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


Support Contact Information: https://www.liveaction.com/support/technical-support/
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.
Starting / Shutting down LiveCapture .................................................. 48

Chapter 3  
**Capture Engines** ................................................................. 49
About Capture Engine ............................................................... 50
Using the Capture Engine Manager ............................................. 50
  Navigating the Capture Engine Manager window ..................... 50
  Creating new engine groups ................................................... 52
  Connecting to a Capture Engine .............................................. 52
  Capture Engine details windows ............................................. 54
  Discover Capture Engines ...................................................... 55
  Reconnect button .................................................................. 55
  Configuring a Capture Engine ................................................ 56
    Engine Configuration—General .............................................. 56
    Engine Configuration—Security ............................................ 57
    Engine Configuration—Edit Access Control ........................... 59
  Updating Capture Engine settings ......................................... 61
  Updating Capture Engine ACL settings ................................... 62
    Credentials dialog ................................................................ 66
  Using Capture Engines with Omnipeek .................................. 67
    Connecting to a Capture Engine from Omnipeek ................... 67
    Capturing from a Capture Engine ....................................... 69
  Third-party authentication with Capture Engines .................... 70

Chapter 4  
**Capture Adapters for LiveCapture** ......................................... 72
About capture adapters ............................................................ 73
1G capture adapter ................................................................. 73
  1G capture adapter I/O bracket ............................................. 73
  LED status ............................................................................ 73
10G capture adapter ............................................................... 74
  10G capture adapter (2-port) I/O bracket ............................... 74
  10G capture adapter (4-port) I/O bracket ............................... 75
  LED status ............................................................................ 75
40G capture adapter ............................................................... 76
  40G capture adapter I/O bracket ............................................. 76
  LED status ............................................................................ 76
100G capture adapter ............................................................. 77
  100G capture adapter I/O bracket ........................................... 77
  LED status ............................................................................ 77
  Enabling PTP support for capture adapters ......................... 78
    Configuration parameters ............................................... 79
    Synchronizing the capture engine clock ............................. 80
  Connecting the external time synchronization adapter ........... 81
  Troubleshooting the capture adapters .................................. 81
  Verifying link status ............................................................. 81

Appendix A  
**Hardware Specifications** ....................................................... 83
LiveCapture technical specifications ........................................ 84
  LiveCapture 1100 ................................................................. 84
  LiveCapture 3100 ................................................................. 85
Capture adapter technical specifications ................................... 86
  1G capture adapter specifications ........................................ 86
  10G capture adapter (2-port) specifications ......................... 86
  10G capture adapter (4-port) specifications ......................... 87
  40G capture adapter specifications ..................................... 87
  100G capture adapter specifications .................................... 88
Introduction

In this chapter:

About LiveCapture ................................................................. 2
What’s included ................................................................. 3
Front / rear panels ............................................................. 4
Inside the appliance .......................................................... 7
Installing LiveCapture ......................................................... 10
Connecting Extended Storage to LiveCapture 3100 .................. 11
LiveCapture Activation ....................................................... 12
Starting / shutting down LiveCapture .................................... 20
Contacting LiveAction support .......................................... 20
About LiveCapture

Congratulations on your purchase of LiveCapture™! LiveCapture appliances are designed and optimized for raw packet capture and analysis, without dropping a packet. Packets are captured and stored at up to 40 Gbps (LiveCapture 3100 with external storage attached) in standard packet file formats for easy access to the packet data. Stored packet files can be indexed with a variety of characteristics to make retrieval of relevant packets significantly faster. LiveCapture works together with Omnipeek (Windows software), LiveAction’s award-winning network analysis software.

With Omnipeek, users can initiate forensic searches for packet data on the LiveCapture appliance. The packets meeting the search criteria are analyzed on the appliance using the built-in analytical software, and the results are visualized and further analyzed using Omnipeek. Packet files can also be downloaded and stored for off-line analysis by Omnipeek. LiveCapture is widely used in enterprises alongside network monitoring solutions to provide the most complete data required for true root-cause analysis – the packets themselves.

LiveCapture is available in the following configurations:

<table>
<thead>
<tr>
<th></th>
<th>LiveCapture 1100</th>
<th>LiveCapture 3100</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chassis</strong></td>
<td>1U</td>
<td>2U</td>
</tr>
<tr>
<td><strong>Processor</strong></td>
<td>1 x Intel® Xeon® Bronze 3106</td>
<td>2 x Intel® Xeon® Gold 6126</td>
</tr>
<tr>
<td><strong>Base Frequency</strong></td>
<td>1.70 GHz</td>
<td>2.6 GHz</td>
</tr>
<tr>
<td><strong>Max Turbo Frequency</strong></td>
<td></td>
<td>3.7 GHz</td>
</tr>
<tr>
<td><strong>Cores</strong></td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td><strong>Thread</strong></td>
<td>8</td>
<td>24</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td>32 GB</td>
<td>192 GB</td>
</tr>
<tr>
<td><strong>Expansion Slots</strong></td>
<td>1 x 16 FH/HL</td>
<td>64 TB / 128 TB Configuration: 1 x 16 FH/FL 2 x 8 FH/FL 1 x 8 FH/HL 96 TB Configuration: 1 x 8 FH/FL 1 x 8 FH/HL 3 x 16 FH/FL 1 x 16 LP/HL</td>
</tr>
<tr>
<td><strong>NOTE:</strong> A total of one capture adapter can be added to the LiveCapture 1100.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integrated Network Interfaces</strong></td>
<td>4 x 1GBASE-T IDRAC</td>
<td>4 x 1GBASE-T IDRAC</td>
</tr>
<tr>
<td><strong>Storage-OS</strong></td>
<td>Included as part of Storage-Data</td>
<td>2 x 2 TB NLSAS (4 TB) or 2 x 1.8 TB SAS (3.6 TB)</td>
</tr>
<tr>
<td><strong>Storage-Data</strong></td>
<td>4 x 4 TB NLSAS (16 TB)</td>
<td>16 x 8 TB NLSAS (128 TB) or 16 x 4 TB NLSAS (64 TB) or 12 x 8 TB NLSAS (96 TB)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> A total of three capture adapters can be added to the LiveCapture 3100.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Capture Adapter Options**

