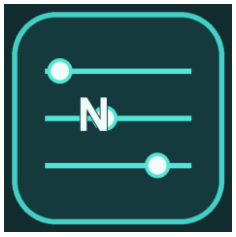


Nexus Packet Sniffer User Manual

Windows x64 packet capture, filtering, and PCAP export

Item	Information
Product version	1.0
About dialog version	1.0 (2026.05.27)
Manual version	1.0

Contents

1. Product overview and supported scope

Nexus Packet Sniffer is a Windows x64 desktop packet capture utility. It uses WinDivert at the NETWORK layer to capture matching IP packets and write classic PCAP files for Wireshark or other compatible analyzers. Its WPF interface controls filters, duration, file size, and output location. Captured packets are not reinjected.

Typical use cases

1. Reproduce a short network issue for a specific source or destination IP, port, TCP, or UDP exchange.
2. Create a PCAP evidence package for network, application, or security teams.
3. Bound a Windows Server capture by duration and file size.
4. Troubleshoot local services, inbound connections, or a selected application protocol.

Item	Supported scope
Packet scope	IPv4 and IPv6 IP packets; All IP, TCP+UDP, TCP, or UDP
Output	Classic PCAP with LINKTYPE_ETHERNET and the .pcap extension
Operating systems	Windows Server 2012/2012 R2/2016/2019/2022/2025 x64; Windows 10/11 for development and testing
Privilege	Run as administrator so WinDivert can be loaded and used
Not included	Non-IP/link-layer traffic such as ARP, RARP, and STP; payload is not displayed in the UI

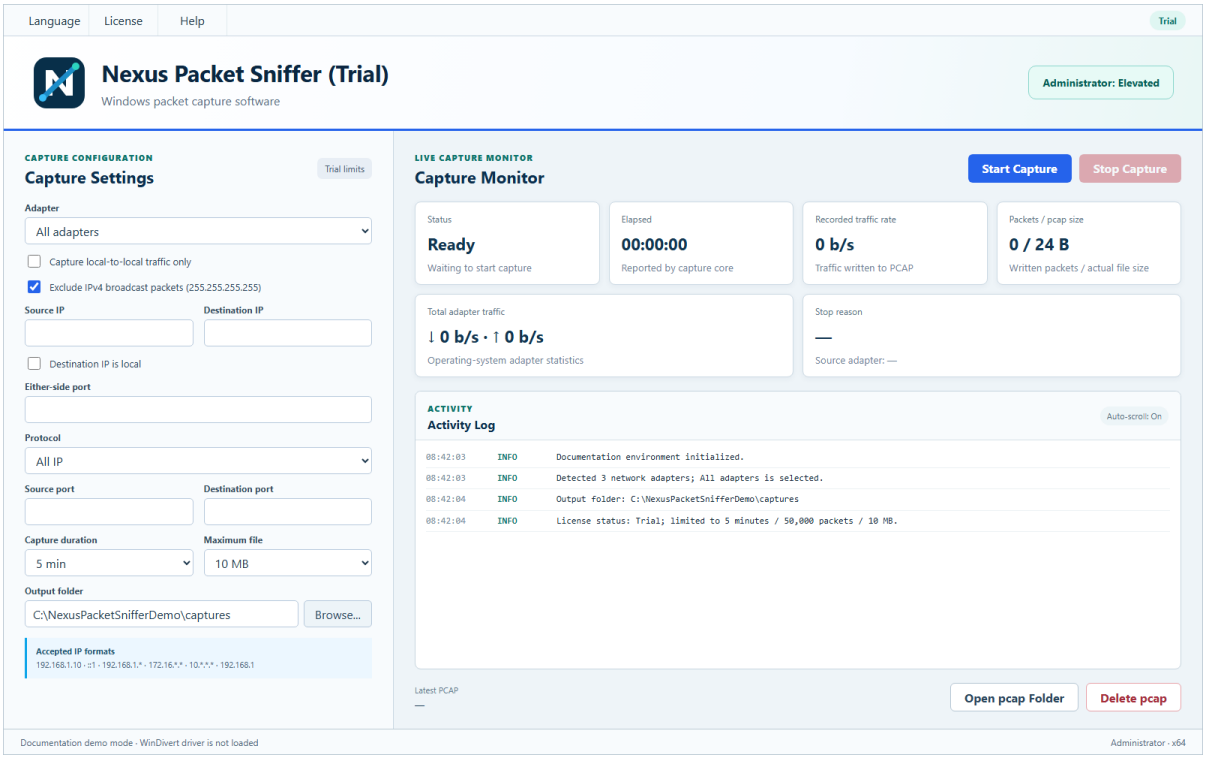
2. Requirements, deployment, and startup

Requirement	Description
Platform	64-bit Windows; 32-bit environments are not supported
Runtime privilege	Run as administrator
Driver component	WinDivert with compatible x64 program files
Disk space	Keep more free space than the selected limit and allow for repeated captures

Important: Without elevation, the application may fail to load WinDivert, enumerate usable interfaces, or start capture.

