Nexus Flow 使用手冊

Windows 即時網路流量監控、PCAP 分析與報表匯出

項目	資訊
適用產品版本	1.0.31
手冊版本	1.1
發行日期	2026-06-11

目錄

1. 產品定位與核心能力

Nexus Flow 是 Windows x64 免安裝網路流量監控工具。它以 WinDivert 擷取本機封包，將封包彙整成 flow，並依主機、服務與程式呈現下載、上傳、封包率、活躍連線、DNS、國家、ASN 與風險資訊。

主要使用情境

1. 即時查看本機與遠端主機之間的 TCP、UDP、ICMP、IPv4 與 IPv6 流量。
2. 依網卡、方向、Port、IP/CIDR、程式名稱或 PID 縮小觀察範圍。
3. 檢視 Top Hosts、Top Services、Top Programs 與 SQL Server TDS 等關注流量。
4. 匯入 classic PCAP/CAP 做離線彙整，或將即時封包持續寫入 PCAP。
5. 以 CSV、JSON、Excel、HTML 或 PDF 交付 flow 明細或摘要。

支援範圍

項目	現行支援
平台	Windows x64；WPF / .NET 8；Portable EXE
即時擷取	WinDivert ；需要系統管理員權限
資料來源	即時擷取、classic .pcap、.cap
分析維度	Flow、主機、服務、程式、DNS、國家、ASN、風險、告警
輸出	PCAP、CSV、JSON、XLSX、HTML、PDF

2. 運作方式與資料流程

Nexus Flow 將封包擷取、flow 彙整、名稱解析、風險判斷與畫面呈現分成不同階段。理解資料流程有助於判斷篩選條件在何時套用，以及為何 DNS、程式名稱或 GeoIP 欄位可能稍後才補齊。

階段	輸入	主要工作	輸出

階段	輸入	主要工作	輸出
擷取	本機網卡封包或 classic PCAP	WinDivert sniff mode 或離線讀檔	封包樣本
彙整	封包樣本	依方向、位址、連接埠與協定建立 flow	Flow 記錄與統計
補充資訊	遠端 IP、Port、PID	服務名稱、程式、DNS、國家、ASN、組織	可讀欄位
呈現	Flow 與摘要	總覽、Inspect、Hosts、Services、Programs	即時畫面
交付	目前累積資料	CSV、JSON、Excel、HTML、PDF、PCAP	報表或擷取檔

6. 核心擷取、彙整、搜尋與報表產生均在本機執行。
7. 只有使用者主動更新 GeoIP/ASN 資料或啟用 Webhook 時，才會使用網路連線。
8. 左側 Port、IP 與程式條件會影響保留或顯示的 flow；上方搜尋主要篩選畫面，不會改寫原始擷取檔。
9. DNS、程式與 GeoIP/ASN 解析受快取、權限、資料庫版本與封包時序影響，可能暫時顯示未知。

3. 系統需求、部署與啟動

正式交付包為單一 ZIP。程式自帶 .NET 執行環境，不需要另外安裝 .NET、Microsoft Office 或 PDF 軟體。

項目	需求
作業系統	Windows 10 / Windows 11 x64；建議使用仍受支援且已更新的版本
權限	必須以系統管理員身分執行，以載入 WinDivert 驅動
磁碟	程式、日誌、GeoIP/ASN 資料、PCAP 與報表所需空間；需求依流量與保存時間增加
網路	即時擷取不需外部服務；線上更新 GeoIP/ASN 時需要網際網路

部署與啟動

10. 將 NexusFlow_Portable_v1.0.31_WinDivert_KapsekSelfSigned.zip 解壓縮至受信任的本機資料夾；不要直接從 ZIP 內執行。
11. 確認 NexusFlow.exe 與套件附帶的第三方授權聲明存在。
12. 在 NexusFlow.exe 上按右鍵，選擇「以系統管理員身分執行」。
13. 若 Windows SmartScreen 或端點防護提出提示，先依組織流程驗證來源、簽章與雜湊。
14. 首次啟動時選擇語系，輸入正式授權，或按「使用試用版」。

4. 授權、試用版與產品資訊

授權視窗支援繁體中文、簡體中文與英文。正式授權以 Email 與 25 碼授權碼離線驗證；授權資料使用 Windows DPAPI 保護並儲存在目前 Windows 使用者設定中。

1. 授權視窗可選擇語言、輸入 Email 與授權碼，或進入五分鐘試用模式。

功能	試用版	正式授權
即時擷取	累計最多 5 分鐘	不受試用時間限制
PCAP 持續寫入 / 匯出	停用	可用
CSV / JSON / Excel / HTML / PDF	停用	可用
PCAP 匯入與畫面檢視	可用	可用

