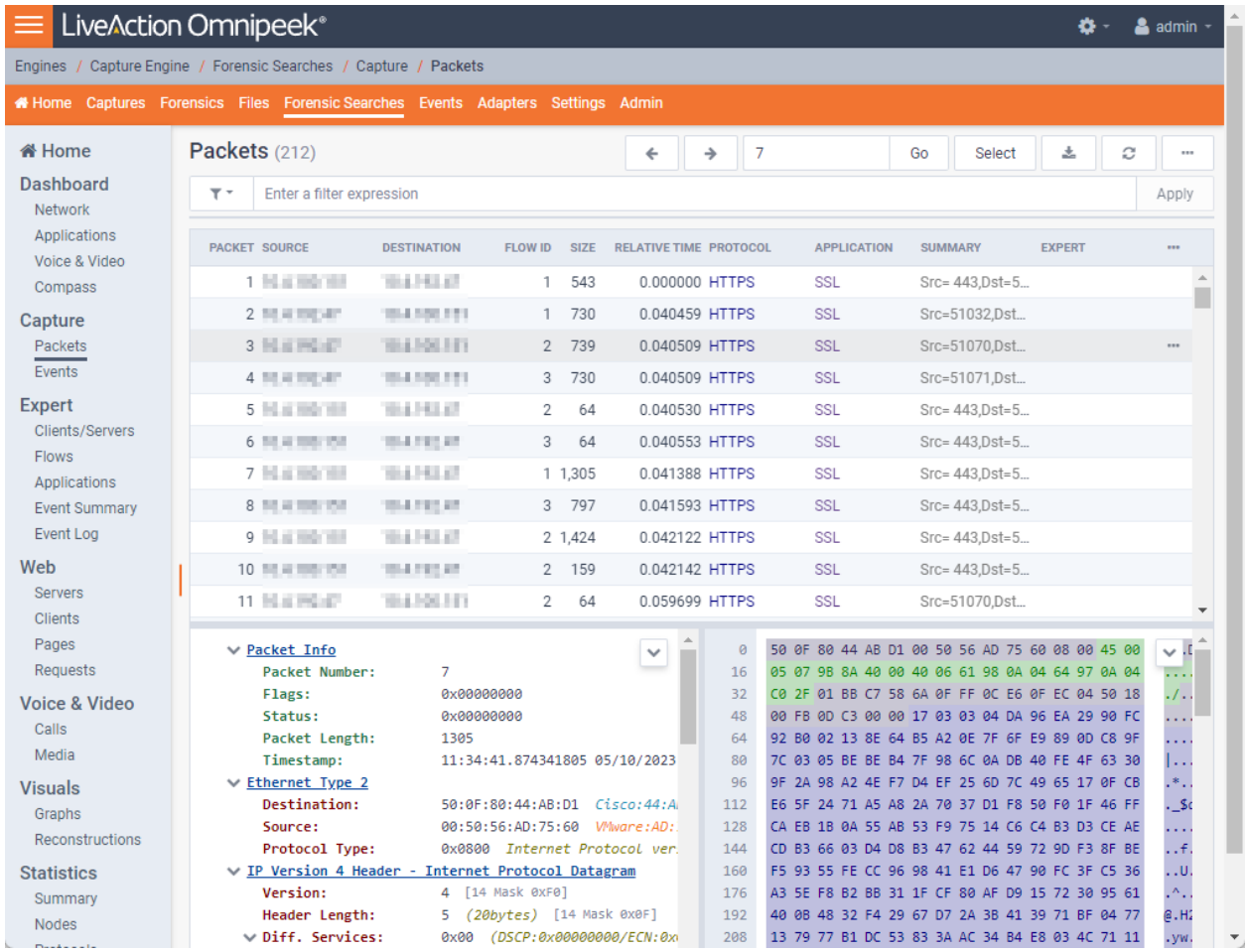
The time range can be adjusted to include more (or less) packets. This can work in conjunction with the filter, which when widened, will include more packets from the other flows between the source and destination IP.

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.



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.


LiveAction Omnipeek
admin
Engines / Capture Engine / Forensic Searches / Capture / Packets
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Home
Dashboard
Network
Applications
Voice & Video
Compass
Capture
Packets
Events
Expert
Clients/Servers
Flows
Applications
Event Summary
Event Log
Web
Servers
Clients
Pages
Requests
Voice & Video
Calls
Media
Visuals
Graphs
Reconstructions
Statistics
Summary
Nodes
Packets (212)
Go
Select
Enter a filter expression
Apply
PACKET SOURCE DESTINATION FLOW ID SIZE RELATIVE TIME PROTOCOL APPLICATION SUMMARY EXPERT
1 1 543 0.000000 HTTPS SSL Src= 443,Dst=5...
2 1 730 0.040459 HTTPS SSL Src=51032,Dst...
3 2 739 0.040509 HTTPS SSL Src=51070,Dst...
4 3 730 0.040509 HTTPS SSL Src=51071,Dst...
5 2 64 0.040530 HTTPS SSL Src= 443,Dst=5...
6 3 64 0.040553 HTTPS SSL Src= 443,Dst=5...
7 1 1,305 0.041388 HTTPS SSL Src= 443,Dst=5...
8 3 797 0.041593 HTTPS SSL Src= 443,Dst=5...
9 2 1,424 0.042122 HTTPS SSL Src= 443,Dst=5...
10 2 159 0.042142 HTTPS SSL Src= 443,Dst=5...
11 2 64 0.059699 HTTPS SSL Src=51070,Dst...
Packet Info
Packet Number: 7
Flags: 0x00000000
Status: 0x00000000
Packet Length: 1305
Timestamp: 11:34:41.874341805 05/10/2023
Ethernet Type 2
Destination: 50:0F:80:44:AB:D1 Cisco:44:A
Source: 00:50:56:AD:75:60 VMware:AD:
Protocol Type: 0x0800 Internet Protocol ver
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:0x
0 50 0F 80 44 AB D1 00 50 56 AD 75 60 08 00 45 00
16 05 07 9B 8A 40 00 40 06 61 98 0A 04 64 97 0A 04
32 C0 2F 01 BB C7 58 6A 0F FF 0C E6 0F EC 04 50 18
48 00 FB 0D C3 00 00 17 03 03 04 DA 96 EA 29 90 FC
64 92 B0 02 13 8E 64 B5 A2 0E 7F 6F E9 89 0D C8 9F
80 7C 03 05 BE BE B4 7F 98 6C 0A DB 40 FE 4F 63 30
96 9F 2A 98 A2 4E F7 D4 EF 25 6D 7C 49 65 17 0F CB
112 E6 5F 24 71 A5 A8 2A 70 37 D1 F8 50 F0 1F 46 FF
128 CA EB 1B 0A 55 AB 53 F9 75 14 C6 C4 B3 D3 CE AE
144 CD B3 66 03 D4 D8 B3 47 62 44 59 72 9D F3 8F BE
160 F5 93 55 FE CC 96 98 41 E1 D6 47 90 FC 3F C5 36
176 A3 5E F8 B2 BB 31 1F CF 80 AF D9 15 72 30 95 61
192 40 0B 48 32 F4 29 67 D7 2A 3B 41 39 71 BF 04 77
208 13 79 77 B1 DC 53 83 3A AC 34 B4 E8 03 4C 71 11

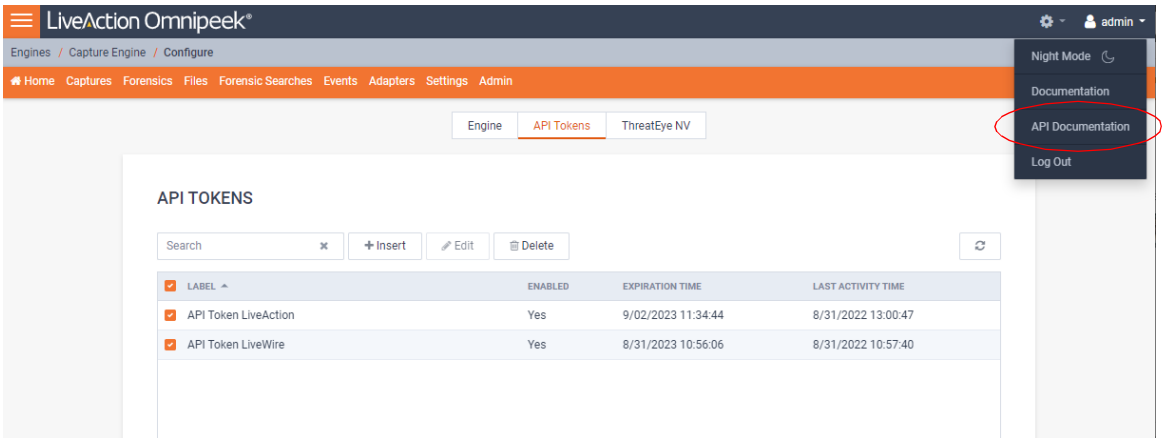
Creating and Managing API Tokens

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.