<table>
<thead>
<tr>
<th>LiveCapture 1100</th>
<th>LiveCapture 3100</th>
</tr>
</thead>
<tbody>
<tr>
<td>1G Capture Adapter (4-port)</td>
<td>1G Capture Adapter (4-port)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> A total of one capture adapter can be added to the LiveCapture 1100.</td>
<td>10G Capture Adapter (2- or 4-port)</td>
</tr>
<tr>
<td></td>
<td>40G Capture Adapter (2-port)</td>
</tr>
<tr>
<td></td>
<td>100G Capture Adapter (2-port)</td>
</tr>
<tr>
<td><strong>NOTE:</strong> A total of three capture adapters can be added to the LiveCapture 3100.</td>
<td></td>
</tr>
</tbody>
</table>

**Additional**

<table>
<thead>
<tr>
<th>LiveCapture 1100</th>
<th>LiveCapture 3100</th>
</tr>
</thead>
<tbody>
<tr>
<td>PERC H840 Adapter (used only for storage subsystem)</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

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

The Capture Engine software pre-installed on LiveCapture works in conjunction with Omnipeek, a separate software program required for the monitoring and analysis of the packets captured remotely by LiveCapture. For detailed instructions on how to view and analyze remote captures from within the Omnipeek console, please see the Omnipeek User Guide or Omnipeek online help. For more information on the Capture Engine software, please see Chapter 3, Capture Engines.

**What’s included**

Your standard LiveCapture package includes:

- LiveCapture packet capture and analysis appliance
- Capture Engine software pre-installed in LiveCapture
- Two power cords
- Rack-mount rails
- Chassis bezel
Front / rear panels

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

LiveCapture 1100 front panel

1. Left control panel
   - Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless) LED.
2. Hard drive #0
   - 3.5 inch hot-swappable hard drive/SSD.
3. Optical drive
   - One optional slim SATA DVD-ROM drive or DVD+/−RW drive.
4. Hard drive #1
   - 3.5 inch hot-swappable hard drive/SSD.
5. Hard drive #2
   - 3.5 inch hot-swappable hard drive/SSD.
6. VGA port
   - Enables you to connect a display device to the system.
7. Hard drive #3
   - 3.5 inch hot-swappable hard drive/SSD.
8. USB port
   - The USB port is USB 2.0 compliant.
9. Right control panel
   - Contains the power button, USB port, iDRAC Direct micro USB port, and the iDRAC Direct status LED.
10. 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.

LiveCapture 1100 back panel
### LiveCapture 3100 Front Panel

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Serial port</td>
</tr>
<tr>
<td>2</td>
<td>iDRAC Enterprise port</td>
</tr>
<tr>
<td>3</td>
<td>Ethernet ports (2) (The port labeled 'Gb 1' is the eth0 management port)</td>
</tr>
<tr>
<td>4</td>
<td>Full height riser slot</td>
</tr>
<tr>
<td>5</td>
<td>Power supply unit (2) AC 550 W. Both power supplies should be plugged in to power to provide redundancy.</td>
</tr>
<tr>
<td>6</td>
<td>Ethernet ports (2)</td>
</tr>
<tr>
<td>7</td>
<td>USB 3.0 port (2) Use the USB 3.0 port to connect USB devices to the system. These ports are 4-pin, USB 3.0-compliant.</td>
</tr>
<tr>
<td>8</td>
<td>VGA port</td>
</tr>
<tr>
<td>9</td>
<td>CMA power port</td>
</tr>
<tr>
<td>10</td>
<td>System identification button The System Identification (ID) button is available on the front and back of the systems. 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.</td>
</tr>
</tbody>
</table>

### LiveCapture 3100 Front Panel

![LiveCapture 3100 Front Panel Diagram](image)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Left control panel Contains system health and system ID, status LED, and iDRAC Quick Sync 2 (wireless) LED.</td>
</tr>
<tr>
<td>2</td>
<td>Hard drive # 0 3.5 inch hot-swappable hard drive</td>
</tr>
<tr>
<td>3</td>
<td>Hard drive # 1 3.5 inch hot-swappable hard drive</td>
</tr>
<tr>
<td>4</td>
<td>Hard drive # 2 3.5 inch hot-swappable hard drive</td>
</tr>
<tr>
<td>5</td>
<td>Hard drive # 3 3.5 inch hot-swappable hard drive</td>
</tr>
<tr>
<td>6</td>
<td>Hard drive # 4 3.5 inch hot-swappable hard drive</td>
</tr>
<tr>
<td>Item</td>
<td>Indicator, Button, or Connector</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
</tr>
</tbody>
</table>
| 1    | Full-height PCIe expansion card slot (3) | The PCIe expansion card slot (riser 1) connects up to three full-height PCIe expansion cards to the system.  
**Note:** Depending on your configuration, the capture adapters are installed here. |
| 2    | Half-height PCIe expansion card slot | The PCIe expansion card slot (riser 2) connects one half-height PCIe expansion cards to the system.  
**Note:** On the LiveCapture 3100, the RAID controller is installed here. 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. |
<p>| 3    | Rear handle | The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6. |
| 4    | Drive # 12 | 3.5 inch hot-swappable hard drive. This drive is the system HDD (RAID 1) |
| 5    | Drive # 13 | 3.5 inch hot-swappable hard drive. This drive is the system HDD (RAID 1). |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Indicator, Button, or Connector</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Power supply unit (2)</td>
<td>AC 1100 W. Both power supplies should be plugged into power to provide redundancy.</td>
</tr>
<tr>
<td>7</td>
<td>NIC ports</td>
<td>The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. From left to right, the ports are configured as eth0, eth1, eth2, and eth3.</td>
</tr>
<tr>
<td>8</td>
<td>USB port (2)</td>
<td>The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.</td>
</tr>
<tr>
<td>9</td>
<td>VGA port</td>
<td>Enables you to connect a display device to the system.</td>
</tr>
<tr>
<td>10</td>
<td>Serial port</td>
<td>Enables you to connect a serial device to the system. Typically used for console access, and also optional access to hardware.</td>
</tr>
<tr>
<td>11</td>
<td>iDRAC dedicated port</td>
<td>Enables you to remotely access iDRAC. iDRAC is very useful for remote management and direct access of the appliance.</td>
</tr>
<tr>
<td>12</td>
<td>System identification button</td>
<td>The System Identification (ID) button is available on the front and back of the systems. 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.</td>
</tr>
</tbody>
</table>