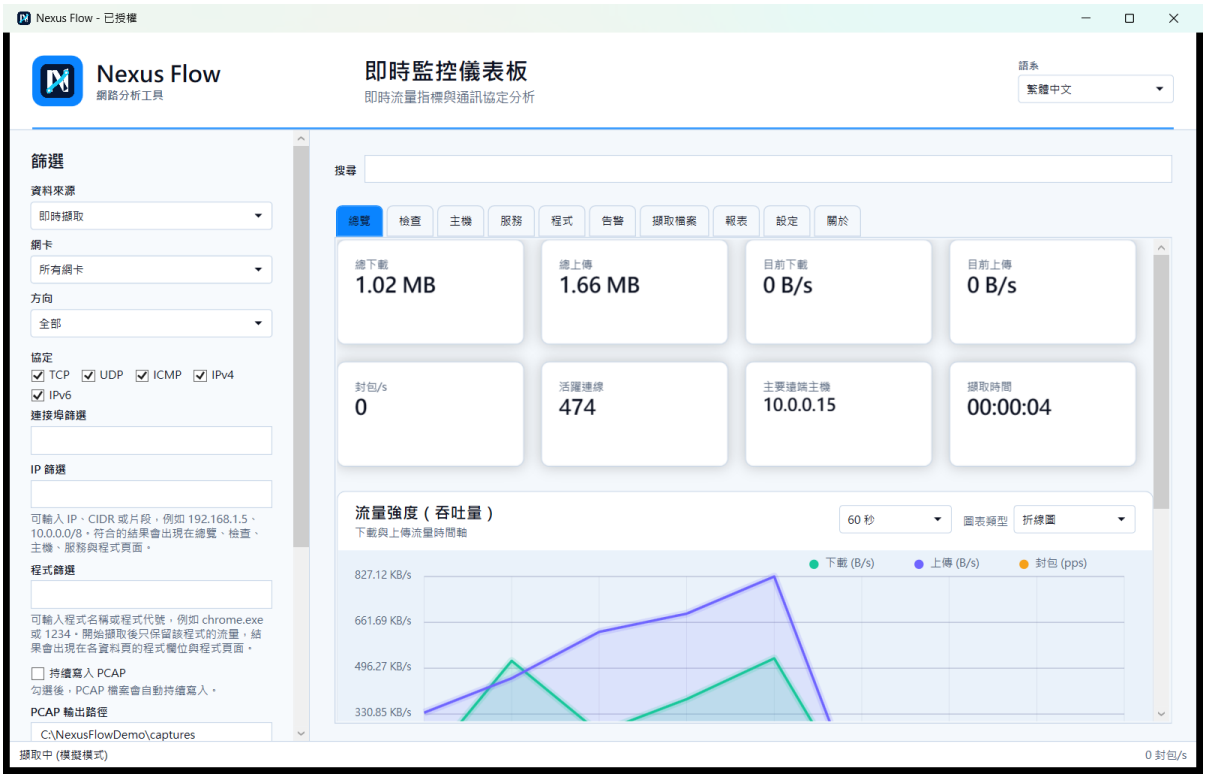
啟用正式授權

15. 在授權視窗選擇所需語系。
16. 輸入購買授權時使用的 Email。
17. 輸入格式為 XXXXX-XXXXX-XXXXX-XXXXX-XXXXX 的授權碼。
18. 按「啟用」。成功後主視窗標題列顯示「已授權」。
19. 若只需評估，按「使用試用版」；試用時間只在開始即時擷取後累計。

2. 關於頁說明產品、第三方授權與試用版限制；畫面版本文字可能與正式交付版不同。

5. 主畫面與操作區域

主視窗由 Header、左側篩選與操作區、搜尋列、十個功能頁籤及底部狀態列組成。語系可在右上角即時切換；主題固定跟隨 Windows。



3. 總覽頁同時顯示八項即時指標、流量時間軸、Top Hosts 與 Top Services。

區域	用途
Header	產品名稱、儀表板標題、語系切換
左側面板	資料來源、網卡、方向、協定、Port/IP/程式篩選、PCAP 與擷取操作
搜尋	跨 flow、主機、服務、程式、告警與擷取檔案比對關鍵字
頁籤	總覽、檢查、主機、服務、程式、告警、擷取檔案、報表、設定、關於
狀態列	擷取狀態、模擬/正式模式與目前封包率

6. 第一次擷取：快速開始

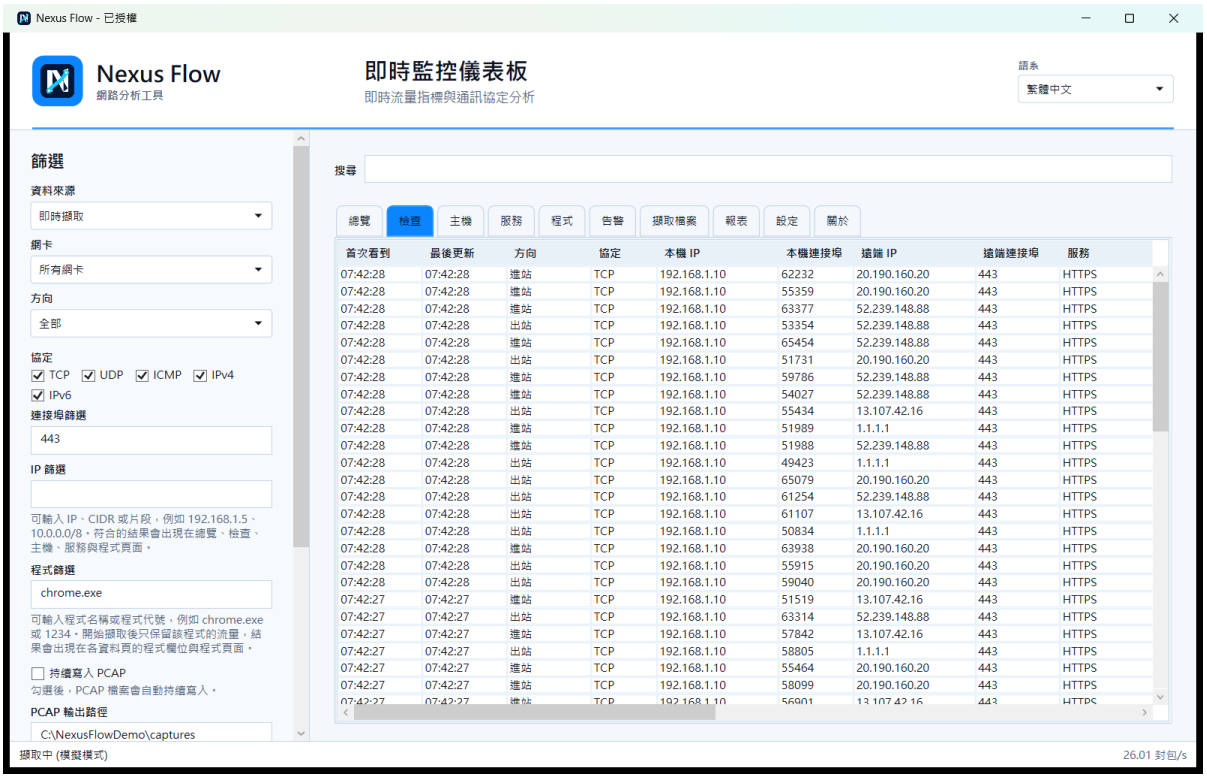
20. 以系統管理員身分啟動並完成授權或選擇試用版。
21. 在「資料來源」選擇「即時擷取」。
22. 選擇所有網卡或指定網卡，並設定方向與協定。

23. 需要時輸入 Port、IP/CIDR、程式名稱或 PID。
24. 若要保存原始封包，正式授權使用者可先勾選「持續寫入 PCAP」。
25. 按「開始擷取」，確認底部狀態列顯示擷取中。
26. 在總覽、檢查、主機、服務或程式頁確認資料。
27. 完成後按「停止擷取」；再依需要匯出報表或檢查 PCAP。

重要:「暫停介面」只停止畫面刷新，背景擷取與統計仍會繼續；要停止使用驅動與停止累計試用時間，必須按「停止擷取」。

7. 即時擷取、篩選與暫停介面

控制項	用法與範例
資料來源	即時擷取；或切換 PCAP 匯入並選擇檔案
網卡	所有網卡，或指定實體/虛擬介面
方向	全部、進站、出站
協定	TCP、UDP、ICMP、IPv4、IPv6，可複選
Port	443；80,443；10000-10100
IP	192.168.1.5；10.0.0.0/8；或位址片段
程式	chrome.exe；sqlservr.exe；或 PID 1234



4. Port 443 與 chrome.exe 篩選情境；Inspect 只保留符合條件的 HTTPS flow。

控制項	實際行為
開始擷取	依目前網卡、方向、協定與篩選條件開始；擷取中變更部分選項會重新開始並清空統計
停止擷取	停止 WinDivert、結束試用計時並關閉持續 PCAP writer
暫停介面	停止畫面更新，但底層擷取仍可能持續；再次按下可恢復顯示
清除統計	清空目前 flow、摘要與圖表，不等同刪除已寫入的 PCAP 檔
匯出 CSV	將目前累積的完整 Flow 集合輸出；上方搜尋不會自動限制匯出集合
匯出為 PCAP	擷取中切換持續寫入的開始或停止，並非真正的一次性快照