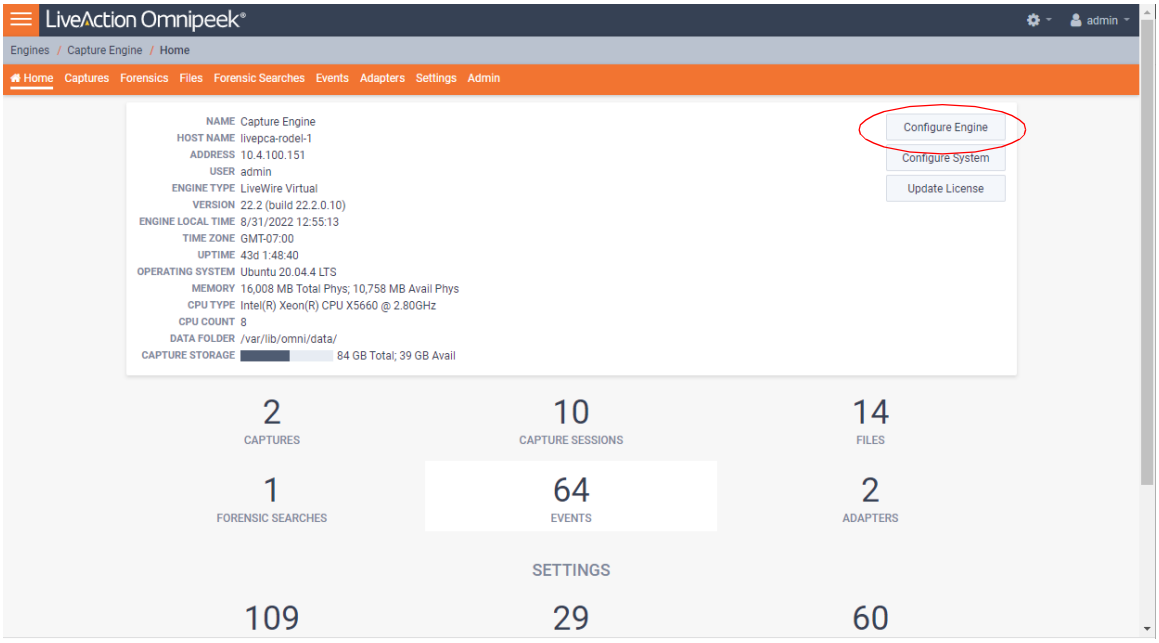


Creating an API Token

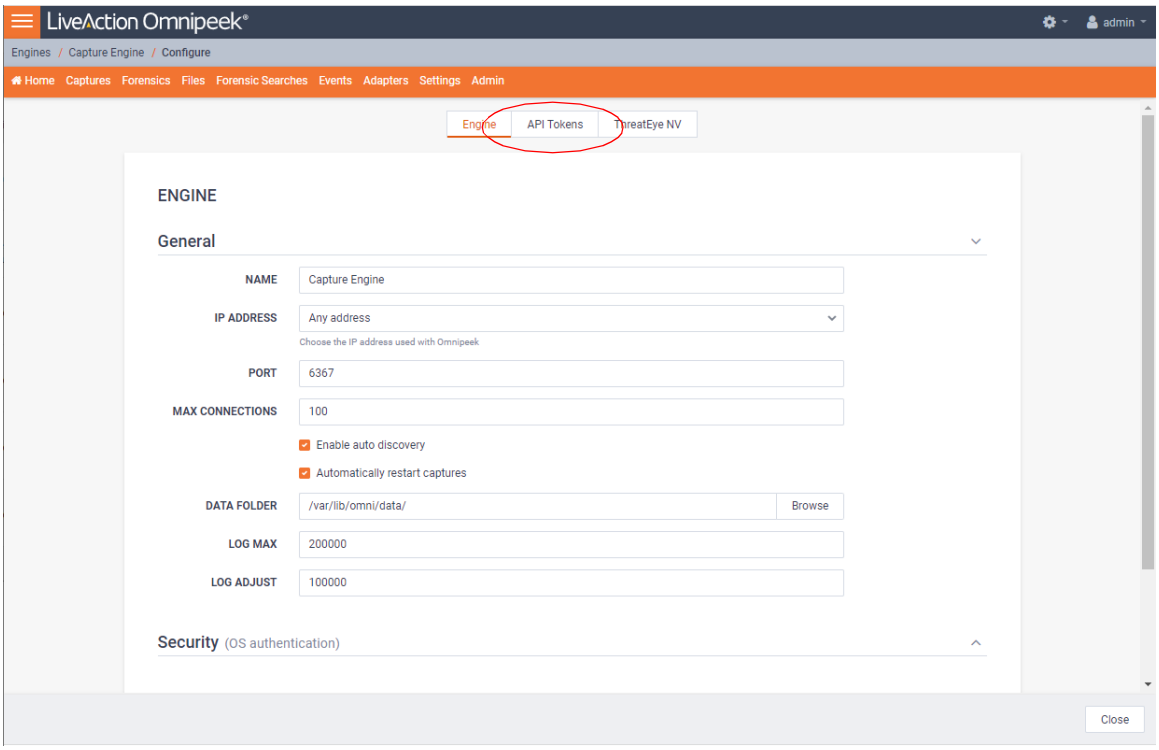
Note An API token has all of the permissions/policies as the user that created the API token.

To create an API token:

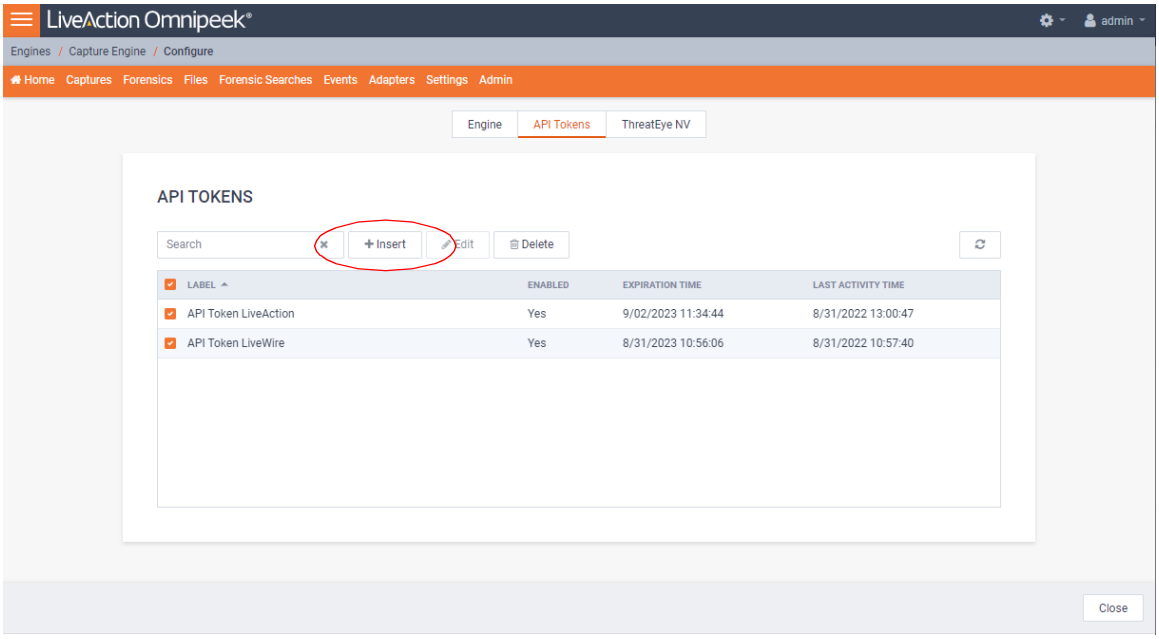
1. Use Omnipeek to view the *Home* page.



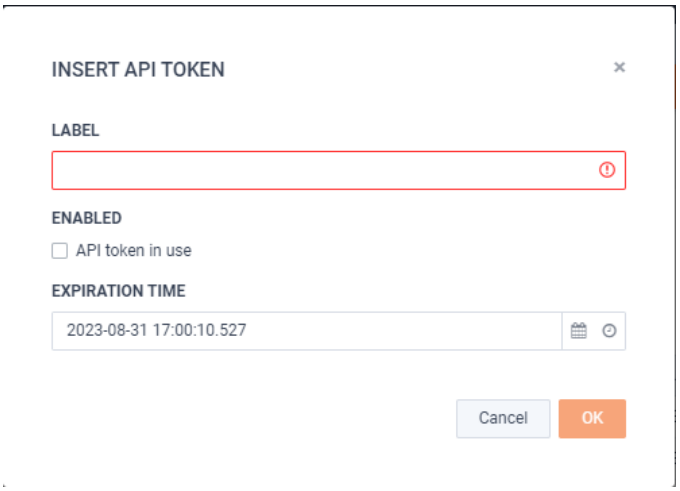
2. Click **Configure Engine**. The *Engine* page appears.



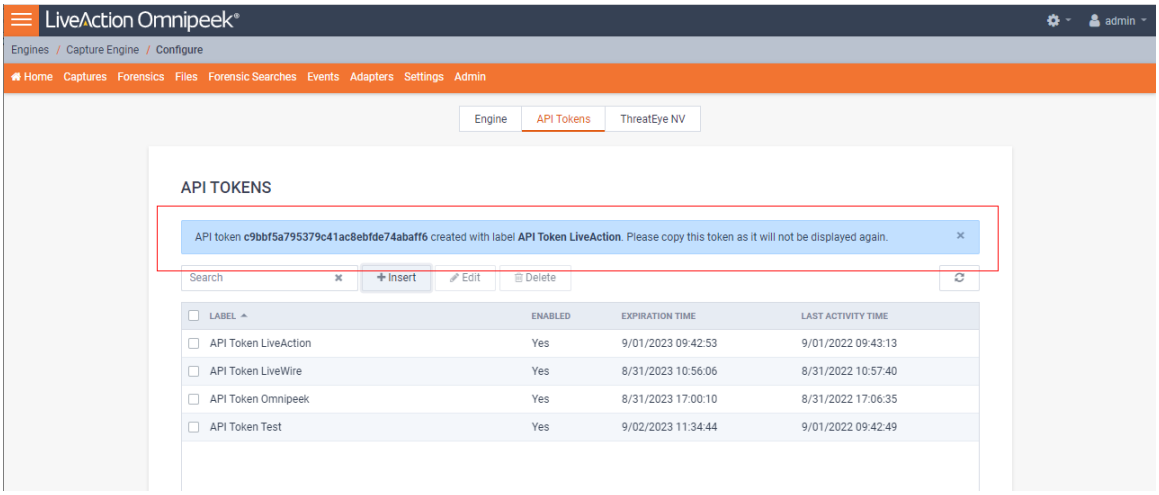
3. Click **API Tokens**. The *API Tokens* page appears.



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



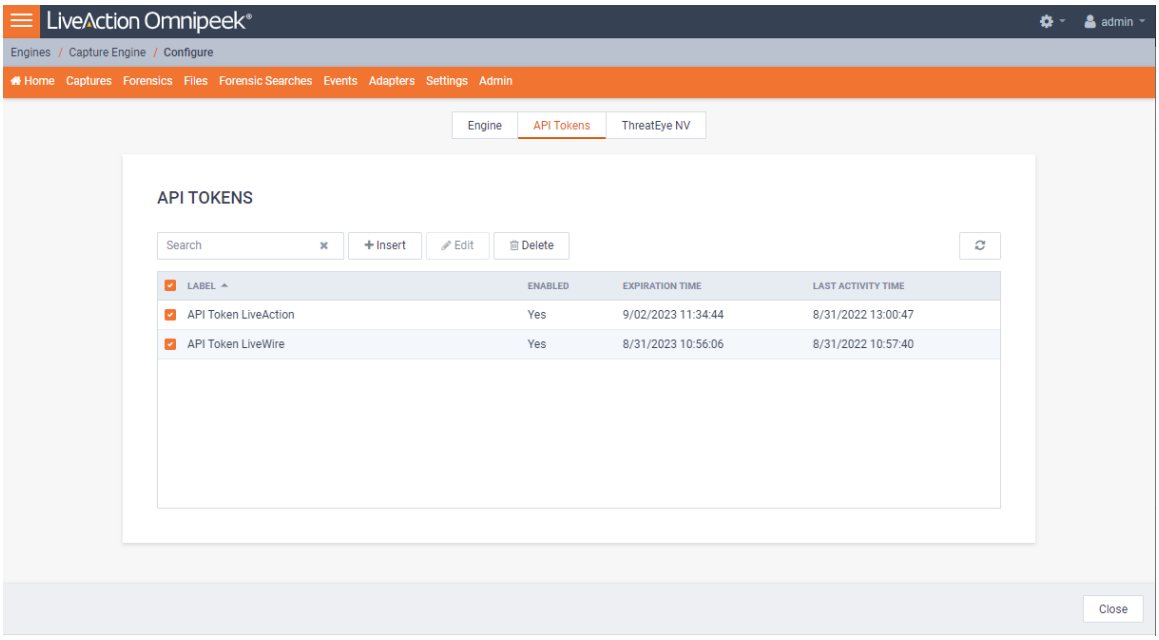
5. Configure the dialog:
   - *Label*: Enter a descriptive label for the API token. A descriptive label helps you to identify the API token.
   - *Enabled*: Select the check box to enable the API token.
   - *Expiration Time*: Click the Select date and Select time icons to set the date and time in whcich 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.



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.



- *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 98.
- *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.

Capture Engines

In this chapter:

About Capture Engine

Pre-installed on LiveWire, Capture Engine captures and analyzes network traffic in real time and records that traffic for post-capture analysis. With Capture Engine, network engineering teams can monitor distributed networks remotely and quickly identify and remedy performance bottlenecks without leaving the office.

Capture Engine works in conjunction with Omnipeek, a separate software program required for the monitoring and analysis of the packets captured remotely by LiveWire. 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 120, and also the *Omnipeek User Guide* or Omnipeek online help.