**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.

**LiveCapture 1100 internal components**
Note  The graphic above shows a configuration of ten internal drives installed in the front drive cage of the appliance; however, only a four drive configuration installed in the front drive cage is available with LiveCapture 1100.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Left control panel cable cover</td>
</tr>
<tr>
<td>2</td>
<td>Hard drive backplane</td>
</tr>
<tr>
<td>3</td>
<td>Backplane expander board</td>
</tr>
<tr>
<td>4</td>
<td>Cabling latch</td>
</tr>
<tr>
<td>5</td>
<td>Air shroud</td>
</tr>
<tr>
<td>6</td>
<td>Intrusion switch</td>
</tr>
<tr>
<td>7</td>
<td>Power interposer board</td>
</tr>
<tr>
<td>8</td>
<td>Internal expansion riser</td>
</tr>
<tr>
<td>9</td>
<td>Low profile expansion riser 1</td>
</tr>
<tr>
<td>10</td>
<td>Low profile expansion riser 2</td>
</tr>
<tr>
<td>11</td>
<td>Processor blank</td>
</tr>
<tr>
<td>12</td>
<td>Heat sink</td>
</tr>
<tr>
<td>13</td>
<td>Air shroud</td>
</tr>
<tr>
<td>14</td>
<td>Cooling fan blank</td>
</tr>
<tr>
<td>15</td>
<td>Left control panel cable cover</td>
</tr>
<tr>
<td>16</td>
<td>Information tag</td>
</tr>
</tbody>
</table>

Note  A defective drive should have a consistent RED blinking LED which should make it easier to detect.
### LiveCapture 3100 internal components

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hard drives numbered 0–11 in the front drive cage (see also <em>LiveCapture 3100 front panel</em> on page 5)</td>
</tr>
<tr>
<td>2</td>
<td>Drive backplane</td>
</tr>
<tr>
<td>3</td>
<td>Backplane expander card</td>
</tr>
<tr>
<td>4</td>
<td>Cooling fan (6) in the cooling fan assembly</td>
</tr>
<tr>
<td>5</td>
<td>Hard drive # 14</td>
</tr>
<tr>
<td>6</td>
<td>Hard drive # 15</td>
</tr>
<tr>
<td>7</td>
<td>Hard drive # 16</td>
</tr>
<tr>
<td>8</td>
<td>Hard drive # 17 (Drive not shown)</td>
</tr>
<tr>
<td>9</td>
<td>Mid drive backplane</td>
</tr>
<tr>
<td>10</td>
<td>Rear drive backplane</td>
</tr>
<tr>
<td>11</td>
<td>Hard drive # 13. This drive is the system HDD (RAID 1).</td>
</tr>
<tr>
<td>12</td>
<td>Hard drive # 12. This drive is the system HDD (RAID 1).</td>
</tr>
<tr>
<td>13</td>
<td>System board</td>
</tr>
<tr>
<td>13</td>
<td>Expansion card riser 1</td>
</tr>
<tr>
<td>15</td>
<td>Integrated storage controller card</td>
</tr>
<tr>
<td>16</td>
<td>NVDIMM-N battery</td>
</tr>
</tbody>
</table>
Installing LiveCapture

To install LiveCapture:
1. Place LiveCapture 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: LiveCapture has two redundant high-efficiency “hot-swappable” power supplies. If a power module fails, it should be replaced immediately. If your LiveCapture 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

LiveCapture includes Gigabit Ethernet ports and Integrated Remote Access Controller (iDRAC) ports used for remotely accessing and troubleshooting LiveCapture. See Front / rear panels on page 4 for the location of these ports. For information on using iDRAC, see Integrated Remote Access Controller (iDRAC) on page 41.

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

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

System fans

LiveCapture 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 LiveCapture is under warranty, please contact LiveAction Technical Support to arrange for a replacement fan.

**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 Extended Storage to LiveCapture 3100

The storage capacity of any LiveCapture 3100 with 128 TB of total hard disk capacity can be increased through the addition of Extended Storage for LiveCapture 3100. Extended Storage is available in a configuration of 96 TB. Up to two Extended Storage units can be added for a total of 320 TB. If you purchased Extended Storage with your LiveCapture 3100, the instructions to connect it to your LiveCapture 3100 are provided below.

**To connect Extended Storage to LiveCapture 3100:**

1. Make sure both Extended Storage and LiveCapture 3100 are powered OFF.
2. Select a suitable location for both Extended Storage and LiveCapture 3100. 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 Extended Storage.

**Note** If you have multiple Extended Storage 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 Extended Storage box is labeled with a number, and every Extended Storage cable is labeled to the exact port it needs to get plugged into.

4. Facing the rear of LiveCapture 3100, insert one connector of the SAS external cascading cable into the left RAID port (RAID 1) of the RAID controller on LiveCapture 3100 so that the release handle is on the top. The connector is keyed and only fits in one way.

**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 Extended Storage, insert the other end of the SAS external cascading cable into the RAID 1 port of the RAID controller on Extended Storage so that the release handle is on the top. The connector is keyed and only fits in one way.
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 Extended Storage by pressing the power button on the front of the chassis. You may see brief bursts of LED activity as the expander in Extended Storage scans the drives.

