Nexus Flow User Manual

Windows real-time network flow monitoring, PCAP analysis, and reporting

Item	Information
Product version	1.0.31
Manual version	1.1
Release date	2026-06-11

Contents

1. Product Positioning and Core Capabilities

Nexus Flow is a portable Windows x64 network-flow monitor. It captures local packets with WinDivert, aggregates them into flows, and presents download, upload, packet rate, active connections, DNS, country, ASN, and risk information by host, service, and process.

Primary use cases

1. Observe TCP, UDP, ICMP, IPv4, and IPv6 traffic between the local computer and remote hosts.
2. Narrow the scope by interface, direction, port, IP/CIDR, process name, or PID.
3. Review Top Hosts, Top Services, Top Programs, and traffic such as SQL Server TDS.
4. Import classic PCAP/CAP for offline aggregation or continuously write live packets to PCAP.
5. Deliver flow details or summaries as CSV, JSON, Excel, HTML, or PDF.

Supported scope

Item	Current support
Platform	Windows x64; WPF / .NET 8; portable EXE
Live capture	WinDivert; administrator privileges required
Data sources	Live capture, classic .pcap, .cap
Dimensions	Flow, host, service, process, DNS, country, ASN, risk, notification
Output	PCAP, CSV, JSON, XLSX, HTML, PDF

2. Processing Model and Data Flow

Nexus Flow separates packet capture, flow aggregation, name enrichment, risk evaluation, and presentation. Understanding this path helps explain when filters take effect and why DNS, process, or GeoIP fields may be populated later.

Stage	Input	Primary work	Output
Capture	Local interface packets or classic PCAP	WinDivert sniff mode or offline file reading	Packet samples
Aggregation	Packet samples	Build flows by direction, address, port, and protocol	Flow records and statistics
Enrichment	Remote IP, port, and PID	Service, process, DNS, country, ASN, and organization	Readable fields

Stage	Input	Primary work	Output
Presentation	Flows and summaries	Overview, Inspect, Hosts, Services, and Programs	Live views
Delivery	Accumulated data	CSV, JSON, Excel, HTML, PDF, and PCAP	Reports or capture files

6. Core capture, aggregation, search, and report generation run locally.
7. Network access is used only when the user updates GeoIP/ASN data or enables a webhook.
8. Left-side port, IP, and process filters affect retained or displayed flows. Global search primarily filters views and does not rewrite a source PCAP.
9. DNS, process, and GeoIP/ASN enrichment depends on caches, privileges, database version, and packet timing, so values can temporarily remain unknown.

3. Requirements, Deployment, and Startup

The release is delivered as a ZIP archive. It includes the .NET runtime and does not require a separate .NET, Microsoft Office, or PDF installation.

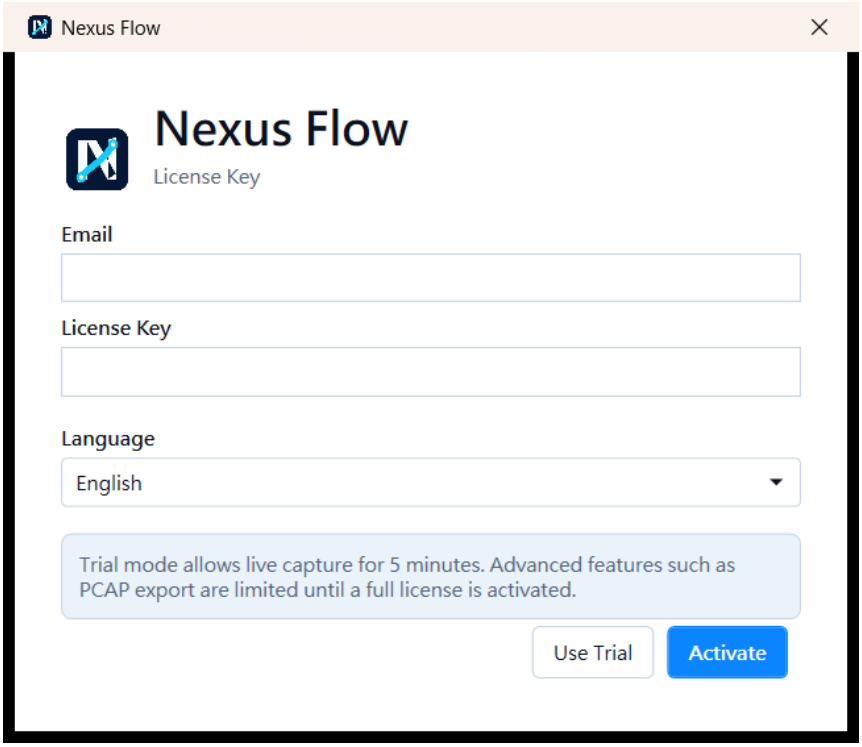
Item	Requirement
Operating system	Windows 10 or Windows 11 x64; use a supported, updated release
Privileges	Run as administrator so the WinDivert driver can load
Storage	Space for the application, logs, GeoIP/ASN data, PCAP, and reports; usage grows with traffic and retention
Network	Live capture needs no cloud service; online GeoIP/ASN updates require internet access

Deployment and startup

10. Extract NexusFlow_Portable_v1.0.31_WinDivert_KapsekSelfSigned.zip to a trusted local folder. Do not run the executable from inside the ZIP.
11. Confirm that NexusFlow.exe and the packaged third-party notices are present.
12. Right-click NexusFlow.exe and select Run as administrator.
13. If SmartScreen or endpoint protection prompts, verify the source, signature, and hash according to organizational policy.
14. At first startup, choose a language and activate a license or select Use Trial.

4. Licensing, Trial Mode, and Product Information

The license window supports Traditional Chinese, Simplified Chinese, and English. A full license is validated offline from an email address and 25-character key. License data is protected with Windows DPAPI under the current Windows user.