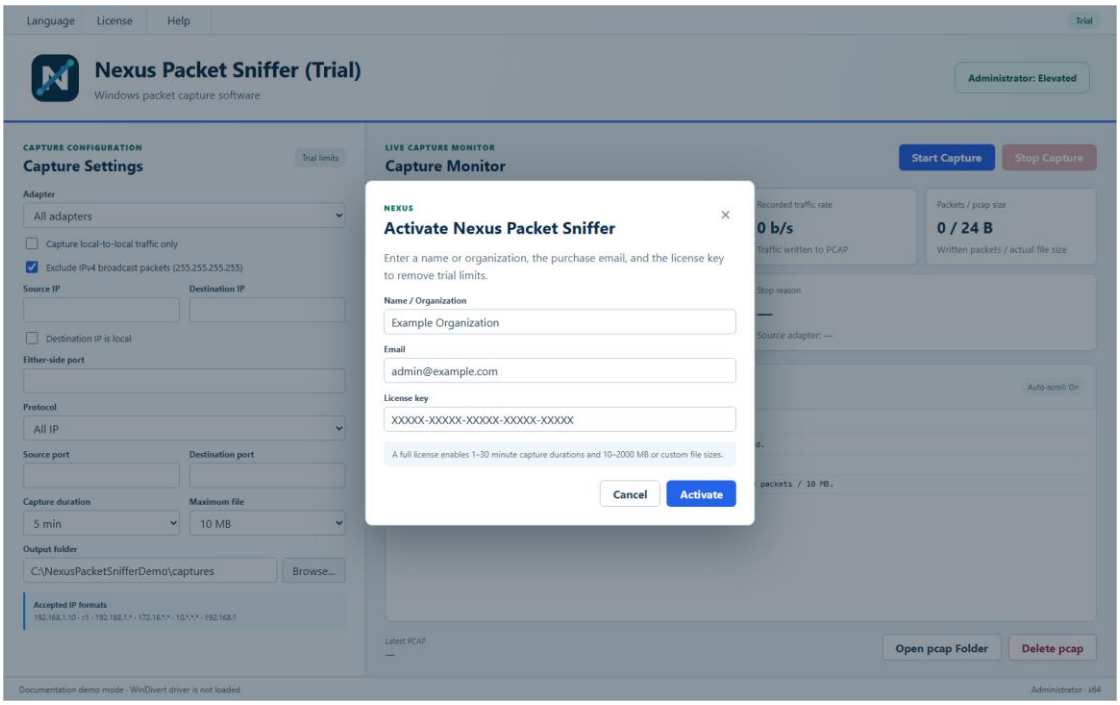
3. Trial, licensing, and activation

Before activation, the product runs in trial mode. The trial verifies the basic workflow but limits duration, packet count, and file size; capture stops at the first limit. A license removes the trial packet-count limit and enables longer durations and larger or custom file sizes.



1. Trial main window and fixed limits

Capability	Trial	Licensed
Maximum duration	5 minutes	1, 3, 5, 10, 15, 20, or 30 minutes
Packet count	50,000 packets	No trial packet-count limit
File size	10 MB	10, 50, 100, 250, 500, 1000, 2000 MB, or custom
Custom size	Hidden/unavailable	Available



