瞭解端點診斷工具(CEDT)

目錄

簡介

本檔案將說明CEDT，從您的系統收集診斷資料並將其上傳到Cisco TAC支援案例。

必要條件

該工具可用於MacOS和Windows。請下載該工具。

思科建議您瞭解以下主題：

- MacOS:按兩下思科端點診斷工具(CEDT)。app啟動。
- Windows:按兩下CEDT.exe啟動。
- 活動的網際網路連線。
- Cisco TAC案例ID和權杖（僅在您想要直接上傳結果時需要）。

收集的系統資料

該工具按類別收集此系統資料。不會捕獲任何型別的個人資料。

一般系統資訊

Data	macOS	Windows
OS, hardware, CPU, RAM, storage	`system_profiler` `SPSoftwareDataType` `SPHardwareDataType`	`systeminfo`, WMI classes (`Win32_OperatingSystem`, `Win32_ComputerSystem`, `Win32_BIOS`)
Kernel parameters	`sysctl -a`	N/A

網路設定

Data	macOS	Windows
Network interfaces & IP addresses	`ifconfig -a`	`ipconfig /all`
Routing table	`netstat -rn`	`netstat -rn`
DNS configuration	`scutil --dns`	(included in `ipconfig /all`)
Network services	`networksetup -listallnetworkservices`	`netsh interface show interface`
WiFi profiles	N/A	`netsh wlan show profiles`

產品資訊

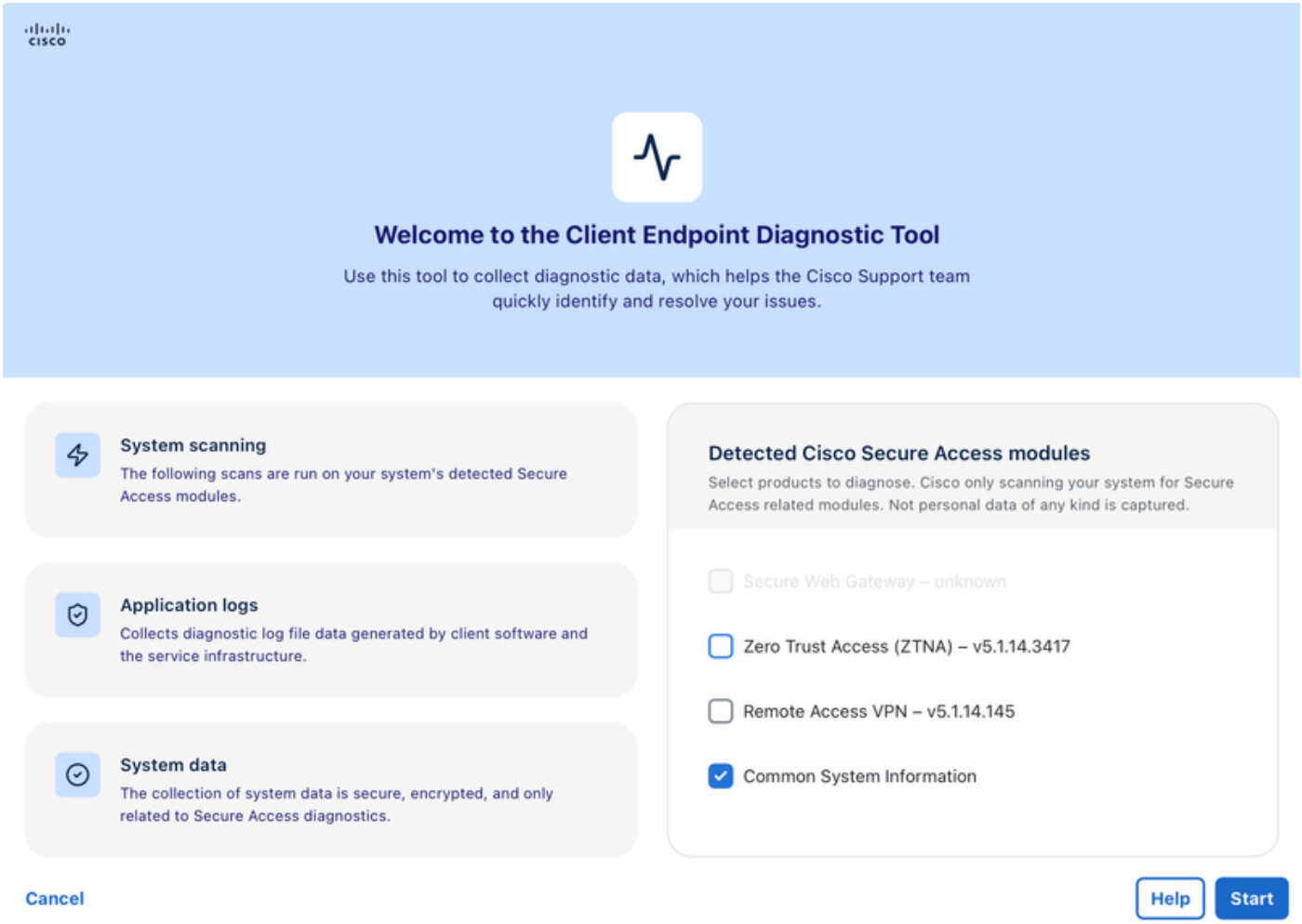
Data	macOS	Windows
Cisco preferences/config files	`/Library/Preferences/com.cisco.*`	Registry exports (`HKLM\SOFTWARE\Cisco`, `HKCU\SOFTWARE\Cisco`, `acsock` service)
Installation directories	`ls -laR /opt/cisco`	`%ProgramFiles%\Cisco`, `%ProgramFiles(x86)%\Cisco`, `%ProgramData%\Cisco`
Running Cisco processes	`ps aux | grep -i cisco`	`tasklist | findstr /i cisco`, WMI `Win32_Process`
Installed Cisco products	`mdfind` for Cisco apps	WMI `Win32_Product` (vendor Cisco)
Application logs	Cisco Secure Client log directories	`%ProgramData%\Cisco\Cisco Secure Client\Logs`
Event logs	N/A	Windows Event Log (`Cisco Secure Client - Zero Trust Access`, Application provider `*Cisco*`)
Crash reports	`~/Library/Logs/DiagnosticReports/cisco*` (last 7 days)	N/A

逐步演練

歡迎螢幕

啟動CEDT時，會顯示「歡迎」螢幕。它概述了該工具的作用：

- 系統掃描 — 掃描您的系統，查詢檢測到的思科安全訪問模組。
- 應用程式日誌 — 收集由客戶端軟體和服務基礎結構生成的診斷日誌檔案資料。
- 系統資料 — 系統資料的收集是安全的、加密的，並且僅與Secure Access診斷相關。