Using the Capture Engine Manager

The Capture Engine Manager is installed by default when you install Omnipeek. You can run the Capture Engine Manager from the Omnipeek computer to do the following:

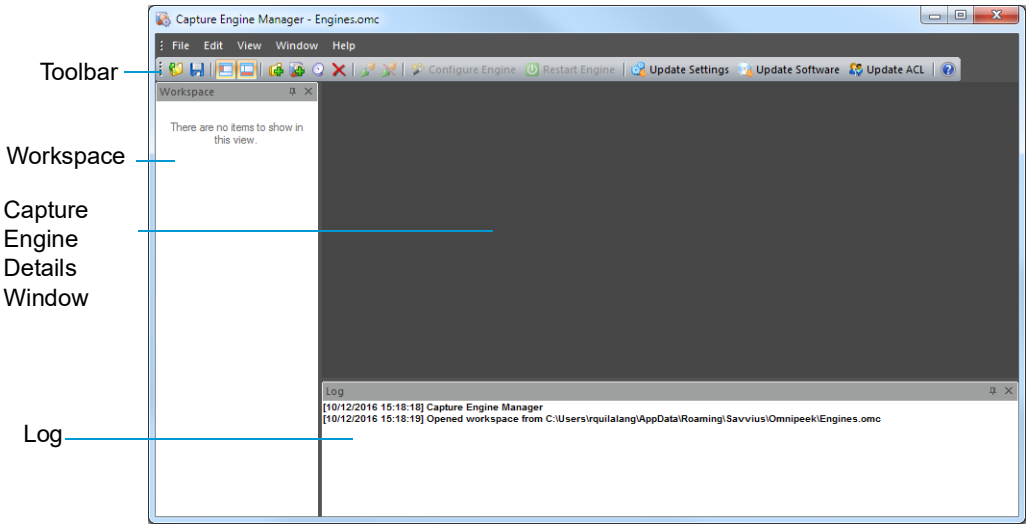
- Update and configure the Capture Engine on LiveWire
- Display the status and configuration of Capture Engines
- Update settings for filters, alarms, remote graph templates, and capture templates
- Distribute security settings to all Capture Engines running within the same domain
- View the Audit log

Navigating the Capture Engine Manager window

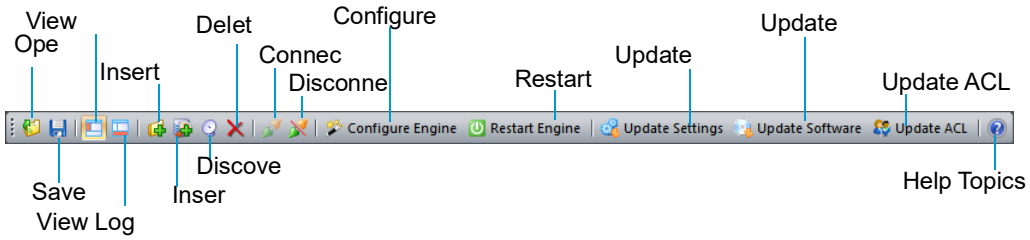
To start the Capture Engine Manager from the Omnipeek computer:

- Choose **Start** > **All Programs** > **LiveAction** > **LiveAction Capture Engine Manager for Omnipeek**. The **Capture Engine Manager** appears.
- On the **Start** menu, click **LiveAction Capture Engine Manager for Omnipeek**. The Capture Engine Manager appears.

The parts of the **Capture Engine Manager** window are described below.



- *Toolbar:* The toolbar allows you to control the following program functions:



- *Open:* Click to open a Capture Engine Manager Workspace *(*.omc)* file.

Note Opening a Capture Engine Manager Workspace *(*.omc)* file other than the ***engines.omc*** default file (located in *C:\Users\<username>\AppData\Roaming\LiveAction\Omnipeek)*, will no longer synchronize the list of Capture Engines displayed in Omnipeek and Capture Engine Manager.

- *Save:* Click to save the Capture Engine Manager Workspace *(*.omc)* file.
- *View Workspace:* Click to hide/show the Workspace pane.
- *View Log Window:* Click to hide/show the Log pane.
- *Insert Group:* Click to insert a new Capture Engine group.
- *Insert:* Click to insert a new Capture Engine.
- *Discover:* Click to discover Capture Engines via UDP multicast. See 'Discover Capture Engines' on page 108.
- *Delete:* Click to delete the selected Capture Engine group or single Capture Engine.
- *Connect*: Click to display the **Connect** dialog, allowing you to connect to the selected Capture Engine. See 'Connecting to a Capture Engine' on page 105.
- *Disconnect*: Click to disconnect the Capture Engine Manager from the Capture Engine displayed in the active window.
- *Configure Engine:* Click to start the **Capture Engine Configuration Wizard** to configure the Capture Engine. See 'Configuring a Capture Engine' on page 109.
- *Restart Engine*: Click to restart the Capture Engine. See 'Reconnect button' on page 108.
- *Update Settings:* Click to update the settings for **Filters**, **Alarms**, or **Graphs** for the Capture Engine. See 'Updating Capture Engine settings' on page 114.
- *Update Software:* Click to update the Capture Engine software for one or more Capture Engines using the Update Service.
- *Update ACL:* Click to distribute a single Access Control List (ACL) to multiple Capture Engines running on machines belonging to the same Domain. See 'Updating Capture Engine ACL settings' on page 115.
- *Help Topics:* Click to display online help for the Capture Engine Manager application.

- *Workspace:* This area displays the list of currently defined Capture Engines. Both Omnipeek and Capture Engine manager maintain the same list of Capture Engines. Making a change in either program automatically updates the list in the other program.

Note Right-click inside the Workspace to display a context-menu with additional options for displaying the list of Capture Engines; inserting and discovering Capture Engines; editing, deleting, or renaming Capture Engines; connecting and disconnecting Capture Engines; forgetting all passwords; and importing and exporting Capture Engines.

- *Capture Engine Details window:* This area displays the details and tabbed views for the Capture Engine. Each Capture Engine window can also have an **Analysis Modules** and **Audit Log** view, in addition to **Status, Filters, Alarms,** and **Graphs** views. Double-click any Capture Engine in the Workspace to view the details for that Capture Engine.
- *Log:* This area shows the messages sent to the Log file, including program start and the status of update tasks.
  - You can right-click inside the log to save, copy, or clear the contents of the Log file.
  - Choose **File** > **Save log** to save the Log file as a text file.

> **Tip** You can float the Workspace and Log panes, or drag either to dock it in a different location. To toggle between floating and docking, double-click the title bar of the window.

Creating new engine groups

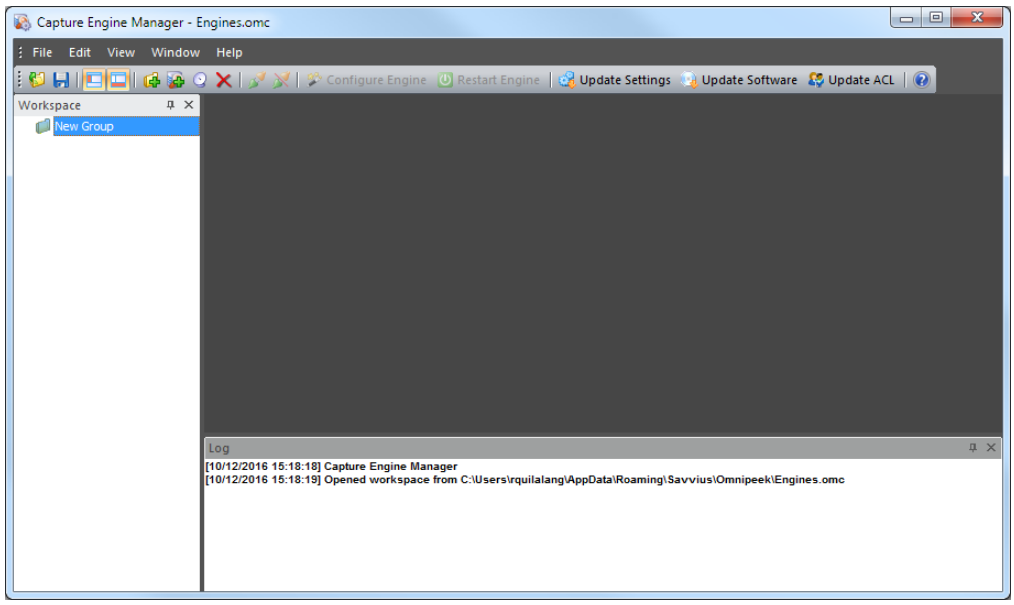
You can organize Capture Engines in groups or add single Capture Engines one at a time to the Workspace.

To create a new group in the Workspace:

1. Select the location in the Workspace under which the new group should appear.
2. Click **Insert Group** in the toolbar.

   The new group appears with its default name (*New Group*) ready to edit.

> **Tip** To change the name of a group in a Workspace file, right-click and choose **Rename**.

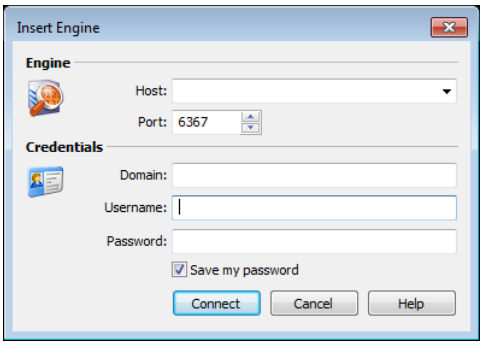


Connecting to a Capture Engine

You can connect to a Capture Engine and add it to the Workspace.

To add a Capture Engine to the Workspace:

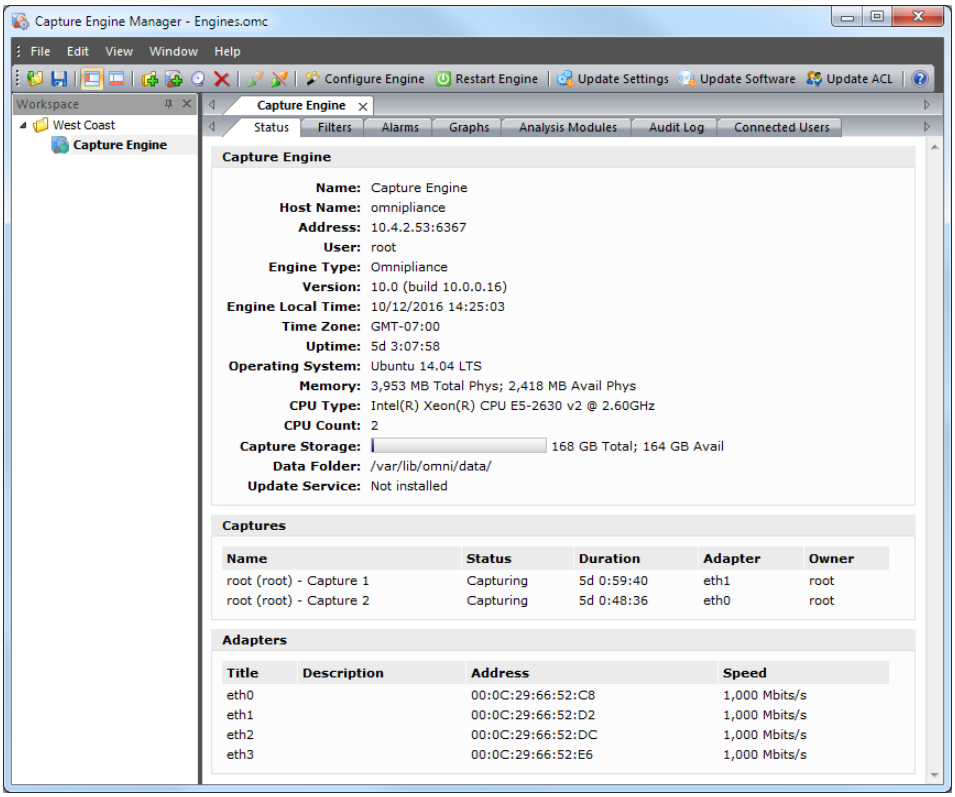
1. Select the location in the Workspace under which the new Capture Engine should appear.
2. Click **Insert Engine**. The **Insert Engine** dialog appears.