7. Turn on the power to LiveCapture 3100. The system is ready for use as soon as the LiveCapture 3100 boot sequence completes.

Note
If the LiveCapture 3100 and Extended Storage arrived from the factory as a matched pair, then it is not necessary to re-image the units. If you are connecting a new Extended Storage to an existing LiveCapture 3100 that has already been placed into service, you will need to re-image the LiveCapture 3100 and Extended Storage together as a single unit in order to use Extended Storage. See Reimaging LiveCapture with an ISO image on page 45.

LiveCapture Activation

Once LiveCapture 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 LiveCapture 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 LiveCapture, so please have this information readily available:

• IP address of LiveCapture
• 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 LiveCapture via Omnipeek.
To activate LiveCapture via Omnipeek:

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

   - **Username**: Type the username for LiveCapture. The default is `admin`.
   - **Password**: Type the password for LiveCapture. 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.** LiveCapture is now activated and you can begin using the product. The activation process is complete.
Note: If the automatic activation does not complete successfully, go back and select the manual activation process. Personal firewalls or other network restrictions may block automatic activations.

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

Activate Your LiveAction Product

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

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

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

Product Key or Serial Number:

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

First Name:

Last Name:

Email Address:

Company:

ACTIVATE PRODUCT

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

7. Click DOWNLOAD LICENSE FILE to save the license file to your computer. You will need the license file in the following steps.

8. Return back to the Manual Activation window, and click Choose License File.

9. Navigate to the license file downloaded above and click Open.
10. Click **Next** in the **Manual Activation** window. LiveCapture is now activated and you can begin using the product. The activation process is complete.

### Activation via Omnipeek

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

**To activate LiveCapture 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 LiveCapture.
   - **Port**: Enter the TCP/IP port used for communications. Port 6367 is the default for LiveCapture.
   - **Domain**: Type the Domain for login to LiveCapture. If LiveCapture is not a member of any Domain, leave this field blank.
   - **Username**: Type the username for LiveCapture. The default is **admin**.
   - **Password**: Type the password for LiveCapture. The default is **admin**.
   - **Save my password**: Select this option to remember your password to connect to LiveCapture.
3. Click **Connect** to connect to LiveCapture. If LiveCapture has not yet been activated, the activation message appears in the **Capture Engines** window.

4. Click **Activate** LiveCapture. 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, LiveCapture is now activated and you can begin using the product. The activation process is complete.

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

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

![Manual Activation Dialog](image)

   **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](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**. LiveCapture is now activated and you can begin using the product. The activation process is complete.

**Starting / shutting down LiveCapture**

**To start LiveCapture:**
- Press the power button in the upper right corner on the front of the chassis.

**To shutdown LiveCapture:**
- 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 LiveCapture and use the ‘shutdown’ command from the command prompt (`admin@livecapture`):

  ```
  shutdown -h now
  ```

**Note** You can also use the iDRAC interface to shutdown and start LiveCapture. See *Starting / Shutting down LiveCapture* on page 48.

**Attaching the front bezel**

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

**Contacting LiveAction support**

Please contact LiveAction support at [https://www.liveaction.com/contact-us](https://www.liveaction.com/contact-us) if you have any questions about the installation and use of LiveCapture.

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/](https://www.liveaction.com/support/technical-support/) for instructions.
Configuring LiveCapture

In this chapter:

Logging-in to LiveCapture command line ................................................................. 22
Using the LiveAdmin utility ...................................................................................... 22
Using DMS to manage and configure LiveAction appliances .................................... 34
Configuring network settings by command script ..................................................... 38
Using LiveCapture with Omnipeek ........................................................................ 40
Integrated Remote Access Controller (iDRAC) ......................................................... 41
Logging-in to LiveCapture command line

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

- Remotely, using remote SSH software such as **Putty**
- Locally, by connecting a monitor, mouse and keyboard to LiveCapture
- Locally, via the serial port

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

  username: *admin*
  password: *admin*

After you have logged into LiveCapture 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 LiveCapture 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 24.
- **Authentication**: The Authentication view lets you change the password for LiveCapture. See Authentication on page 25.
- **Monitor**: The Monitor view displays the health of the overall system. See Monitor on page 26.
- **Network**: The Network view lets you configure the primary network interfaces network settings and the hostname of the system. See Network on page 26.
- **Omni**: The Omni view lets you enable the Device Management Server (DMS) for the appliance. See Omni on page 28.
- **Support**: The Support view let you download logs from the system that would be helpful in troubleshooting issues. See Support on page 30.
• **Time:** The *Time* view lets you configure the system’s Timezone and NTP servers. See *Time* on page 31.

• **TLS:** The *TLS* view lets you change the self-signed certificates that LiveAdmin and Omnipeek use for HTTPS. See *TLS* on page 32.

• **Update:** The *Update* view lets you update the appliance using a software update package. See *Update* on page 33.

• **Administrator:** The *Administrator* context menu in the upper right lets you restart LiveCapture, power off LiveCapture or log out from the LiveAdmin utility. See *Restart and power off* on page 34.

**Important!** LiveCapture comes pre-configured to obtain its IP address via DHCP. The IP address is required to configure LiveCapture, 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 34.

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

**Login**

**To log into the LiveAdmin utility:**

1. Connect LiveCapture to your network router or switch with an Ethernet cable.

2. From a browser window on a computer connected to the same network as LiveCapture, enter the IP address for LiveCapture 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 26.
• **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 LiveCapture.

- **Current Password**: Enter the current password for LiveCapture. The default is `admin`.
- **New Password**: Enter the new password for LiveCapture. 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 LiveCapture. 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 specify whether LiveCapture 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 LiveCapture. If **DHCP** is selected, then LiveCapture is configured by a DHCP server.

**Important!**  
LiveCapture is pre-configured to a static IP address. The default is 192.168.1.21. We strongly recommend the use of a static IP address for LiveCapture. 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 LiveCapture. To help you look up the IP address, the MAC Address of LiveCapture is displayed as the **Ethernet Address**.