28. 開始擷取前確認條件。擷取中變更網卡、方向或協定會重新啟動擷取並清除既有統計。

29. Port、IP 與程式文字條件會套用至後續彙整與畫面；若要建立乾淨的比較基準，先停止並清除統計。

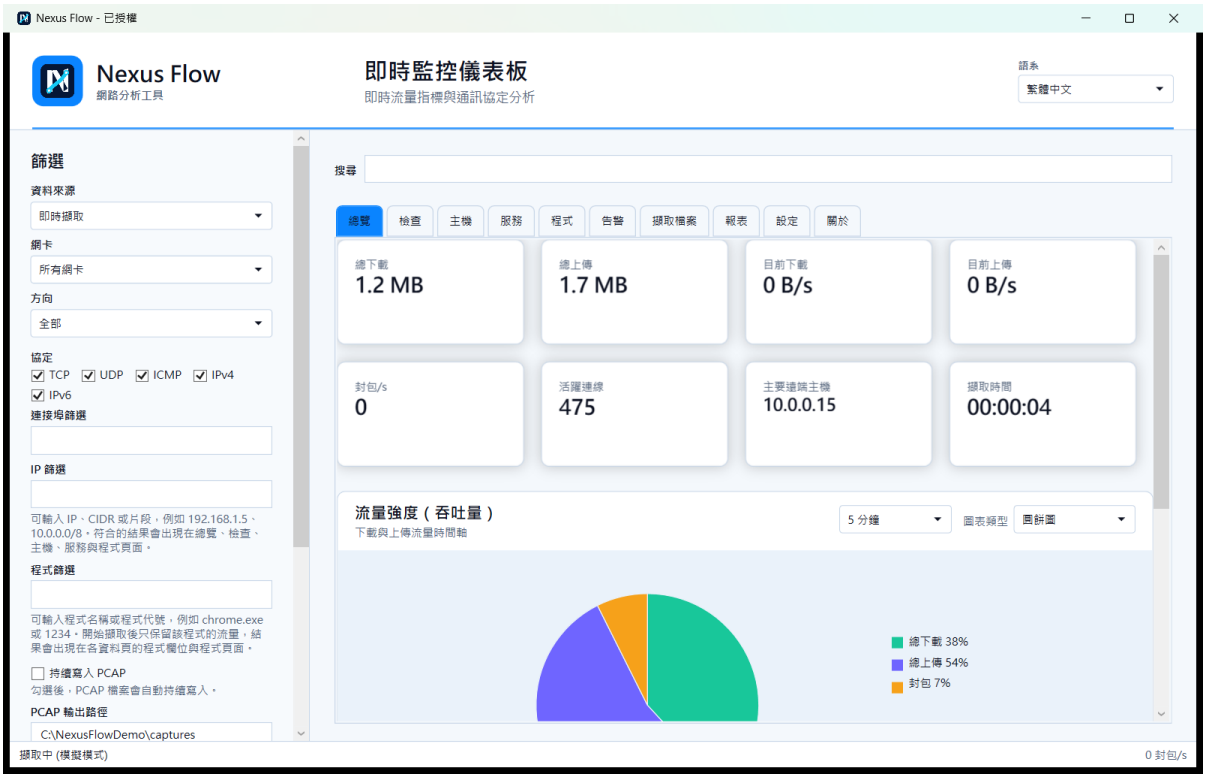
30. 「清除統計」會清除目前 flow 與圖表，但不會自動停止正在執行的擷取。

31. 「暫停介面」適合暫時凍結畫面閱讀；再次按下可恢復刷新。

8. 總覽指標與流量圖表

指標	解讀方式
總下載 / 總上傳	自本次統計起點累積的位元組，依方向換算
目前下載 / 目前上傳	最近取樣區間的即時速率
封包/s	最近取樣區間每秒封包數
活躍連線	目前彙整器內仍視為作用中的 flow 數
主要遠端主機	目前累積流量最大的遠端 IP
擷取時間	自擷取開始或統計重設後的經過時間

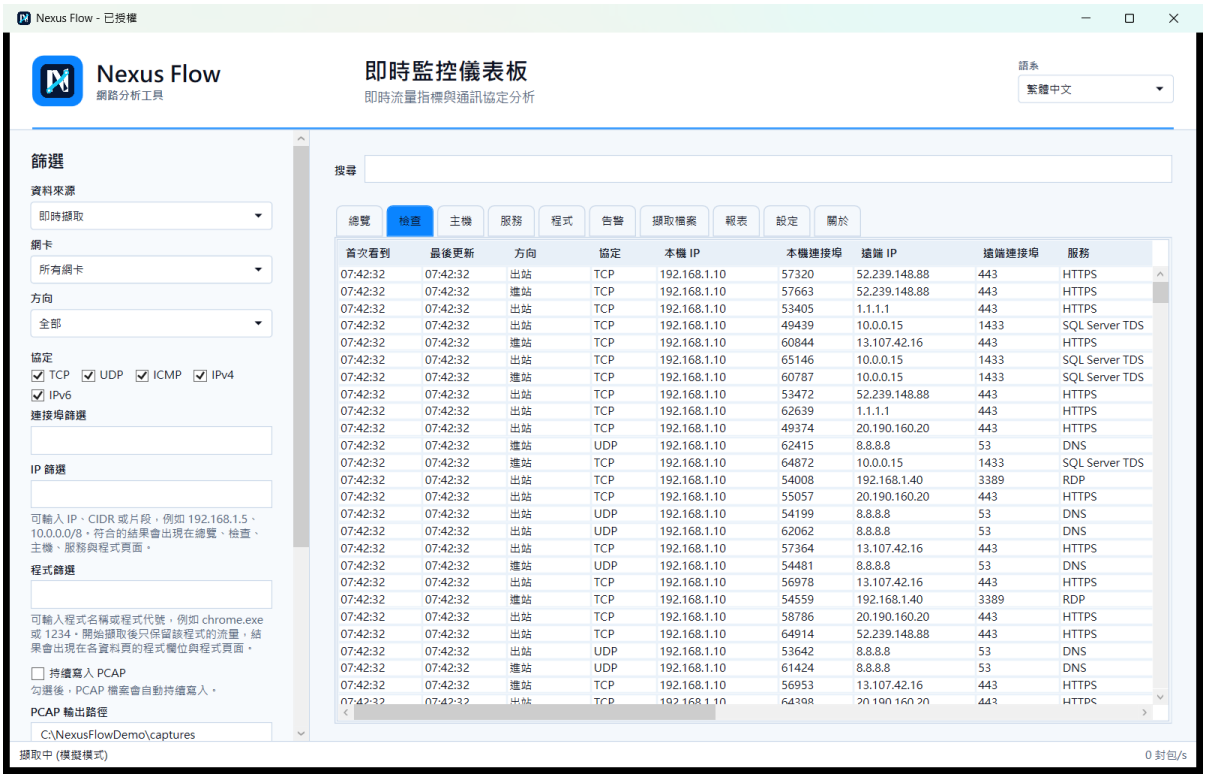
設定	選項與用途
時間範圍	60 秒、5 分鐘、15 分鐘、30 分鐘
折線圖	適合比較下載、上傳與封包率的變化趨勢
面積圖	強調流量量級與時間分布
長條圖	適合逐取樣點比較下載與上傳
圓餅圖	比較目前累積下載、上傳與封包的占比