3. Complete the dialog:
   - *Host:* Enter the IP address or DNS name of the engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
   - *Username:* Type the Username for login to the Capture Engine.
   - *Password:* Type the Password for login to the Capture Engine.

Note If you leave the *Username* and *Password* fields blank, the Capture Engine Manager attempts to log in using the current Windows login credentials.

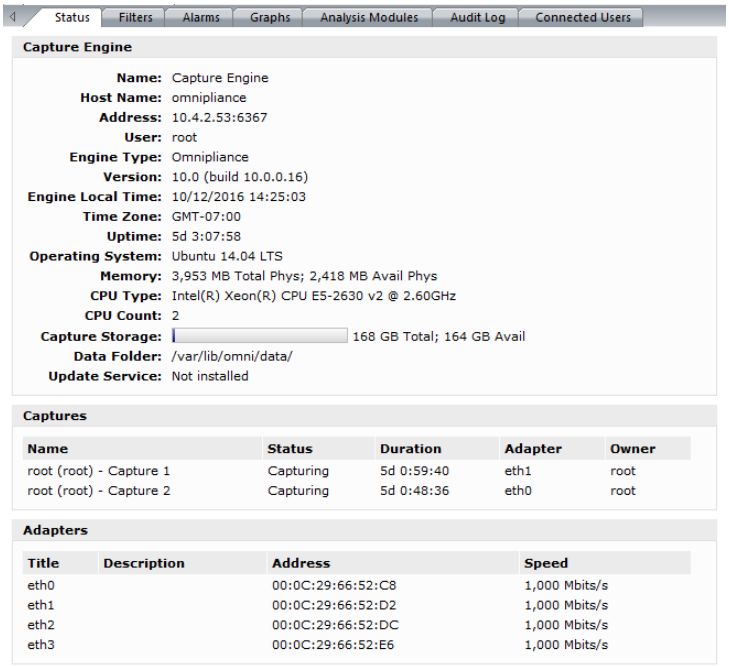
4. Click **Connect**. When the connection is established, the Capture Engine is added to the Workspace and its **Capture Engine** window is displayed showing details for that Capture Engine. See 'Capture Engine details windows' on page 107.



Note When you close the **Capture Engine Manager** window, you are automatically disconnected from any Capture Engine displayed in the Capture Engine Manager. When you start the Capture Engine Manager again, all Capture Engines are in a disconnected state. You will need to reconnect to any Capture Engine that you want to configure or update.

Capture Engine details windows

A **Capture Engine** details window displays status information about the Capture Engine and lists the filter, alarm, and graph settings that can be distributed from the Capture Engine to other Capture Engines using the Capture Engine Manager. A Capture Engine details window can have the following tabs: **Status**, **Filters**, **Alarms**, **Graphs, Analysis Modules**, and **Audit Log** and **Connected Users**.



- The **Status** tab displays details about the connected Capture Engine. It includes the *Name*, *IP Address* and *Port* configured for the Capture Engine, *User*, product and file *Version* for the Capture Engine, and whether or not the *Update Service* is running.
  - *Captures:* Shows all the captures defined for the Capture Engine, including the Name, Status (Capturing or Idle), Duration, Adapter it is using, and the Owner.
  - *Adapters:* Shows all the adapters available to the Capture Engine, including the Title, Description, physical Address, and the network Speed.

Tip To print the **Status** tab of a Capture Engine window, make it the active window and choose **File** > **Print...**.

- The **Filters** tab lists all the filters defined for the Capture Engine
- The **Graphs** tab lists all the remote graph templates defined for the Capture Engine
- The **Analysis Modules** tab displays summary information about each analysis module installed on the Capture Engine
- The **Audit Log** tab lists all available information regarding events taking place on the Capture Engine. You can go to the first and last page of the log, and you can search the log.

- The **Connected Users** tab lists all users currently connected to the Capture Engine. Click **Refresh** to refresh the list.

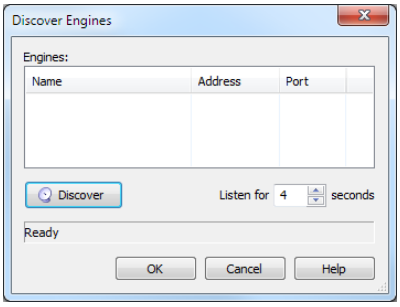
You can distribute settings from the **Filters**, **Alarms**, and **Graphs** tabs to other Capture Engines. For details, see 'Updating Capture Engine settings' on page 114.

Discover Capture Engines

When you click **Discover** in the toolbar, the **Discover Engines** dialog appears. This dialog lets you search for Capture Engines installed on the local segment of your network. You can then insert one or more of the Capture Engines that are found into the Workspace.

To discover Capture Engines:

1. Click **Discover** in the toolbar. The **Discover Engines** dialog appears.



   - *Engines:* Displays the Capture Engines found on the local segment of your network.
   - *Discover:* Click to search for Capture Engines installed on the local segment of your network. The status message will change from *Listening...* to *Finished* when all network-available Capture Engines are discovered.
   - *Listen time:* Enter the number of seconds that the Capture Engine Manager will listen for responses to the discovery request. You can enter a minimum of 2 and a maximum of 60 seconds.

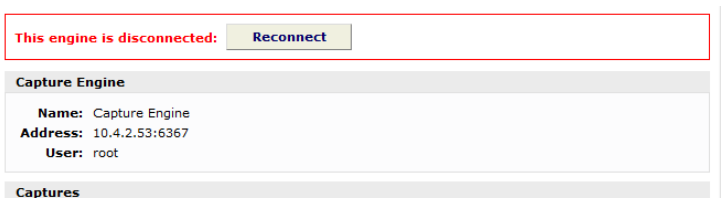
2. Click **Discover** on the dialog. All Capture Engines found on the local segment of your network are displayed in the Engines list.
3. Discovered Capture Engines have the check box next to their name selected. Clear the check boxes of the Capture Engines that you do not want to add to the Workspace and click **OK**. Only the selected Capture Engines are added to the Workspace.

> **Tip** Right-click in the *Engines* pane of the **Discover Engines** dialog and select **Uncheck all** to deselect all Capture Engines.

Reconnect button

To reconnect to a Capture Engine listed in the Workspace:

1. Open the **Status** tab of the **Capture Engine** window for the desired Capture Engine.
2. Click **Reconnect**.



When you click **Reconnect**, the Capture Engine Manager applies the most recently used login information for the selected Capture Engine.

Note If you wish to log in under a different *Username*, or if the configuration for the IP address and/or port have changed since your last login in the same session, you must use the **Connect** dialog directly. See 'Connecting to a Capture Engine' on page 105.

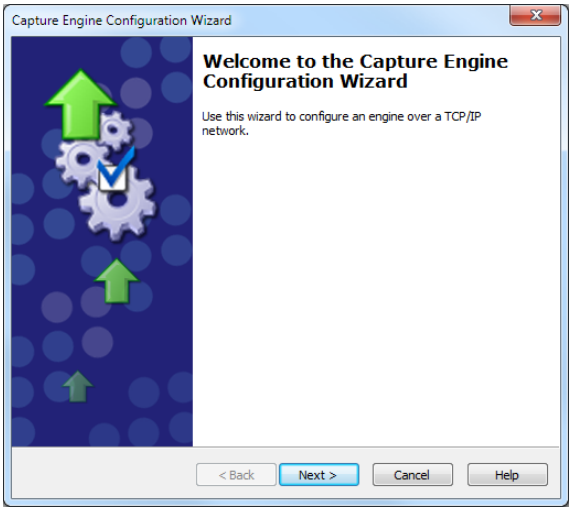
Configuring a Capture Engine

To configure a Capture Engine, you must use the **Capture Engine Configuration Wizard** of the Capture Engine Manager.

Note The **Capture Engine Configuration Wizard** of the Capture Engine Manager also appears when you first install a Capture Engine and are prompted to configure it.

To configure a Capture Engine from the Omnipeek computer:

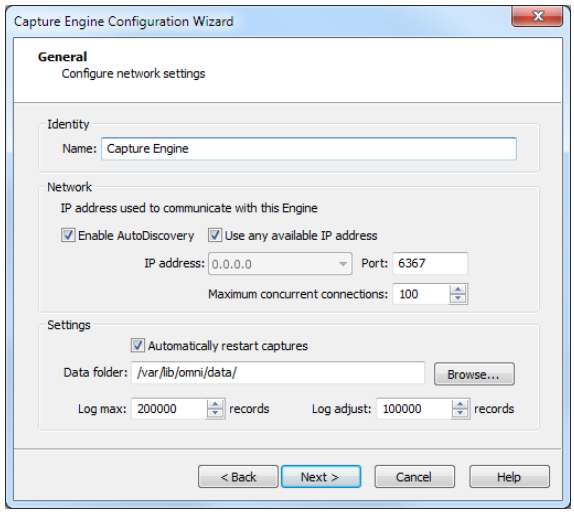
1. Choose **Start** > **All Programs** > **LiveAction** > **LiveAction Capture Engine Manager for Omnipeek**. The **Capture Engine Manager** window appears.
2. Connect to a Capture Engine in the Workspace (see 'Connecting to a Capture Engine' on page 105) and click **Configure Engine** in the toolbar. The **Capture Engine Configuration Wizard** appears.



3. Click **Next**. The **General** view of the **Capture Engine Configuration Wizard** appears.
4. Configure the settings in the **General**, **Security**, and **Edit Access Control** views. See 'Engine Configuration—General' on page 109; 'Engine Configuration—Security' on page 110; and 'Engine Configuration—Edit Access Control' on page 112.
5. When prompted, click **Yes** to send the configuration changes to the Capture Engine. The configuration changes won't take effect until the Capture Engine is restarted.

Engine Configuration—General

The **General** view of the **Capture Engine Configuration Wizard** lets you configure the name, address, capture restart, local disk use, and log settings for the Capture Engine.

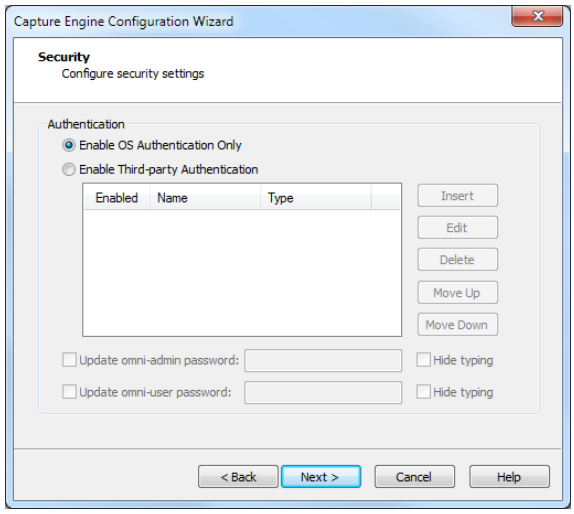


- *Name:* Type a name for the Capture Engine. This name appears in the **Capture Engines** window in Omnipeek.
- *Enable AutoDiscovery:* Select this check box to enable the Capture Engine to respond to autodiscovery requests which arrive from the Capture Engine Manager.
- *Use any available IP address:* Select this check box to accept communications on any and all IP addresses assigned to the computer on which the Capture Engine is installed.
- *IP address:* Select the IP address used to communicate with the Capture Engine. The Capture Engine will respond to communications only on that address. This option is not available when *Use any available IP address* is selected.
- *Port:* Type a port used for communications. The default port is 6367.
- *Maximum concurrent connections:* Type or select the maximum number of concurrent Omnipeek connections allowed for the Capture Engine.
- *Automatically restart captures:* Select this check box to automatically restart captures whenever the Capture Engine restarts. When enabled, the Capture Engine remembers any capture (active or idle) defined for it, and restores the capture whenever the Capture Engine itself is restarted.
- *Data folder:* Type or browse to the location for the data folder. The Capture Engine uses this location to store packet files created when the *Capture to Disk* option is used. The contents of the data folder appear in the **Files** tab of the Omnipeek **Capture Engines** window.
- *Log max:* Select or enter the maximum number of records in the application log. These are the log records you see in the Capture Engine log view. You can enter a range between 100,000 to 100,000,000 records (do not include commas). The default is 200000.
- *Log adjust:* Select or enter the number of application log records that are deleted (the oldest records are deleted first) when the maximum number of log records is reached. You can enter a range between 10,000 to 100,000,000 messages (do not include commas). The default is 100000.