- **IP Address**: This setting lets you specify the IP address that you are assigning to LiveCapture.

- **Netmask**: A Netmask, combined with the IP address, defines the network associated with LiveCapture.

- **Gateway**: Also known as ‘Default Gateway.’ When LiveCapture 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 LiveCapture 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, 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 LiveCapture, 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 LiveCapture to manage and configure LiveCapture from the cloud. See *Using DMS to manage and configure LiveAction appliances* on page 34.

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

**Factory reset**

*Factory reset* is unavailable from the LiveAdmin utility for LiveCapture appliances.

**Backup**

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

- **Encrypt**: Select this data to encrypt the system backup. You will need to enter a password that is required to restore the backup to LiveCapture.
- **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 LiveCapture a backup that was previously performed on LiveCapture. 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 LiveCapture that would be helpful in troubleshooting issues.
• **Download logs**: Click to download the `logs.tgz` file to your default location.

The `logs.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/omnipref.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 LiveCapture. Select from the list the location closest to your LiveCapture.

• **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 LiveCapture require accurate timestamps to properly analyze data.

To synchronize the LiveCapture 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 LiveCapture, 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 LiveCapture.

**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 LiveCapture.

**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 LiveCapture and log out from the utility.

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

To power off LiveCapture:
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 28.

---

**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](https://mypeek.liveaction.com) and [https://cloudkeys.liveaction.com](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 manage and configure LiveAction appliances:
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.

**Note** When you click the **LIVEWIRE/LIVECAPTURE** tab it defaults to the **Devices** view. You can navigate between the **Devices** and **Templates** views by using the sidebar made visible by clicking the hamburger menu in the top left.

A description of the LiveAction appliance page is provided here:

- **Actions**: Click to perform the options below on the selected appliances.

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

**Upgrade**

• **No Change**: Select to not perform an upgrade on the selected appliances.
• **Disable**: Select to disable the upgrade on the selected appliances.
• **Enable**: Select to enable the upgrade on the selected appliances.
• **Select Date**: When Enabled, you can select a date and time to perform an upgrade of the selected appliances.
• **Apply**: Click to apply the changes to the selected appliances.
• **Template**: Click to select a template to apply to the selected appliances. Templates allow you to apply version-specific settings to one or more appliances.

To create a template: From the sidebar activated by clicking the hamburger menu, navigate to **Templates**, click **Add Template**, select the version number, and complete the **ADD TEMPLATE** dialog.

• **Change Password**: Click to change the password of the selected appliances.
• **Search**: Use the Search field to locate a specific appliance.
• **Device Serial**: Displays the serial number of the appliance.
• **Device Name**: Displays the name of the appliance. See **Settings** in **Edit policy** on page 37 to change the device name.
• **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.
• **Location**: Displays the location of the appliance. See **Settings** in **Edit policy** on page 37 to change the location.
• **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.
• **Date**: Displays the date the appliance was entered into the system.
• **Registered**: Displays whether or not the customer has registered the appliance. A check mark indicates that the device has been registered.
• **Version**: Displays the version number of the software installed on the appliance.
• **Engine Type**: Displays the type of appliance, which can be **LiveWire**, **LiveCapture**, or **LiveWire Virtual**.
• **Shared Users Count**: Displays the number of secondary users that have access to the appliance.
• **Activation Status**: Displays a check mark if the license on the device is valid and not expired.
• **Configuration Status**: Displays any status associated with configuration.
• **Scheduled Action(s)**: Displays any ‘Actions’ scheduled for the appliance.
• **Actions**: Click to access additional actions to perform on the selected appliances.
• **View Policy**: Click to display the current configuration for the appliance.
• **Edit Policy**: Click to change the current policy configuration for the appliance. See *Edit policy*.
• **Manage Users**: Click to manage who has access to the appliance. See *Manage users* on page 38.

3. Select the check box of the appliance(s) you wish to manage and configure, and then click the desired action. Only devices that have a valid license (Activation Status is checked) will be selectable. Once one device is selected, you can only select additional devices of the same version.

**Edit policy**

Click the *Edit Policy* icon displayed in the *Actions* column to display the settings below.

• **Settings**: This tab allows you to change the device name, location, and address.
  - **Device Name**: Displays the name of the device. Type a new name to change the name.
  - **Location**: Displays the location of the device. Type a new location to change the location. We suggest entering the physical location of the appliance for the organization.
  - **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 following options are available:
    - **Address**: Displays the static address assigned to the device. Type a new address to change the static address.
    - **Netmask**: Displays the netmask address assigned to the device. Type a new address to change the netmask address.
    - **Gateway**: Displays the gateway address assigned to the device. Type a new address to change the gateway address.
  - **DNS**: Enter the address of any DNS servers to add to the configuration.
  - **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.
  - **Delete DNS**: Click to delete the DNS server from the configuration.

• **Time Settings**: This tab allows you to change the timezone and other time settings of the device.
  - **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.
  - **Add Server**: Click to add the NTP server to the configuration.
  - **NTP Servers**: Displays the NTP servers added to the configuration.
  - **Edit NTP Server**: Click to edit or update the NTP server.
  - **Delete NTP Server**: Click to delete the NTP server from the configuration.

• **Authentication**: This tab allows you to change the authentication protocol of the device.
  - **Enable OS authentication only**: Select this option to enable OS authentication.
  - **Enable third-party authentication**: Select this option to enable third-party authentication.
    - **Add**: Click to add a new authentication setting. You will need to configure the new authentication setting.
    - **Search**: Enter the text string to search.
    - **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.

• **Upgrade Settings**: This tab allows you to schedule a date and time in which the device will check for a new software version of the device.
  • **Enable Upgrade**: Click the check box to enable the device to check for new software versions for the device.
  • **Select Date**: If **Enable Upgrade** is enabled, select the date and time at which the device will check for a new software version of the device.