5. 圓餅圖以目前累積的下載、上傳與封包量呈現流量組成。

9. 檢查明細與全域搜尋

「檢查」頁逐列顯示 Flow。畫面欄位依序包含「首次看到」、「最後更新」、「方向」、「協定」、「本機 IP」、「本機連接埠」、「遠端 IP」、「遠端連接埠」、「服務」、「程式」、「程式代號」、「國家」、「自治系統」、「網域」、「封包」、「流量」、「狀態」與「風險」；可使用水平捲軸查看後方欄位。

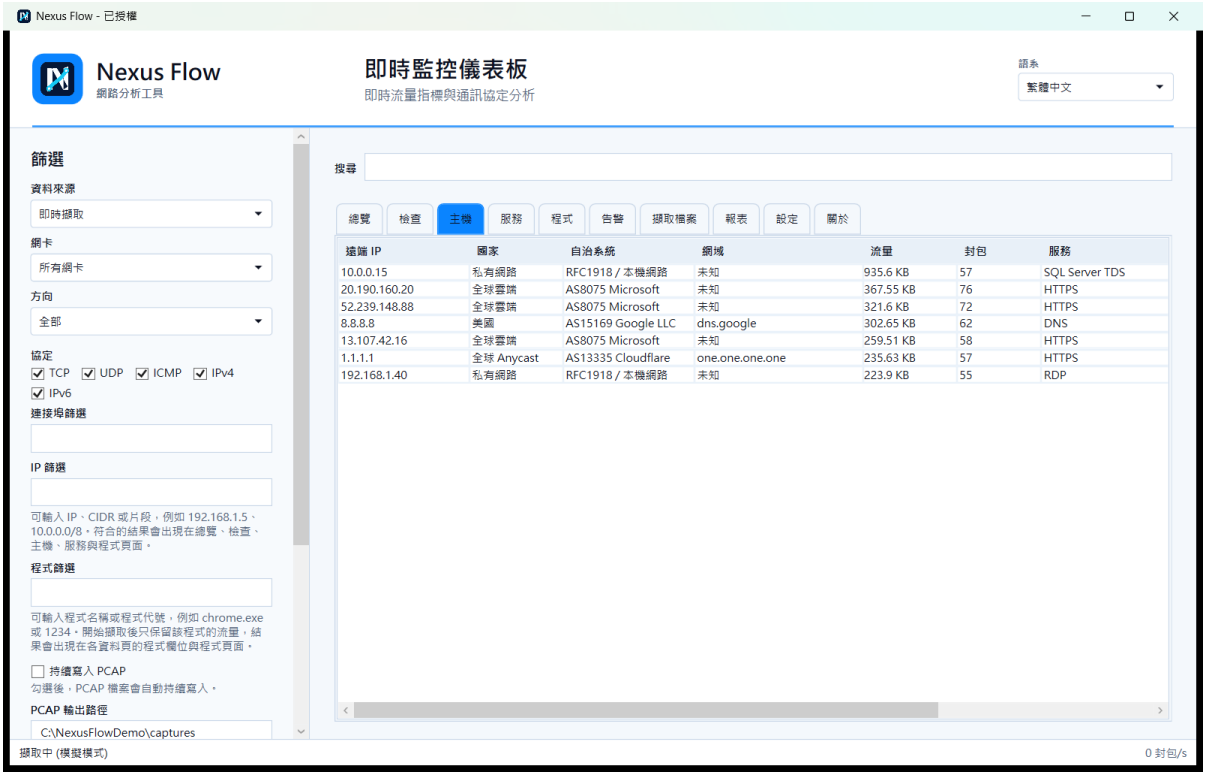


6.「檢查」頁以逐筆 Flow 呈現時間、方向、端點、服務、程式與流量等欄位。

欄位群組	包含內容	使用重點
時間	首次看到、最後更新	定位流量發生區間與持續時間
網路	方向、協定、本機 / 遠端 IP 與連接埠	確認通訊雙方與服務端連接埠
應用	服務、程式、程式代號、網域	找出通訊用途與發起程序
識別	國家、自治系統、網域	辨識網路歸屬與名稱解析；需先準備 GeoIP/ASN 資料
統計	封包、流量、狀態、風險	依資料量與風險進行排序與調查

重要: 上方「搜尋」會過濾目前畫面與摘要檢視；CSV/Excel 的匯出實作使用完整 Flow 集合，因此不要把畫面搜尋結果誤認為報表匯出範圍。需要交付特定子集時，應先另行篩選匯出檔。