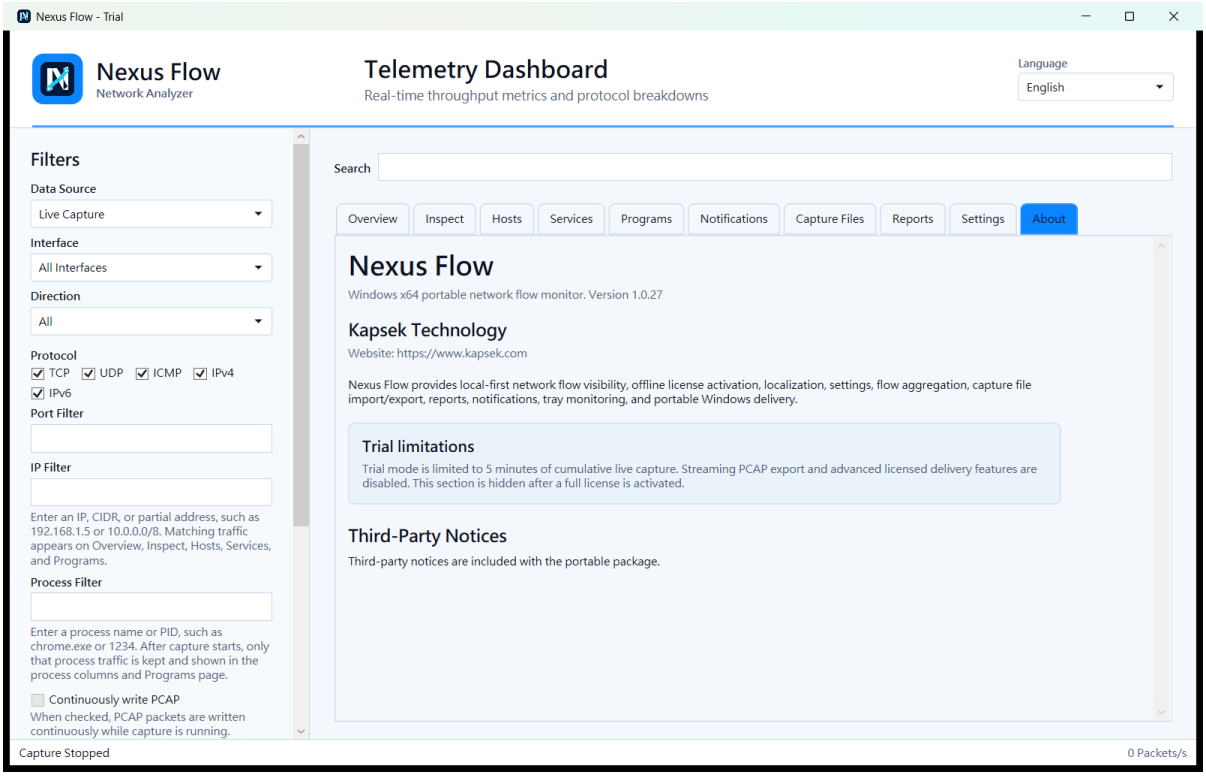
1. The license window provides language selection, Email and license-key entry, and access to the five-minute trial.

Feature	Trial	Full license
Live capture	5 cumulative minutes	No trial-time limit
Continuous PCAP / PCAP export	Disabled	Available
CSV / JSON / Excel / HTML / PDF	Disabled	Available
PCAP import and on-screen analysis	Available	Available

Activate a full license

15. Select the required language in the license window.
16. Enter the email address used to purchase the license.
17. Enter the key in XXXXX-XXXXX-XXXXX-XXXXX-XXXXX format.
18. Select Activate. The main-window title shows Licensed after success.

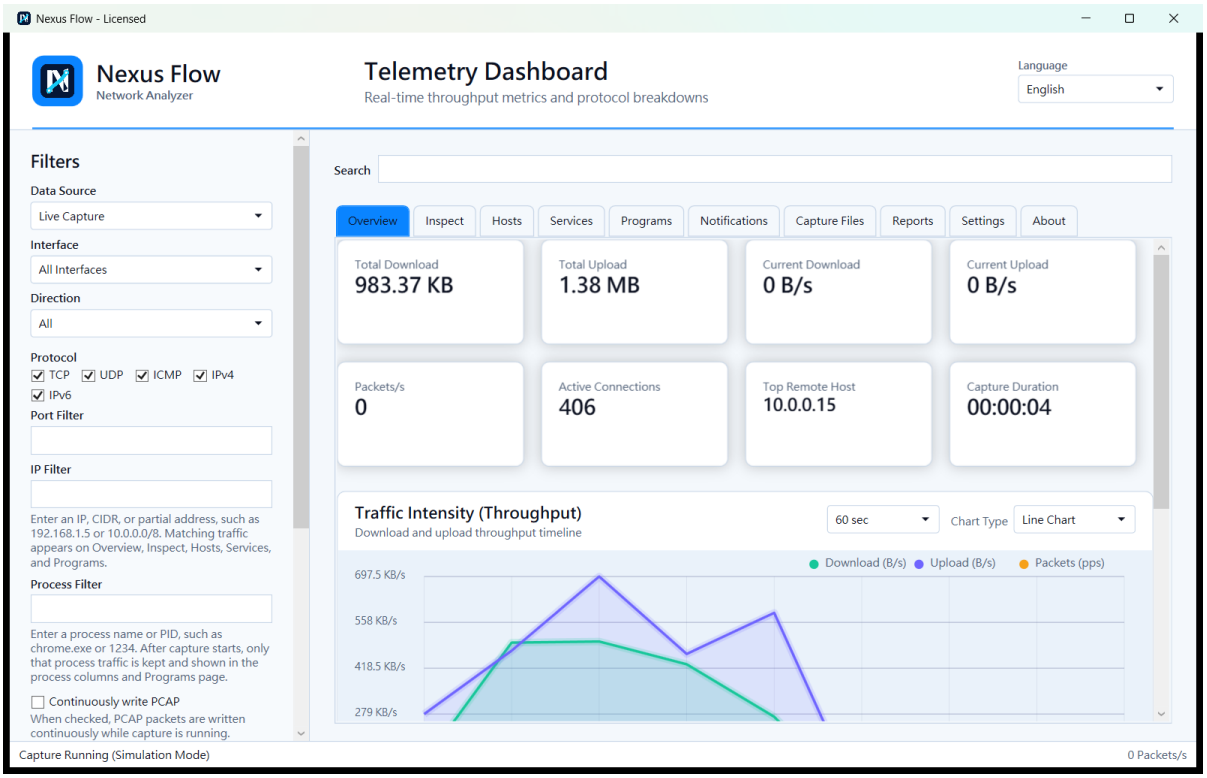
19. For evaluation, select Use Trial. Trial time accrues only while live capture is running.



2. About describes the product, third-party notices, and trial restrictions; its displayed version can differ from the delivery version.

5. Main Window and Work Areas

The main window contains a header, left filter/action panel, search box, ten functional tabs, and a bottom status bar. Language changes are available in the upper-right corner; the theme follows Windows.



3. Overview combines eight live metrics, a traffic timeline, Top Hosts, and Top Services.

Area	Purpose
Header	Product name, dashboard title, and language selector
Left panel	Data source, interface, direction, protocols, port/IP/process filters, PCAP, and capture controls
Search	Keyword matching across flows, hosts, services, programs, notifications, and capture files
Tabs	Overview, Inspect, Hosts, Services, Programs, Notifications, Capture Files, Reports, Settings, About
Status bar	Capture state, simulation/production state, and current packet rate