### Manage users

Click the **Manage users** icon displayed in the **Actions** column to display the settings below.

• **Add User**: These settings allow you to add other users access to the device along with associated privileges.
  • **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.
  • **Role**: Displays the role of the user. Possible Role values are **Full Access** and **Monitor Only**.
  • **Add**: Click to add the user to the list of secondary users below.

• **Primary User**: Displays the primary user assigned to the device.

• **Secondary User(s)**: Displays the additional non-primary users assigned to the device.

### Configuring network settings by command script

You can configure LiveCapture network settings by using the ‘omni-interface’ command script from the ‘root’ user command prompt (`root@LiveCapture`). 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
**Connecting to LiveCapture through the serial port**

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

**To connect to LiveCapture:**

1. **Connect a serial console cable from your laptop to the serial port on the back of LiveCapture.** The cable must be an RS-232 (null modem) cable with a female DB-9 connector for the serial port on LiveCapture.

2. **Using any serial terminal program (e.g., HyperTerminal or Putty), establish a connection to LiveCapture.** Make sure the appropriate terminal settings match the default settings below for LiveCapture:
   - 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 LiveCapture has been established, the LiveCapture login prompt appears.**

4. **Log into LiveCapture as you normally would.** The LiveCapture command prompt (`admin@livecapture`) 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 38. Additionally, please configure an NTP server as described in [*Time*](#) on page 31.
Using LiveCapture with Omnipeek

Any computer on the network with the Omnipeek Windows software installed can now access the Capture Engine running on LiveCapture. 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 67, 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 LiveCapture lets you remotely access LiveCapture as if you were in the same room as the LiveCapture. Using an Internet browser, you can easily perform tasks such as accessing a remote console, reimaging LiveCapture, rebooting, shutting down, and starting LiveCapture (even if LiveCapture is off).

iDRAC and network security

iDRAC is a powerful tool for performing various tasks remotely on LiveCapture; 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 LiveCapture is set to a strong, unique password. See Changing the default password on page 43.

- **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 LiveCapture requires its own IP address for communication. You can set this in one of two ways:

- Access the BIOS settings for LiveCapture 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 LiveCapture 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 LiveCapture, and connect an Ethernet cable from your network to the iDRAC port.
2. Reboot or restart LiveCapture.
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 LiveCapture.
7. Press [Esc] to back out of each menu, then press Enter to confirm exit.

Connecting to iDRAC on LiveCapture

You can use an Internet browser window to connect to iDRAC on LiveCapture. 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 LiveCapture using your browser:

1. From a computer connected to the network, open an Internet browser window.
2. Enter the iDRAC IP address of LiveCapture 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 LiveCapture.
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, reimagining, rebooting, starting, and shutting down LiveCapture.

**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 LiveCapture.

**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 LiveCapture login window appears.

2. Log into LiveCapture using LiveCapture login user name and password. The **admin@livecapture:~#** command prompt appears once you are logged into LiveCapture.
Reimaging LiveCapture with an ISO image

You can reimagine LiveCapture remotely using iDRAC and an ISO image available from LiveAction technical support. See Contacting LiveAction support on page 20.

To reimagine LiveCapture:

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 `livecapture-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.
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 LiveCapture has rebooted, you can proceed to configuring the management IP, time zone, NTP, and other settings for LiveCapture as you normally would. See those sections in this guide for instructions.

**Rebooting LiveCapture**

To reboot LiveCapture:

- 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 LiveCapture**

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

To start or shut down LiveCapture:

- From the iDRAC dashboard, if LiveCapture 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 LiveCapture.
Capture Engines

In this chapter:

About Capture Engine ............................................................... 50
Using the Capture Engine Manager .............................................. 50
Configuring a Capture Engine ....................................................... 56
Updating Capture Engine settings ................................................. 61
Updating Capture Engine ACL settings ....................................... 62
Using Capture Engines with Omnipeek ....................................... 67
Third-party authentication with Capture Engines ............................ 70
About Capture Engine

Pre-installed on LiveCapture, 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 LiveCapture. 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 67, 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 LiveCapture
- 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 55.

• **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 52.

• **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 56.

• **Restart Engine**: Click to restart the Capture Engine. See Reconnect button on page 55.

• **Update Settings**: Click to update the settings for Filters, Alarms, or Graphs for the Capture Engine. See Updating Capture Engine settings on page 61.

• **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 62.

• **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 54.
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 61.

**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.

   ![Discover Engines dialog](image)

   • **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**

   ![Reconnect button](image)
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 52.

## 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 52) 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.


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 70.
  - **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.

![Capture Engine Configuration Wizard](image)

- **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 66.

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 66.

**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.
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.

![Edit Access Control](image)

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

![Add Users to ACL](image)

**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.
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 61).
   - the **Select engines** view of the **Capture Engine Update ACL Wizard** (see **Updating Capture Engine ACL settings** on page 62).

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 52 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 55 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.

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

6. 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.

![Capture Engine capture window](image)

**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 50.

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 57.

**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 LiveCapture

In this chapter:

About capture adapters ................................................................. 73
1G capture adapter ........................................................................... 73
10G capture adapter ....................................................................... 74
40G capture adapter ....................................................................... 76
100G capture adapter ................................................................. 77
Enabling PTP support for capture adapters ..................................... 78
Connecting the external time synchronization adapter .................. 81
Troubleshooting the capture adapters .......................................... 81
About capture adapters

The capture adapters for LiveCapture 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 LiveCapture are available in the following configurations:

- 1G capture adapter—Four port PCI Express Gigabit adapter (see 1G capture adapter on page 73)
- 10G capture adapter—Two or four port 10 Gigabit adapter (see 10G capture adapter on page 74)
- 40G capture adapter—Two port 40 Gigabit adapter (see 40G capture adapter on page 76)
- 100G capture adapter—Two port 100 Gigabit adapter (see 100G capture adapter on page 77)

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

For more information on using capture adapters with LiveCapture 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.