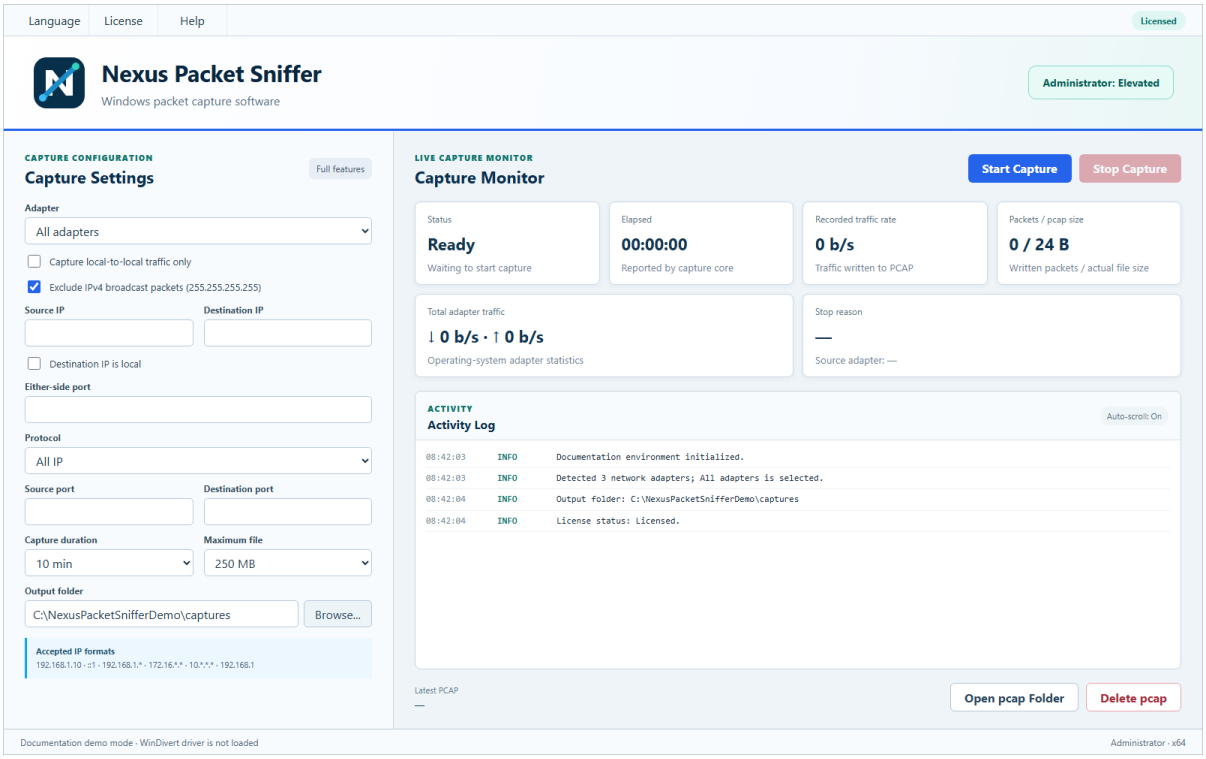
2. License activation dialog

Activation

5. Open the License menu and choose the command to enter a license key.
6. Enter the name or organization, purchase email, and official license key.
7. Select Activate and wait for the status to change to Licensed.
8. Verify that the full duration and file-size options are now available.

4. Main window and menus

The left side of the main window contains capture settings. The right side presents live status and events. The top menus provide language, license, help, and About functions, while the status badge shows Trial or Licensed.



3. Licensed main window

Area	Purpose
Top menus	Language, license, help, and About
Capture settings	Interface, source/destination IP, ports, protocol, and scope options
Limits and output	Duration, file size, and output folder
Controls	Start/stop capture, open the PCAP folder, and delete PCAP files
Live monitor	Status, packet and byte counts, elapsed time, current file, and stop reason
Event log	Startup, write, stop, and error messages

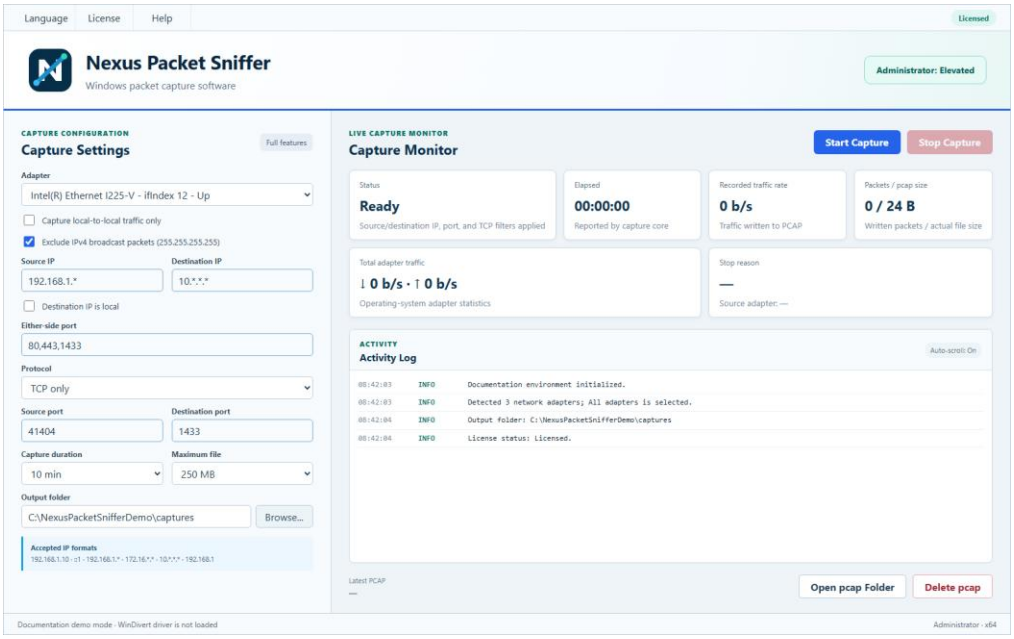
5. Quick start: complete the first capture

9. Start the application as administrator.
10. Select the interface to monitor. If unsure, begin with the physical or virtual interface carrying the traffic.
11. Leave IP and port fields empty and select All IP for a minimal first test.
12. The trial uses fixed limits. For a licensed test, start with 1 minute and 10 MB.
13. Choose an output folder with write permission and sufficient free space.
14. Select Start Capture, generate a small amount of test traffic, and watch packet count and file size increase.
15. Select Stop, wait for Stopped, then open the folder and PCAP.

Important: The first test should create a non-empty .pcap that Wireshark can open. If packet count remains zero, check the interface, direction, and filters.

6. Interface, IP, port, and protocol filters

Source IP, destination IP, source port, destination port, protocol, and scope options are applied together with AND logic. Additional filters improve precision but also make a zero-packet result more likely when conditions do not match.