在右側，該工具會自動檢測系統上安裝的任何思科安全訪問模組。您可以看到每個檢測到的模組的

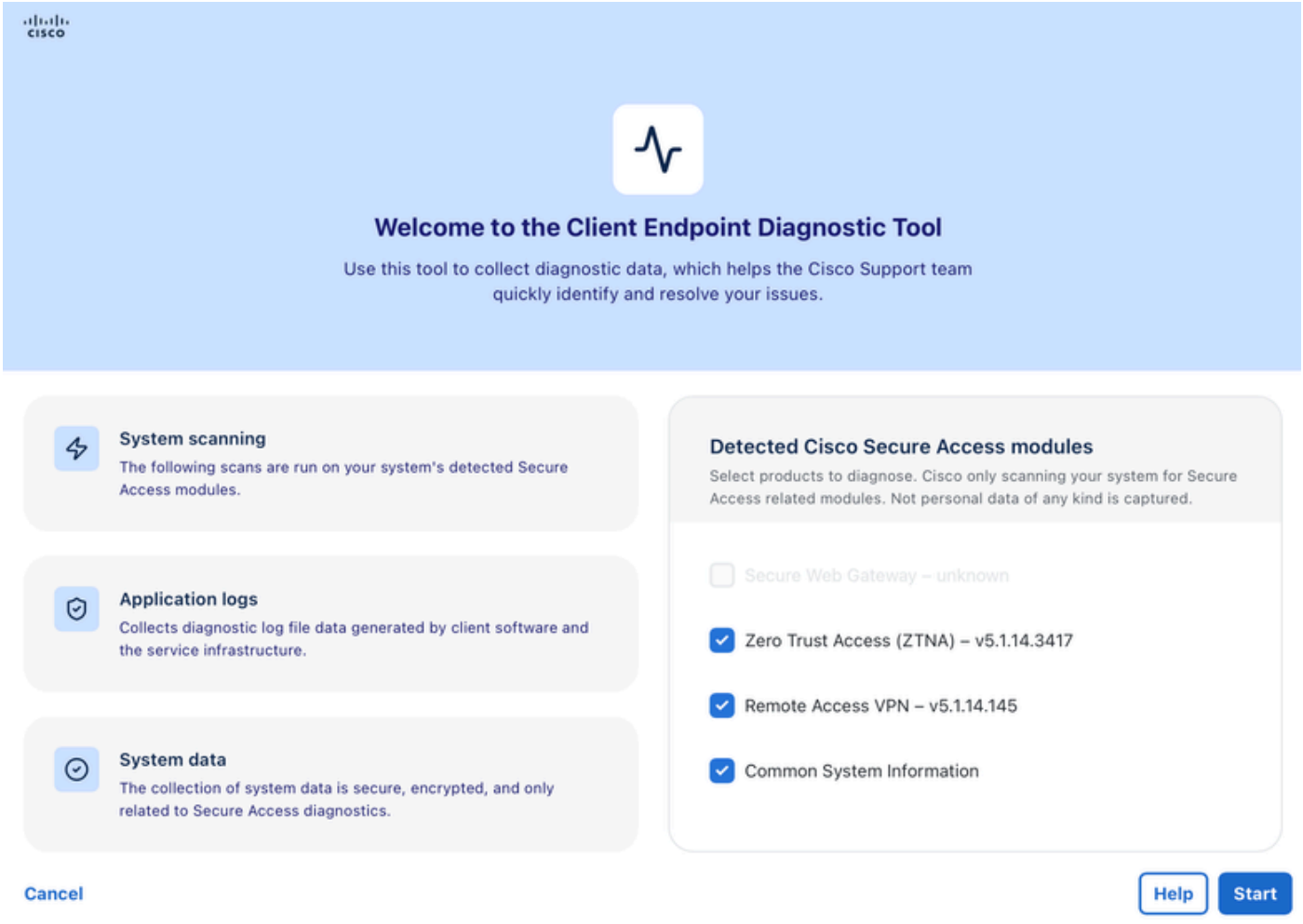
獲取方塊及其版本號：

- 零信任存取(ZTNA)
- 安全Web閘道(SWG)
- 遠端存取VPN(RAVPN)
- 通用系統資訊（始終可用）

動作

1. 選擇或取消選擇您要診斷的產品。
2. 按一下Let's Start以繼續，或按一下Help以獲取詳細資訊。

附註：此工具僅收集與Secure Access相關的模組的資料。不會捕獲任何型別的個人資料。



步驟 1:診斷資料收集

此螢幕允許您選擇要包括的診斷測試和資料收集模組。

網路診斷

選擇要運行的連線測試：

- DNS查詢 — 對指定主機執行DNS解析測試。支援用於目標查詢的自定義解析程式IP。所有結果都整合到一個帶有結構化節分隔符的輸出檔案(dns/dns_lookups.txt)中。
- 資料包捕獲 — 捕獲指定持續時間的網路資料包（需要管理員許可權）。
- Ping主機 — 對指定的主機執行ping操作以檢查連通性。
- 策略測試輸出 — 使用思科策略測試終端(policy.test.sse.cisco.com)測試針對指定URL的策略實施。 支援多個以逗號分隔的主機（最多10台）。 結果包括在策略測試導航過程中自動捕獲的HAR資料。
- 網路速度測試 — 根據思科速度測試終端(speed.test.sse.cisco.com)測量上傳/下載速度和延遲。 收集下載速度（6個並行流）、上傳速度（3個並行流）和ping延遲/抖動（10個ICMP示例）。 結果以JSON和文本摘要格式儲存。
- URL可達性 — 檢查是否使用HTTP GET請求可以訪問指定的URL。預設支援HTTP（埠80）和HTTPS（埠443）。可以在URL(例如https://example.com:8443)中指定非標準埠。 每次檢查最多20個URL，每個URL超時為30秒。每個URL收集的資料包括：URL、可訪問性狀態、HTTP狀態代碼、響應時間(ms)、內容長度、已解析的IP地址、TLS版本和時間戳。結果儲存到reachability/reachability_results.json和reachability/reachability_summary.txt。

資料收集

選擇模組以收集效能和連線資料：

- HAR捕獲 — 從瀏覽器會話記錄HTTP存檔(HAR)資料。目前僅支援Google Chrome（通過無頭瀏覽器自動化使用Chrome DevTools協定）。 該工具會自動檢測您系統上的Chrome安裝。

