Nexus TDS Insight User Manual

SQL Server TDS packet analysis, login identification, and report export

Product version	1.0 (20260527)
Manual version	1.0
Release date	2026-06-10

Contents

1. Product Overview

Nexus TDS Insight is a portable Windows tool for analyzing SQL Server TDS traffic. It reads PCAP/PCAPNG files locally, rebuilds TCP sessions, detects TDS, TLS, LOGIN7, SSPI, SQL_BATCH, and RPC traffic, and summarizes clients, servers, login identities, databases, applications, SQL statements, and observed session duration.

Primary use cases

1. Identify which clients, accounts, and applications connected to SQL Server.
2. Review SQL statements and session timing during incident response or change validation.
3. Identify TLS sessions and determine when login data is hidden by encryption.
4. Export filtered findings as CSV, HTML, or PDF, or preserve the complete parse result as JSON.

Supported scope

Input formats	Classic PCAP and PCAPNG
Network encapsulation	Ethernet, Linux SLL, raw IPv4/IPv6, and VLAN
Core protocols	TCP, SQL Server TDS, and TLS record detection
Login data	LOGIN7 and some NTLM Type 3 identities; Kerberos identities are usually unavailable from packet contents alone
Outputs	Session list, details, CSV, JSON, HTML, and PDF

2. System Requirements and Startup

Most users should start the product from dist\NexusTDSInsight.exe. Python, Node.js, and IIS are not required. The launcher extracts the web assets to the current user's local application data folder and opens them in the default browser.

Operating system	Windows 10 or Windows 11; use a currently supported release
Permissions	Standard user permissions; access to protected capture files may require additional file permissions
Browser	A modern browser with JavaScript, File API, and WebCrypto support
Memory	Usage grows with capture size; split large captures into smaller time windows
Network	Analysis is offline; purchase and support links require Internet access

Startup

5. Open the dist subfolder in the product directory.
6. Run NexusTDSInsight.exe.
7. If Windows displays an Unknown Publisher or SmartScreen warning, verify the file source and hash before proceeding under your organization's policy.
8. Confirm that the header shows Nexus TDS Insight version 1.0 (20260527).

The About dialog shows the product name, version, and copyright.

3. Licensing and Trial Mode

Without a valid license, the product runs in trial mode. The license is stored in the current browser's local storage. Changing browser profiles, clearing site data, or using another Windows account may require reactivation.

Capability	Trial mode	Licensed
Visible sessions	First 10 sessions that contain a DB user	All parsed sessions
Sessions without DB user	Hidden	Visible
CSV / JSON / HTML / PDF	Disabled	Enabled
Header badge	Trial mode	Licensed owner

Activation

9. Select 授權 (License) at the top, then 輸入授權金鑰... (Enter license key).
10. Enter the name or organization, email address, and license key used for the purchase.
11. Select 驗證授權 (Validate license). The header badge and export buttons update immediately after success.
12. A revoked or blacklisted license is rejected. A previously stored license may also be removed at startup.

The license dialog requests the owner or organization, email address, and license key.

4. Main Screen

The main screen contains the top menus, product header, input area, search toolbar, notification center, session table, and details panel.

Initial trial-mode screen. Export buttons are disabled while unlicensed or when no result is available.

Area	Purpose
License / Help	View license state, enter a license, open purchase/support links, and view version information
Product header	Shows version and license state; contains CSV/JSON/HTML/PDF and Clear actions
PCAP / PCAPNG	Select or drag a capture file; parsing starts automatically
SQL Server Port	Defaults to 1433; accepts multiple comma-separated ports
PFX / PEM / Key	Provides RSA private-key material; PFX/P12 can use a password
Counters	Packets, TCP streams, and SQL sessions
Search / filters	Keyword search and All / Has user / TLS filters
Notifications	Trial restrictions, TLS decryption messages, and parse warnings

5. Quick Start

Use the following workflow for a first analysis.