![1G capture adapter I/O bracket diagram]

LED status

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

<table>
<thead>
<tr>
<th>LED</th>
<th>State and Color</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System LED</td>
<td>Off</td>
<td>The power is off.</td>
</tr>
<tr>
<td></td>
<td>Constant red</td>
<td>During start-up: Power is on. The adapter is checking the power supplies.</td>
</tr>
<tr>
<td></td>
<td>Flashing red</td>
<td>After start-up: The power is on. There is a fatal hardware error.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>LED</th>
<th>State and Color</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant yellow</td>
<td>During start-up: The power is on. The power supplies are working.</td>
<td></td>
</tr>
<tr>
<td>Flashing yellow</td>
<td>There is a new entry in the hardware log.</td>
<td></td>
</tr>
<tr>
<td>Constant green</td>
<td>The FPGA is loaded, and the system is running.</td>
<td></td>
</tr>
</tbody>
</table>

**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.
- **Constant 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 (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.

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

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

<table>
<thead>
<tr>
<th>LED</th>
<th>State and Color</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System LED</td>
<td>Off</td>
<td>The power is off.</td>
</tr>
<tr>
<td></td>
<td>Constant red</td>
<td>During start-up: Power is on. The adapter is checking the power supplies.</td>
</tr>
</tbody>
</table>
Enabling PTP support for capture adapters

The capture adapters for LiveCapture 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 LiveCapture. 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 80.

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 LiveCapture 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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameters</th>
<th>Description</th>
<th>Values</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>TimeSyncOsTimeReference</td>
<td>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.</td>
<td>None - adapter-0 - adapter-1 - adapter-2...</td>
<td>None</td>
</tr>
<tr>
<td>AdapterN</td>
<td>PtpDhcp</td>
<td>Enables/disables DHCP support on the PTP port. Set to DISABLE if a static IP address will be used.</td>
<td>ENABLE - DISABLE</td>
<td>DISABLE</td>
</tr>
<tr>
<td>AdapterN</td>
<td>PtpIpAddr</td>
<td>Specifies a static IP address for the PTP port.</td>
<td>Any valid IPv4 address (e.g. 192.168.1.10)</td>
<td>Not set</td>
</tr>
<tr>
<td>AdapterN</td>
<td>PtpGw</td>
<td>Specifies a gateway address for the PTP port.</td>
<td>Any valid IPv4 address (e.g. 192.168.1.10)</td>
<td>Not set</td>
</tr>
<tr>
<td>AdapterN</td>
<td>PtpNetMask</td>
<td>Specifies the netmask for the static address specified with PtpIpAddr.</td>
<td>Any valid IPv4 netmask (e.g. 255.255.255.0)</td>
<td>Not set</td>
</tr>
</tbody>
</table>

**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.
Synchronizing the capture engine clock

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

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

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

For the capture adapters for LiveCapture 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 78.

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:

   ![Diagram](image)

   - Rx
   - Tx
   - SFP/SFP+ Module
   - Rx
   - Tx
   - SFP/SFP+ Module

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:

LiveCapture technical specifications ......................................................... 84
Capture adapter technical specifications .................................................... 86
### LiveCapture technical specifications

#### LiveCapture 1100

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1 x Intel® Xeon® Bronze 3106</td>
</tr>
<tr>
<td>Base Frequency</td>
<td>1.70 GHz</td>
</tr>
<tr>
<td>Cores</td>
<td>8</td>
</tr>
<tr>
<td>Thread</td>
<td>8</td>
</tr>
<tr>
<td>Memory</td>
<td>32 GB</td>
</tr>
<tr>
<td>Expansion Slots</td>
<td>1 x 16 FH/HL</td>
</tr>
</tbody>
</table>

**NOTE:** A total of one capture adapter can be added to the LiveCapture 1100.

<table>
<thead>
<tr>
<th>Integrated Network Interfaces</th>
<th>4 x 1GBASE-T iDRAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage-OS</td>
<td>Included as part of Storage-Data</td>
</tr>
<tr>
<td>Storage-Data</td>
<td>4 x 4 TB NLSAS (16 TB)</td>
</tr>
<tr>
<td>Chassis</td>
<td>1U Rackmount</td>
</tr>
<tr>
<td>Dimensions (WxHxD):</td>
<td>17.08 x 1.68 x 27.26 in. (434 x 42.7 x 692.4 mm)</td>
</tr>
<tr>
<td>Weight:</td>
<td>Up to 38.58 lb (17.5 kg) Maximum</td>
</tr>
<tr>
<td>System Cooling</td>
<td>Five chassis cooling fans (hot-pluggable)</td>
</tr>
</tbody>
</table>

**System Input Requirements**

| AC Input Voltage:            | 100-240 V AC                                     |
| Rated Input Current:         | 7.4 A-3.7 A                                      |
| Rated Input Frequency:       | 50/60 Hz                                         |

**Power Supply (2 units)**

| Rated Output Power:          | 550 W                                            |

**Operating Environment**

| Operating Temperature:       | 50° to 95° F (10° to 35° C)                      |
| Non-operating Temperature:  | -40° to 149° F (-40° to 65° C)                    |
| Operating Relative Humidity: | 10% to 80% (non condensing)                      |
| Non-operating Relative Humidity: | 5% to 95% (non condensing)                     |
| Heat dissipation (maximum):  | 2559 BTU/ Hour                                   |
# LiveCapture 3100