Note Setting the *Log max* or *Log adjust* value to a large number of records or messages can slow down the performance of entries written to the log.

Engine Configuration—Security

The **Security** view of the **Capture Engine Configuration Wizard** lets you set security and authentication settings.



- *Authentication:*
  - *Enable OS Authentication Only:* Select this check box to use the Operating System authentication only, and to disable all other third-party authentication mechanisms.
  - *Enable Third-party Authentication:* Select this check box to enable third-party authentication using an Active Directory, RADIUS, or TACACS+ authentication server. For more information on enabling Third-party authentication, see 'Third-party authentication with Capture Engines' on page 123.
  - *Insert:* Click to display the **Edit Authentication Setting** dialog, which allows you to name the setting and select from one of the following *Third-party Authentication* types:
    - *Active Directory:* Select this type to enable Active Directory authentication, and then configure the host information: *Host* (domain controller) and *Port* settings (Capture Engine (Windows)); or *Realm* (domain controller) and *KDC* settings (Capture Engine (Linux)).
    - *RADIUS:* Select this type to enable RADIUS authentication, and then configure the *Host* (IP address), *Port*, and *Secret* settings (select *Hide Typing* to hide the settings) for the RADIUS authentication server.
    - *TACACS+:* Select this type to enable TACACS+ authentication, and then configure the *Host* (IP address), *Port*, and *Secret* settings (select *Hide Typing* to hide the settings) for the TACACS+ authentication server.
  - *Edit:* Click to edit the selected authentication setting.
  - *Delete:* Click to delete the selected authentication setting.
  - *Move Up:* Click to move the selected authentication setting higher up in the list.
  - *Move Down:* Click to move the selected authentication setting lower up in the list.

Note The order of the authentication settings in the list determines the order an authentication server is authenticated against.

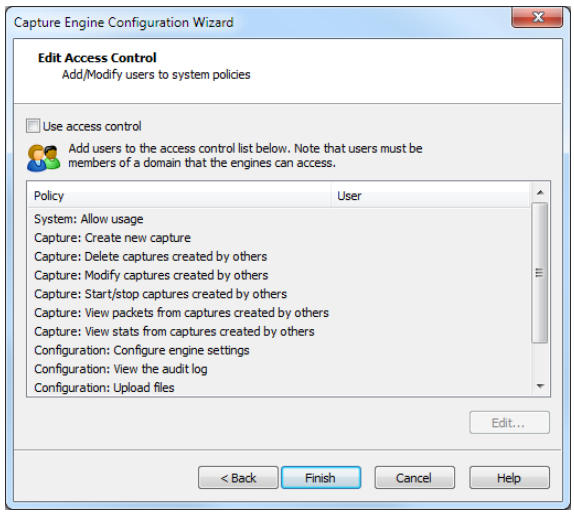
Authentication settings are attempted in groups in a top/down order. For example, if the first setting at the top is a RADIUS setting, then all RADIUS settings in the list are attempted first before attempting the next group type in list. If an authentication server can not be reached because of either an incorrect or unreachable server IP, incorrect port, or incorrect shared secret, then the next setting in the group is attempted. If communication with the authentication server is good, but the user cannot be authenticated because of either an incorrect username, password, or a disabled account, then the next group type is attempted (if authenticating a RADIUS or TACACS+ setting), or the next setting in the list is attempted (if authenticating an Active Directory setting).

Note The Capture Engine operates within the security environment configured in the operating system. Refer to your operating system documentation for instructions on configuring security settings for your operating system.

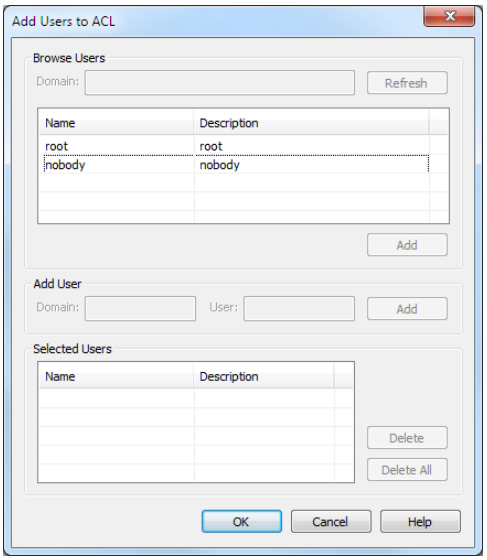
Engine Configuration—Edit Access Control

The **Edit Access Control** view of the **Capture Engine Configuration Wizard** lets you define which users have access to a Capture Engine and which classes of actions (policies) each user is allowed to perform.

Note There are several ways to create a new user in your operating system. Refer to your operating system documentation for instructions on creating new user profiles.



- *Use access control:* Select this check box to enable Access Control.
- The *Policy* column lists the predefined policies:
  - *System: Allow usage*
  - *Capture: Create new capture*
  - *Capture: Delete captures created by others*
  - *Capture: Modify captures created by others*
  - *Capture: Start/Stop captures created by others*
  - *Capture: View packets from captures created by others*
  - *Capture: View stats from captures created by others*
  - *Configuration: Configure engine settings*
  - *Configuration: View/modify matrix switch settings (Capture Engine (Windows) only)*
  - *Configuration: View the audit log*
  - *Configuration: Upload files*
- The *User* column lists which users have access to a certain policy.
- *Edit:* Select a policy and then click **Edit** to define which users have access to the policy. The **Add Users to ACL** dialog appears:



Browse Users

- *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
- *Refresh:* Click to poll the Domain controller to retrieve the list of users.

Note Large Domains with hundreds of users may take several minutes to load.

- *Name/Description:* Displays the name and description for each defined user. Both the name and the description are taken from the operating system security settings (local or Domain).
- *Add:* Click to add the selected user to the *Selected Users* table.

Add User

Note If the Capture Engine is not a member of any Domain, you can ignore *Add User*.

- *Domain:* Type the Domain for the Capture Engine.
- *User:* Type the name of the User you wish to add to the *Selected Users* table.
- *Add:* Click to add the selected user to the *Selected Users* table.

Selected Users

- *Name/Description:* Displays the name and description of users allowed to perform the selected policy.
- *Delete:* Click to remove the selected user from the *Selected Users* table.
- *Delete all:* Click to remove all users from the *Selected Users* table.

Tip A *Policy* that has no users associated with it is effectively reserved for users with Administrator or root level privileges.

Considerations when configuring Access Control

Please note the following when configuring Access Control:

- Users with Administrator or root level privileges always have access to all features of the Capture Engine.

- If the Capture Engine is installed on a machine under local control, the local user with Administrator or root level privileges (and equivalents) has access to the Capture Engine regardless of the settings in the **Edit Access Control** view.
- If the Capture Engine is installed on a machine under Domain control, the Domain Administrator always has access regardless of the settings in the **Edit Access Control** view.
- When *Use access control* is selected and no other users are added to the **Edit Access Control** view (the initial default settings), then only the user with Administrator (local or Domain, depending on the computer setup) or root level privileges has access to the Capture Engine.

Considerations when disabling Access Control

When access control is disabled, the only restrictions on the use of the Capture Engine are those imposed by the operating system security settings. Examples of relevant permissions controlled by operating system security settings include:

- **Login privilege:** A user must be able to log in to the machine on which the Capture Engine is running in order to use the program.

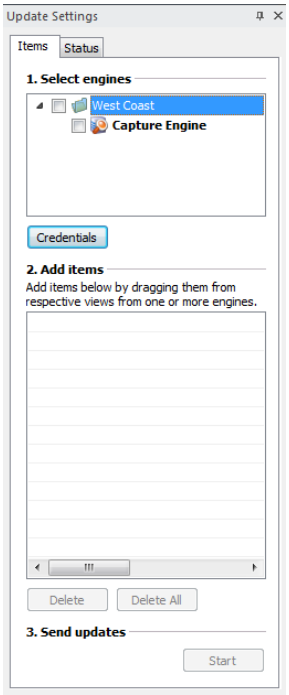
Updating Capture Engine settings

The Capture Engine Manager lets you distribute settings for filters, alarms, and graphs from one or more connected Capture Engines to one or more selected Capture Engines.

Important! You must have Administrator or root level privileges for the Capture Engine where you are distributing settings.

To update settings for one or more Capture Engines:

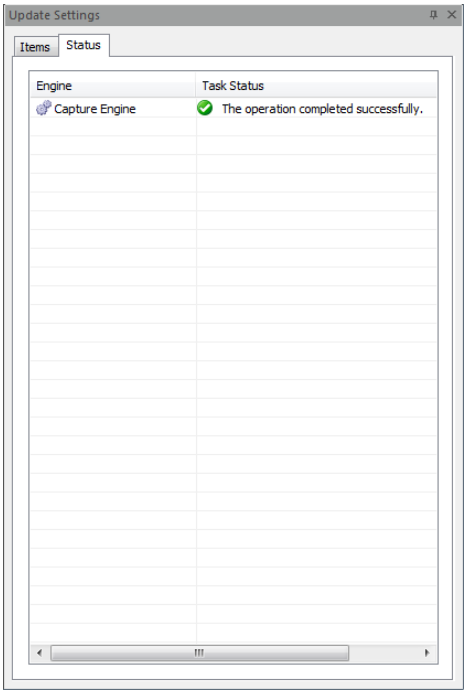
1. Click **Update Settings** in the toolbar. The **Update Settings** dialog appears and lists the Capture Engines defined in the Workspace.



2. Select the check box of the Capture Engines you are updating. You can right-click inside the view to expand all/collapse all lists, or check all /uncheck all Capture Engines.

Note You can click **Credentials** to enter the login credentials that can be used to connect to one or more Capture Engines when distributing software updates or new settings. See 'Credentials dialog' on page 119.

3. Open the Capture Engine window of any connected Capture Engine in the Workspace and select the **Filters**, **Alarms**, or **Graphs** tab.
4. Drag-and-drop an item from the **Filters**, **Alarms**, or **Graphs** tab to the *Add items* section of the **Update Settings** dialog. You can add any combination of filters, alarms, or graphs settings.
5. Click **Start** to send the settings to the selected Capture Engines.
6. Click the **Status** tab to see the current status of all configuration updates for each target Capture Engine.



Note To update the settings for a target Capture Engine that has *Use access control* enabled, you must log in either as a user associated with the *System: Allow usage* policy or as a user with Administrator or root level privileges (local or Domain) for the host machine. If the target Capture Engine does not have *Use access control* enabled, any user with read/write privileges to the Data folder directory of the target Capture Engine can use the **Update Settings** dialog.

Updating Capture Engine ACL settings

The Access Control List (ACL) limits access to a Capture Engine by associating *Users* (defined in the operating system) with classes of tasks on the Capture Engine, called *Policies*. These associations are set in the configuration of each Capture Engine.

The Capture Engine Manager also lets you add the same Domain username and Policy associations to the ACLs of multiple Capture Engines, all of which are operating under the same Domain control.