6. First Capture: Quick Start

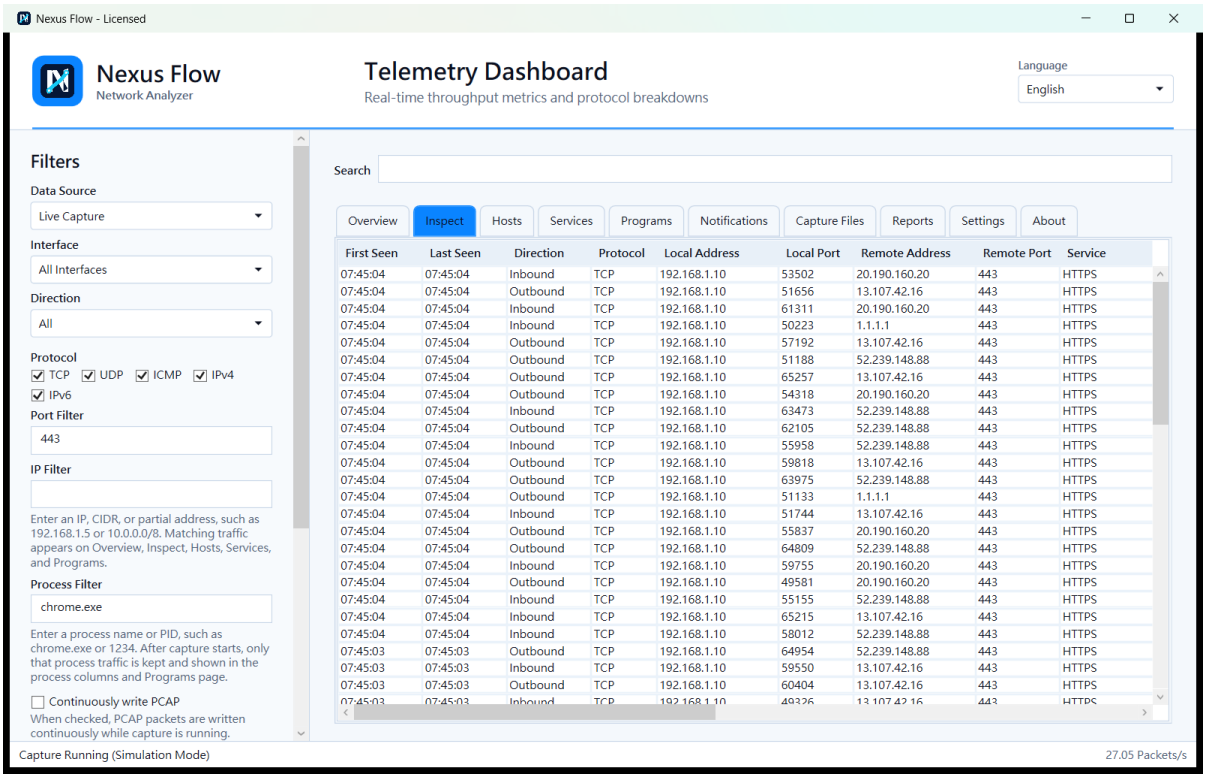
20. Start the application as administrator and activate it or select trial mode.
21. Choose Live Capture under Data Source.
22. Select All Interfaces or one interface, then configure direction and protocols.
23. Enter a port, IP/CIDR, process name, or PID when needed.

24. To retain raw packets, licensed users can enable Continuously write PCAP before capture.
25. Select Start Capture and confirm the bottom status bar shows capture running.
26. Review data on Overview, Inspect, Hosts, Services, or Programs.
27. Select Stop Capture when finished, then export reports or review the PCAP as required.

Important: Pause UI stops screen refresh only. Background capture and aggregation continue. Use Stop Capture to release capture activity and stop trial-time accounting.

7. Live Capture, Filters, and UI Pause

Control	Usage and examples
Data source	Live Capture, or PCAP Import followed by file selection
Interface	All Interfaces or a specific physical/virtual adapter
Direction	All, Inbound, Outbound
Protocol	TCP, UDP, ICMP, IPv4, IPv6; multiple selections allowed
Port	443; 80,443; 10000-10100
IP	192.168.1.5; 10.0.0.0/8; or a partial address
Process	chrome.exe; sqlservr.exe; or PID 1234



4. Port 443 and chrome.exe filter scenario; Inspect retains matching HTTPS flows.

Control	Actual behavior
Start Capture	Starts with the current interface, direction, protocols, and filters; changing some controls during capture restarts and clears statistics
Stop Capture	Stops WinDivert, ends trial timing, and closes the continuous PCAP writer
Pause UI	Stops display refresh while underlying capture may continue; press again to resume
Clear Statistics	Clears current flows, summaries, and charts without deleting PCAP files already written
Export CSV	Exports the complete accumulated Flow collection; global search does not automatically constrain it
Export PCAP	During capture, toggles continuous writing on or off rather than creating a true one-time snapshot

28. Confirm filters before capture. Changing interface, direction, or protocol during capture restarts capture and clears existing statistics.

29. Port, IP, and process text filters affect subsequent aggregation and display. Stop and clear statistics when a clean comparison baseline is required.

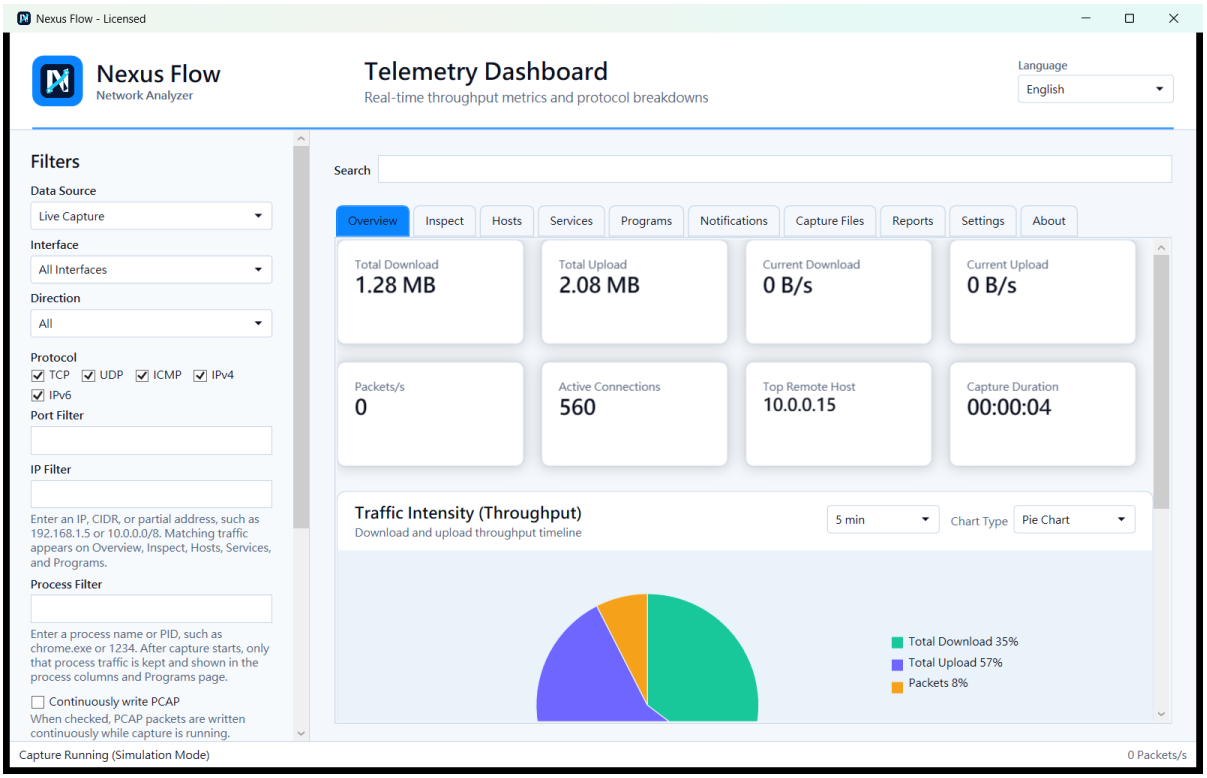
30. Clear Statistics removes current flows and charts but does not automatically stop active capture.