13. Check the license state. Activate the product first if all sessions or report export are required.

14. Enter the SQL Server port. Separate multiple ports with commas, for example 1433,14330.
15. To attempt TLS 1.2 RSA decryption, enter the PFX/P12 password before selecting PFX/P12/PFXA, or select a PEM/KEY private key.
16. Select a PCAP/PCAPNG file or drag it into the dashed drop area.
17. Wait for the counters and session table to update. Parsing occurs locally and depends on capture size.
18. Use search, filters, and column sorting to locate the target session.
19. Select a session row to inspect details and SQL statements.
20. Confirm the active filters, then export the required report format.

Important: A successful parse updates packet, TCP stream, and SQL session counters and displays at least one table row. A TLS session with a blank user is still a connection; review the notification center before drawing conclusions.

6. Capture and Decryption Settings

Setting	Operation and effect
PCAP / PCAPNG	One capture at a time; choosing another file replaces the current result
SQL Server Port	Default 1433; integers from 1 through 65535, separated by commas
Include port-only TCP sessions	Lists matching TCP sessions even when TDS/TLS is not identified
PFX / P12 password	Changing the value or pressing Enter reruns the current capture
Clear	Removes the capture, key files, password, search, filters, notifications, and details

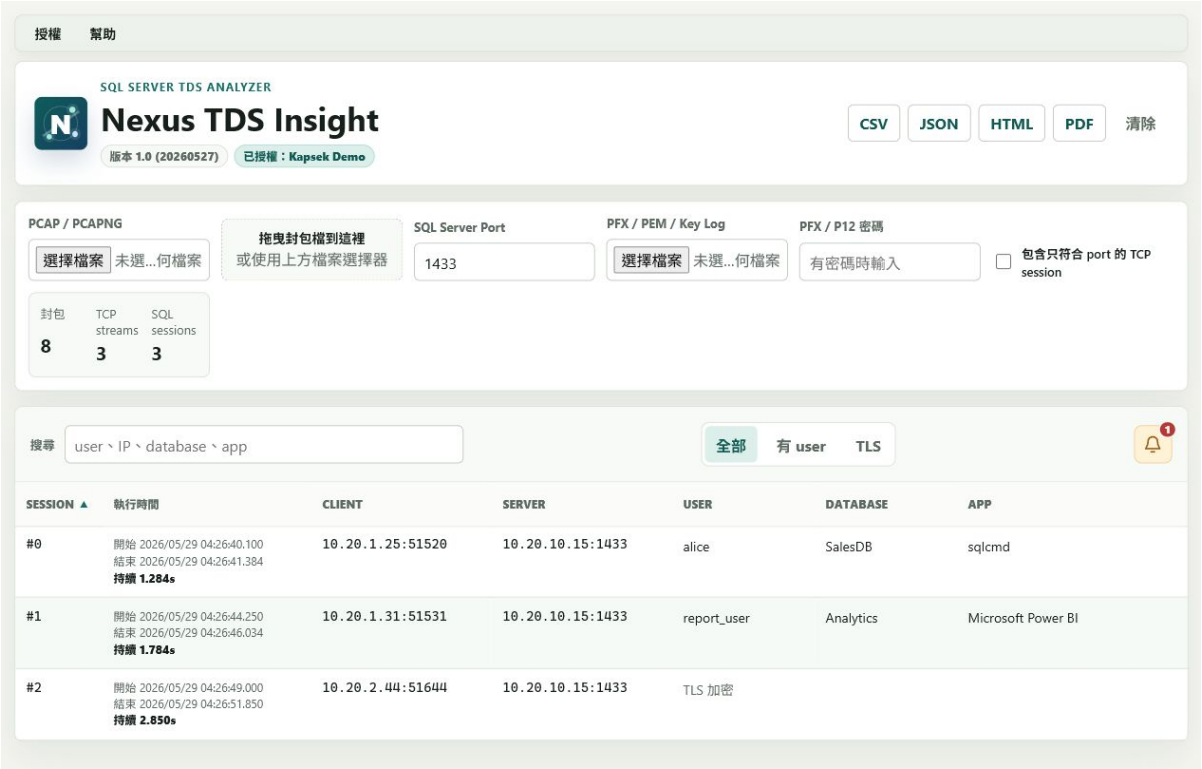
TLS decryption capabilities and limits

21. The browser version attempts to read RSA private keys from PEM, KEY, TXT, or PFX/P12/PFXA files.
22. This works only when the capture contains a full handshake using a supported TLS 1.2 RSA key-exchange suite.
23. TLS 1.2 ECDHE, TLS 1.3, and resumed TLS without the full handshake/master secret cannot be decrypted with the server private key alone.
24. The picker label includes Key Log/.log, but the current browser implementation does not consume key logs. Use an advanced TShark/key-log workflow instead.