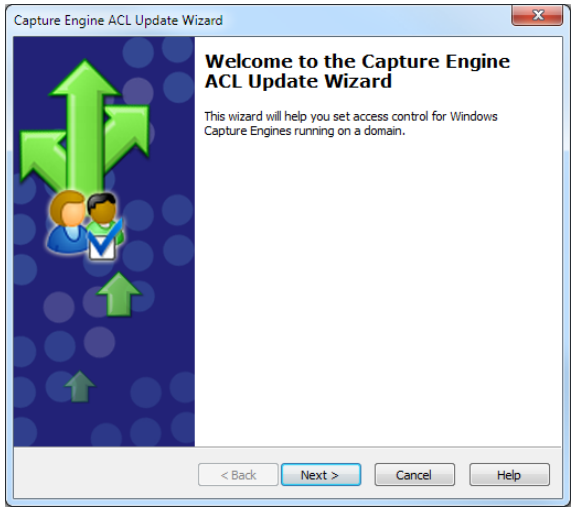
Note To use the ACL with Omnipliance Linux, you must first add the user to the Linux OS and then add the same user to the first ACL policy, "System: Allow usage." You can then limit that user's permission by adding the user to any of the other ACL policies.

Important! The Capture Engine Manager must be able to log in to each target Capture Engine as a user with the correct permissions to update the ACL on that Capture Engine, as described above. For detailed login information, see 'Credentials dialog' on page 119.

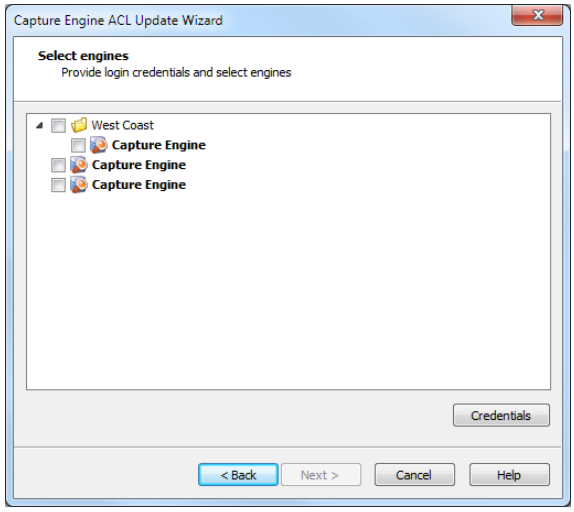
Note To use the **Capture Engine ACL Update Wizard**, you must present the correct login credentials for each target machine. For a Capture Engine with *Use access control* enabled, any user associated with both the *System: Allow usage* and *Configuration: Configure engine settings* policies can configure the Capture Engine. Any user with Administrator privileges (local or Domain) on the target machine can configure the Capture Engine, regardless of any settings in its ACL.

To distribute an ACL update to one or more Capture Engines in a single domain:

1. Click **Update ACL** in the toolbar. The **Capture Engine ACL Update Wizard** appears.



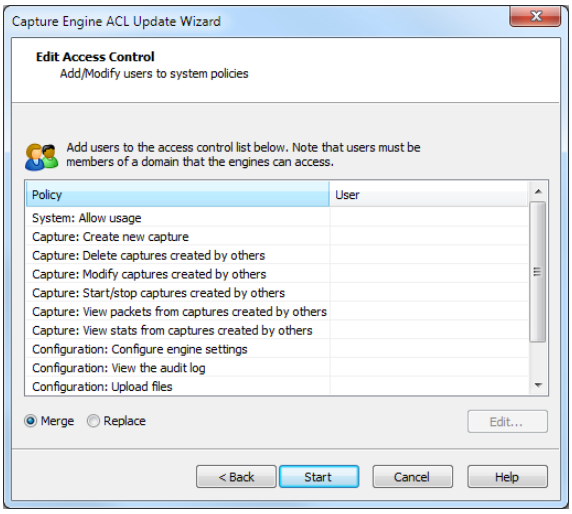
2. Click **Next**. The **Select engines** view appears and lists the Capture Engines defined in the Workspace.



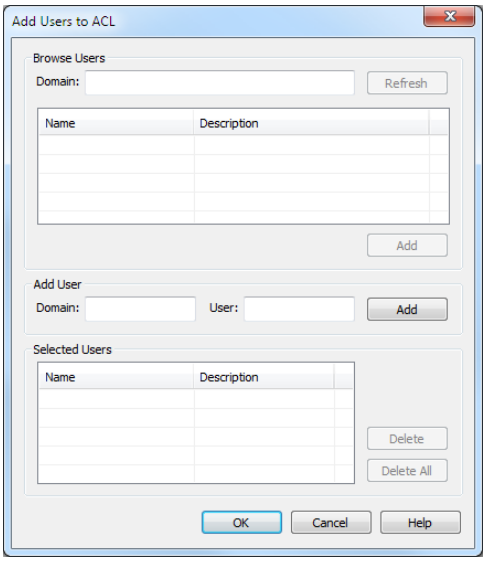
3. Select the check box of the Capture Engines you are updating. You can right-click inside the view to expand all / collapse all lists, or check all / uncheck all Capture Engines.

Note You can click **Credentials** to enter the login credentials that can be used to connect to one or more Capture Engines when distributing software updates or new settings. See 'Credentials dialog' on page 119.

4. Click **Next** to open the **Edit Access Control** view. From this view, you can associate any *User* defined for the current Domain with any *Policy* defined for the selected Capture Engines.



5. Select a *Policy* in the list and click **Edit**. The **Add Users to ACL** dialog appears.



Browse Users

- *Domain* (Capture Engine (Windows) only)*:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
- *Refresh:* Click to poll the Domain controller to retrieve the list of users.

Note Large Domains with hundreds of users may take several minutes to load.

- *Name/Description:* Displays the name and description for each defined user. Both the name and the description are taken from the operating system security settings (local or Domain).
- *Add:* Click to add the selected user to the *Selected Users* table.

Add User (Capture Engine (Windows) only)

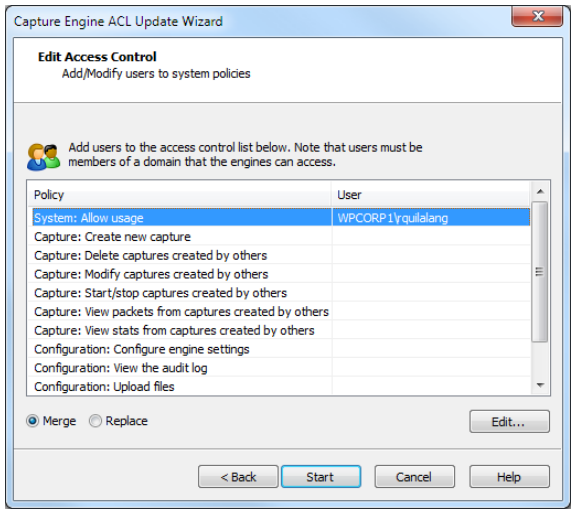
- *Domain:* Type the Domain for the Capture Engine.
- *User:* Type the name of the User you wish to add to the *Selected Users* table.
- *Add:* Click to add the selected user to the *Selected Users* table.

Selected Users

- *Name/Description:* Displays the name and description of users allowed to perform the selected policy.
- *Delete:* Click to remove the selected user from the *Selected Users* table.
- *Delete all:* Click to remove all users from the *Selected Users* table.

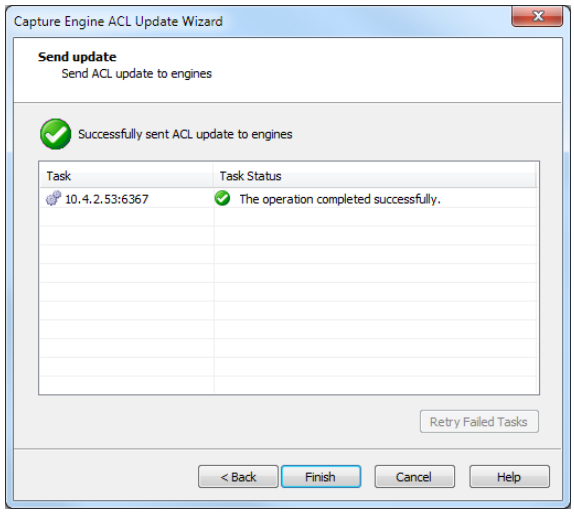
Tip A *Policy* that has no users associated with it is effectively reserved for users with Administrator or root level privileges.

6. Enter the name of the *Domain* and click **Refresh**. The dialog will poll the Domain controller to retrieve a list of users.
7. Select a user you want to associate with the current Policy and click **Add**. The user will appear in the *Selected Users* table of the dialog. Repeat this step until you have added all the users you wish to associate with the current Policy.
8. Click **OK** to close the dialog and return to the **Edit Access Control** view. The users from the *Selected Users* table appear in the *Users* column beside the appropriate *Policy*. You can choose to *Merge* users to the existing Access Control List, or *Replace* the existing Access Control List with a new list defined here.



9. Continue in this manner until you have fully defined the ACL.
10. Click **Start** to begin distributing the ACL to the listed Capture Engines. The **Send update** dialog appears and displays the task status.

Tip If at least one task fails, you can click **Retry Failed Tasks** to send the update again to the Capture Engines that did not complete the task successfully.



Note In order to be able to retrieve the list of Domain users, you must be logged on as a user with Administrator privileges (local or Domain). Additionally, you must have logged on to a computer under the Domain control of the target Domain during the current session of Windows. Your Domain login can have been as a Domain user of any kind, Administrator or otherwise.

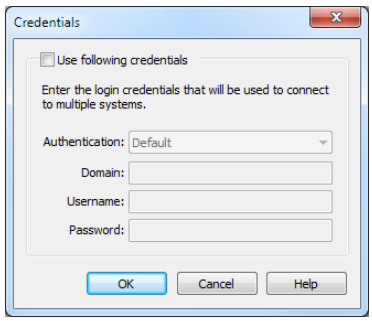
11. Click **Finish** to close the **Capture Engine Update ACL Wizard**.

Credentials dialog

The **Credentials** dialog lets you present a single set of credentials when you distribute software updates, setting updates, or ACL updates to Capture Engines.

To open the Credentials dialog:

1. Click **Credentials...** in any of the following views:
   - the **Items** tab of the **Update Settings** dialog (see 'Updating Capture Engine settings' on page 114).
   - the **Select engines** view of the **Capture Engine Update ACL Wizard** (see 'Updating Capture Engine ACL settings' on page 115).



2. Select the *Use following credentials* check box to enable credentials.
3. Complete credential information for *Authentication*, *Domain*, *Username*, and *Password*. See 'Connecting to a Capture Engine' on page 105 for details.
4. Click **OK** to accept your changes.

Using Capture Engines with Omnipeek

Capture Engines have no user interface of their own and rely on an Omnipeek console to provide a user interface through the **Capture Engines** window. The **Capture Engines** window in Omnipeek is used for interaction between Omnipeek and a Capture Engine.