4. Source/destination IP, port, and TCP filter example

Field	Format and rule
Exact IPv4	For example, 192.168.1.25
Trailing IPv4 wildcard	Examples: 192.168.1.*, 172.16.*.*, 10.*.*.*; wildcards must be a continuous suffix
IPv4 prefix shorthand	For example, 192.168.1, interpreted as that prefix range
IPv6	Valid IPv6 addresses are supported; IPv6 subnet notation and zone IDs are not
Source/destination compatibility	When both are specified, they must use the same IP family
Port	1-65535, comma-separated; for example, 80,443,1433
Protocol	All IP, TCP+UDP, TCP, or UDP
Local only	Restricts capture to loopback/local communication
Destination local	Restricts capture to inbound packets whose destination is local
Exclude broadcast	Excludes only IPv4 limited broadcast 255.255.255.255

7. Duration, file size, and output folder

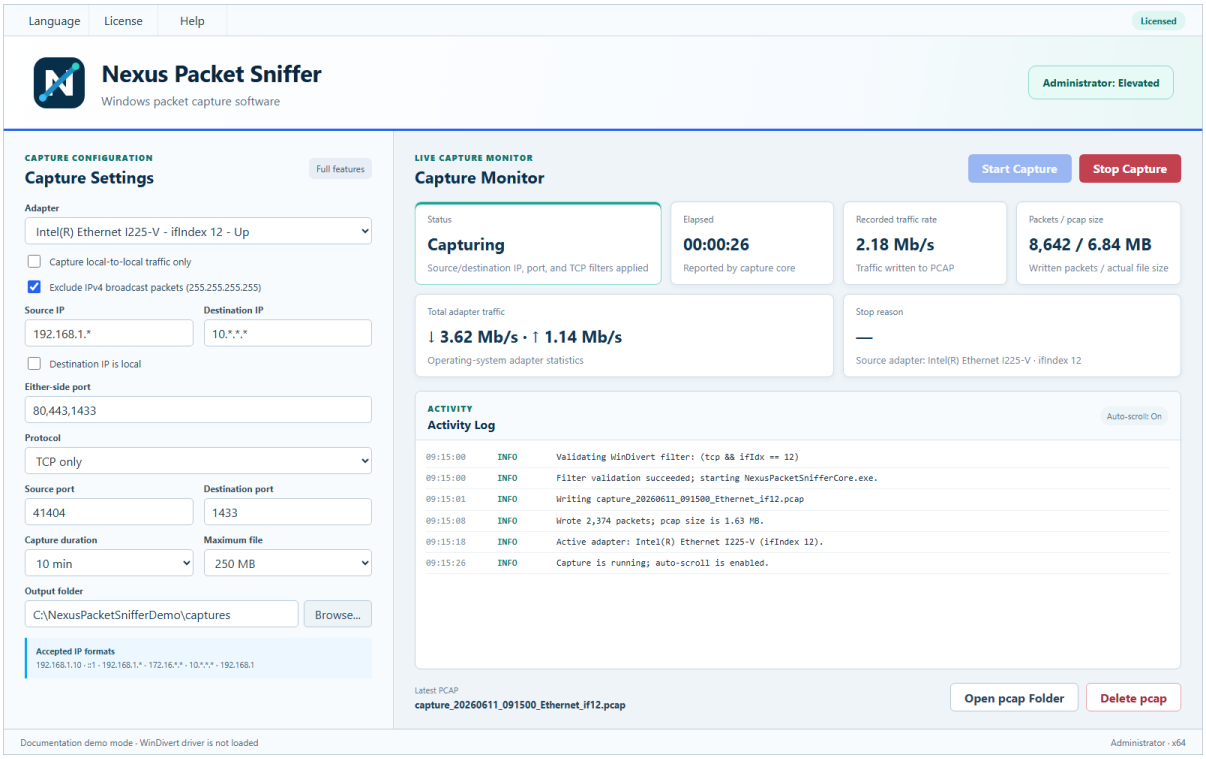
Duration and file size are the primary safeguards for disk usage and evidence scope. A licensed user may select presets or a custom MB value. Trial mode is fixed at 5 minutes, 50,000 packets, and 10 MB.

Setting	Recommendation
Duration	Begin with 1-5 minutes for reproduction; estimate traffic before a long capture
File size	Test with 10-100 MB; a high-volume interface may reach the limit quickly
Custom MB	Licensed only; enter a positive integer and reserve sufficient disk space
Output folder	Use a stable local disk; avoid an unreliable or disconnecting network share
File name	Includes start time and an interface part; a sequence suffix resolves conflicts

Important: Capture stops at the first limit. Selecting 30 minutes does not guarantee a 30-minute file because the size limit may be reached earlier.