25. Private keys and passwords are sensitive. Use them only on controlled endpoints under your organization's key-management policy.

7. Session List, Search, and Filters

After parsing, the table displays one row per TCP stream. Scroll horizontally for all columns. Select a column heading to toggle ascending or descending order, and drag a column boundary to resize it. Sort state and widths are retained in the current browser.



Licensed sample result with two identified logins and one TLS session.

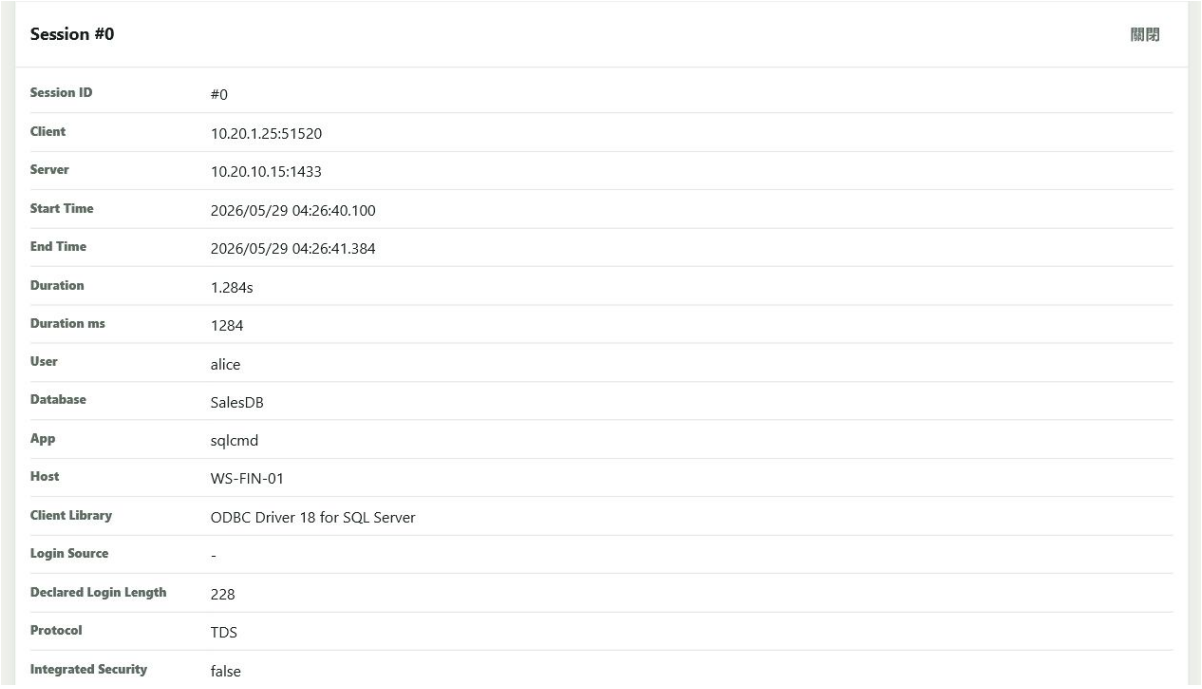
26. Search covers session ID, client/server IP, user, database, app, host, SQL, encryption information, and notes.
27. Has user keeps only sessions with a parsed display user.
28. TLS keeps only sessions where TLS was detected.
29. CSV, HTML, and PDF use the currently licensed, searched, and filtered session set.