Connecting to a Capture Engine from Omnipeek

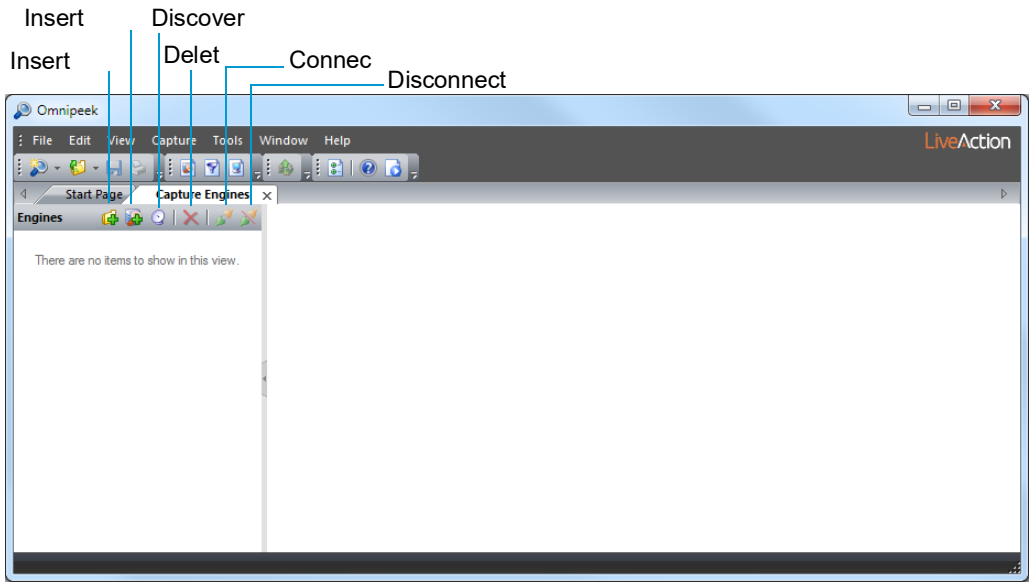
In order to view packets and data from a Capture Engine, you must first connect to the Capture Engine from the **Capture Engines** window.

To connect to a Capture Engine from Omnipeek:

1. Do one of the following to display the **Capture Engines** window:
   - Choose **View** > **Capture Engines**.
   - Click **View Capture Engines** on the Start Page.

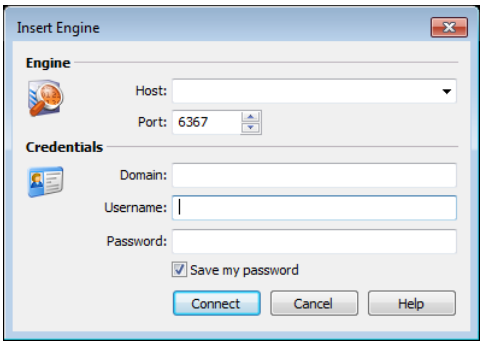
   The **Capture Engines** window appears and displays the list of currently defined Capture Engines.

> **Note** Both Omnipeek and Capture Engine Manager maintain the same list of Capture Engines. Making a change in either program automatically updates the list in the other program.

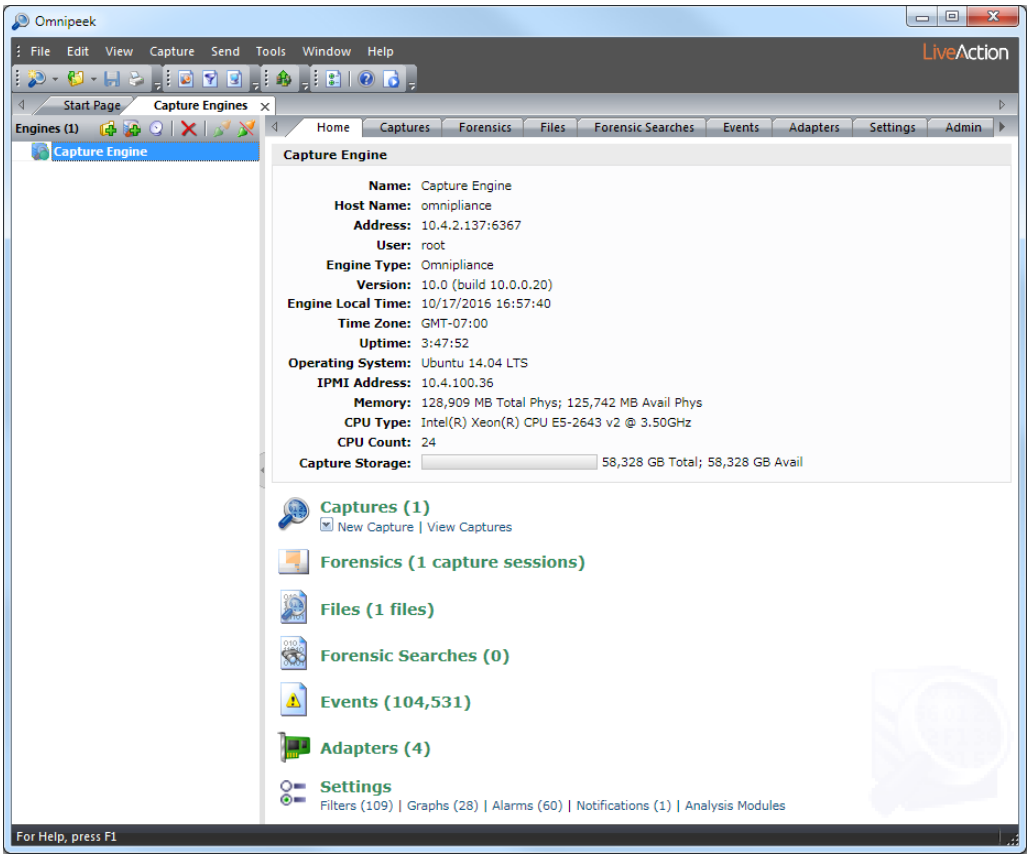


2. Click **Insert Engine**. The **Insert Engine** dialog appears.

> **Note** You can also click **Discover Engine** in the toolbar to find all of the Capture Engines available on your network segment. See 'Discover Capture Engines' on page 108 for details.

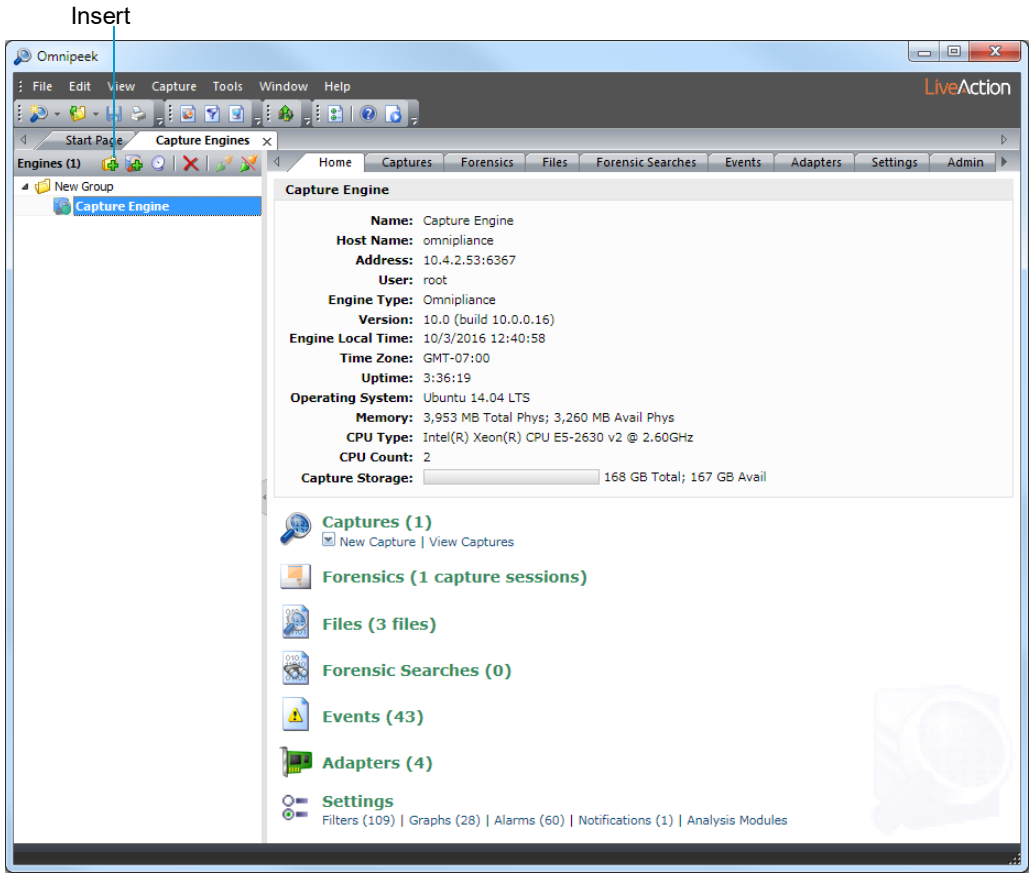


3. Complete the dialog:
   - *Host:* Enter the IP address of the Capture Engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Type the Domain for the Capture Engine. If the Capture Engine is not a member of any Domain, leave this field blank.
   - *Username:* Type the Username for login to the Capture Engine.
   - *Password:* Type the Password for login to the Capture Engine.
4. Click **Connect**. When the connection is established, the Capture Engine appears in the **Capture Engines** window.



Tip You can add multiple Capture Engines to the **Capture Engines** window by clicking **Insert Engine**.

5. Click **Insert Group** to add a group of Capture Engines to the **Capture Engines** window.
6. Select the Capture Engine group and then click **Insert Engine** to add an Capture Engine to the group.



Capturing from a Capture Engine

You can select from the following options to capture packets from a Capture Engine:

- *New Capture...*: This option lets you create a new capture window based on the capture settings that you define.
- *New "Forensics Capture"*: This option lets you create a new capture window based on pre-configured capture settings optimized for post-capture forensics analysis.
- *New "Monitoring Capture"*: This option lets you create a new capture window based on pre-configured capture settings optimized to produce higher level expert and statistical data in a continuous capture.
- *Edit Capture Templates*: This option opens the **Capture Templates** dialog and allows you to create new or edit existing capture templates.

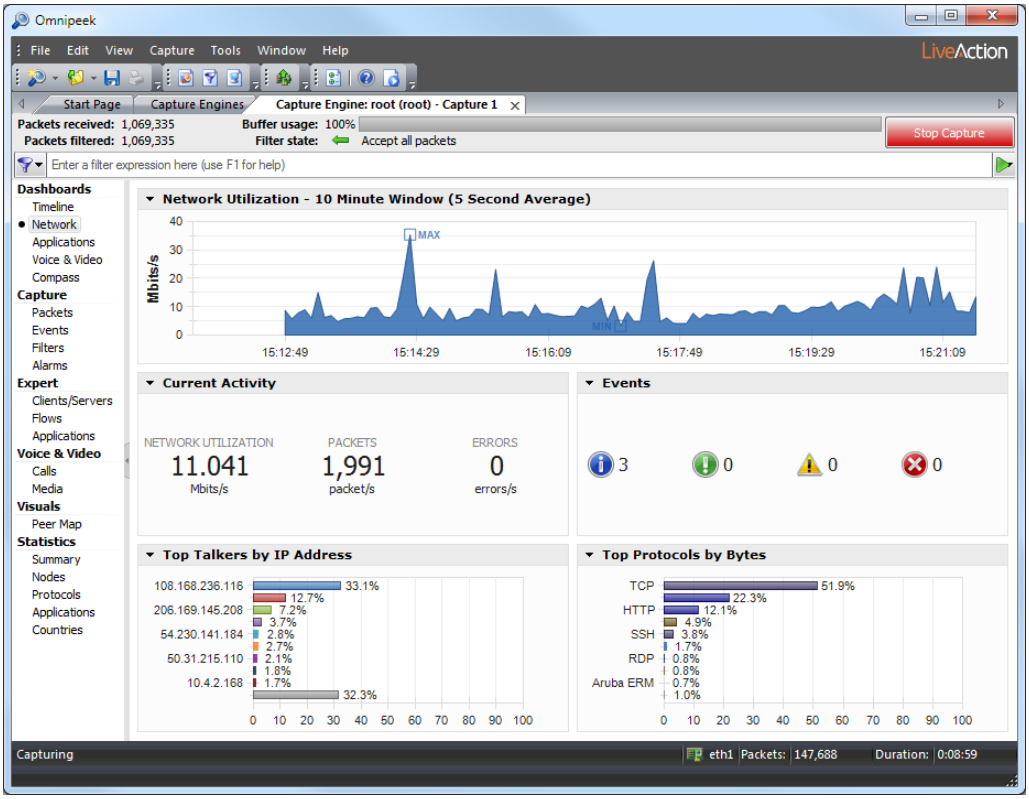
> **Note** For more information about each of the optimized capture formats, please see the *Omnipeek User Guide* or online help.

