

Omnipeek 24.1.0

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 24.1.0.

This installer is for Omnipeek. If you also use Capture Engine for Windows, you must run that installer and configure Capture Engine on a machine and note the IP address. You will use this IP address when connecting to Capture Engine from Omnipeek. You may need to disable any antivirus software before running the Omnipeek installer.

Note Capture Engines are pre-installed on LiveWire appliances.

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

Please read the Omnipeek Getting Started Guide for an overview of the features of Omnipeek. Online Help is available from the Help menu within the program. Please also visit <https://docs.liveaction.com/> for a comprehensive library of LiveAction documentation.

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 Omnippeek 24.1.0

New Features

- Improved Packet File Indexing by reducing indexing database size
- Added Distributed Forensic Search cross launch across multiple integrations
- Improved filtering at the adapter/hardware level to increase performance where filters are required
- Added UTC toggle to LiveWire Omnippeek
- Enabled application classification for LiveFlow without CTD
- Added a LiveNX 'catch all' interface for LiveWire's capture adapter
- Added support for saving packets files directly from the Forensics view in LiveWire Omnippeek (no analysis)
- Added support for locally defined admin groups and LDAP/AD groups, simultaneously
- Improved active directory feedback in role-based access control interface
- Increased load balancing for improved performance on LiveWire PowerCore and Core (Gen2)
- Improved Reconstructions View Sidebar Content Tab when switching from image to hex data for images over 100 KB
- Improved displaying Forensic Searches as a table/list
- Open/drop a packet file in the Forensics view in LiveWire Omnippeek

Key Bug Fixes

- Fixed an issue where a filter currently applied to another capture could not be edited
- Fixed an issue where packets were truncated under specific conditions
- Fixed an issue where NTP configuration was updating the wrong files
- Fixed an issue where passive name resolution resulted in unresponsive state
- Fixed an issue in forensic search when certain analysis options were enabled in Windows Capture Engine
- Fixed an issue that occurs when closing the Reconstruction Contents view
- Fixed an issue that resulted in an empty Packets view when data is rolling out
- Fixed an issue displaying Tab Packet Size % value
- Fixed an issue displaying file sizes in the Files view

Known Issues

- 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.
- Those wanting to use RSA SecurID for authentication should choose RADIUS authentication in Omnippeek, and then enable their RSA authentication server's RADIUS option.
- Filtering when opening a capture file does not work with encrypted files (such as those created by ORA) since Omnippeek has no means of filtering them before they are decrypted and opened.
- 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.
- Application classification may return different results if all the packets that make up a flow are not present, in particular the TCP handshake packets.

-
- Cisco and Aruba access points may report incorrect signal and noise percent values in Omnippeek.
 - 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.
 - If the installer launches Omnippeek for you, it is not possible to open a file by double-clicking or 'dragging and dropping' it in Omnippeek.

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/>.