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>2 x Intel® Xeon® Gold 6126</td>
</tr>
<tr>
<td>Base Frequency</td>
<td>2.6 GHz</td>
</tr>
<tr>
<td>Max Turbo Frequency</td>
<td>3.7 GHz</td>
</tr>
<tr>
<td>Cores</td>
<td>12</td>
</tr>
<tr>
<td>Thread</td>
<td>24</td>
</tr>
<tr>
<td>Memory</td>
<td>192 GB</td>
</tr>
<tr>
<td>Expansion Slots</td>
<td>64 TB / 128 TB Configuration:</td>
</tr>
<tr>
<td></td>
<td>1 x 16 FH/FL</td>
</tr>
<tr>
<td></td>
<td>2 x 8 FH/FL</td>
</tr>
<tr>
<td></td>
<td>1 x 8 FH/HL</td>
</tr>
<tr>
<td></td>
<td>96 TB Configuration:</td>
</tr>
<tr>
<td></td>
<td>1 x 8 FH/FL</td>
</tr>
<tr>
<td></td>
<td>1 x 8 FH/HL</td>
</tr>
<tr>
<td></td>
<td>3 x 16 FH/FL</td>
</tr>
<tr>
<td></td>
<td>1 x 16 LP/HL</td>
</tr>
<tr>
<td><strong>NOTE:</strong></td>
<td>A total of three capture adapters can be added to the LiveCapture 3100.</td>
</tr>
</tbody>
</table>
| Integrated Network Interfaces | 4 x 1GBASE-T  
                          | iDRAC                                                                       |
| Storage-OS              | 2 x 2 TB NLSAS (4 TB)                                                      |
|                         | or                                                                          |
|                         | 2 x 1.8 TB SAS (3.6 TB)                                                    |
| Storage-Data            | 16 x 8 TB NLSAS (128 TB)                                                   |
|                         | or                                                                          |
|                         | 16 x 4 TB NLSAS (64 TB)                                                    |
|                         | or                                                                          |
|                         | 12 x 8 TB NLSAS (96 TB)                                                    |
| Chassis                 | 2U Rackmount                                                               |
| Dimensions (WxHxD):     | 17.09 x 3.42 x 28.17 in. (434 x 86.8 x 715.5 mm)                            |
| Weight:                 | Up to 72.91 lb (33.1 kg) Maximum                                            |
| System Cooling          | Six chassis cooling fans (hot-pluggable)                                   |
| System Input Requirements| AC Input Voltage: 100-240 V AC, autoranging                                |
|                         | Rated Input Frequency: 50/60 Hz                                            |
| Power Supply (2 units)  | 1100 W                                                                      |
| Rated Output Power:     | 1100 W                                                                      |
| Operating Environment   | 50° to 95° F (10° to 35° C)                                                 |
| Operating Relative Humidity | 10% to 80% (non condensing)                                              |
| Non-operating Relative Humidity | 5% to 95% (non condensing)                                              |
| Heat dissipation (maximum): | 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

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

### 10G capture adapter (2-port) specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Standard:</td>
<td>IEEE 802.3 10 Gbps Ethernet LAN</td>
</tr>
<tr>
<td>Physical interface:</td>
<td>2 x SFP or SFP+ ports</td>
</tr>
<tr>
<td><strong>Supported SFP modules</strong></td>
<td>Multi-mode SX, single-mode LX and ZX, 1000BASE-T or 10/100/1000BASE-T</td>
</tr>
<tr>
<td><strong>Supported SFP+ modules</strong></td>
<td>Multi-mode SR, single-mode LR and ER, 10GBASE-CR</td>
</tr>
<tr>
<td><strong>Supported dual-rate modules</strong>:</td>
<td>Multi-mode SR and single-mode LR</td>
</tr>
</tbody>
</table>
### 10G capture adapter (4-port) specifications

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

### 40G capture adapter specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Network interfaces</strong></td>
<td></td>
</tr>
<tr>
<td>Standard:</td>
<td>IEEE 802.3 40 Gbps Ethernet LAN</td>
</tr>
<tr>
<td>Physical interface:</td>
<td>2x QSFP+ ports</td>
</tr>
<tr>
<td>Supported optical transceivers:</td>
<td></td>
</tr>
<tr>
<td>Supported QSFP+ modules:</td>
<td>40GBASE-SR4, 40GBASE-LR4, and 40GBASE-SR-BiDi</td>
</tr>
<tr>
<td>Supported QSFP28 modules:</td>
<td>100GBASE-SR4 and 100GBASE-LR4</td>
</tr>
</tbody>
</table>
## 100G capture adapter specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environment</strong></td>
<td></td>
</tr>
<tr>
<td>Operating temperature:</td>
<td>32°F to 113°F (0° to 45°C)</td>
</tr>
<tr>
<td>Operating humidity:</td>
<td>20% to 80%</td>
</tr>
<tr>
<td><strong>Regulatory approvals and compliances</strong></td>
<td></td>
</tr>
<tr>
<td>PCI-SIG®</td>
<td></td>
</tr>
<tr>
<td>NEBS level 3</td>
<td></td>
</tr>
<tr>
<td>CE</td>
<td></td>
</tr>
<tr>
<td>CB</td>
<td></td>
</tr>
<tr>
<td>RoHS</td>
<td></td>
</tr>
<tr>
<td>REACH</td>
<td></td>
</tr>
<tr>
<td>cURus (UL)</td>
<td></td>
</tr>
<tr>
<td>FCC</td>
<td></td>
</tr>
<tr>
<td>ICES</td>
<td></td>
</tr>
<tr>
<td>VCCI</td>
<td></td>
</tr>
<tr>
<td>C-TICK</td>
<td></td>
</tr>
</tbody>
</table>

### Network interfaces

- **Standard:** IEEE 802.3 40 Gbps Ethernet LAN
- **Physical interface:** 2x QSFP+ ports

### Supported optical transceivers:

- **Supported QSFP+ modules:** 40GBASE-SR4, 40GBASE-LR4, and 40GBASE-SR-BiDi
- **Supported QSFP28 modules:** 100GBASE-SR4 and 100GBASE-LR4

### Environment

- **Operating temperature:** 32°F to 113°F (0° to 45°C)
- **Operating humidity:** 20% to 80%

### Regulatory approvals and compliances

- PCI-SIG®
- NEBS level 3
- CE
- CB
- RoHS
- REACH
- cURus (UL)
- FCC
- ICES
- VCCI
- C-TICK