目前不支援Firefox和Safari。HAR輸出遵循HAR 1.2規範，包括完整的網路跟蹤（包括JS觸發的XHR/fetch呼叫）。

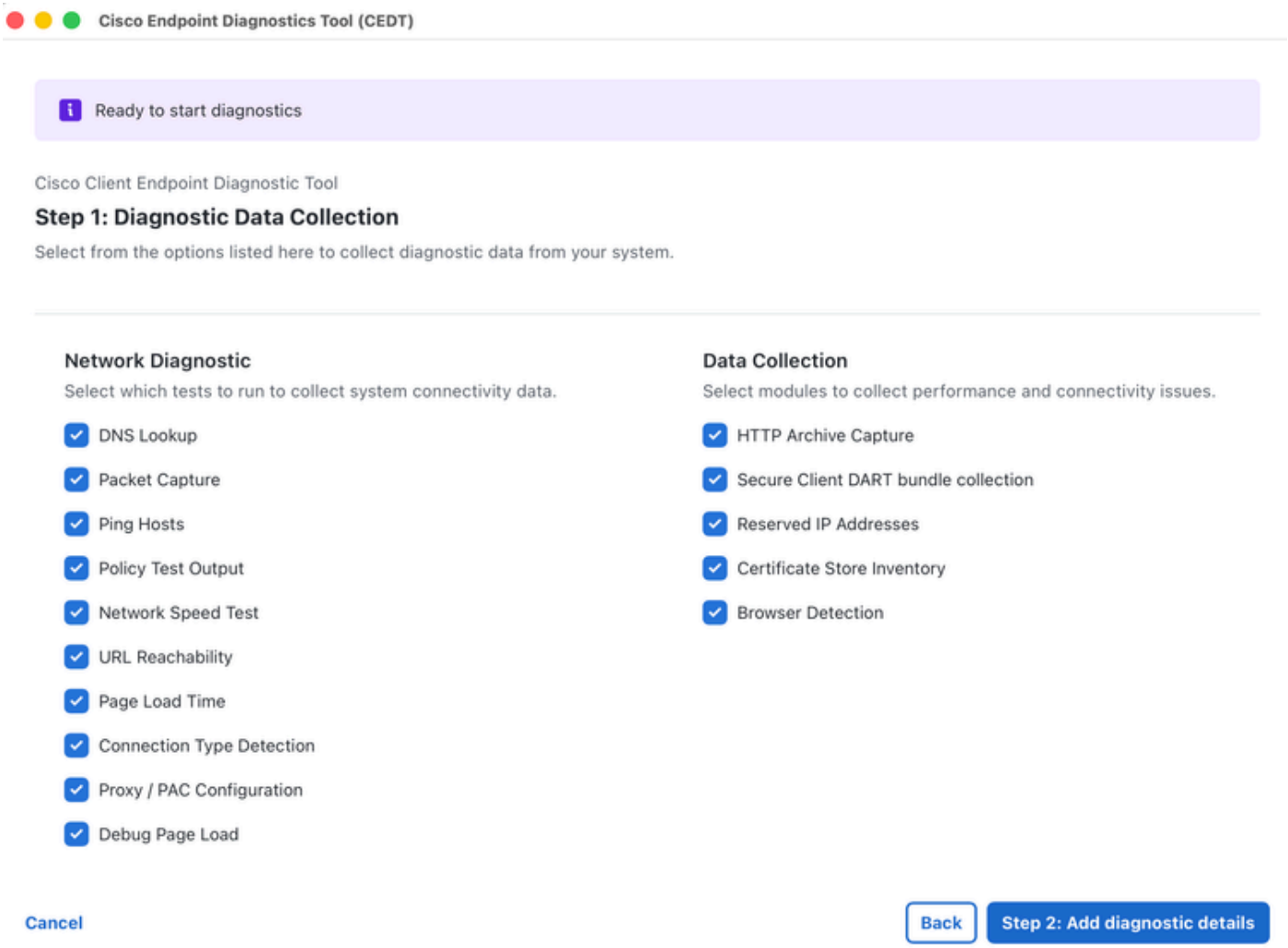
- DART捆綁包集合 — 從思科安全客戶端收集DART診斷捆綁包。這包括所有模組日誌，包括零信任訪問(ZTA)日誌(例如Windows上的flowlog.db，位於C:\ProgramData\Cisco\Cisco Secure Client\ZTA\logs\)。
- 保留的IP — 運行保留的IP診斷檢查。請參見下一部分，瞭解收集的診斷完整清單。

偵錯

- 啟用調試標誌 — 收集終端活動的詳細日誌以診斷終端問題。只有在檢測到並選擇了至少一個Cisco Secure Access產品時，此選項才可用。

平台特定的

- DebugView捕獲(Windows) — 在Windows安全終結點聯結器上啟用調試日誌記錄。此選項僅在Windows系統上可用。



動作

1. 選中或取消選中所需的診斷選項。
2. 按一下「Step 2:新增診斷詳細資訊以繼續。
3. 按一下Back返回到「歡迎」螢幕，或按一下Cancel退出。

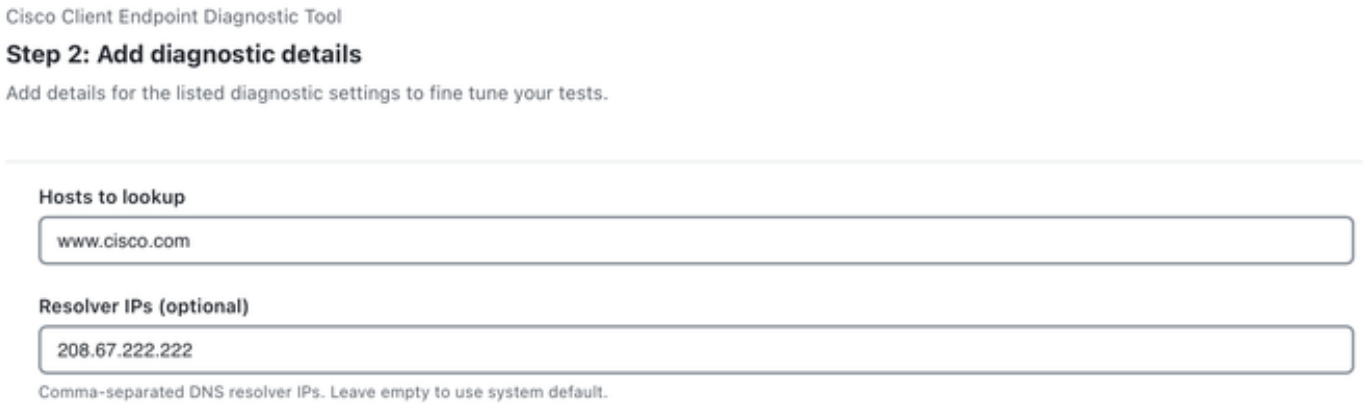
步驟 2:新增診斷詳細資訊

通過此螢幕，可以為每個已啟用的診斷測試配置特定引數。僅顯示您在步驟1中啟用的測試設定。

DNS查詢設定

- 要查詢的主機 — 輸入一個或多個主機名（以逗號分隔）。 範例：cisco.com
- 解析程式IP（可選） — 輸入自定義DNS解析程式IP（以逗號分隔）。 範例：208.67.222.222、208.67.220.220。保留為空可使用系統預設DNS解析程式。指定時，會針對每個解析程式查詢每台主機，從而提供不同DNS伺服器之間的比較DNS解析結果。

所有DNS查詢結果都整合到一個輸出檔案中：dns/dns_lookups.txt，每個主機/解析程式組合都帶有結構化TextFSM部分分隔符。



資料包捕獲設定

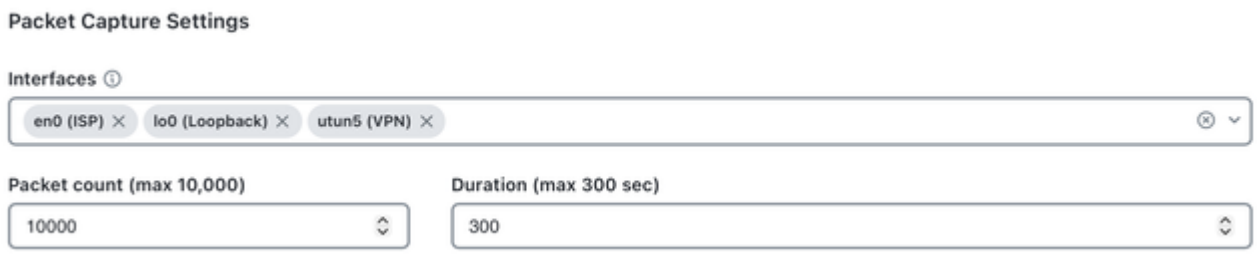
- 介面 — 選擇要捕獲的網路介面（或保留為全部）。
  - 當設定為All（自動模式）時：
    - macOS/Linux:該工具運行tcpdump -D以列舉所有可用介面，然後為處於啟動和運行狀態的介面(不包括斷開連線的介面)進行過濾器。 如果未找到活動介面，則它將回退到特殊的any介面。捕獲將在所有匹配的介面上並行運行。
    - Windows:使用所選捕獲後端在所有NIC上進行捕獲（請參閱下一節中的「工具」）。 使用未選擇介面的dumpcap時，最多可同時捕獲前3個檢測到的介面。
- Packet count — 每個介面要捕獲的資料包數。預設:100.最大值：10,000.

