收集詳細的ZTNA日誌以進行故障排除

目錄

簡介

本文檔介紹如何收集詳細的ZTA故障排除日誌、何時啟用以及分步執行。

背景資訊

隨著組織越來越多地採用零信任架構(ZTA)來保護使用者、裝置和應用，對連線和策略實施問題進行故障排除變得越來越複雜。與傳統基於外圍的模型不同，ZTA依賴於跨身份、裝置狀態、網路環境和基於雲的策略引擎的多項即時決策。出現問題時，高級日誌通常不足以查明根本原因。

收集詳細的ZTA級別跟蹤對於深入瞭解客戶端行為、策略評估、流量攔截和雲服務互動至關重要。這些跟蹤使工程師能夠超越基於症狀的故障排除，分析導致訪問失敗、效能下降或意外策略結果的事件確切順序。

收集日誌

在建立TAC案例之前進行預檢查

這些預檢查將幫助TAC團隊更有效地識別問題。向工程師提供此資訊有助於他們儘快解決您的問題：

- 問題是什麼？有多少使用者受到影響？
- 哪些作業系統和版本會受到影響？

- 問題是一致還是間歇性的？如果是間歇性的，它是使用者專用還是廣泛使用？
- 問題是在更改後開始還是部署後一直存在？
- 有已知的觸發因素嗎？
- 是否有變通辦法？

要收集的日誌

- DART捆綁包
- ZTNA調試跟蹤模式日誌
- Wireshark捕獲（所有介面，包括環回）
- 觀察到的錯誤消息
- 問題的時間戳
- CSC ZTA模組狀態螢幕快照
- 受影響使用者的使用者名稱

接下來的幾節將詳細介紹如何啟用和收集這些日誌。

啟用ZTNA調試跟蹤模式

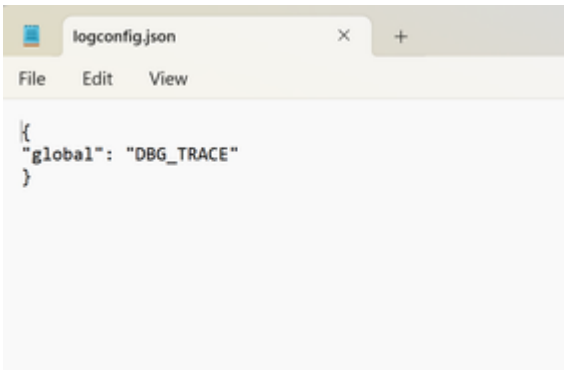
建立名為logconfig.json、具有以下詳細資訊的檔案：

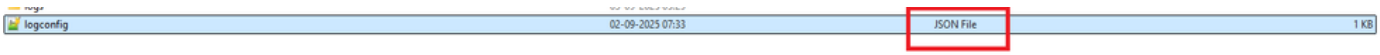
```
{ "global": "DBG_TRACE" }
```

 警告：請確保使用名稱儲存您的檔案logconfig.json。

建立檔案後，根據作業系統將其放在適當的位置：

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS:/opt/cisco/secureclient/zta





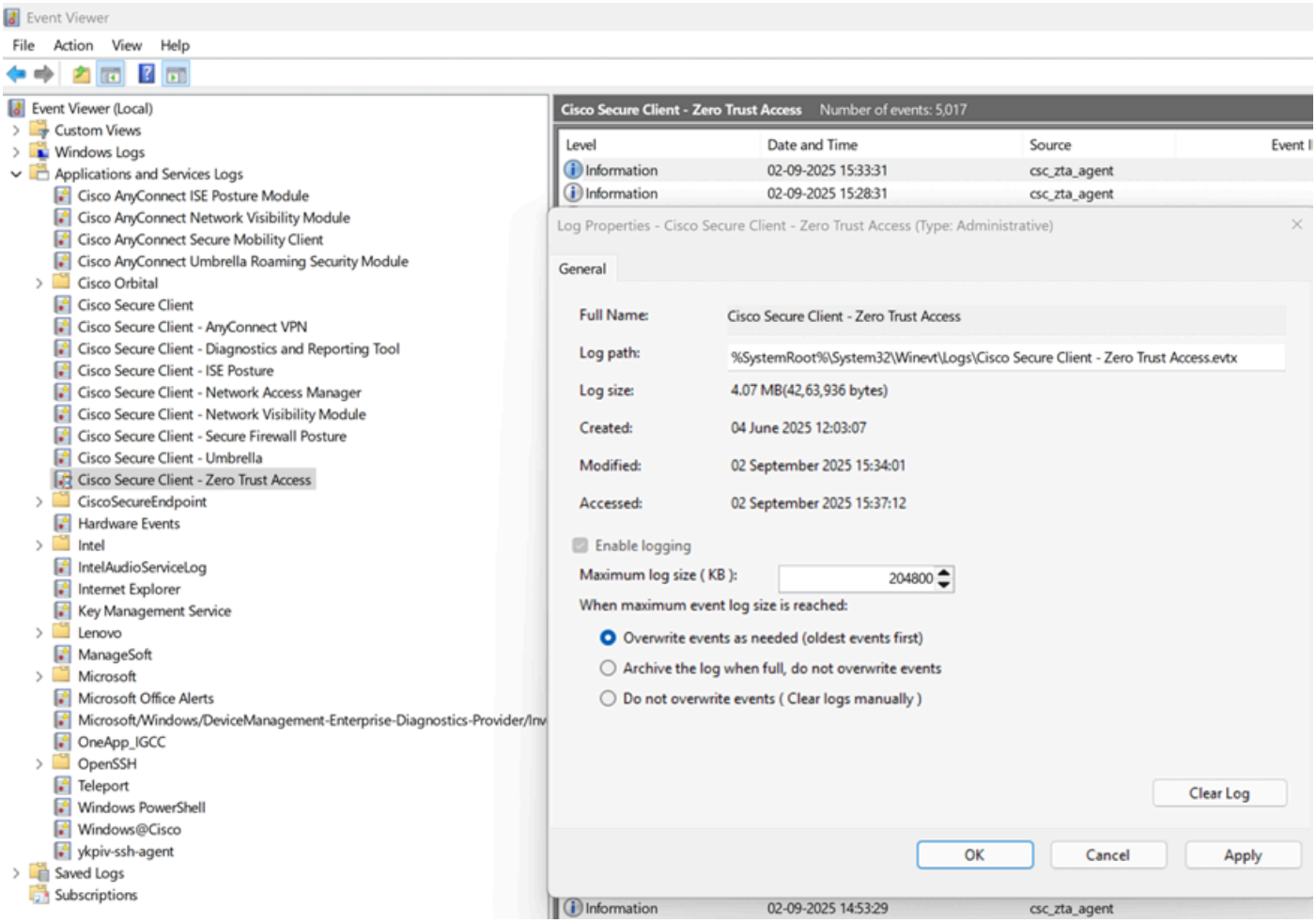
附註：建立指定檔案後，必須重新啟動零信任訪問代理服務(請檢查步驟重新啟動ZTA服務)。 如果無法重新啟動服務，請重新啟動電腦。

