Omnipeek Network Analysis Software 22.4.1 Readme

Please read this document for important installation notes, a list of recent changes, and currently known issues. This document covers LiveAction Omnipeek 22.4.1.

Contents

Installation Notes

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 LiveCapture and LiveWire network capture appliances.

If you are performing a silent install of Omnipeek on a Windows 7 or Windows Server 2008 R2 machine, you must have the hotfix described at https://support.microsoft.com/en-us/kb/2921916 already installed; otherwise, an error message appears instructing you to apply the hotfix.

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.

Capture Engine Manager for Omnipeek

The Capture Engine Manager is included with Omnipeek. It provides an interface for configuring and updating remote Capture Engines. See the Capture Engine Manager Readme for more information on Capture Engine Manager.

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. PDF versions of the User Guide, Getting Started Guide, and Capture Engine Getting Started Guide are in the Documents directory where you installed Omnipeek.

Recommended System Requirements

The system requirements for Omnipeek are:

- Windows 11, Windows 10, Windows 8.1 64-bit, Windows 7 64-bit, Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008 R2 64-bit

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 22.4.1

Omnipeek / Omnipeek Web

Key Bug Fixes

- Fixed an issue where forensic searches with filters sometimes result in zero packets (OD-3161)

What's New In Omnipeek 22.4

Omnipeek / Omnipeek Web

- Reconstruct file contents from packets for TFTP protocol (OD-2971)
- Support reading and writing FCS bytes in PCAP/PCAPng files (OD-2997)
- Improved the decoding of SSL/TLS (OD-3018)
- Added decoding for 29West (OD-3006)
- Update application identification library to the latest release (OD-2998)
- Improved the decoding for BGP (OD-2883)
- Create a packet file per day even if the file size doesn’t hit the configured file size (OD-2875)
- Add support for Dynamic Link Exchange Protocol (DLEP) (OD-2829)
- Improved decoding of LTPv3 by including sublayers (OD-2744)
- Improved decoding of SIP message body (OD-2731)
- Added support for Palo Alto Networks Heartbeat Ethertype (OD-2666)
- Added decode for H.265/HEVC (OD-2101)

Key Bug Fixes

- Fixed NetBIOS/CIFS decode issue where decode would end prematurely (OD-3074)
- Fixed STUN decode issue where the IP address was not decoded correctly (OD-3053)
- Fixed an issue where TLSv1.2 packets were sometimes decoded as TLSv1.3 packets (OD-3026)
- Fixed an issue where the packet list from a filtered forensic search sometimes became corrupted (OD-3001)
- Fixed an issue with RAW PCAP files where files with IPv6 traffic were not being read correctly (OD-2746)

LiveWire Appliances

- Reconstruct file contents from packets for TFTP protocol (OD-2971)
- Support reading and writing FCS bytes in PCAP/PCAPng files (OD-2997)
- Improved the decoding of SSL/TLS (OD-3018)
- Added decoding for 29West (OD-3006)
- Update application identification library to the latest release (OD-2998)
- Remove the tcadmin user from all installs (OD-2953)
- Integrate LiveWire and LiveNX MIBs into a single LiveAction MIB (OD-2886)
- Improved the decoding for BGP (OD-2883)
- Create a packet file per day even if the file size doesn’t hit the configured file size (OD-2875)
- Add support for Dynamic Link Exchange Protocol (DLEP) (OD-2829)
- Improved decoding of LTPv3 by including sublayers (OD-2744)
- Improved decoding of SIP message body (OD-2731)
- Added support for Palo Alto Networks Heartbeat Ethertype (OD-2666)
- Added decode for H.265/HEVC (OD-2101)

Key Bug Fixes

- Fixed NetBIOS/CIFS decode issue where decode would end prematurely (OD-3074)
- Fixed STUN decode issue where the IP address was not decoded correctly (OD-3053)
- Fixed issue where filtering RTP flows in LiveNX would result in different results for Basic Flow and Voice and Video (OD-3071)
- Fixed an issue where the LiveWire Gen2 appliance would not boot into Rescue mode (OD-3057)
- Fixed an issue where TLSv1.2 packets were sometimes decoded as TLSv1.3 packets (OD-3026)
- Fixed an issue where the packet list from a filtered forensic search sometimes became corrupted (OD-3001)
- Fixed an issue where LiveWire would sometimes crash as a result of using the download packets feature (OD-3000)
- Fixed an issue with RAW PCAP files where files with IPv6 traffic were not being read correctly (OD-2746)

LiveCapture Appliances

- Reconstruct file contents from packets for TFTP protocol (OD-2971)
- Support reading and writing FCS bytes in PCAP/PCAPng files (OD-2997)
- Improved the decoding of SSL/TLS (OD-3018)
- Added decoding for 29West (OD-3006)
- Update application identification library to the latest release (OD-2998)
- Remove the tcadmin user from all installs (OD-2953)
- Integrate LiveCapture and LiveNX MIBs into a single LiveAction MIB (OD-2886)