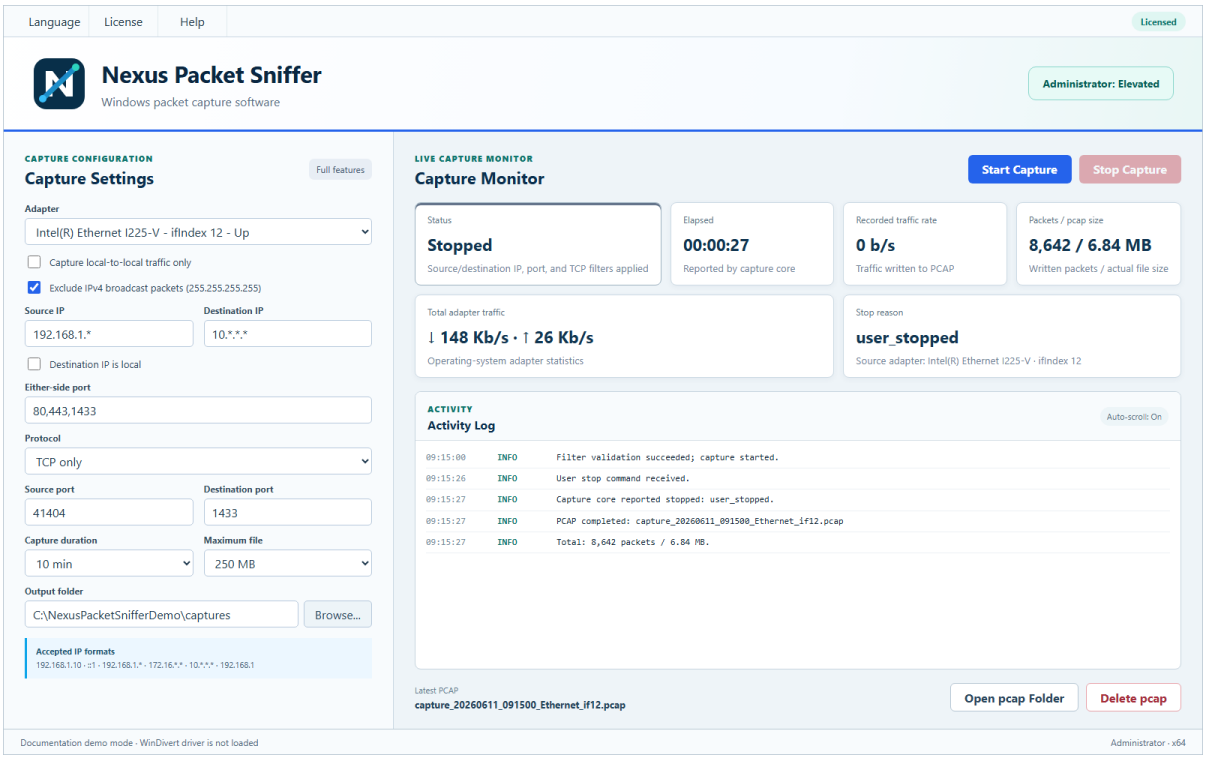
8. Live monitoring and stop conditions

After capture starts, settings are locked to prevent mid-run changes. The monitor continuously updates state and counters. Use the event log to confirm startup, identify the active file, and understand why capture stopped.



5. Live monitoring during capture

Field	How to interpret it
Status	starting, running, stopped, or error
Packets	Number of packets written to PCAP
Bytes	Processed/written byte count as defined by the application
Elapsed	Time elapsed in the current capture
File size	Current PCAP size
Current file	Full output file name for the current capture
Stop reason	User, duration, packet, size, or error condition



6. Completed capture and stop reason

Stop reason	Meaning and next action
user_stopped	The user selected Stop; wait for file closure before opening or moving it
duration_limit	Duration was reached; repeat after checking capacity if more evidence is required
packet_limit	Trial mode reached 50,000 packets
size_limit	File-size limit was reached; narrow filters or raise the licensed limit
error	Core or file-write error; review events, privilege, driver, and disk

Important: After selecting Stop, wait until status is Stopped. Force-closing the process can leave the PCAP incomplete.

9. PCAP format and Wireshark analysis

Output uses classic PCAP and LINKTYPE_ETHERNET. Because the WinDivert NETWORK layer supplies IP packets, the application creates a synthetic Ethernet header for analyzer compatibility. Synthetic MAC addresses are not physical NIC addresses.