- 持續時間（秒）— 最大捕獲持續時間（秒）。預設:macOS/Linux上20秒，Windows上5秒。最大值：300秒。達到封包計數或持續時間限制時（以先到者為準），擷取會停止。

依平台劃分的封包擷取工具

附註：(Windows):該工具將自動選擇最佳的可用捕獲後端。首選是pktmon（內建於Windows 10 v2004+中），回退到dumpcap（如果已安裝Wireshark），然後作為最後手段使用netsh跟蹤。

Platform	Primary Tool	Fallback 1	Fallback 2
macOS/Linux	`tcpdump`	N/A	N/A
Windows	`pktmon` (Packet Monitor) — captures to ETL, converts to PCAPNG	`dumpcap` (Wireshark) — captures to PCAP	`netsh trace` — captures to ETL



資料包捕獲輸出檔案

使用命名約定將每個介面的捕獲儲存為單獨的檔案：tcpdump/{interface_name}_capture.pcap（例如en0_capture.pcap、eth0_capture.pcap）。還生成後設資料清單檔案(tcpdump/packet_capture_manifest.txt)，記錄使用的平台、資料包計數、持續時間、捕獲的介面和捕獲後端。

Ping設定

- Host/s to ping — 輸入要ping的主機（以逗號分隔）。 示例：www.cisco.com

URL可達性設定

- 要檢查的URL — 輸入要測試的URL（以逗號分隔）。 範例：https://github.com
  - 使用HTTP GET請求測試可達性。
  - 預設埠：80(HTTP)/443(HTTPS)。 將連線埠包括在非標準連線埠的URL中(例如ashttps://example.com:8443)。
  - 每個檢查最大20個URL。
  - 逾時:每個URL30秒。
  - 每個URL收集的資料：URL、可訪問性狀態、HTTP狀態代碼、響應時間(ms)、內容長度、已解析的IP地址、TLS版本和時間戳。
  - 結果儲存到reachability/reachability_results.json和reachability/reachability_summary.txt。

策略測試設定

- 主機URL — 輸入用於策略測試的主機（逗號分隔，最多10個）。 範例：www.cisco.com
- 針對思科策略測試端點執行策略測試：policy.test.sse.cisco.com
- 結果包括結構化策略測試輸出和在測試導航過程中自動捕獲的HAR資料。

HAR捕獲設定

- 目標URL — 輸入HAR捕獲的URL（以逗號分隔）。 範例：https://www.cisco.com/

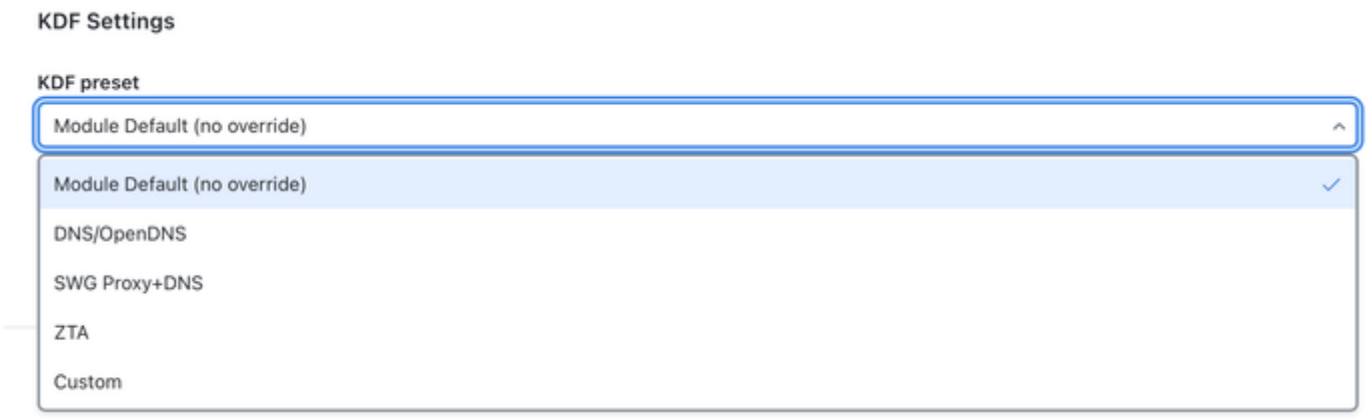
提示：HAR捕獲當前僅支援Google Chrome。該工具使用Chrome DevTools協定（通過chromedp）自動執行無頭的Chrome會話並捕獲網路流量。確保您的系統上安裝了Google Chrome。目前不支援Firefox和Safari。

KDF設置

配置診斷收集期間使用的金鑰派生函式標誌。KDF標志控制思科安全客戶端中啟用的調試類別：

- KDF預設 — 選擇金鑰派生函式預設。
- KDF HEX — 系統會根據選定的預設自動填充十六進位制值。選擇「自定義」時，輸入您自己的十六進位制值。

Preset	Hex Value	Description
Module Default	*(none)*	No KDF override is applied. The Cisco Secure Client's built-in module defaults are used. This preserves the customer's current debug settings.
DNS/OpenDNS	`0x20801FF`	Enables DNS resolution and OpenDNS proxy debug flags via `acsocktool -sdf`.
SWG Proxy+DNS	`0x70C01FF`	Enables SWG + DNS debug flags via `acsocktool -sdf`. Also sets `SWGConfigOverride.json` with `"logLevel": "1"` for enhanced SWG logging.
ZTA (ZTNA)	`0x400080152`	Enables ZTA debug flags via `acsocktool -sdf`. Also sets `logconfig.json` with `"global": "DBG_TRACE"` for maximum verbosity logging. May trigger a VPN agent restart on Windows.
Custom	User-provided	Allows entering a custom hex value for advanced troubleshooting.



保留的IP設定

- NSLookup URLs — 可選的自定義nslookup 主機（以逗號分隔）。 最多10個URL。系統會根據所有已配置的解析程式查詢每個自定義主機。
- 跟蹤URL — 可選的自定義traceroute/tracert主機（以逗號分隔）。 最多10個URL。該工具在macOS/Linux上自動使用traceroute，在Windows上自動使用tracert。
- 解析程式IP — 用於nslookup查詢的可選自定義解析程式IP（以逗號分隔，如208.67.222）。
- 222, 208.67.220.220)。 最多5個IP。指定時，除了三個內建解析器（系統預設DNS、127.0.0.1、208.67.222.222）之外，還會使用自定義解析器。

保留的IP詳細資訊

預設情況下，保留IP診斷程式收集此資料：

預設Traceroute/Tracert目標（自動針對所有這些目標運行）：

目標	目的
208.67.222.222	到OpenDNS主名稱伺服器的路由
208.67.220.220	到OpenDNS輔助名稱伺服器的路由
146.112.255.50	路由到Cisco SWG基礎設施IP
swg-url-proxy-https-sse.sigproxy.qq.opendns.com	路由到SWG代理主機名

- macOS/Linux:使用traceroute命令
- Windows:使用tracert命令

預設NSLookup查詢（自動針對所有這些查詢運行）：

針對解析程式清單中的每個解析程式查詢每個nslookup目標。預設情況下，解析程式清單包括三個內建解析程式：

Resolver	Description
System default DNS	The OS-configured DNS resolver (no explicit server argument)
`127.0.0.1`	Localhost / local DNS proxy (e.g., Cisco Secure Client's local resolver)
`208.67.222.222`	OpenDNS public resolver

