

# Omnipeek 23.1.0

## README

## Omnipeek 23.1.0 Readme

Please read this document for important installation notes, a list of recent changes, and currently known issues. This document covers LiveAction Omnipeek 23.1.0.

### Contents

- [Installation Notes](#)
- [Product Activation](#)
- [Uninstallation Notes](#)
- [Capture Engine Manager for Omnipeek](#)
- [Product Documentation](#)
- [Recommended System Requirements](#)
- [What's New In Omnipeek 23.1.0](#)
- [Known Issues](#)
- [Technical Tips and Additional Product Information](#)
- [How to Contact LiveAction Online Support](#)

### 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 23.1.0

### Omnipeek / Omnipeek Web

#### New Features

- Added support for Two-Factor-Authentication (2FA) (OD-2587)
- Added more file reconstructions from packets (OD-2838)
  - SMTP
  - SMB (CIFS only; v2 and v3 later)
- Added link status to adapters view (OD-1729)
- Added scroll-to-last-packet (OD-1727, 1259)

#### Key Bug Fixes

- Fixed an issue where omnid can crash when using forensic search with reconstructions (OD-3069)
- Fixed an issue where the TCP Expert will sometimes fail (OD-3052)
- Fixed an issue where redirecting the audit log output to file is not working (OD-3023)
- Corrected an error in TNS Refused Expert (OD-2903)

---

## LiveWire & LiveCapture Appliances

### New Features

- Added support for Two-Factor-Authentication (2FA) (OD-2587)
- Added more file reconstructions from packets (OD-2838)
  - SMTP
  - SMB (CIFS only; v2 and v3 later)
- Combined LiveNX and ThreatEye telemetry into a single process (LiveWire only) (OD-2560)
- Relaxed the constraint that RTP packets over UDP must use even number destination ports (LiveWire only) (OD-3295)
- Added support for the Gen 2 Core (OD-3292)
- Allowed hostnames for SFTP Server in Backup/Restore (OD-3263)
- Added support for Factory Reset (using LiveAdmin) for LiveWire Core and PowerCore (OD-2352)
- Added link status to adapters view (OD-1729)
- Added scroll-to-last-packet (OD-1727, 1259)

### Key Bug Fixes

- Fixed an issue where "Reject Matching" Napatech hardware filters are not working (OD-3394)
- Fixed backup incompatibility with versions before v22.4.1 (OD-3205)
- Corrected an issue where packet slicing leads to incorrect byte and bit rate reporting in LiveNX (LiveWire only) (OD-3192)
- Fixed an issue where omnid can crash when using forensic search with reconstructions (OD-3069)
- Fixed an issue where the TCP Expert will sometimes fail (OD-3052)
- Addressed some inconsistency between .pkt and .npkt packet file formats (OD-3025)
- Fixed an issue where redirecting the audit log output to file is not working (OD-3023)
- Corrected an error in TNS Refused Expert (OD-2903)

### 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  
901 Campisi Way, Ste. 222  
Campbell, CA 95008, USA  
+1 (888) 881-1116  
<https://www.liveaction.com>