Omnipeek 24.3.0

Release Notes

Installation Notes

Please read this document for important installation notes, a list of recent changes, and currently known issues. This document covers LiveAction Omnipeek 24.3.0.

Product Activation

When you install Omnipeek, the installer sends a secure message to a Web server. This process will assist us in reducing software piracy, as we can ensure that our software products are used solely by authorized customers. Automatic activation will fail if the computer uses a proxy server to access the Internet. Use Manual activation instead. For more information, please visit https://www.liveaction.com/support/frequently-asked-questions/.

Uninstallation Notes

To remove Omnipeek, re-run the installer and choose "Remove"; or remove it via the Control Panel. All files created during the installation will be removed; however, you may need to manually delete the Omnipeek folder to remove files created after installation.

Product Documentation

When you install Omnipeek, the installer sends a secure message to a Web server. This process will assist us in reducing software piracy, as we can ensure that our software products are used solely by authorized customers. Automatic activation will fail if the computer uses a proxy server to access the Internet. Use Manual activation instead. For more information, please visit *https://www.liveaction.com/support/frequently-asked-questions/*.

Recommended System Requirements

The system requirements for Omnipeek are:

- Windows 11, Windows 10, Windows Server 2022, Windows Server 2019, Windows Server 2016

Omnipeek supports most rack mount, desktop and portable computers as long as the basic system requirements to run the supported operating systems are met. Depending on traffic and the particular usage of Omnipeek, the requirements may be substantially higher.

The following system is recommended for Omnipeek:

- Intel Core i3 or higher processor
- 4 GB RAM
- 40 GB available hard disk space

Factors that contribute towards superior performance include high speed and multiple CPUs, additional RAM, high performance disk storage subsystem, and as much additional hard disk space as is required to save the trace files that you plan to manage.

Supported operating systems require users to have Administrator level privileges in order to load and unload device drivers, or to select a network adapter for the program's use in capturing packets. For more information, please see our Web site at *https://www.liveaction.com/products*.

What's New In Omnipeek 24.3.0

New Features

○ Updated LiveWire Group Authentication, which allows LiveWire appliances to be added to a "group" where they share an authentication token allowing distributed actions to be taken without the user having to login manually to each appliance.

○ Added support for an upcoming LiveWire Edge appliance update. This appliance will have RJ45 console access as well as OOB management but is otherwise similar in performance to the existing LiveWire Edge.

○ Added OTEL Expert Output, which allows LiveFlow to trigger on additional Expert analytics and send those events to any upstream service that accepts standard OTEL events.

○ Enhanced Grid Configuration Sync, which adds the ability to sync Capture configurations between LiveWire appliances and all necessary supporting configuration (Alarms, Filters and Graphs).

○ Added Docker and OCI container deployment options. LiveWire can now be deployed as a container similar to our Virtual option. This option currently does not support features that are dependent on SNMP support (LiveFlow Router Map, LiveNX Discovery, etc.)

○ Added support for LiveFlow IPFIX output to a IPv6 Target.

○ Added support for Oracle Cloud for LiveWire Virtual.

○ Added ability to update a Forensic Search name after creation.

○ Added a new MPLS/VLAN/VXLAN Statistics View.

○ Added ability to filter flows (by network data) in Expert Flows.

○ Added Preset values to time controls in Forensic Search.

○ Added MPLS/VLAN/VXLAN columns to Expert Flows.

○ Added custom decoder columns to LiveWire Omnipeek.

○ Updated the Distributed Forensic Search Start/End Time fields.

Key Bug Fixes

○ Fixed a bug where LiveFlow router map interface name could have same name as adapter.

○ Fixed a bug that allowed duplicate interface names in the LiveFlow router map.

○ Fixed a bug where drag and drop for decryption keys shows a misleading error message.

○ Fixed a bug where Reconstructed SMB payloads are incorrect.

○ Fixed a bug where TCPDUMP adapter list was lost upon version upgrade.

○ Fixed a bug where incorrect decode caused some packets to show up as IPv6 when they should not.

○ Fixed a bug where a crash occurs in SMB reassembly.

○ Fixed a bug where a white page is revealed when scrolling down in expert columns drop-down.

○ Fixed a bug in LiveFlow where the tls_parser does not properly handle flows with certificate but no CHLO.

○ Fixed a bug in LiveFlow where In IF and Out IF is displayed as ifindex 100 instead of IfName.

Known Issues

○ The following Expert events won't work in a monitoring capture when using a Napatech card: TLS Forbidden Version, TLS Slow Handshake, TLS Certificate Invalid Before Date, TLS Certificate Invalid After Date. (OD-4291)

○ If a filter was created using an application with version 23.2 or earlier, the filter won't be converted to use new application IDs and will have to be recreated. (OD-3682)

○ Those wanting to use RSA SecurID for authentication should choose RADIUS authentication in Omnipeek, and then enable their RSA authentication server's RADIUS option. (OD-2590)

- Filtering when opening a capture file does not work with encrypted files (such as those created by ORA) since Omnipeek has no means of filtering them before they are decrypted and opened. (33175)

- Application classification is done with entire packet contents before slicing is applied when saving packets, so when the file is reloaded the entire packet is no longer present which may result in different (or no) application classification. (30074)

- Application classification may return different results if all the packets that make up a flow are not present, in particular the TCP handshake packets. (30081)

- Cisco and Aruba access points may report incorrect signal and noise percent values in Omnipeek. (29604, 29616)

- In a tcpdump capture, if no packets are filtered and you stop the capture on some remote systems (e.g., Mac OS and Debian Linux), the remote tcpdump processes might not shut down. You may need to SSH into the remote system and shut down the tcpdump processes manually. (29576)

- If the installer launches Omnipeek for you, it is not possible to open a file by double-clicking or 'dragging and dropping' it in Omnipeek. (26149, 26155)

Technical Tips and Additional Product Information

- **Open Source Software**
  This product may include open source software. See the Copyrights folder for more information.

How to Contact LiveAction Online Support

If you can't find the answers that you are looking for in the online help or the User Guide, you can get the most current information from our website. To access the LiveAction website, launch your web browser and go to *https://www.liveaction.com/support/technical-support/*.