如果配置了自定義解析器IP（例如208.67.222.222），則會將這些解析器IP新增到解析器清單中

，並且還會根據它們查詢每個nslookup目標。

NSLookup目標：

Target	Query Type	Purpose
`debug.opendns.com`	TXT (`-type=txt`)	OpenDNS debug record — returns device identity, organization ID, policy flags, and server info
`swg-url-proxy-https-sse.sigproxy.qq.opendns.com`	A (default)	SWG proxy hostname resolution — verifies DNS is correctly resolving the SWG proxy endpoint

例如，使用預設的3個解析程式時，這會產生6 nslookup查詢（2個目標x 3個解析程式）。 新增一個自定義解析程式IP會將此問題增加為8個查詢（2個目標x 4個解析程式）。

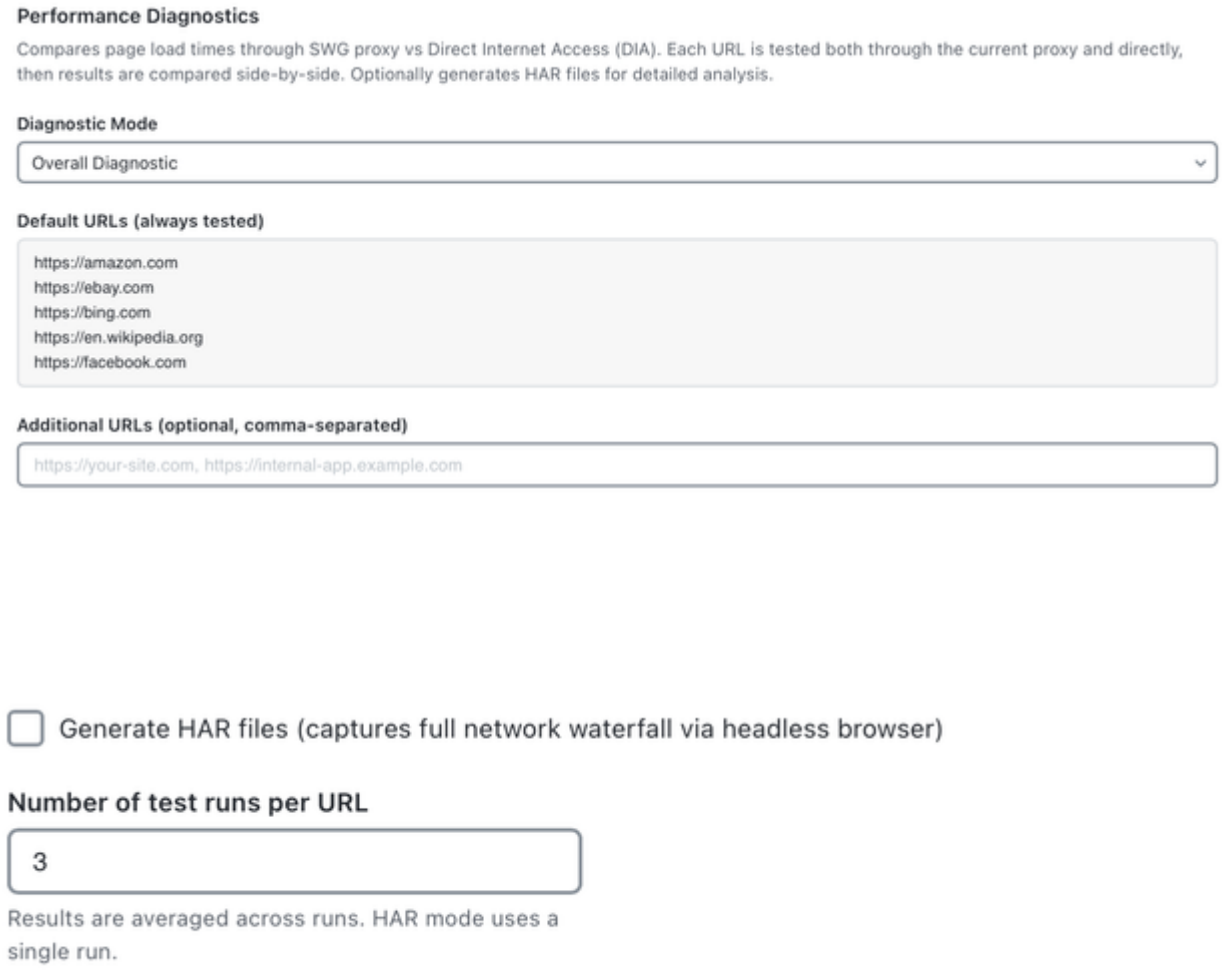
每個自定義使用者提供的NSLookup URL都根據相同的完整解析程式清單（內建+自定義解析程式）進行查詢。

所有結果都整合到一個檔案中：reserved_ip/reserved_ip_diagnostics.txt，按節(traceroute、nslookup)分組，使用可讀標題表示每個條目的目標和解析程式。

效能診斷

比較通過SWG代理與直接網際網路訪問(DIA)的頁面載入時間。它有兩種模式：

1 總體診斷模式：通過當前代理和直接測試每個URL，然後逐一比較結果。（可選）生成用於詳細分析的HAR檔案。



2 一個URL診斷模式:我們可以通過當前代理和直接輸入要測試的特定URL，然後將結果並排比較。（可選）生成用於詳細分析的HAR檔案。

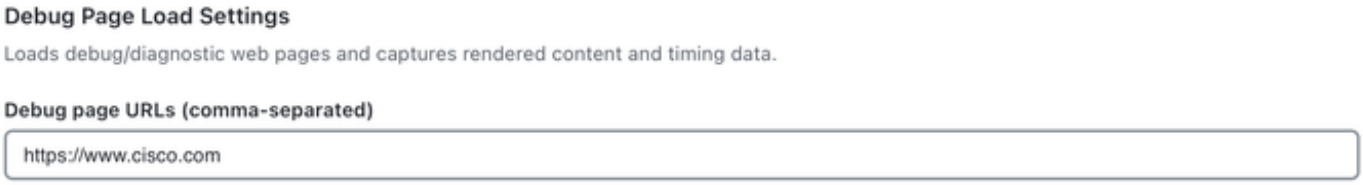
證書儲存清單設定

- 列舉已配置的證書儲存中的證書：

    - 系統
    - 登入
    - 根
    - 以及更多
- 快速識別缺失、過期或不受信任的證書

調試頁面載入設定：

- 載入可配置的調試URL。
- 捕獲：
    - 響應報頭
    - 響應正文
    - 計時資訊
    - SSL後設資料



動作

1. 填寫或調整每個已啟用的診斷的設定。
2. 按一下Start Diagnostics開始診斷運行。
3. 按一下Back返回步驟1，或按一下Cancel退出

附註：帶有驗證錯誤的欄位將突出顯示。您必須先更正這些錯誤，才能開始診斷。

暫停並繼續

當您運行包括高級故障排除的診斷集合(例如ZTNA或SWG跟蹤)時，思科端點診斷工具可以在運行過程中暫停，並要求您在問題繼續之前重現該問題。

這樣，在開啟詳細日誌記錄時您就有時間觸發問題，因此支援團隊會收到更多有用的診斷資料。

- 出現Diagnostics Paused視窗時，請閱讀消息 — 它告訴您哪些日誌記錄功能現在處於活動狀態。
- 重現您正在解決的問題。舉例來說：
    - 重新連線到VPN
    - 開啟發生故障的內部應用程式
    - 重複導致錯誤的步驟
- 重現問題後，按一下Continue