Improved the decoding for BGP (OD-2883)
- Create a packet file per day even if the file size doesn't hit the configured file size (OD-2875)
- Add support for Dynamic Link Exchange Protocol (DLEP) (OD-2829)
- Improved decoding of LTPv3 by including sublayers (OD-2744)
- Improved decoding of SIP message body (OD-2731)
- Added support for Palo Alto Networks Heartbeat Ethertype (OD-2666)
- Added decode for H.265/HEVC (OD-2101)

Key Bug Fixes

- Fixed NetBIOS/CIFS decode issue where decode would end prematurely (OD-3074)
- Fixed STUN decode issue where the IP address was not decoded correctly (OD-3053)
- Fixed an issue where TLSv1.2 packets were sometimes decoded as TLSv1.3 packets (OD-3026)
- Fixed an issue where the packet list from a filtered forensic search sometimes became corrupted (OD-3001)
- Fixed an issue where LiveCapture would sometimes crash as a result of using the download packets feature (OD-3000)
- Fixed an issue with RAW PCAP files where files with IPv6 traffic were not being read correctly (OD-2746)

What's New In Omnipeek 22.2

Omnipeek / Omnipeek Web

- Configurable retention rules for packet storage (OD-2546)
- Added WebViews to Omnipeek Web (OD-2358)
- Reconstructed contents from packets for the HTTP protocol (OD-2603)
- Updated the ThreatEye NV plugin to the latest version (OD-2626)
- Added geo location data to reconstructions view data (OD-2768)
- Enabled Average Network and Application Latency columns to Flows View by default (OD-2728)
- Changed the default packet file save format to .pkt (OD-2714)
- Added Save Payload Functionality for Reconstruction View on Peek Web (OD-2712)
- Need search bars added to Omnipeek Web just as seen in Omnipeek (OD-2706)
- Added a click-through software license agreement statement to the Omnipeek Web and Omnipeek for Windows log-in screens (OD-2540)
- Added Servers/Clients/Pages/Requests counts to Omnipeek Web (OD-2358)

Key Bug Fixes

- Adding other LiveWires in the Omnipeek WebUI fails (OD-2782)
- Omnipeek Web Forensic Search dialog allows no analysis (OD-2766)
- No scroll bar for Distributed Forensic Searches (OD-2760)
- Some columns in the Web views don't sort as expected (OD-2749)
- Saving a packet file from a forensic search with Omnipeek blocks and causes spinning cursor (OD-2670)
- Fixed STUN under TCP protocol detection (OD-2605)
- Getting an error "Unspecified error (Error code 0x0004005)" when selecting Capture Options (OD-2523)
- Supported dynamic codecs sometimes falsely identified as "(unsupported)" (OD-2216)
- MOS-V scores are much lower in 21.3.0 vs 21.2.0 (in some cases) (OD-2056)
- Delete file save warning in Omnipeek (OD-1895)

LiveWire Appliances

- Transitioned to Gen2 Edge device
- Added configurable retention rules for packet storage (OD-2546)
- Reconstructed flow contents from packets for the HTTP protocol (OD-2603)
- Improved Restore UI (LADM-13, OD-2517)
- Automated information gathering from customer systems for better troubleshooting (OD-1439, OD-1848, OD-2581)
- Updated the ThreatEye NV plugin to the latest version (OD-2626)
- Added Turbo support for ThreatEye NV captures on LiveWire Virtual Large (OD-2785)
- Added geo location data to reconstructions view data (OD-2768)
- Displayed the hardware serial number during manual activation (OD-2733)
- Enabled Average Network and Application Latency columns to Flows View by default (OD-2728)
- Changed the default packet file save format to .pkt (OD-2714)
- Added Save Payload Functionality for Reconstruction View on Omnipeek Web (OD-2712)
- Added RAID10 support on the Core/1100 (OD-2547)
- Supported SWDM4 transceivers on Napatech adapters (OD-2544)
- On "Application" restore, do not restore license file (OD-2517)
- Added caller phone number, call ID, and call duration to LiveFlow (OD-2422)
- Tested RAID6 for performance on PowerCore Dual JBOD (OD-2308)

Key Bug Fixes

- Adding other LiveWires in the Omnipeek WebUI fails (OD-2782)
- Omnipeek Web Forensic Search dialog allows no analysis (OD-2766)
- LiveFlow Packet Loss seems too high in LiveNX (OD-2610)

- Fixed STUN under TCP protocol detection (OD-2605)
- Capture engine is slow to respond and shows spinning cursor in Captures view (OD-2535)
- DMS-initiated hostname change only partially updates /etc/hosts file (OD-2524)
- Getting an error "Unspecified error (Error code 0x0004005)" when selecting Capture Options (OD-2523)
- Corrupt omnid pam file cause engine failure (OD-2511)
- Made sure dmsd service is started after omnid service (OD-2433)
- Supported dynamic codecs sometimes falsely identified as "(unsupported)" (OD-2216)
- MOS-V scores are much lower in 21.3.0 vs 21.2.0 (in some cases) (OD-2056)