Column	Meaning
Session	Internal TCP stream identifier
Duration	Observed start, end, and difference for the stream in the capture
Client / Server	Inferred client and SQL Server IP:port endpoints

Column	Meaning
User	LOGIN7 or visible NTLM identity; may be blank when encrypted
Database	Database requested in LOGIN7; not necessarily the effective database principal
App	LOGIN7 application name, such as sqlcmd, Power BI, or a custom application
SQL	Preview of the first statement; complete statements are in Session Details
Protocol	TDS, TLS, TDS + TLS, or TCP
Status	USER, TLS, TDS, or PORT

8. Session Details

Select any session row to expand the details panel. Selecting another row replaces the contents; use 關閉 (Close) to collapse the panel.



Upper Session Details: endpoints, timing, user, database, application, and client library.

Login Source	-
Declared Login Length	228
Protocol	TDS
Integrated Security	false
TLS Detected	false
TDS Detected	true
TDS Types	LOGIN7, SQL_BATCH, TABULAR_RESULT
Encryption	-
Prelogin Details	{ "client": [], "server": [] }
Bytes C->S	426
Bytes S->C	9
TCP Segments	3
SQL Count	1
SQL Statements	-- #1 SELECT TOP (20) OrderId, CustomerName, TotalAmount FROM dbo.Orders ORDER BY OrderDate DESC;
Notes	-

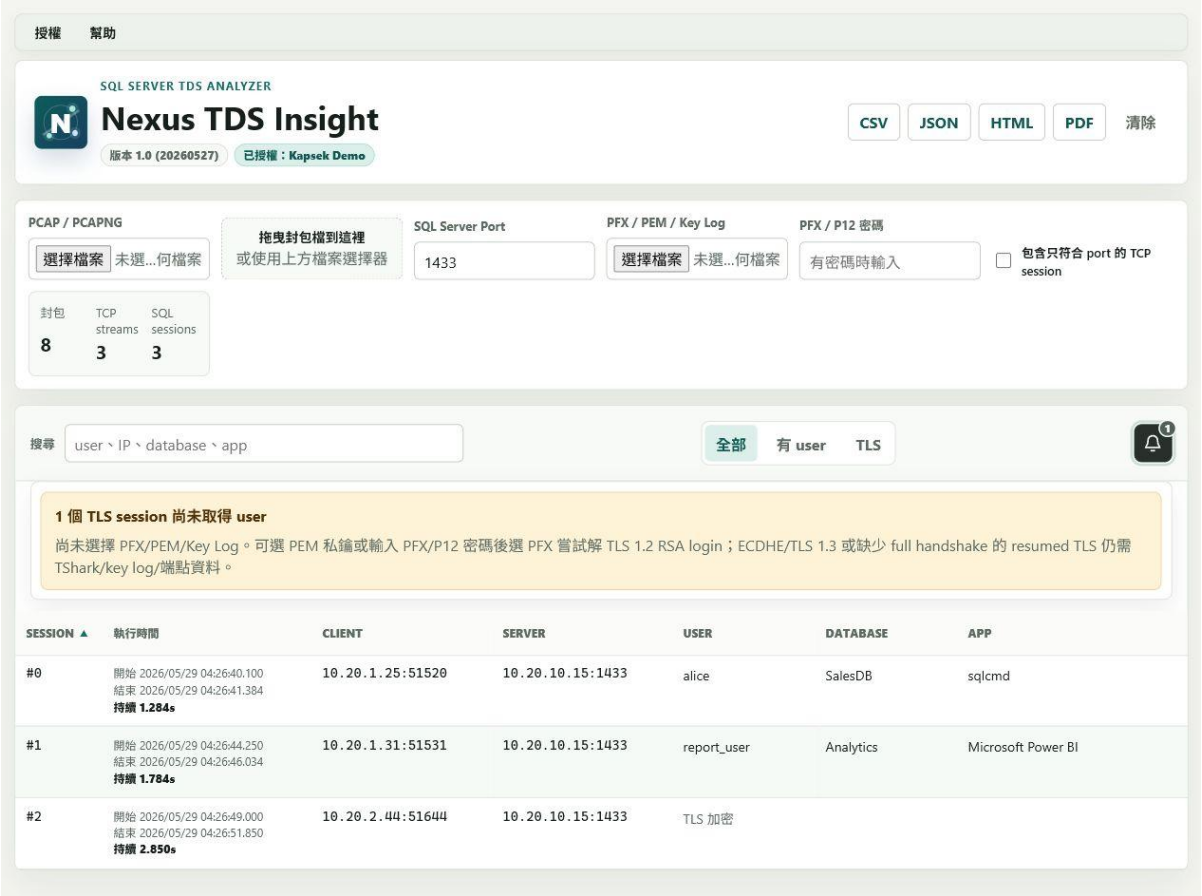
Lower Session Details: protocol, TDS types, traffic counters, and complete SQL statements.