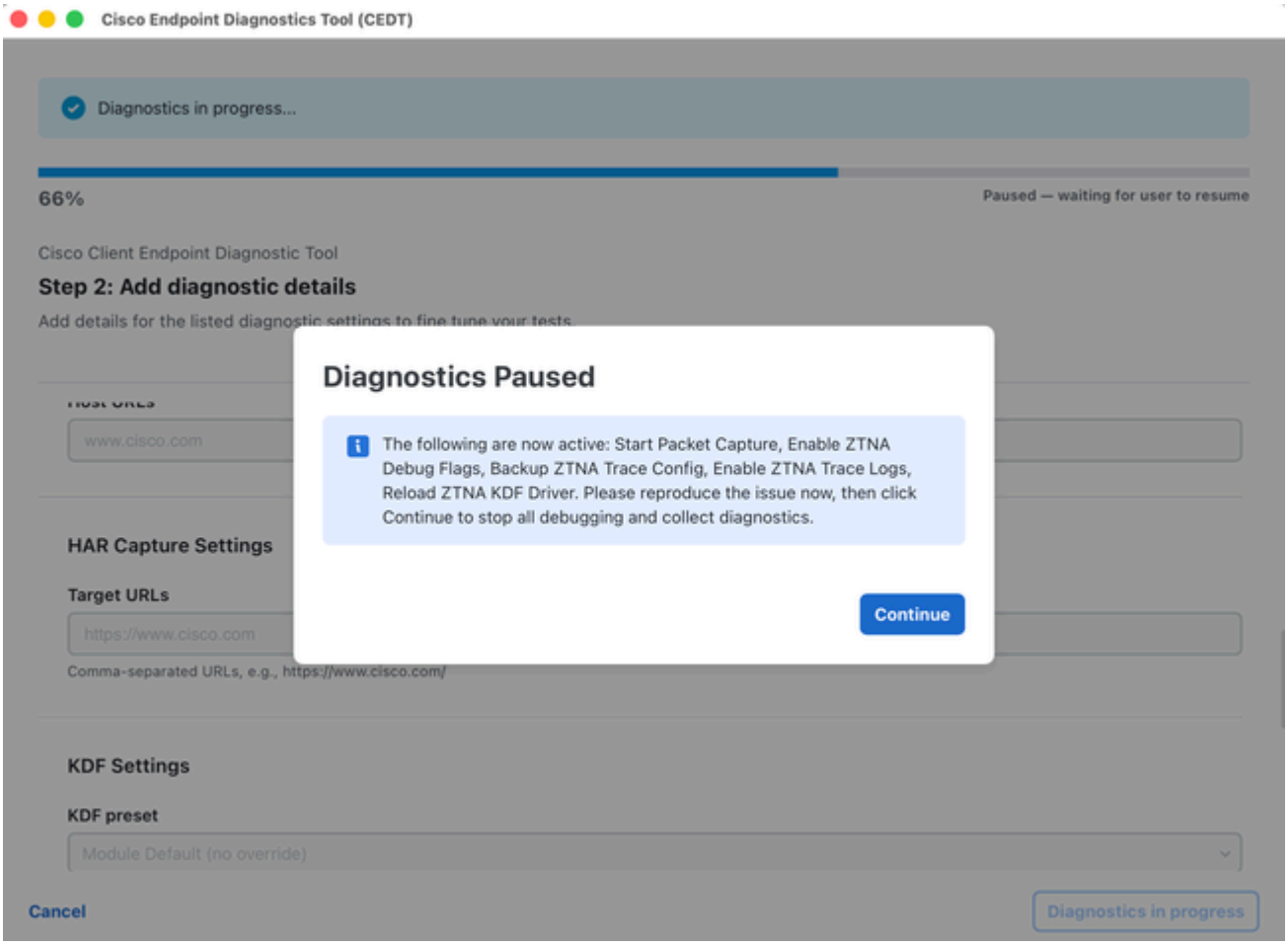
讓跑完吧。然後，該工具將收集檔案、恢復正常設定並建立診斷存檔。

注意：暫停時不要關閉應用程式。在按一下Continue並運行完成之前，日誌記錄將保持活動狀態。

（命令列）

如果從終端運行該工具，則可以在視窗中看到暫停消息，而不是對話方塊。

1. 閱讀終端中顯示的暫停消息。
2. 重現問題。
3. 返回終端並按Enter鍵繼續。
4. 等待運行完成。

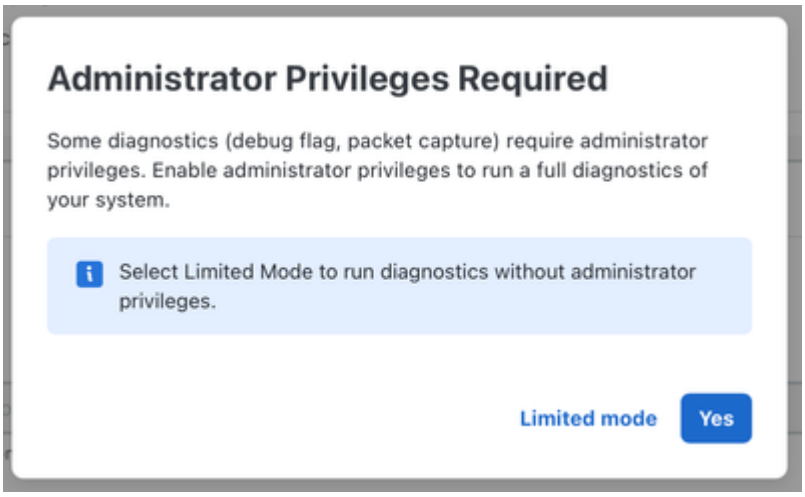


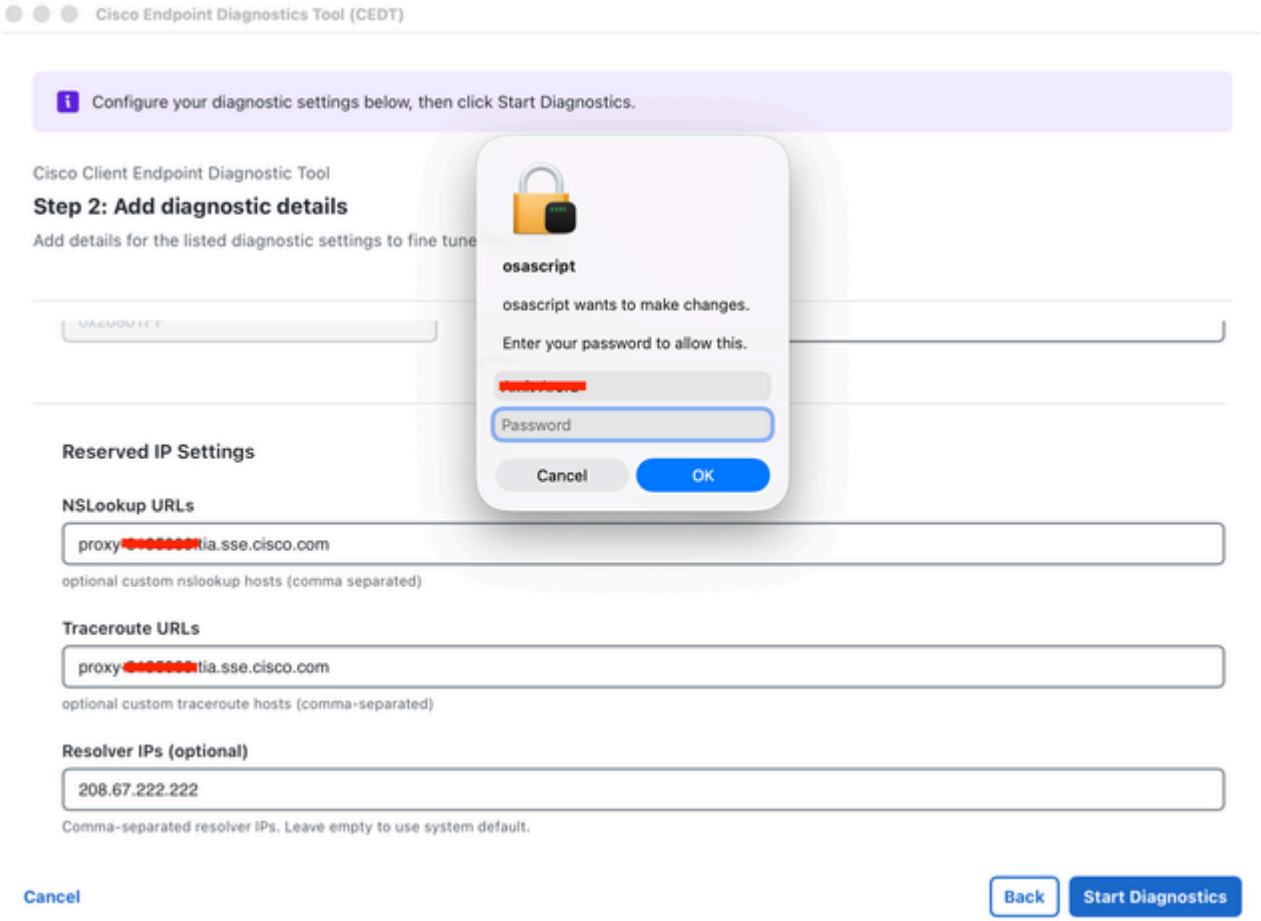
管理員許可權提示

按一下Start Diagnostics後，如果您啟用了需要提升訪問權的功能（如資料包捕獲或調試標誌），該工具將提示您輸入管理員許可權。

此時將顯示一個名為Administrator Privileges Required的對話方塊：