10. 主機分析



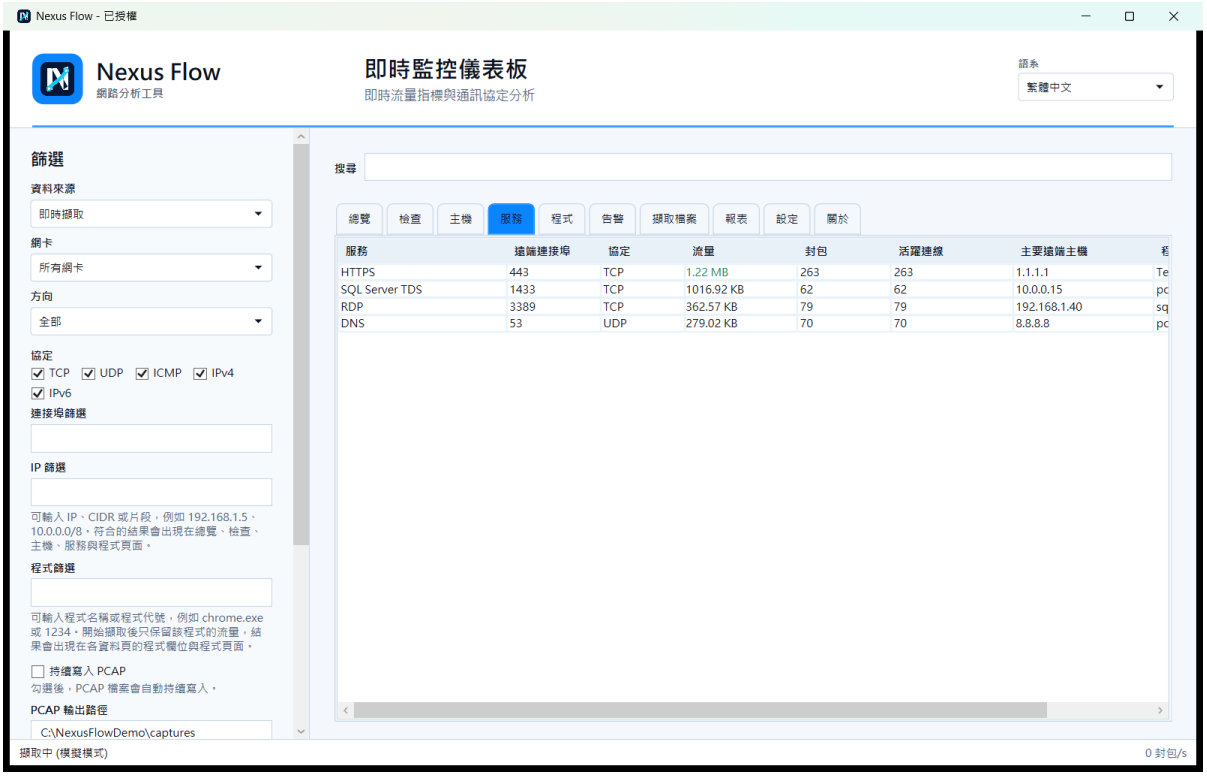
7.「主機」頁依遠端 IP 彙整國家、自治系統、網域、流量、封包、服務與程式。

欄位	說明
遠端 IP / 國家 / 自治系統	遠端端點及其地理與網路歸屬
網域	由 DNS 快取或反向解析取得；未知不代表沒有連線
流量 / 封包	此遠端 IP 在目前統計期間的累積量
服務 / 程式	曾與該主機通訊的服務與本機程序摘要
風險	「正常」或「黑名單」；黑名單資料由產品設定載入

1. 先使用上方「搜尋」縮小資料，再依「流量」、「封包」或「活躍連線」排序。
2. 「主機」適合從可疑 IP 出發；「服務」適合從連接埠或協定出發；「程式」適合從本機應用程式出發。

3. 三個摘要頁皆會受到左側「連接埠篩選」、「IP 篩選」與「程式篩選」影響，但各頁顯示的彙整維度不同。

11. 服務分析



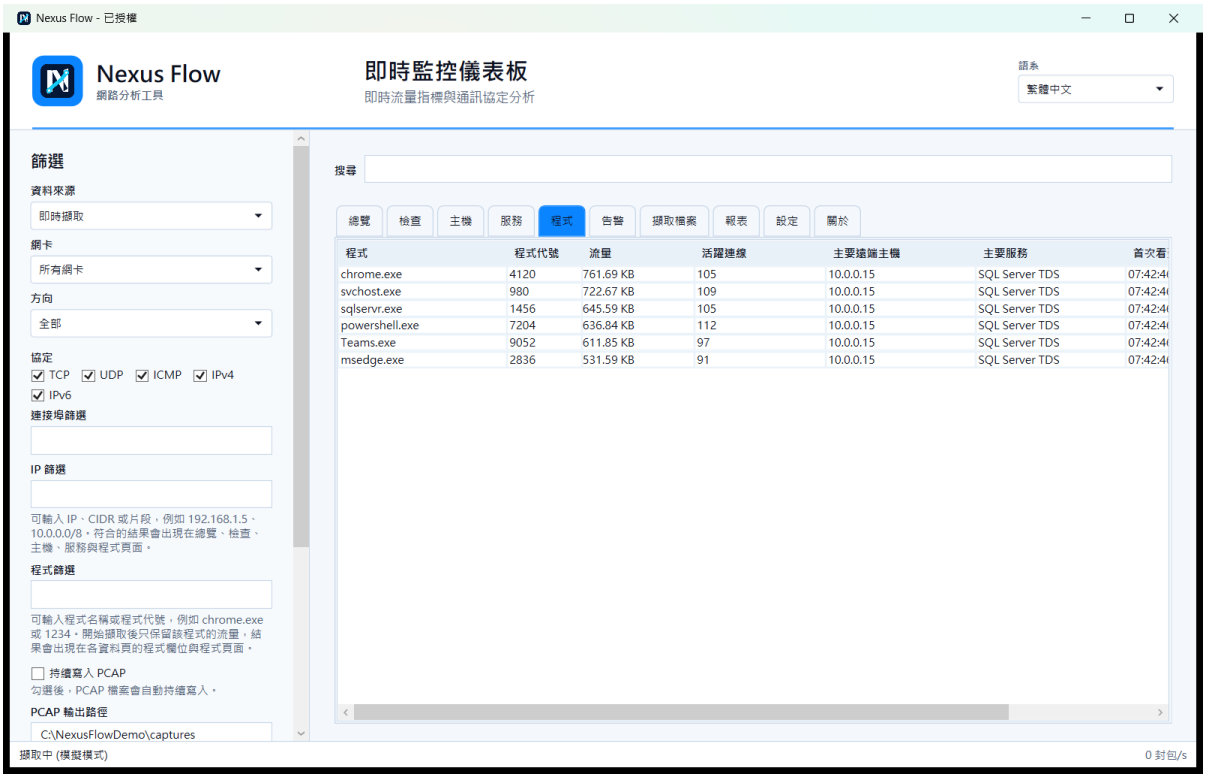
8.「服務」頁依服務、遠端連接埠與協定彙整流量、封包與主要端點。

欄位	說明
服務 / 遠端連接埠 / 協定	例如 HTTPS 443/TCP、DNS 53/UDP、SQL Server TDS 1433/TCP
流量 / 封包	同一服務與協定在目前統計期間的總量
活躍連線	目前仍作用中的相關 flow 數
主要遠端主機	該服務累積流量最大的遠端 IP
程式	使用該服務最多的本機程序

1. 先使用上方「搜尋」縮小資料，再依「流量」、「封包」或「活躍連線」排序。

2. 「主機」適合從可疑 IP 出發；「服務」適合從連接埠或協定出發；「程式」適合從本機應用程式出發。
3. 三個摘要頁皆會受到左側「連接埠篩選」、「IP 篩選」與「程式篩選」影響，但各頁顯示的彙整維度不同。