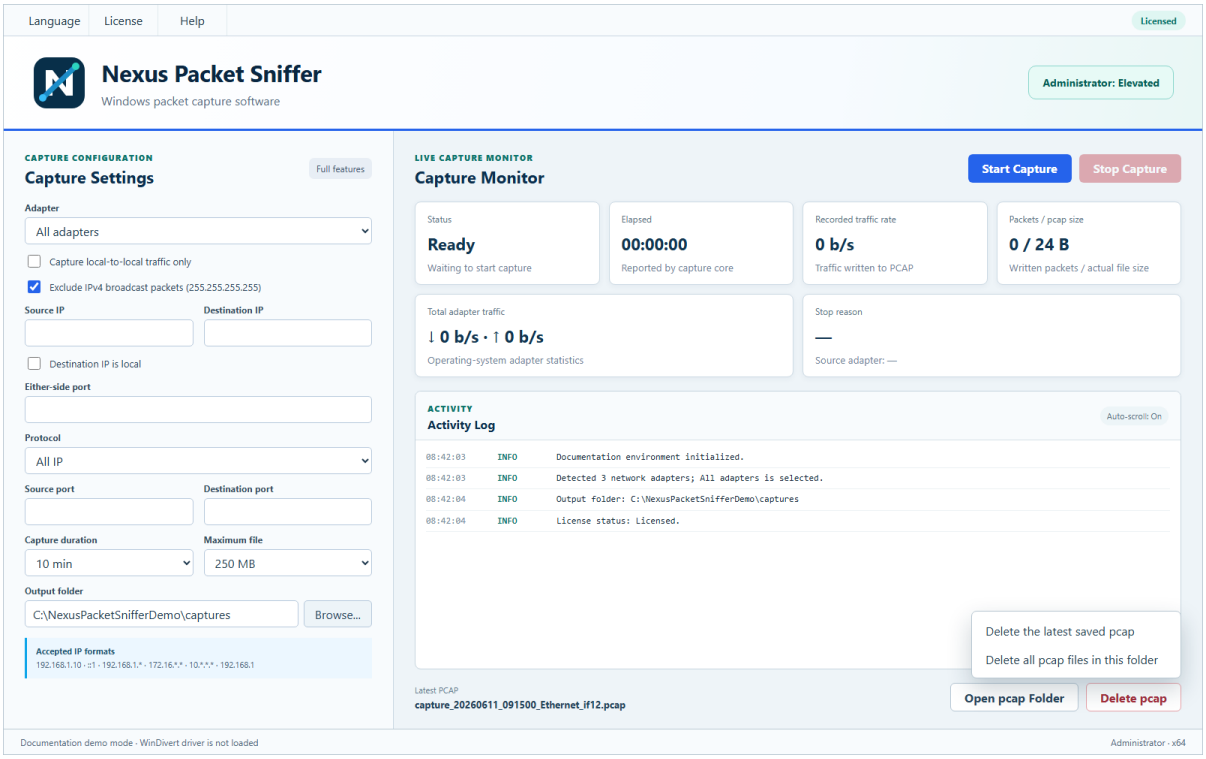
Item	Value/description
Format	Classic PCAP (.pcap)
Link type	LINKTYPE_ETHERNET
Synthetic source MAC	02:00:00:00:00:01
Synthetic destination MAC	02:00:00:00:00:02
Broadcast destination MAC	ff:ff:ff:ff:ff:ff
Payload	Not shown in the UI; retained in PCAP for matching packets

Wireshark workflow

16. Stop capture and confirm that the PCAP has closed.
17. In Wireshark, choose File > Open and select the output .pcap.
18. Narrow the view with display filters such as ip, ipv6, tcp, udp, or tcp.port == 1433.
19. Use network-layer content when evaluating IPs, ports, flags, retransmissions, delay, and payload.
20. Do not infer physical devices, switch paths, or real Layer 2 topology from the synthetic MAC addresses.

10. PCAP file management

The main window can open the current output folder, delete the latest saved PCAP, or delete all PCAP files in that folder. Delete commands are unavailable during capture so the active file cannot be removed.