- 按一下Yes授予管理員許可權。這將觸發本機macOS/Windows憑據提示。
- 按一下Limited mode以繼續操作而不進行高程。已跳過特權任務（資料包捕獲、調試標誌）。
- macOS:您可以從osascript看到標準macOS密碼對話方塊。輸入您的系統密碼，然後按一下OK。
- Windows:出現標準UAC標高提示。按一下Yes以允許。





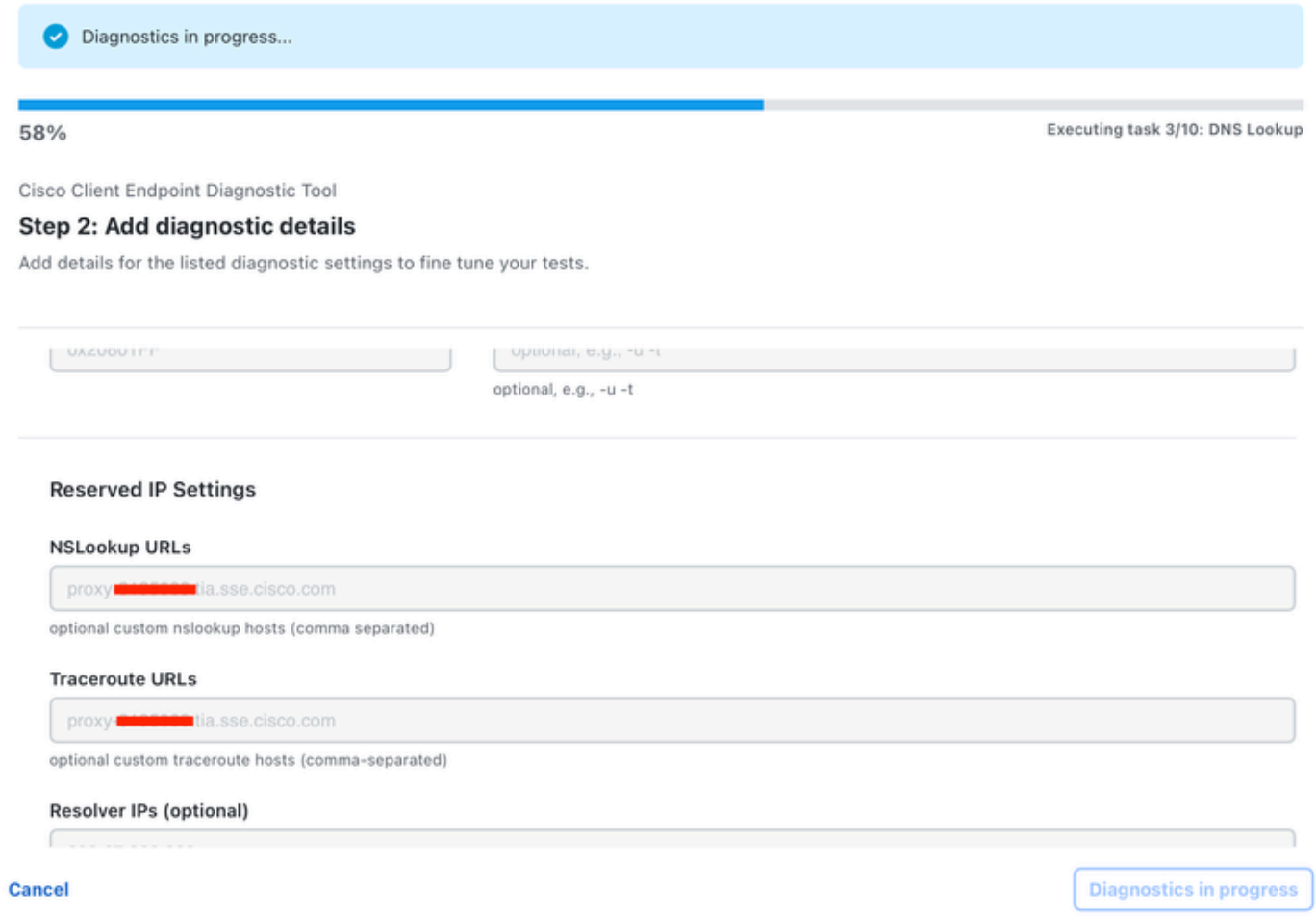
診斷正在進行

啟動後，該工具將運行所有選定的診斷任務：

- 進度條顯示整體完成情況(例如59% — 正在執行任務3/9:DNS查詢)。

- 診斷正在進行..... 標題顯示在頂部。
- 在運行期間，所有設定欄位均被禁用/灰顯。
- 頁尾顯示「Diagnostics in progress」按鈕（已禁用），表示工具正忙。

診斷正在完成，請稍候。請勿關閉應用程式。



1.