12. 程式分析



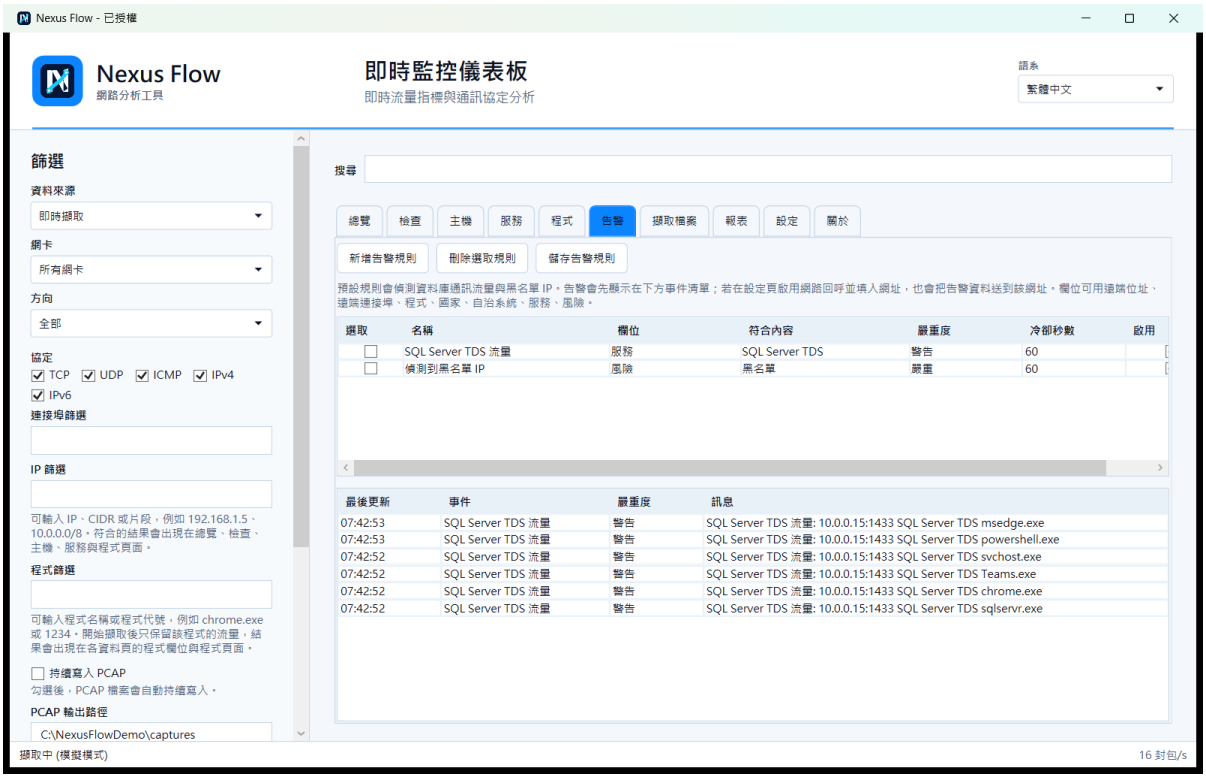
9.「程式」頁依程式與程式代號彙整流量、連線數、主要遠端主機及服務。

欄位	說明
程式 / 程式代號	由 Windows 連線擁有者資料推定；短連線可能顯示「未知」
流量 / 活躍連線	該程序累積流量與目前作用中 flow 數
主要遠端主機 / 主要服務	快速辨識程序主要連線目標與用途
首次看到 / 最後更新	程序在目前擷取期間的活動時間範圍

1. 先使用上方「搜尋」縮小資料，再依「流量」、「封包」或「活躍連線」排序。
2. 「主機」適合從可疑 IP 出發；「服務」適合從連接埠或協定出發；「程式」適合從本機應用程式出發。
3. 三個摘要頁皆會受到左側「連接埠篩選」、「IP 篩選」與「程式篩選」影響，但各頁顯示的彙整維度不同。

13. 告警規則、事件與 Webhook

「告警」頁包含可編輯規則與事件清單。預設規則偵測 SQL Server TDS 服務與黑名單 IP；符合規則時先加入畫面事件，啟用網路回呼後再以 HTTP POST 傳送 JSON。



10.「告警」頁上半部管理規則，下半部顯示符合規則的事件紀錄。

1. 選擇「新增告警規則」，在新列填寫「名稱」、「欄位」、「符合內容」、「嚴重度」、「冷卻秒數」與「啟用」。

2. 「欄位」可使用「遠端 IP」、「遠端連接埠」、「程式」、「國家」、「自治系統」、「服務」或「風險」。
3. 按「儲存告警規則」將規則寫入設定；如要移除規則，先勾選「選取」，再按「刪除選取規則」。未儲存的表格修改不應視為正式配置。
4. 事件符合規則時會出現在下方事件表；相同規則在冷卻期間內不會重複大量通知。
5. 若「設定」頁開啟「啟用網路回呼」，事件也會以 HTTP POST JSON 傳送；失敗只記錄在記錄檔，不會阻塞擷取。

欄位	說明
名稱	規則名稱
欄位	可用值：遠端 IP、遠端連接埠、程式、國家、自治系統、服務、風險
符合內容	不分大小寫的包含比對；空白不觸發
嚴重度	例如 Info、Warning、Critical；作為事件標示與 Webhook 欄位
冷卻秒數	相同規則、遠端端點與程式再次觸發前的冷卻秒數
啟用	取消後不評估該規則

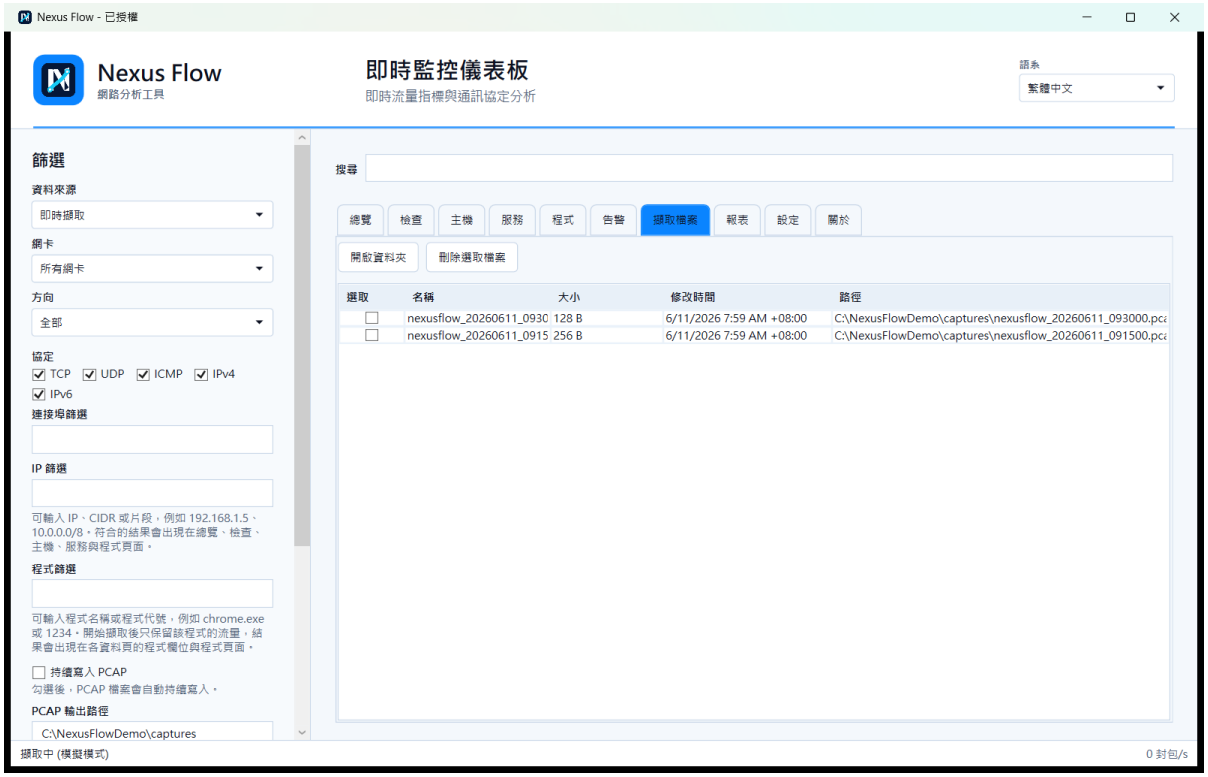
注意: Webhook JSON 包含 product、eventType、severity、time、remoteAddress、remotePort、process、country、asn。產品不提供簽章或重送佇列；接收端應使用 HTTPS、驗證來源並容忍重複/遺失事件。