Group	Key fields
Identity and time	Session ID, Client, Server, Start Time, End Time, Duration, Duration ms
Login	User, Database, App, Host, Client Library, Login Source, Declared Login Length
Protocol	Protocol, Integrated Security, TLS Detected, TDS Detected, TDS Types, Encryption
Traffic	Bytes C->S, Bytes S->C, TCP Segments
SQL and notes	SQL Count, SQL Statements, Notes

Note: Duration is the difference between the first and last observed packet in the TCP stream. It is not necessarily SQL Server CPU time or query execution-plan duration.

9. Notification Center

A notification bell and count appear for trial restrictions, TLS sessions without users, key-reading failures, capture-format problems, and other parse warnings. Select the bell to expand the messages. Read state is saved locally.



The notification center explains why a TLS session has no user and recommends next steps.

30. Read the complete message; it normally identifies missing data, password errors, or unsupported TLS behavior.
31. If no SQL Server session was found, verify the port, capture direction, and whether the login phase is present.
32. If a TLS session has no user, check for a full handshake and matching RSA key; otherwise use endpoint or TShark/key-log evidence.

10. Report Export

Export is enabled only when the product is licensed and at least one session is visible. Confirm search and filter settings before exporting.

Format	Contents and use
CSV	Currently filtered sessions; suitable for Excel, SIEM import, or further processing
JSON	Complete results object with counters, all sessions, warnings, and parsed fields
HTML	Standalone offline report with summary, overview, details, and SQL

Format	Contents and use
PDF	Text-based multipage jsPDF report with summary, overview, details, SQL, and page numbers

33. CSV is UTF-8 and includes endpoints, user, database, app, host, SQL, time, protocol, and notes.
34. If direct PDF generation fails, the product opens or downloads an HTML report that can be printed to PDF.
35. If the browser blocks a new window, check downloads and pop-up settings; the product may fall back to HTML.
36. Reports can contain accounts, IP addresses, database names, and SQL text. Review data classification before sharing.

11. Troubleshooting

Problem	Likely cause	Action
No sessions	Wrong port, non-TCP traffic, or no SQL traffic	Verify the SQL Server port; enable port-only sessions if needed
Session but no user	LOGIN7 missing, TLS encryption, or capture began mid-connection	Recapture the login phase; review Protocol and notifications
Private key does not recover TLS user	ECDHE/TLS 1.3, resumed TLS, wrong PFX password, or mismatched key	Verify handshake/cipher; use endpoint or TShark/key-log evidence
Invalid port	Non-integer or outside 1-65535	Use valid comma-separated values, for example 1433,14330
Export buttons disabled	Trial mode, no result, or empty filter	Activate the product and adjust search/filter settings
PDF not downloaded directly	Browser restriction or jsPDF failure	Use the HTML fallback and print it to PDF
Large capture is slow	Browser memory and single-thread parsing load	Split by time or host with Wireshark/tshark
License missing after restart	Site data cleared, different browser profile, or revoked license	Reactivate; contact support if the valid license remains rejected

12. Known Limitations

37. A server private key cannot decrypt TLS 1.2 ECDHE or TLS 1.3.
38. Resumed TLS without a captured full handshake/master secret cannot be restored from the private key alone.
39. Kerberos identities are usually not recoverable reliably from packet contents.
40. Without LOGIN7, a TDS session may exist while user, database, and app remain blank.
41. SQL extraction uses packet parsing and text heuristics; truncation, reassembly gaps, or unusual RPC traffic may be incomplete.
42. Very long SQL wraps and paginates in PDF; visually review reports before delivery.