LiveAction

Omnipeek 23.3.1

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 23.3.1.

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 23.3.1

Omnipeek / LiveWire Omnipeek

New Features

- Improved performance and stability by replacing the application identification library
- Added notification and enforcement that the .npkt format is required for compression
- Removed "Productivity" and "Risk" metrics from all application analysis
- Added packet reconstruction for SMB3 read and write requests
- Disabled autodiscovery by default to increase security -- users must now opt in
- Added new ACL policies for creating and deleting forensic searches

Key Bug Fixes

- Fixed an issue which caused the TCPdump adapter in Omnipeek for Windows to fail in v23.2
- Fixed an issue where error code 80004005 was sometimes being generated with forensic searches
- Fixed a crash in SMB reconstructions that was affecting many customers
- Fixed an issue where zooming in on a traffic spike in the Compass dashboard could cause a crash
- Fixed an ACL issue where users with no access to delete capture sessions could still select that option

LiveWire & LiveCapture Appliances

New Features

- Improved performance and stability by replacing the application identification library
- Offered FIPS 140-2 compliance for LiveWire
- Removed support for .zip upgrader files, making upgrades more secure
- Changed the reported model numbers for all appliances in the LiveWire Omnipeek UI and the SNMP MIB for better consistency
- Added notification and enforcement that the .npkt format is required for compression
- Removed "Productivity" and "Risk" metrics from all application analysis
- Added DHCP application identification in LiveFlow (LiveWire only)
- Upgraded LiveWire to work with OpenSSL 3
- Added packet reconstruction for SMB3 read and write requests
- Disabled autodiscovery by default to increase security -- users must now opt in
- Added the ability for LiveWire to authenticate to NTP server(s)
- Added new ACL policies for creating and deleting forensic searches

Key Bug Fixes

- Improved stability of DNS analysis in ThreatEye Telemetry (LiveWire only)
- Fixed an issue where LiveWire would limit the number of captures under certain conditions
- Fixed an issue where error code 80004005 was sometimes being generated with forensic searches
- Fixed an issue where duplicate database and index database values were being created and causing errors
- Fixed a crash in SMB reconstructions that was affecting many customers
- Fixed an issue where zooming in on a traffic spike in the Compass dashboard could cause a crash
- Fixed an issue where LiveWire was crashing with “LiveFlow Segmentation Fault” (LiveWire only)
- Fixed an ACL issue where users with no access to delete capture sessions could still select that option

Known Issues

- A new ACL was added to control the ability to perform forensic searches, and this ACL is disabled by default (cannot perform forensic searches) for all users, including the Admin user. If you are using ACLs, be sure to enable the ACL that allows access to perform forensic searches for all users, including the Admin user, that require this access.
- If a filter was created using an application with a previous version, 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 Omnipeek, and then enable their RSA authentication server’s RADIUS option.
- When attempting to save all packets of a large packet file that displays numerous decode columns, it may take several hours to complete.
- 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.
- 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 Omnipeek.
- 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 Omnipeek for you, it is not possible to open a file by double-clicking or 'dragging and dropping' it in Omnipeek.

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/*.