31. Pause UI temporarily freezes the display for reading; select it again to resume updates.

8. Overview Metrics and Traffic Charts

Metric	How to interpret it
Total Download / Upload	Bytes accumulated since capture start or the last statistics reset
Current Download / Upload	Rate calculated for the latest sampling interval
Packets/s	Packets per second during the latest sampling interval
Active Connections	Flows currently considered active by the aggregator
Top Remote Host	Remote IP with the largest accumulated traffic
Capture Duration	Elapsed time since capture start or statistics reset

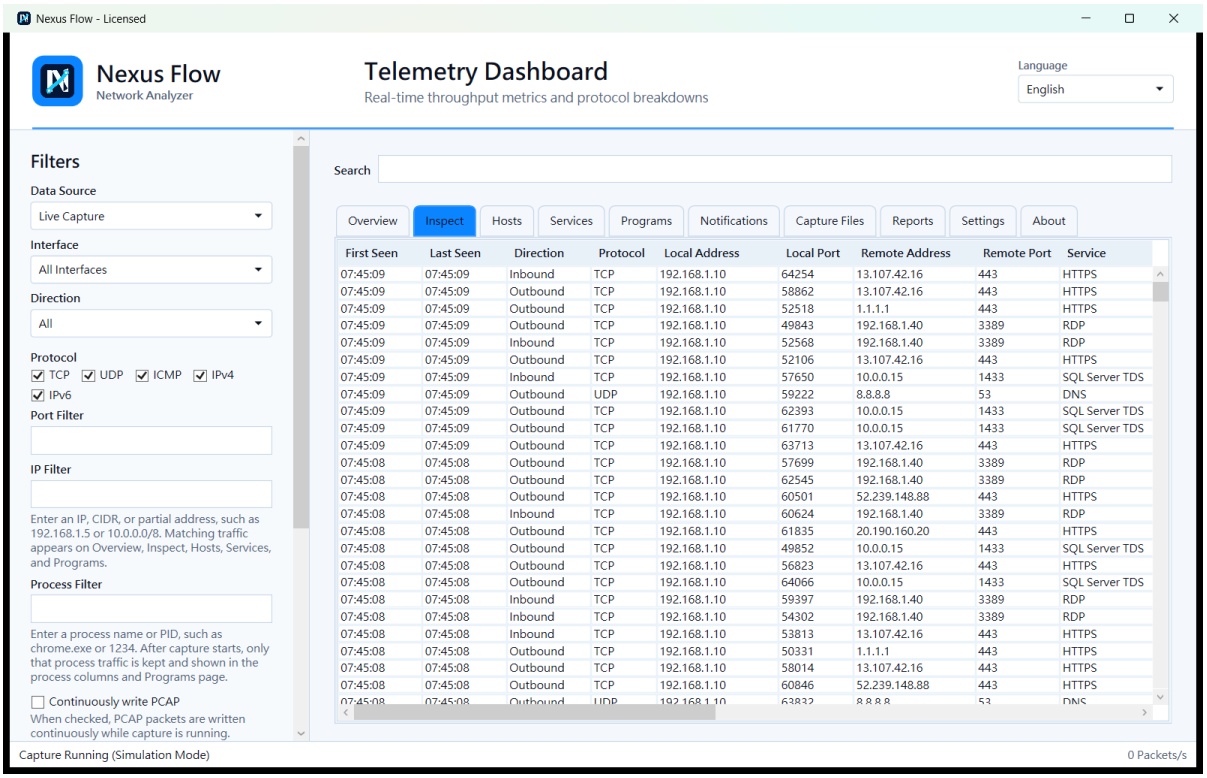
Setting	Options and use
Time range	60 seconds, 5 minutes, 15 minutes, or 30 minutes
Line	Compare download, upload, and packet-rate trends
Area	Emphasize traffic magnitude and time distribution
Bar	Compare download and upload at individual sample points
Pie	Compare accumulated download, upload, and packet shares



5. The pie chart presents the share of accumulated download, upload, and packet volume.

9. Inspect Details and Global Search

Inspect lists individual flows. The displayed columns are First Seen, Last Seen, Direction, Protocol, Local Address, Local Port, Remote Address, Remote Port, Service, Process, PID, Country, ASN, Domain, Packets, Bytes, Status, and Risk. Use the horizontal scrollbar for later columns.

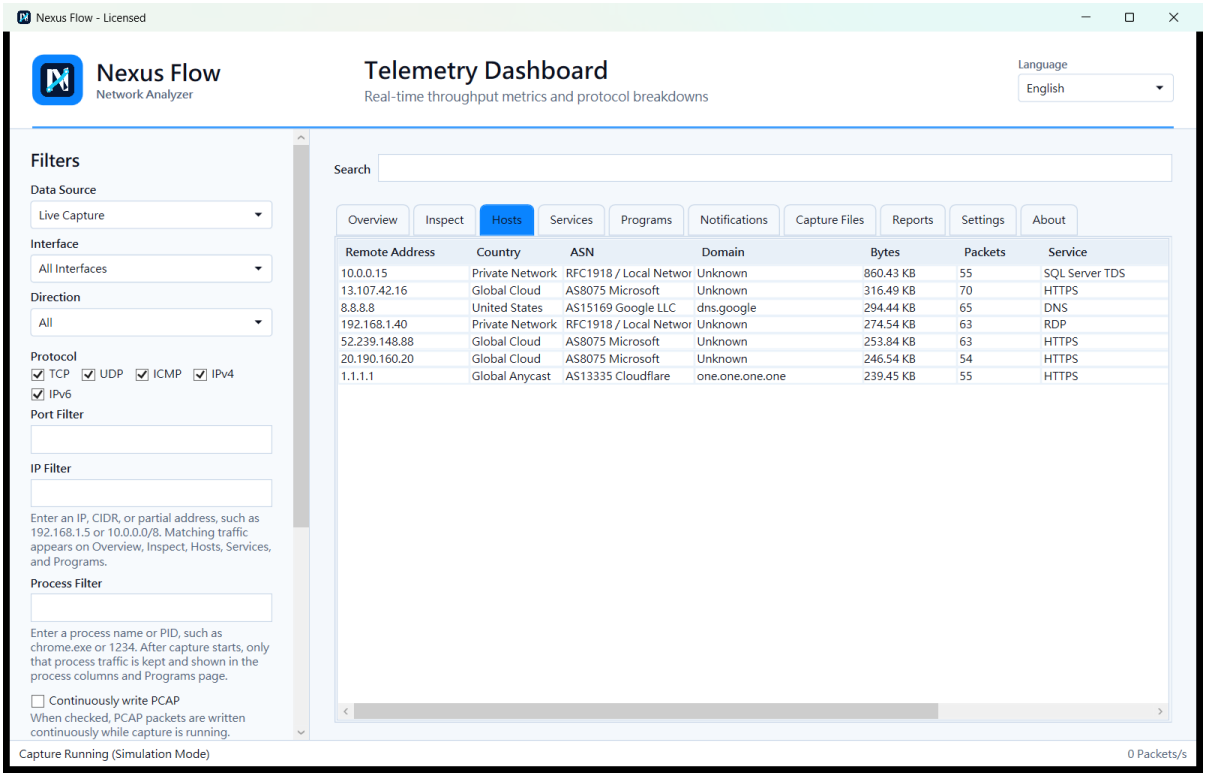


6. Inspect presents each flow with time, direction, endpoints, service, process, and traffic fields.

Field group	Contents	Primary use
Time	First Seen and Last Seen	Locate the activity interval and duration
Network	Direction, protocol, local/remote IP and port	Confirm peers and service-side port
Application	Service, process, PID, and domain	Identify purpose and initiating application
Identity	Country, ASN, and Domain	Identify network ownership and resolved names; requires GeoIP/ASN data
Statistics	Packets, bytes, status, and risk	Sort and investigate by volume or risk

Important: Global search filters the current views. CSV and Excel export use the complete Flow collection, so the visible search result must not be assumed to be the export scope. Filter the exported file separately when delivering a subset.