14. PCAP 匯入、持續寫入與擷取檔案管理

Nexus Flow 可在正式授權下持續寫入即時封包，也可匯入既有 classic PCAP/CAP。PCAP 內容可能包含敏感的網路資料，應依組織保存政策處理。

工作	操作	注意事項
匯入離線檔	「資料來源」選擇「PCAP 匯入」，再選擇 .pcap 或 .cap	選檔器會顯示 .pcapng，但目前讀取器不支援 PCAPNG
開始即時寫入	開始擷取前勾選「持續寫入 PCAP」，或擷取中按「匯出為 PCAP 檔(一次性儲存	試用版停用；檔名為 nexusflow_yyyyMMdd_HHmmss.pcap

工作	操作	注意事項
	目前記錄)」	
停止寫入	停止擷取，或再次按「匯出為 PCAP 檔(一次性儲存目前記錄)」	停止後才會完整關閉檔案並刷新擷取檔案清單
管理檔案	在「擷取檔案」頁按「開啟資料夾」，或選取檔案後按「刪除選取檔案」	刪除動作不可復原；使用中的檔案可能無法刪除



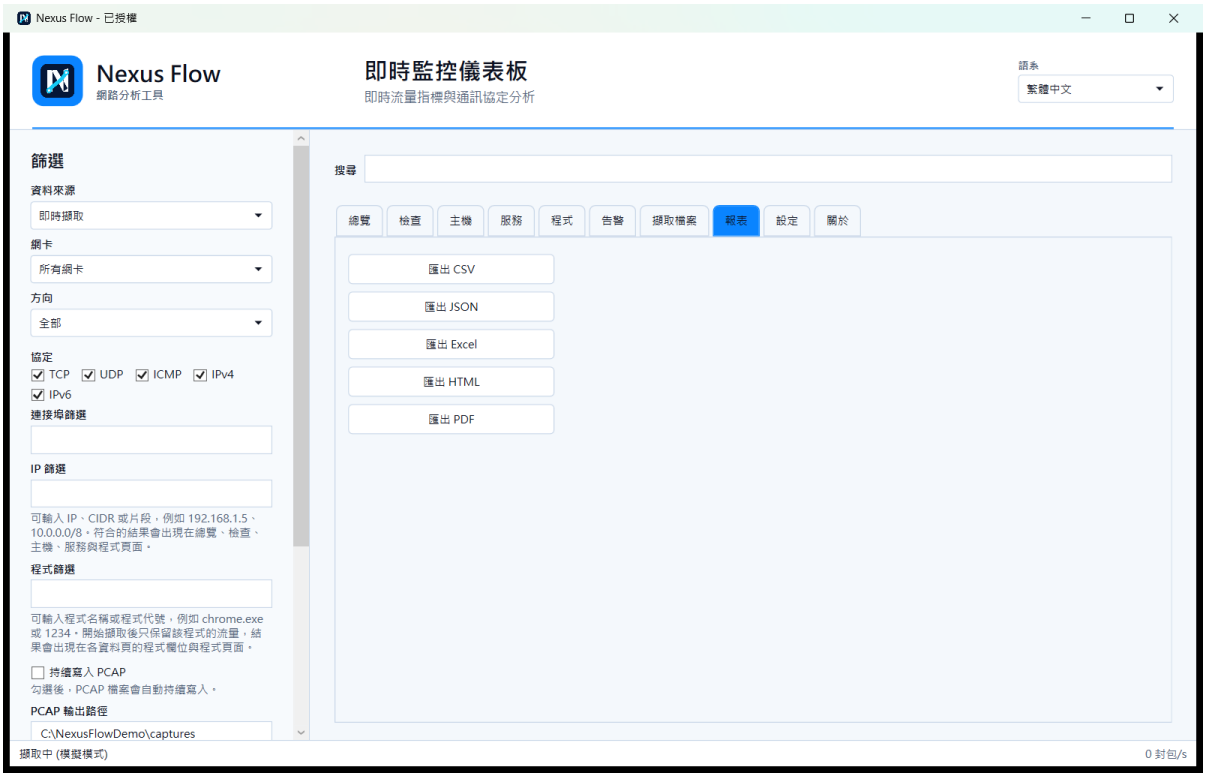
11.「擷取檔案」頁列出 PCAP 名稱、大小、修改時間與完整路徑。

功能	操作與結果
擷取前持續寫入	勾選「持續寫入 PCAP」並開始擷取，自動建立 nexusflow_yyyyMMdd_HHmmss.pcap
擷取中切換寫入	擷取進行時按左側「匯出為 PCAP 檔(一次性儲存目前記錄)」；現版實際行為為開始/停止持續寫入
「擷取檔案」頁	列出預設 captures 目錄的 .pcap，可使用「開啟資料夾」或「刪除選取檔案」
PCAP 匯入	資料來源選擇 PCAP 匯入，選取 classic .pcap 或 .cap
格式	classic PCAP，LINKTYPE_RAW 101

警告: 檔案選擇器會顯示 .pcapng，但現行版本不解析 PCAPNG，會顯示不支援訊息。請先以 Wireshark/tshark 轉成 classic .pcap。