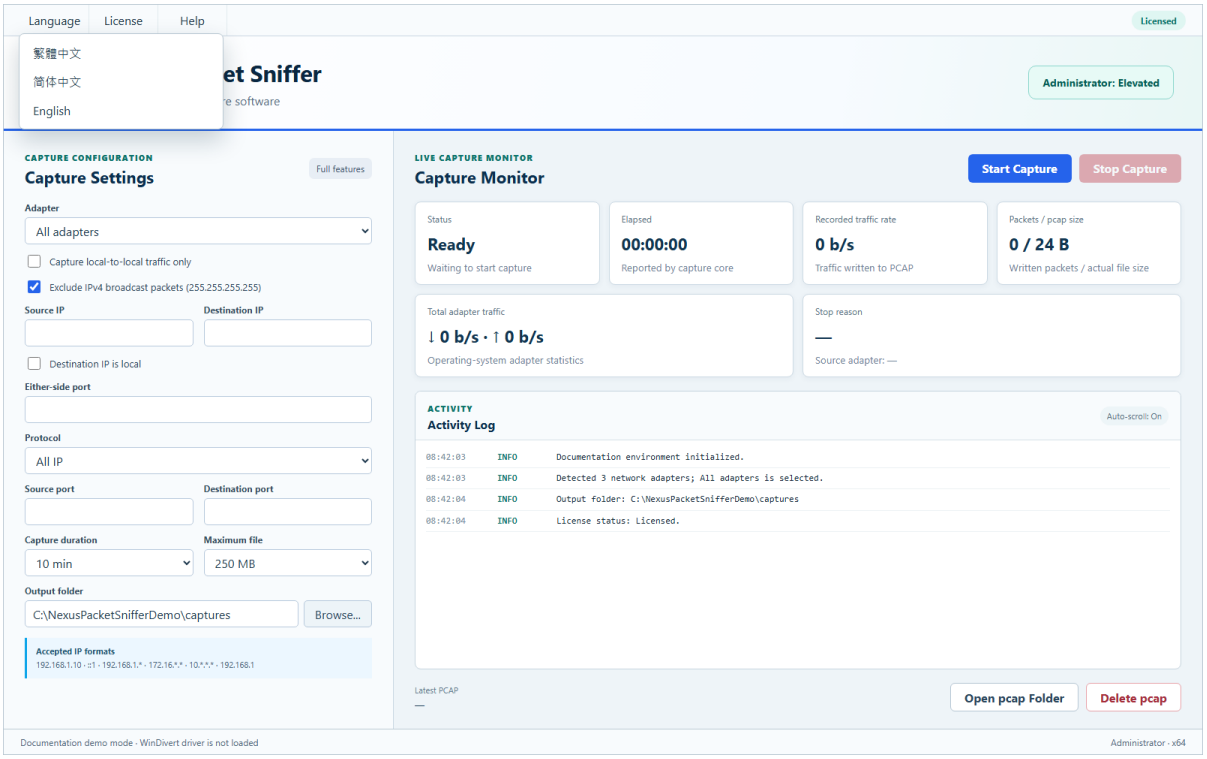


7. PCAP delete menu

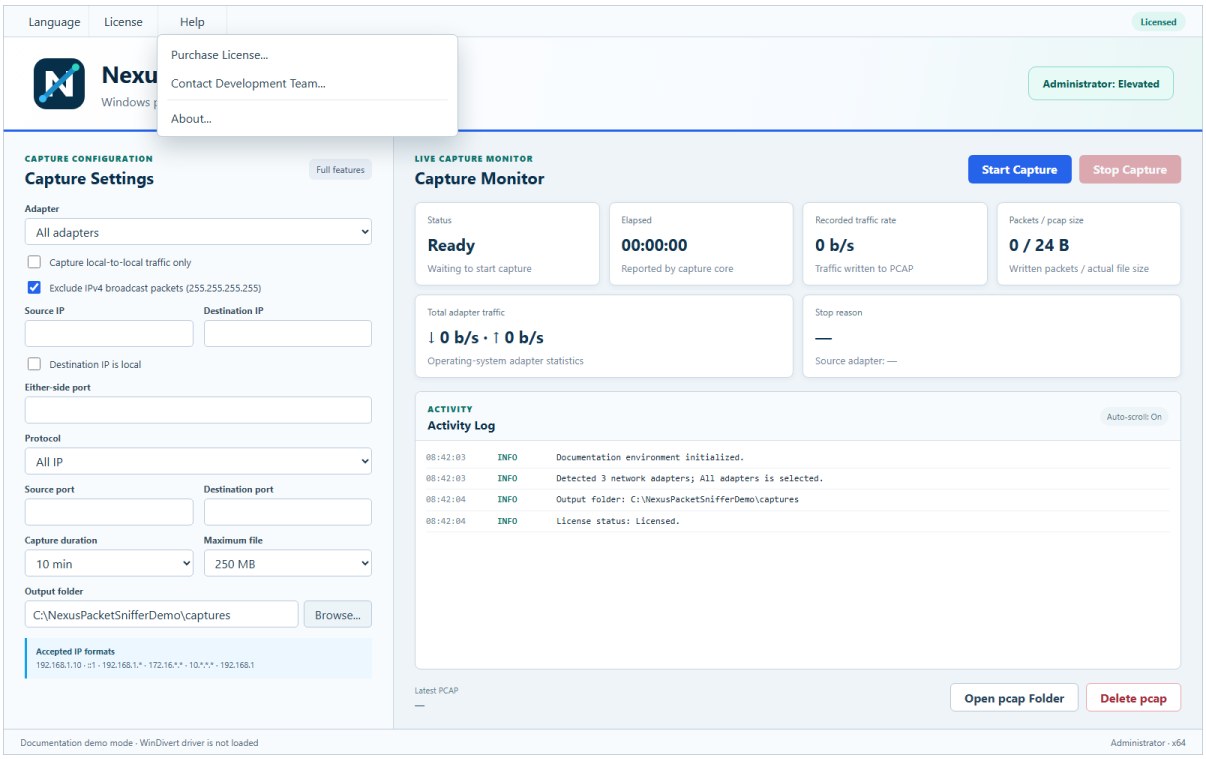
21. Confirm that capture status is Stopped.
22. Use Open pcap Folder to verify the target folder and file names.
23. Before deleting the latest file, confirm that it is no longer needed for analysis or delivery.
24. Before deleting all PCAP files, back up required evidence. The command acts on the currently selected output folder.
25. If deletion fails, close analyzers using the PCAP and verify folder permission.