10. Hosts Analysis

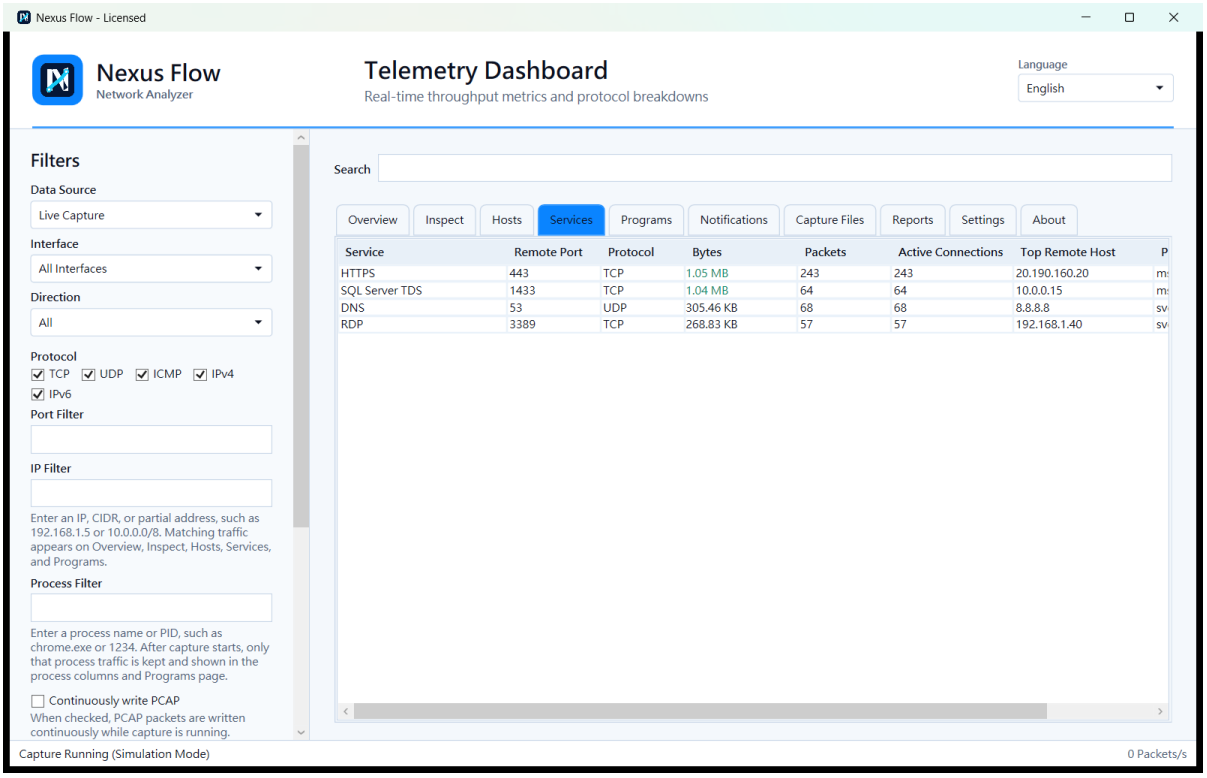


7. Hosts aggregates country, ASN, domain, traffic, packets, services, and processes by remote IP.

Field	Description
Remote IP / Country / ASN	Remote endpoint and its geographic/network ownership
Domain	Derived from DNS cache or reverse resolution; Unknown does not mean no connection
Bytes / Packets	Accumulated volume for the remote IP in the current statistics period
Services / Processes	Summary of services and local applications that communicated with the host
Risk	Normal or Blacklisted, based on product blacklist data

1. Use global search to narrow the data, then sort by bytes, packets, or active connections.
2. Use Hosts to investigate a suspicious IP, Services to investigate a port or protocol, and Programs to investigate a local application.
3. All three summary pages are affected by left-side port, IP, and process filters, but each uses a different aggregation dimension.

11. Services Analysis

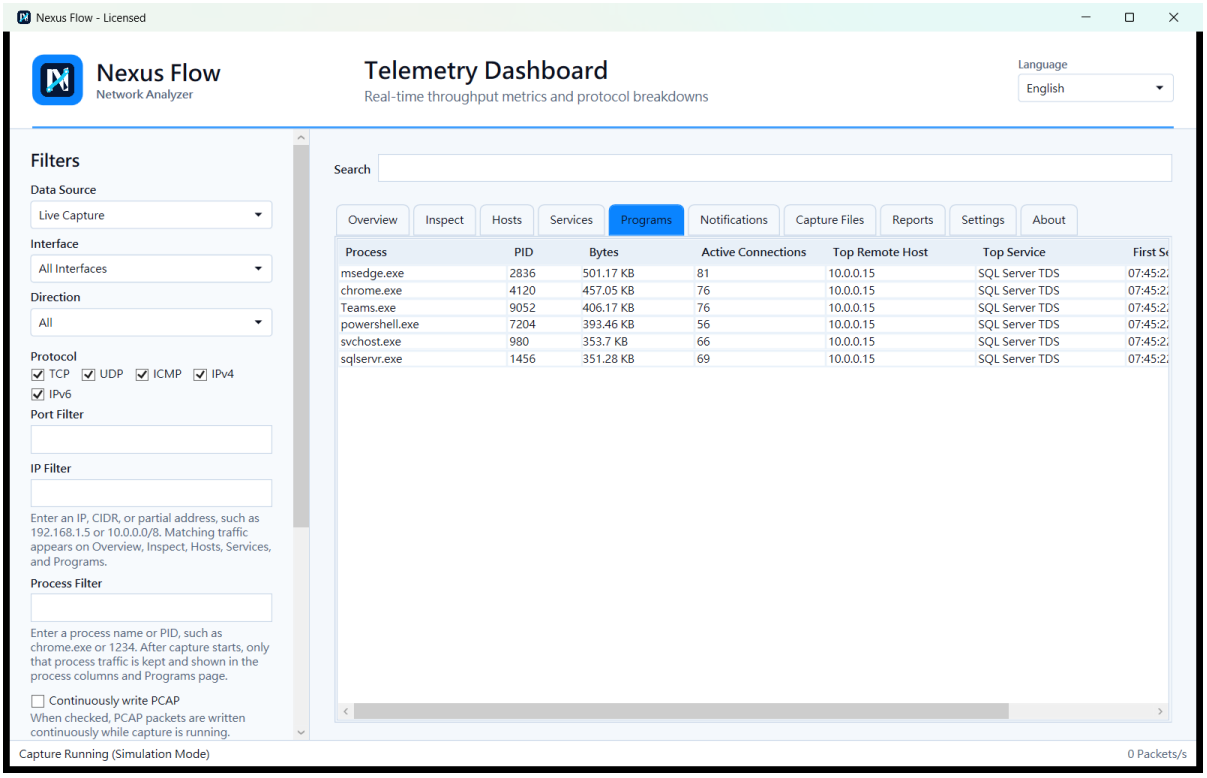


8. Services aggregates traffic, packets, and leading endpoints by service, remote port, and protocol.

Field	Description
Service / Remote Port / Protocol	For example HTTPS 443/TCP, DNS 53/UDP, or SQL Server TDS 1433/TCP
Bytes / Packets	Totals for the service and protocol during the current statistics period
Active Connections	Related flows still considered active
Top Remote Host	Remote IP with the largest traffic for the service
Top Process	Local application using the service most heavily