15. 報表匯出與交付

正式授權使用者可從「報表」頁匯出五種格式。完成後產品顯示檔案路徑，並在檔案總管選取輸出檔。



12.「報表」頁提供「匯出 CSV」、「匯出 JSON」、「匯出 Excel」、「匯出 HTML」與「匯出 PDF」五種輸出。

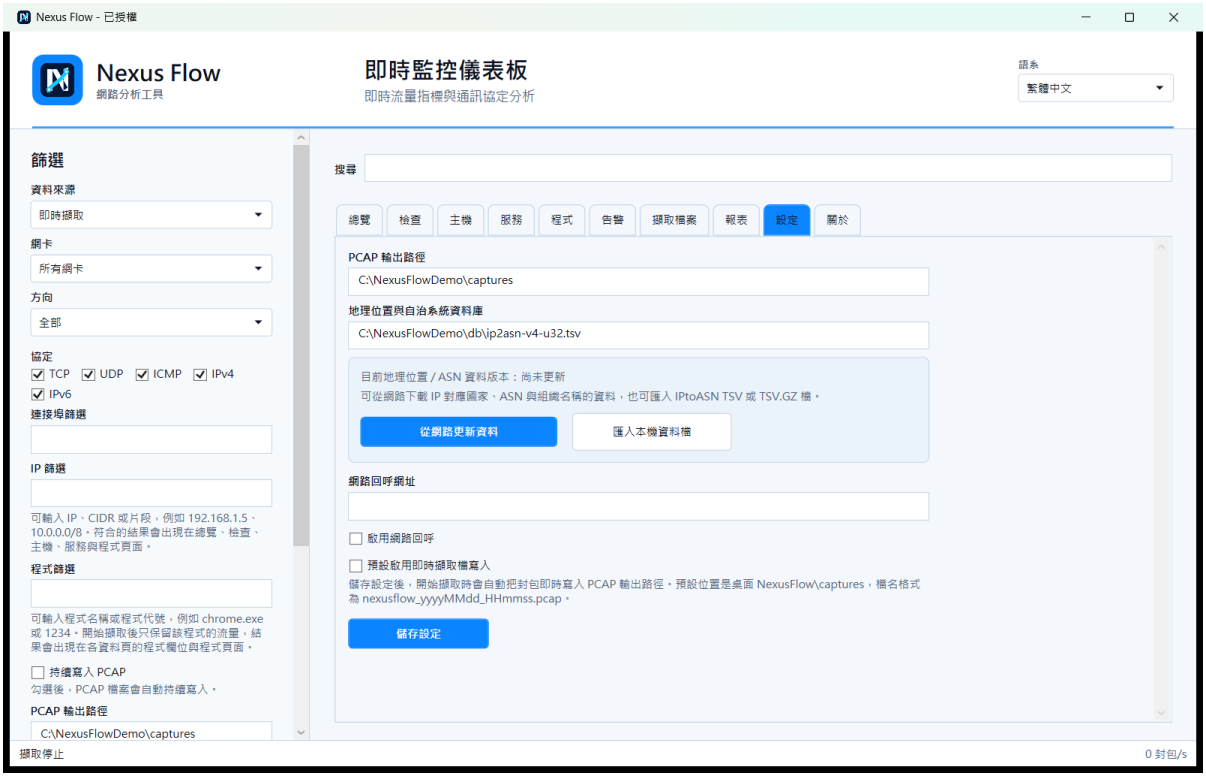
1. 先完成擷取或 PCAP 匯入，確認「檢查」與摘要頁已有資料。
2. 切換到「報表」頁，選擇「匯出 CSV」、「匯出 JSON」、「匯出 Excel」、「匯出 HTML」或「匯出 PDF」。
3. 輸出完成後產品會顯示檔案路徑，並開啟檔案所在資料夾。
4. 交付前抽查時間、端點、程式、DNS、國家/ASN 與報表編碼，並依資料分級遮罩敏感資訊。

格式	內容	預設子目錄
CSV	全部 flow 明細；UTF-8	reports\csv
JSON	snapshot、前 50 筆主機 / 服務 / 程式、前 100 筆告警	reports\json
Excel	全部 flow 明細；.xlsx，不需要 Office	reports\excel
HTML	可用瀏覽器開啟的摘要	reports\html
PDF	簡要摘要與熱門主機	reports\pdf

警告: 報表可能包含內外部 IP、程序名稱、網域、國家、ASN 與告警資訊。PDF 產生器偏向 ASCII 文字；若需要完整中文呈現，優先使用 HTML、Excel、CSV 或 JSON。

16. 設定、GeoIP/ASN 與背景監控

「設定」頁集中管理「PCAP 輸出路徑」、「地理位置與自治系統資料庫」、「網路回呼網址」及「預設啟用即時擷取檔寫入」。設定儲存在目前 Windows 使用者的 settings.json。



13.「設定」頁管理 PCAP 路徑、GeoIP/ASN、網路回呼與預設即時擷取檔寫入。

設定	作用
PCAP 輸出路徑	設定持續寫入與按鈕啟動寫入的目的資料夾
地理位置與自治系統資料庫	指定 ip2asn-v4-u32.tsv；可線上更新或匯入 .tsv/.tsv.gz
網路回呼網址 / 啟用網路回呼	將告警事件以 JSON POST 到指定端點
預設啟用即時擷取檔寫入	儲存後，下次開始擷取時自動寫入 PCAP；試用版停用
儲存設定	寫入 settings.json，並同步左側 PCAP 路徑

1. 「PCAP 輸出路徑」會同步到左側擷取控制區。
2. 「地理位置與自治系統資料庫」可使用「從網路更新資料」，或以「匯入本機資料檔」匯入 IPtoASN TSV/TSV.GZ；更新後既有 Flow 會在後續重新整理時補充資訊。
3. 「網路回呼網址」應使用受控 HTTPS 端點，接收端需自行處理驗證、保留期限與重送策略。
4. 「預設啟用即時擷取檔寫入」只對正式授權有效；試用模式會自動取消。
5. 最小化時主視窗可隱藏至系統匣；系統匣選單可使用「顯示主視窗」、開始/停止擷取、「迷你視窗」或離開。

17. 疑難排解

問題	可能原因	處理方式
程式要求管理員權限	WinDivert 驅動需要提升權限	以系統管理員身分重新啟動；確認 UAC 與端點政策
無法開始擷取	驅動被封鎖、簽章/權限問題、無效條件	查看錯誤碼與 nexusflow.log；確認 WinDivert runtime 與安全政策
畫面沒有資料	條件過窄、選錯網卡/方向、目前沒有流量	選擇「所有網卡」與「全部」方向；清除篩選後重試
試用版自動停止	累計即時擷取已達 5 分鐘	啟用正式授權；PCAP 匯入仍可用
PCAPNG 無法匯入	現版不支援 PCAPNG	先轉換為 classic .pcap
告警沒有送到 Webhook	未啟用、URL 錯誤、TLS/防火牆阻擋	確認設定與接收端日誌；使用 HTTPS 測試端點
報表按鈕無法使用	試用模式	完成正式授權
國家/ASN 顯示未更新	尚未下載或匯入資料庫	在「設定」頁更新或匯入 IPtoASN TSV/TSV.GZ
最小化後找不到視窗	已隱藏到系統匣	按兩下 Nexus Flow 圖示或使用「顯示主視窗」

18. 安全、隱私與已知限制

安全與隱私

1. 即時擷取、彙整、授權驗證與報表產生皆在本機執行；只有使用者啟用的 GeoIP 更新與 Webhook 會連線外部端點。
2. license.dat 與 trial.dat 使用 Windows DPAPI，通常只可由相同 Windows 使用者解密。
3. WinDivert runtime 位於 ProgramData，正式程式會限制資料夾 ACL 並在結束時清理相關驅動服務。
4. PCAP、flow、網域、程序與告警可能構成敏感或個人資料；擷取前應取得授權並依政策保存。
5. 刪除產品資料夾不會自動刪除 LocalAppData、ProgramData、桌面 PCAP 與報表。

已知限制

1. 產品是監控與分析工具，不會封鎖、修改或注入封包，也不是防火牆。
2. 目前不提供 PCAPNG 解析、地圖、雲端帳號、集中管理、Windows Service 或 MSI/MSIX。
3. 程序對應與 DNS/GeoIP 結果受系統權限、快取、資料庫版本與封包時序影響。
4. 主畫面搜尋只影響檢視，不會自動把報表匯出限制為可見列。
5. 「關於」頁文字版號可能與 1.0.31 交付包不一致，應以正式交付資訊為準。