LiveCapture Appliances

- Added configurable retention rules for packet storage (OD-2546)
- Reconstructed contents from packets for the HTTP protocol (OD-2603)
- Improved Restore UI (LADM-13, OD-2517)
- Automated information gathering from customer systems for better troubleshooting (OD-1439, OD-1848, OD-2581)
- Added geo location data to reconstructions view data (OD-2768)
- Displayed the hardware serial number during manual activation (OD-2733)
- Enabled Average Network and Application Latency columns to Flows View by default (OD-2728)
- Changed the default packet file save format to .pkt (OD-2714)
- Added Save Payload Functionality for Reconstruction View on Omnipeek Web (OD-2712)
- Added RAID10 support on the Core/1100 (OD-2547)
- Added support for SWDM4 transceivers on Napatech adapters (OD-2544)
- On "Application" restore, do not restore license file (OD-2517)
- Tested RAID6 packet capture performance on PowerCore Dual JBOD (OD-2308)

Key Bug Fixes

- Omnipeek Web Forensic Search dialog allows no analysis (OD-2766)
- Fixed STUN under TCP protocol detection (OD-2605)
- Capture engine is slow to respond and shows spinning cursor in Captures view (OD-2535)
- DMS-initiated hostname change only partially updates /etc/hosts file (OD-2524)
- Getting an error "Unspecified error (Error code 0x0004005)" when selecting Capture Options (OD-2523)
- Corrupt omnid pam file cause engine failure (OD-2511)
- Made sure dmsd service is started after omnid service (OD-2433)
- Supported dynamic codecs sometimes falsely identified as "(unsupported)" (OD-2216)
- MOS-V scores are much lower in 21.3.0 vs 21.2.0 (in some cases) (OD-2056)

What's New In Omnipeek 22.1

Omnipeek / Omnipeek Web

- Added ability to copy packets to new window in Omnipeek Web
- Added decode and protocol support for GeNeVE protocol
- Updated sparklines for active sessions in the Forensics view
- Improved software filter performance
- Added port 48879 for IVXLAN to protocol identification
- Added HomePlug AV Protocol to ProtoSpecs
- Show node name and address at the same time
- Added ability to create a filter while creating a capture
- Updated Expert settings so that they are easier to find in Omnipeek Web
- Added UI to configure remote syslog
- Added ability to allow users to schedule backups
- Added Decode RTP/OPUS Audio Codec (Dynamic RTP)
- Added Decode HomePlugAV Protocol
- Added ability to allow users to cancel the 'save file' process

LiveWire Appliances

- Added intelligent packet capture
- Improved performance (Turbo Mode) for LiveWire Edge and Virtual
- Added Web analytics to LiveFlow
- Added Dynamic Slicing to Hardware Profiles
- Provided mechanism to monitor the download status of upgrade from DMS
- Added caller phone number and call ID to LiveFlow
- Added RAID support to the Core
- Improved software filter performance
- Converted upgrade file format from .zip to .enc
- Added report flows with high latency in LiveFlow
- Added ability to send SNMP traps when a drive is failed and has failed
- Excluded CRC and Frame error packets from LiveFlow

Added ability to send both name and hostname to DMS
- Enhanced SNMP reporting for appliances
- Added ability to allow users to schedule backups

LiveCapture Appliances

- Provided mechanism to monitor the download status of upgrade from DMS
- Added RAID support to the 1100
- Improved software filter performance
- Converted upgrade file format from .zip to .enc
- Added ability to send SNMP traps when a drive is failed and has failed
- Added ability to send both name and hostname to DMS
- Enhanced SNMP reporting for appliances
- Added ability to allow users to schedule backups

Bug Fixes

- Enabling TACACS messes up PAM (OD-2511)
- Installing certs works for LiveAdmin but not for OmniWeb (OD-2505)
- When LiveCapture was re-licensed to LiveWire, the Engine Type did not change (OD-2455)
- Make sure dmsd service is started after omnid service (OD-2433)
- Liveadmin restarts networking when IP values are not changed (OD-2401)
- When using Omnipeek Web, downloading the results from large forensic searches can hang the system (OD-2232)
- Some interactions with the WebUI trigger background tasks that block the entire WebUI (OD-2231)
- HTTP response header Content Security Policy is missing (OD-273)
- LiveAction enterprise OIDs don't work after changing hostname via LiveAdmin (LADM-29)
- Updating hostname in LiveAdmin doesn't update /etc/hosts (LADM-24)
- Backup requires restarting service message no longer needed (LADM-23)

Known Issues

- When attempting to save all packets of a large packet file that displays numerous decode columns, it may take several hours to complete. (OD-740)
- 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.
- **Omnipeek Only: Viewing the Compass dashboard on a Windows Server 2012 R2 System**.
  To view the Compass dashboard in Omnipeek running on a Windows Server 2012 R2 system, you must manually enable Flash Player through the Server Manager. (27654)

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/.

LiveAction, Inc
960 San Antonio Road, Ste. 200
Palo Alto, CA 94303, USA
+1 (888) 881-1116
https://www.liveaction.com