1. Use global search to narrow the data, then sort by bytes, packets, or active connections.
2. Use Hosts to investigate a suspicious IP, Services to investigate a port or protocol, and Programs to investigate a local application.
3. All three summary pages are affected by left-side port, IP, and process filters, but each uses a different aggregation dimension.

12. Programs Analysis



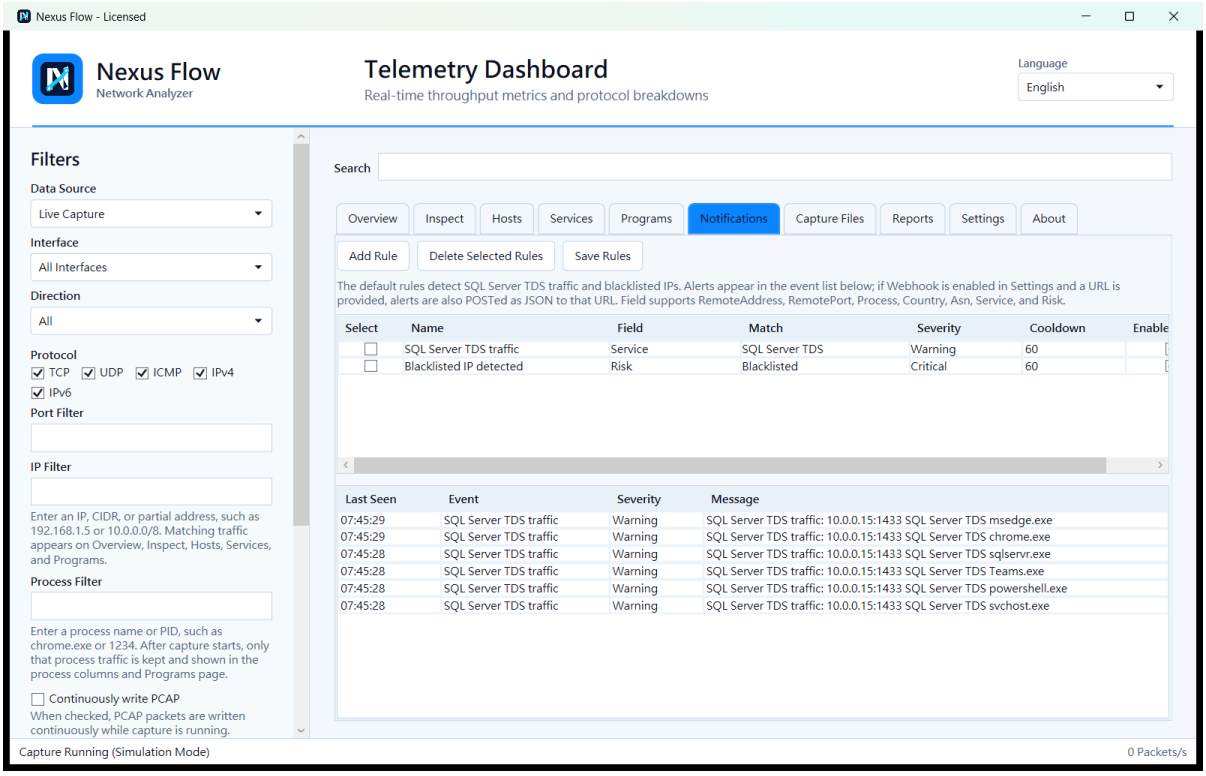
9. Programs aggregates traffic, connections, leading remote host, and service by process and PID.

Field	Description
Process / PID	Inferred from Windows connection-owner data; short flows can remain Unknown
Bytes / Active Connections	Accumulated traffic and currently active flows for the process
Top Remote Host / Service	Quick indication of the application's principal destination and purpose
First / Last Seen	Observed activity range during the current capture

1. Use global search to narrow the data, then sort by bytes, packets, or active connections.
2. Use Hosts to investigate a suspicious IP, Services to investigate a port or protocol, and Programs to investigate a local application.
3. All three summary pages are affected by left-side port, IP, and process filters, but each uses a different aggregation dimension.

13. Notification Rules, Events, and Webhooks

Notifications contains editable rules and an event list. Default rules detect SQL Server TDS service traffic and blacklisted IP addresses. A match creates an on-screen event and, when enabled, sends JSON through an HTTP POST webhook.



10. Notifications manages rules in the upper grid and matched events in the lower grid.

1. Select Add Rule and complete Name, Field, Match, Severity, Cooldown, and Enabled.
2. Field supports RemoteAddress, RemotePort, Process, Country, Asn, Service, and Risk.
3. Select Save Rules to persist the grid. To remove rules, select them in the Select column and choose Delete Selected Rules. Unsaved edits should not be treated as deployed configuration.
4. Matched events appear in the lower grid. Cooldown suppresses repeated events from the same rule.
5. When a webhook is enabled, events are also sent as HTTP POST JSON. Failures are logged and do not block capture.

Field	Description
Name	Rule name
Field	Accepted values: RemoteAddress, RemotePort, Process, Country, Asn, Service, Risk
Match	Case-insensitive substring match; blank values do not trigger