11. Language, help, and version information

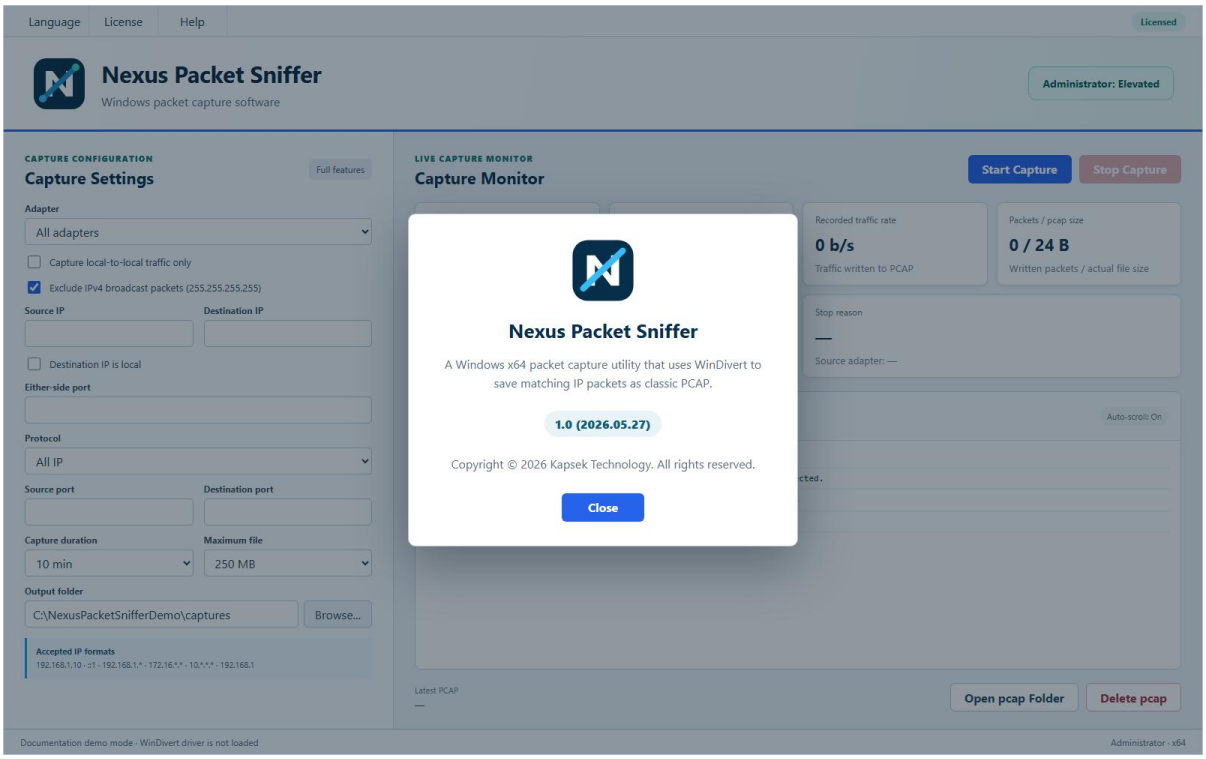
Use the Language menu to switch among Traditional Chinese, Simplified Chinese, and English. Verify that current labels and messages update after switching.



8. Traditional Chinese, Simplified Chinese, and English menu



9. Help and support menu



10. About dialog and version information

26. Use organization-approved channels for Purchase License and Contact Development Team.
27. A support request should include product version, Windows version, reproduction steps, error text, and a sanitized event log.
28. Do not attach an unsanitized PCAP or license key unless support explicitly requests it and transfer is approved.
29. The About dialog reports version 1.0 (2026.05.27); include it with issue reports.

12. Troubleshooting

Symptom	Likely cause	Action
Capture does not start	Not elevated; WinDivert is missing or blocked	Run as administrator; verify x64 components and endpoint protection policy
Packet count stays at zero	Wrong interface, over-filtering, or direction mismatch	Clear IP/ports, select All IP, and identify the interface carrying traffic
Invalid IP format	Wildcard placement or an IPv6 zone ID is invalid	Use an exact address or a valid trailing IPv4 wildcard
Invalid port format	Zero, greater than 65535, or nonnumeric text	Use comma-separated integers from 1 through 65535
PCAP stops quickly	High traffic reached size or trial packet limit	Narrow filters; with a license, raise size or use a shorter reproduction window
PCAP cannot be deleted	Capture is running, Wireshark has it open, or permission is missing	Stop capture, close the analyzer, and verify folder permission
Disk space error	Insufficient capacity in output folder	Clean or change the local folder and lower the file limit
Unexpected MAC in Wireshark	The product uses a synthetic Ethernet header	Analyze IP and transport fields; do not treat the MAC as a physical source

13. Known limitations and operational reference

Known limitations

30. The NETWORK layer does not capture non-IP traffic such as ARP, RARP, or STP.
31. Exclude broadcast applies only to IPv4 limited broadcast 255.255.255.255, not all multicast or IPv6 multicast.
32. IPv4 wildcards must be a continuous suffix; 192.*.1.* is not supported.
33. IPv6 subnet notation and zone IDs are not supported.
34. Source and destination IP filters must use the same IP family when both are set.
35. Payload is not shown in the main UI; inspect PCAP in Wireshark only under approved security conditions.
36. Synthetic Ethernet MAC addresses are not physical MACs and cannot establish Layer 2 ownership.

Operational reference

Category	Operational reference
Trial stop conditions	5 minutes, 50,000 packets, or 10 MB; first limit wins
Licensed duration	1/3/5/10/15/20/30 minutes
Licensed size	10/50/100/250/500/1000/2000 MB or custom
Port	1-65535, comma-separated
IP	Exact IPv4/IPv6; trailing IPv4 wildcard or prefix shorthand
Setting logic	Fields use AND; empty means unrestricted
PCAP naming	capture_{yyyyMMdd_HHmmss}_{adapterPart}.pcap with sequence suffix on conflicts