To begin a remote capture from a Capture Engine:

1. Do one of the following:
   - On the **Home** tab, select the type of remote capture to perform by selecting *New Capture* under the *Captures* heading.
   - On the **Captures** tab, select the type of remote capture to perform by clicking the small arrow next to **Insert**.
   - On the **Adapters** tab, select the type of remote capture to perform by selecting *New Capture* under the name of the adapter you wish to use.

   The remote **Capture Options** dialog appears.

2. Make any desired changes to the capture option settings.
3. Click **OK**. A Capture Engine capture window appears.



Note The views in the left-hand navigation pane that are available in a Capture Engine capture window depend on the type of Capture Engine that is connected, and the *Analysis Options* capture settings configured for that capture window. See the *Omnipeek User Guide* or online help for details on using the features available from Capture Engine capture windows.

4. Click **Start Capture** to begin capturing packets. **Start Capture** changes to **Stop Capture.**
5. Click **Stop Capture** when you want to stop collecting packets into the remote capture buffer.

Third-party authentication with Capture Engines

Third-party authentication of Capture Engines allows administrators of Capture Engines to easily manage logon credentials (after a set of Capture Engines have been deployed), without having to make changes on every Capture Engine individually.

Administrators and users can also sign on to Capture Engines with one set of credentials without requiring the same account on every Capture Engine computer. You can use Active Directory, RADIUS, and TACACS+ authentication to maintain logon credentials.

To use third-party authentication, you must first set up third-party authentication on the Capture Engine (using Capture Engine Manager from the Omnipeek computer), and then log in to the Capture Engine from Omnipeek.

Setting up third-party authentication on the Capture Engine:

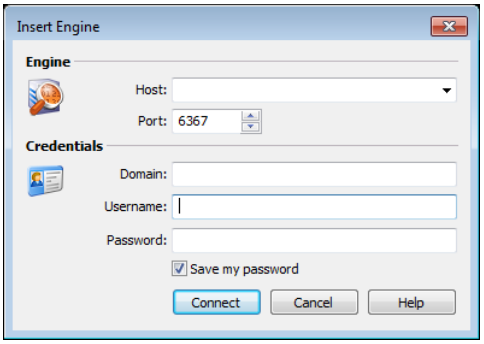
1. Start the Capture Engine Manager from Omnipeek, connect to the Capture Engine, and then add the Capture Engine to the Workspace. See 'Using the Capture Engine Manager' on page 103.
2. Click *Configuration* to run the **Capture Engine Configuration Wizard**.

3. When the **Capture Engine Configuration Wizard** appears, click **Next** twice. The **Security** view of the wizard appears.

   The **Security** view of the **Capture Engine Configuration Wizard** allows you to configure the third-party authentication settings that allow the Capture Engine to communicate with, and authenticate to, the authentication servers. See 'Engine Configuration—Security' on page 110.

Logging in to the Capture Engine from the Omnipeek computer:

1. From Omnipeek, click **Insert Engine** in the **Capture Engines** window. The **Insert Engine** dialog appears.



2. Complete the dialog:
   - *Host:* Enter the IP address of the Capture Engine that you want to connect to.
   - *Port:* Enter the TCP/IP Port used for communications. The default port is 6367.
   - *Domain:* Leave this field blank. This field is not used for Capture Engine (Linux).
   - *Username:* Type the Username for login to the Capture Engine using the specified credentials.
   - *Password:* Type the Password for login to the Capture Engine using the specified credentials.
3. Click **Connect.** The Omnipeek console sends the credentials to the Capture Engine over an encrypted channel.

   The Capture Engine decrypts the credentials, and then sends a request to the specific authentication server:
   - A negative response will prompt the Capture Engine to send an error message back to the console (**Access Denied**).
   - An affirmative response allows the user to log on.

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 126)
- 10G capture adapter—Two or four port 10 Gigabit adapter (see '10G capture adapter' on page 127)
- 40G capture adapter—Two port 40 Gigabit adapter (see '40G capture adapter' on page 129)
- 100G capture adapter—Two port 100 Gigabit adapter (see '100G capture adapter' on page 130)

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*.

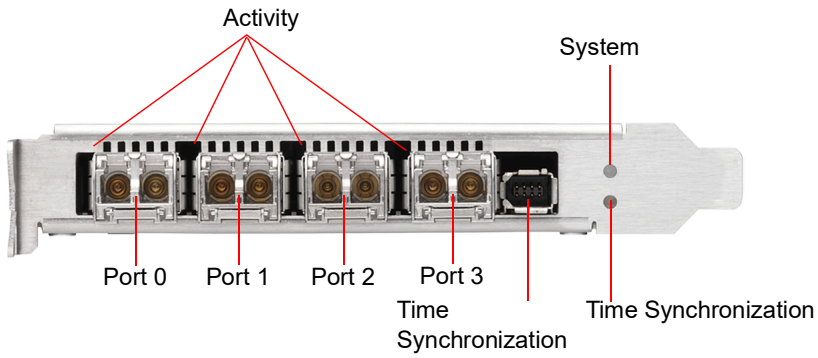
1G capture adapter

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:

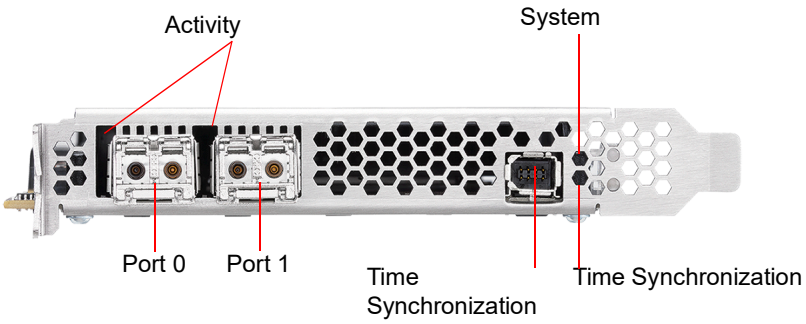
- Two or four 850nm MMF SFP+ optical transceivers with LC connectors
- Two or four 1310nm SMF SFP+ optical transceivers with LC connectors

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
```

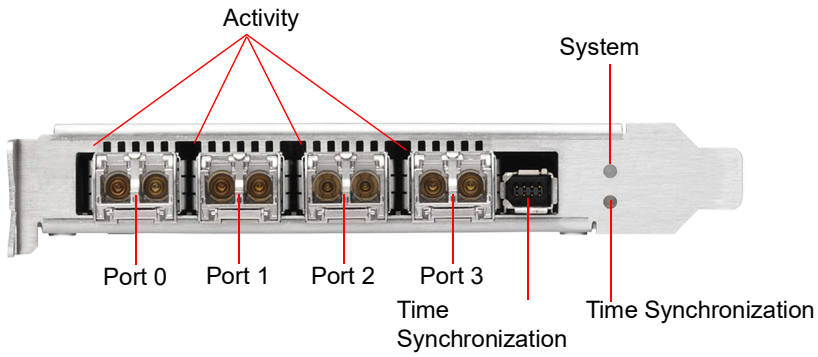
10G capture adapter (2-port) I/O bracket

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.

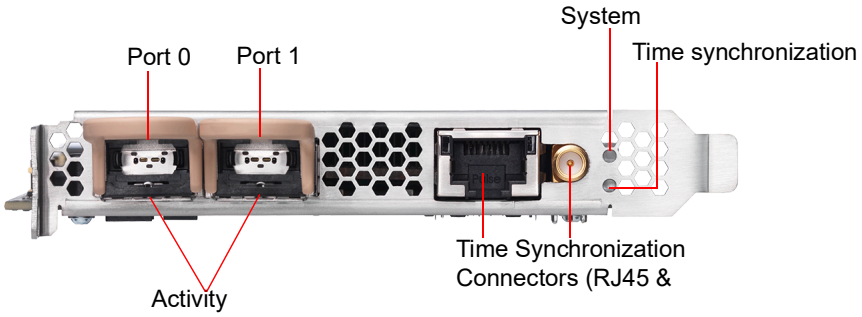
LED	State and Color	Condition
	Flashing green synchronous with the PPS or NT-TS pulse	The Ethernet link on the PTP port is down and the following condition is fulfilled: When the SMA port of the external time synchronization connector is configured as a: • PPS or NT-TS input connector: A driver is loaded, 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 time-stamping. The 40G Adapter is available with two QSFP+ interfaces.

40G capture adapter I/O bracket

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



LED status

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

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

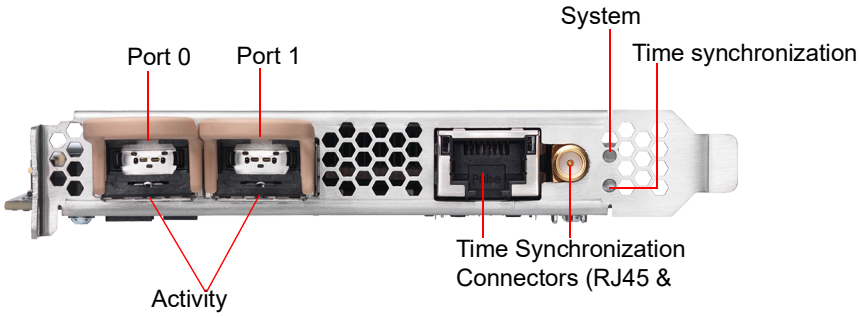
100G capture adapter

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 time-stamping. The 100G capture adapter is available with two QSFP28 interfaces.

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

100G capture adapter I/O bracket

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



LED status

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

LED	State and Color	Condition
System LED	Off	The power is off.
	Constant red	During start-up: Power is on. The adapter is checking the power supplies.

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 133.

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 time-stamps from being reported, ensure that the Capture Engine's clock is synchronized with the PTP or NTP server (if NTP's time source is pointed at the PTP grandmaster clock).

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

- Enable 'TimeSyncOsTimeReference' in */etc/omni/ntoverrides.ini*—This option synchronizes the OS time to a Napatech adapter clock, which in turn should be configured to point to the PTP grandmaster clock as its time reference
- If NTP server references PTP as its time source, run '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 131.

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.

Hardware Specifications

In this appendix:

LiveWire technical specifications

LiveWire Edge

Specification	Description
Processor	Intel® Atom® C3758
Base Frequency Cores	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	AMD® 1x7313
Base Frequency Cores Thread	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	240 TB SAS storage, RAID 0 or optional RAID 6 **NOTE**: Optional external storage with LiveWire TeraVault — Up to 960 TB 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:	IIEEE 802.3 10 Gbps Ethernet LAN
Physical interface:	4x SFP or SFP+ ports
Supported SFP modules:	Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T
Supported SFP+ modules:	Multi-mode SR, single-mode LR and ER, 10GBASE-CR
Supported dual-rate modules:	Multi-mode SR and single-mode LR
Environment	
Power consumption:	27 Watts including SFP+ SR modules
Operating temperature:	32° F to 113° F (0° C to 45° C)
Operating humidity:	20% to 80%
Regulatory approvals and compliances	PCI-SIG® CE CB RoHS REACH cURus (UL) FCC CSA VCCI C-TICK

40G capture adapter specifications

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

100G capture adapter specifications

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