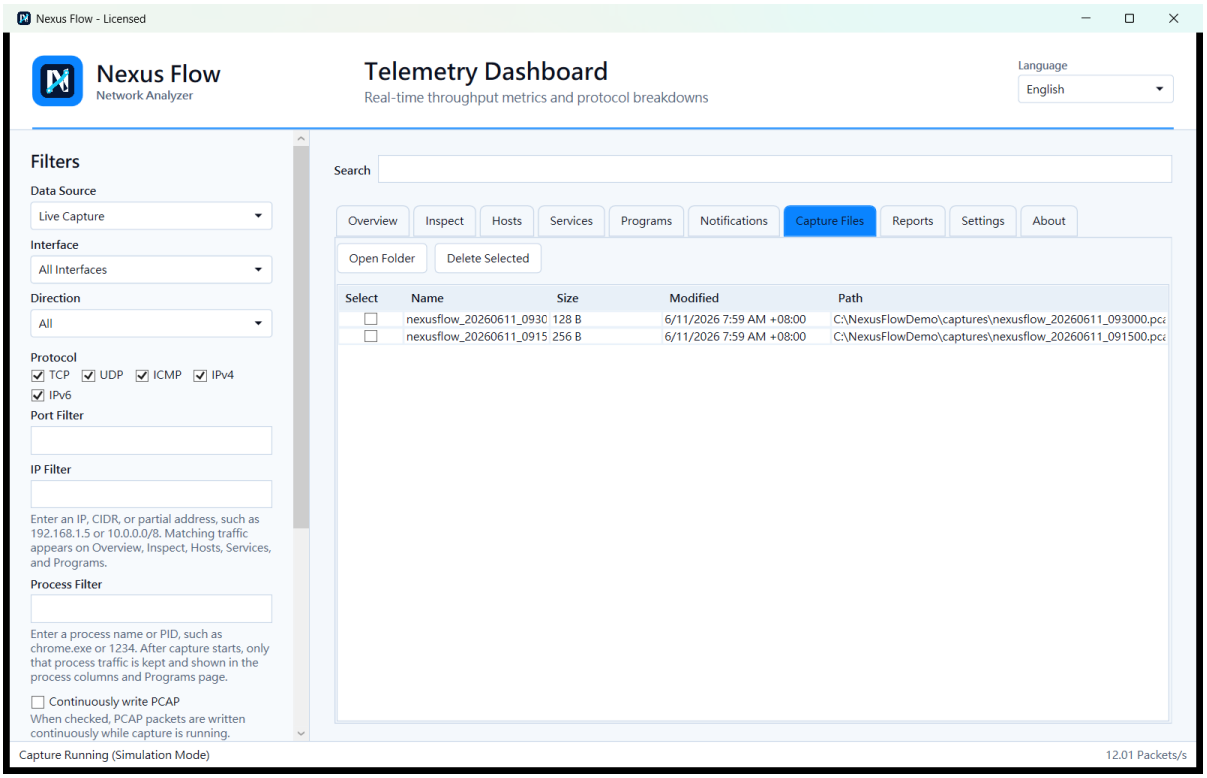
Field	Description
Severity	For example Info, Warning, Critical; included in the event and webhook
Cooldown	Delay before the same rule, remote endpoint, and process can fire again
Enabled	Clear to stop evaluating the rule

Note: Webhook JSON contains product, eventType, severity, time, remoteAddress, remotePort, process, country, and asn. Nexus Flow does not add a signature or delivery queue. Use HTTPS, authenticate the receiver, and tolerate duplicate or missing events.

14. PCAP Import, Continuous Writing, and Capture File Management

With a full license, Nexus Flow can continuously write live packets and can import existing classic PCAP/CAP. PCAP may contain sensitive network data and should follow organizational retention and access controls.

Task	Operation	Important behavior
Import an offline file	Under Data Source, choose PCAP Import and select .pcap or .cap	The picker displays .pcapng, but the current reader does not parse PCAPNG
Start live writing	Select Continuously write PCAP before capture, or select Export PCAP (one-time current records) during capture	Disabled in trial; filename is nexusflow_yyyyMMdd_HHmmss.pcap
Stop writing	Stop capture or select Export PCAP (one-time current records) again	The file closes fully and the capture list refreshes only after stopping
Manage files	On Capture Files, select Open Folder or choose files and select Delete Selected	Deletion cannot be undone; an open file may fail to delete



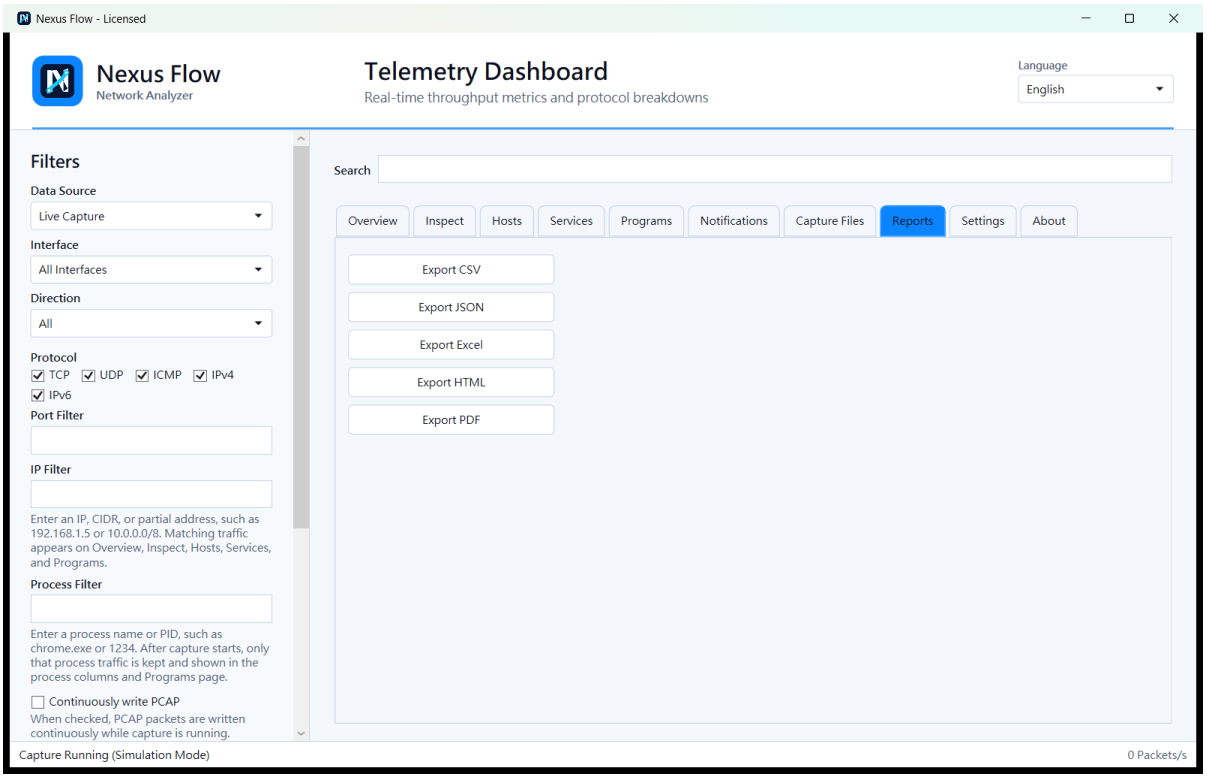
11. Capture Files lists PCAP name, size, modified time, and full path.

Feature	Operation and result
Start-of-capture writing	Enable Continuously write PCAP, then start capture; creates nexusflow_yyyyMMdd_HHmmss.pcap
Toggle writing during capture	Select the left Export PCAP button while capture is running. Despite its one-time wording, the current behavior starts or stops continuous writing
Capture Files	Lists .pcap files in the default captures directory; open the folder or delete selected files
PCAP import	Choose PCAP Import and select classic .pcap or .cap
Format	Classic PCAP, LINKTYPE_RAW 101

Warning: The file picker lists .pcapng, but the current version does not parse PCAPNG and reports it as unsupported. Convert the file to classic .pcap with Wireshark or tshark first.

15. Report Export and Delivery

Licensed users can export five formats from Reports. After completion, Nexus Flow displays the path and selects the output file in File Explorer.