診斷完成 — 上傳到TAC

完成所有診斷後，將出現完成對話方塊：

診斷完成。上傳檔案至TAC案件。

該對話方塊顯示：

- 存檔 — 生成的診斷存檔的檔名（如cisco_diagnostics.tar.gz）。
- 檔案大小 — 歸檔檔案的大小（如7.72 MB）。
- SHA256 — 用於完整性驗證的歸檔檔案的校驗和。

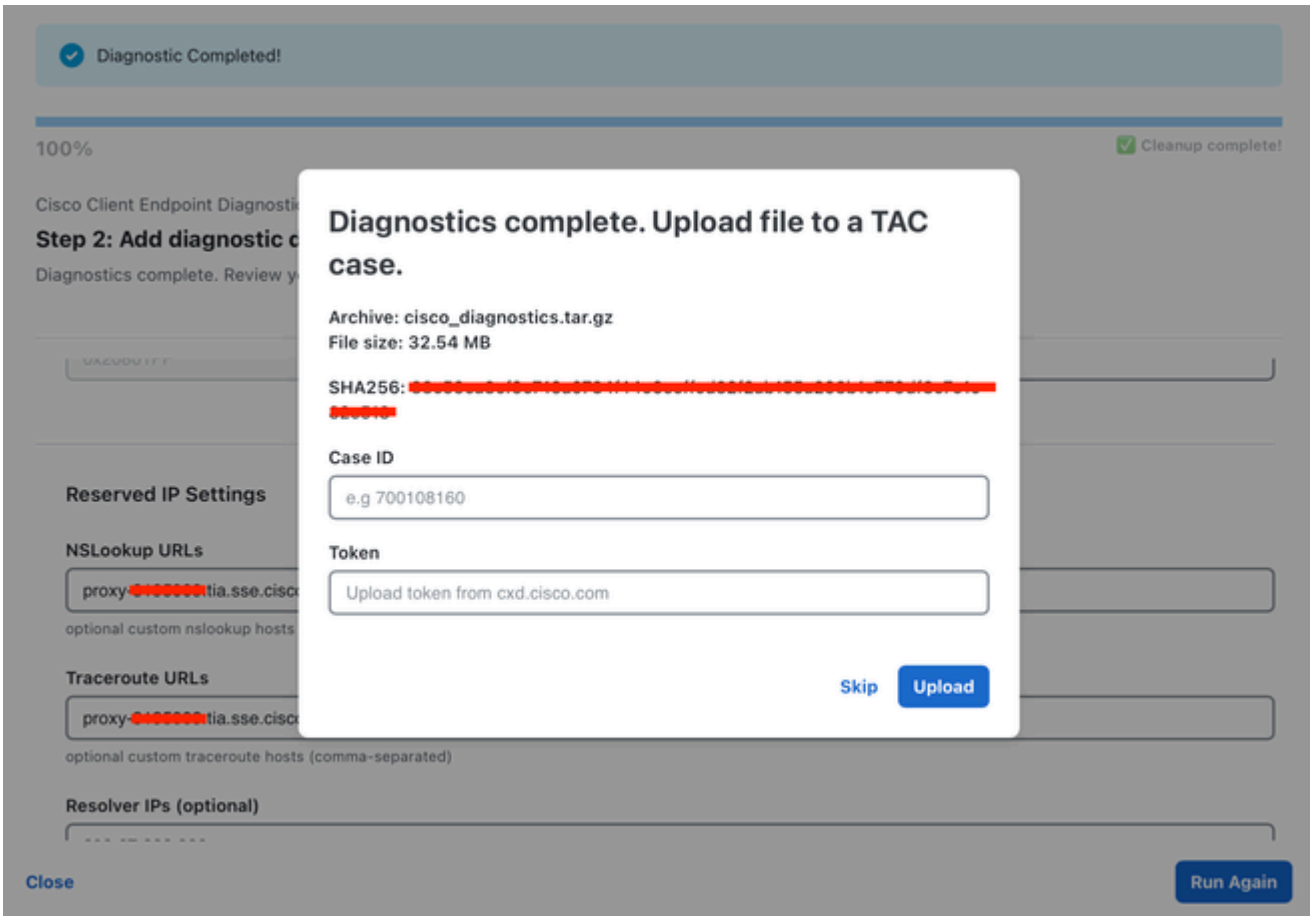
上傳到TAC案例的步驟：

1. 輸入您的Case ID(例如698746730)。
2. 輸入您的權杖（由思科支援提供）。
3. 按一下「Open TAC Case」以開始上傳。

進度條顯示上傳狀態(例如上傳……85.0%(6.56 MB / 7.72 MB)。

要跳過上載，請執行以下操作：

- 按一下Skip關閉對話方塊而不上載。存檔檔案仍儲存在本地。



上傳完成 — 最終螢幕

成功上傳後，完成橫幅將更新為：

診斷存檔已成功上載到案例[案例ID]

進度條顯示100%處於清理完成狀態。

動作

- 按一下Run Again開始新的診斷運行。
- 按一下Close退出應用程式。

輸出位置

診斷輸出儲存到：

- macOS:~/Desktop/cisco_diagnostics/
- Windows:%USERPROFILE%\Desktop\cisco_diagnostics\

輸出存檔檔案(cisco_diagnostics.tar.gz)以結構化格式包含所有收集的診斷資料。

疑難排解

Issue	Resolution
No products detected	Ensure Cisco Secure Client is installed and running on your system.
Packet Capture greyed out	Enable it in Step 1, and grant administrator privileges when prompted.
Debug Flags greyed out	At least one Cisco Secure Access product must be detected and selected.
DebugView greyed out	This option is only available on Windows.
Upload fails	Verify your Case ID and Token are correct. Check your internet connection.
"Administrator credentials could not be obtained"	You cancelled the password prompt or entered an incorrect password. Click Start Diagnostics again to retry.
Limited mode warning	Some privileged tasks were skipped. Re-run with administrator privileges for a full diagnostic.

常見問題

Q:此工具收集哪些資料？
A:該工具僅收集系統資訊（作業系統、硬體、網路配置）、應用程式日誌、思科產品配置和已安裝模組資料，以及與思科安全訪問模組相關的網路診斷資料。有關詳細的細分資訊，請參閱上節收集了哪些系統資料。未捕獲任何個人資料。

Q:是否需要管理員/根使用者訪問許可權？

A:管理員訪問許可權是可選的，但建議使用。如果沒有該標誌，則會跳過某些診斷（資料包捕獲、調試標誌）。該工具會提示您並允許您選擇。

Q:我可以多次運行該工具嗎？
A:會。每次運行完成後，可以按一下「再次運行」以啟動新的診斷會話。

Q:輸出儲存在何處？
A:診斷歸檔檔案將儲存到cisco_diagnostics資料夾下的Desktop（案頭）。

Q:如果我沒有TAC案例ID呢？
A:您可以在上傳對話方塊中按一下「跳過」。存檔檔案仍儲存在本地。您可以稍後手動將其上傳到TAC案例，或與您的支援工程師共用。

Q:資料是否已加密？
A:診斷歸檔檔案被壓縮(tar.gz)，敏感資料在打包前自動進行編輯。

Q:HAR捕獲支援哪些瀏覽器？
A:HAR捕獲目前僅支援Google Chrome。該工具使用Chrome DevTools協定實現無頭瀏覽器自動化。在運行HAR捕獲之前確保已安裝Chrome。

Q暫停畫面從不出現。有什麼不對嗎？

A:不一定。僅當為方案成功啟用詳細日誌記錄時，才會顯示暫停步驟。檢查應用中的運行日誌 — 如果跳過啟用步驟，工具將繼續運行，而不暫停。

Q這輪漲勢似乎陷入了僵局。我該怎麼辦？

A:查詢「Diagnostics Paused」視窗 — 它可能位於其他視窗後面。只有按一下Continue(或在命令列中按Enter)後，運行才會繼續。

問：這條消息列出了我不期望的功能。這是正常的嗎？

A:會。該消息顯示為您的平台啟用的工具所啟用的任何日誌記錄功能以及您選擇的診斷選項。

問：暫停期間我關閉了應用。現在怎麼辦？

A:再次運行診斷集合，然後讓它完成。如果您不確定日誌記錄是否處於開啟狀態，請與您的支援工程師聯絡以獲取指導。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。