12. Reports provides CSV, JSON, Excel, HTML, and PDF output.

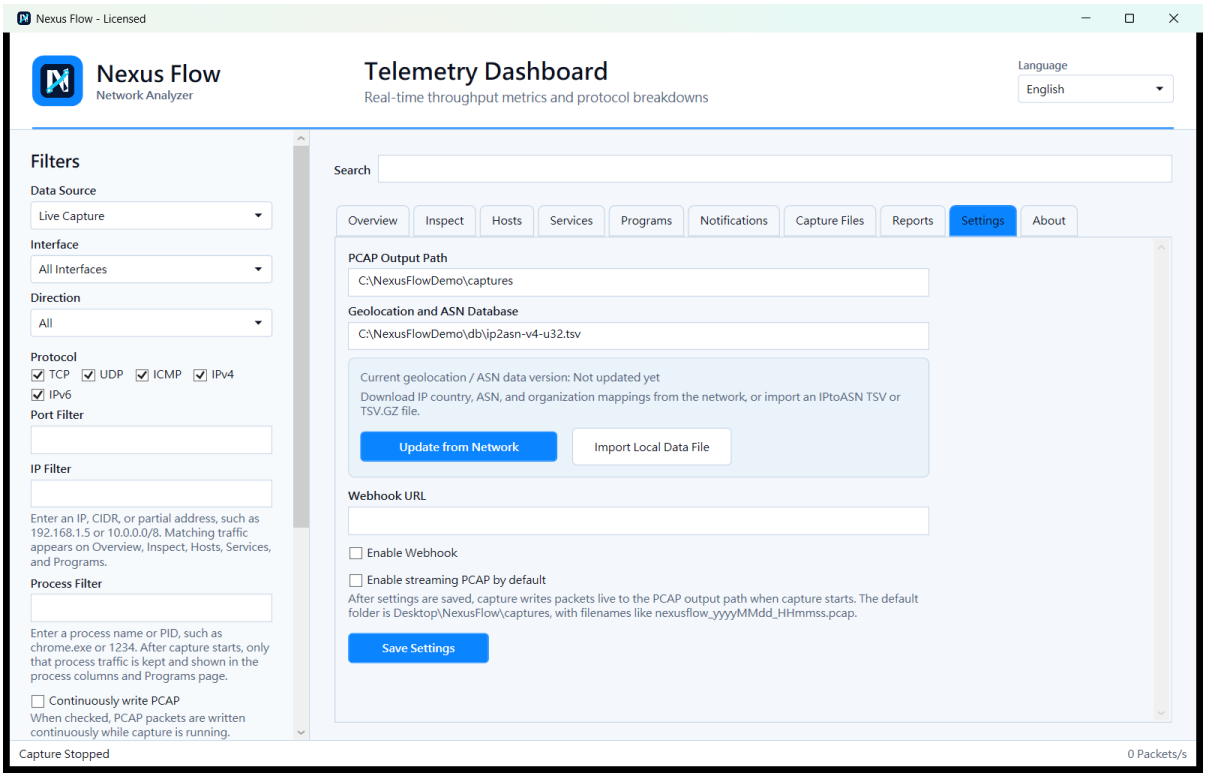
1. Complete a live capture or PCAP import and confirm that Inspect and the summary pages contain data.
2. Open Reports and select Export CSV, Export JSON, Export Excel, Export HTML, or Export PDF.
3. After export, Nexus Flow displays the output path and opens the containing folder.
4. Before delivery, verify times, endpoints, processes, DNS, country/ASN, and character encoding, then redact sensitive information as required.

Format	Content	Default subfolder
CSV	All flow details; UTF-8	reports\csv
JSON	Snapshot, Top 50 Hosts/Services/Programs, Top 100 notifications	reports\json
Excel	All flow details; .xlsx; Office not required	reports\excel
HTML	Browser-readable summary	reports\html
PDF	Compact summary and Top Hosts	reports\pdf

Warning: Reports can include internal/external IP addresses, process names, domains, country, ASN, and notifications. The built-in PDF favors ASCII text. Prefer HTML, Excel, CSV, or JSON when non-ASCII text must be preserved.

16. Settings, GeoIP/ASN, and Background Monitoring

Settings centralizes PCAP Output Path, Geolocation and ASN Database, Webhook URL, Enable Webhook, and Enable streaming PCAP by default. Values are saved in settings.json for the current Windows user.



13. Settings controls PCAP paths, GeoIP/ASN, webhooks, and default continuous writing.

Setting	Effect
PCAP output path	Destination used for continuous writing and button-started writing
Geolocation and ASN Database	Path to ip2asn-v4-u32.tsv; update online or import .tsv/.tsv.gz
Webhook URL / Enable Webhook	POST notification events as JSON to the specified endpoint
Enable streaming PCAP by default	After saving, automatically writes PCAP at next capture start; disabled in trial
Save Settings	Writes settings.json and synchronizes the left-panel PCAP path

1. The PCAP output path is synchronized to the left-side capture controls.
2. Under Geolocation and ASN Database, select Update from Network or Import Local Data File for IPtoASN TSV/TSV.GZ. Existing flows receive enrichment on later refreshes.
3. Use a controlled HTTPS webhook endpoint. The receiver is responsible for authentication, retention, and retry policy.
4. Default continuous PCAP writing applies only to a full license; trial mode clears the setting.

5. When minimized, the main window can hide in the system tray. The tray menu provides Show, start/stop capture, Mini Window, and exit commands.

17. Troubleshooting

Problem	Likely cause	Action
Administrator prompt	WinDivert requires elevation	Restart as administrator; verify UAC and endpoint policy
Capture does not start	Driver blocked, signature/privilege issue, invalid filter	Review error code and nexusflow.log; verify runtime and security policy
No data on screen	Overly narrow filters, wrong interface/direction, no current traffic	Select All Interfaces and All under Direction; clear filters
Trial stops automatically	Five cumulative capture minutes used	Activate a full license; PCAP import remains available
PCAPNG import fails	PCAPNG is not supported	Convert to classic .pcap first
Webhook receives no event	Disabled, wrong URL, TLS/firewall block	Verify settings and receiver logs; test an HTTPS endpoint
Report buttons unavailable	Trial mode	Activate a full license
Country/ASN not populated	Database not downloaded/imported	Update or import IPtoASN TSV/TSV.GZ in Settings
Window missing after minimize	Hidden in system tray	Double-click the Nexus Flow icon or select Show

18. Security, Privacy, and Known Limitations

Security and privacy

1. Capture, aggregation, license validation, and report generation run locally. Only user-enabled GeoIP update and webhook features contact external endpoints.
2. license.dat and trial.dat use Windows DPAPI and are normally decryptable only by the same Windows user.
3. The WinDivert runtime is under ProgramData. The production application restricts ACLs and cleans related driver services at exit.
4. PCAP, flows, domains, processes, and notifications can be sensitive or personal data. Obtain authorization and apply retention controls.
5. Deleting the portable application folder does not automatically remove LocalAppData, ProgramData, desktop PCAP, or reports.

Known limitations

1. Nexus Flow monitors and analyzes traffic; it does not block, modify, or inject packets and is not a firewall.
2. The current release does not provide PCAPNG parsing, maps, cloud accounts, centralized management, a Windows service, or MSI/MSIX.
3. Process mapping and DNS/GeoIP results depend on privileges, cache, database version, and packet timing.
4. Main-window search filters the display only and does not automatically restrict report exports to visible rows.
5. The About-page text version may differ from the 1.0.31 delivery. Use formal release information as the authority.