在事件檢視器中增加ZTA日誌大小

在Windows PC上，啟用跟蹤級別日誌記錄後，必須手動增加ZTA日誌檔案大小。

1. 未解決.Event Viewer
2. 在左窗格中，展開Applications and Services Logs。
3. 按一下右鍵Cisco Secure Client – Zero Trust Access，然後選擇Properties。
4. 在Maximum log size (KB)下，將值設定為204800（相當於200 MB）。

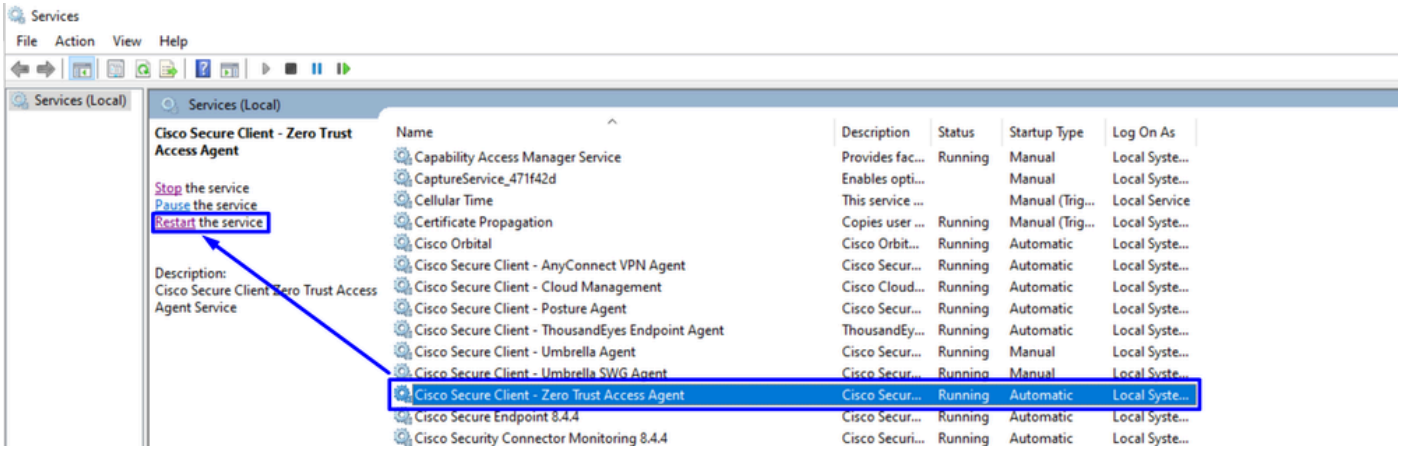
要完成定稿，請單**Apply**擊，然後OK。



正在重新啟動ZTA服務

Windows

- 使Windows + R用開啟Run Search writeservices.msc，然後按Enter
- 找到該服務Cisco Secure Client - Zero trust Access Agent，然後按一下Restart。完成後，驗證CSC ZTA模組狀態以確認其處於活動狀態



附註：如果由於缺少管理訪問許可權而無法重新啟動ZTA服務，則完全系統重新啟動是您的

下一個選項。

MacOS

Stop Service

```
sudo "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app/Contents/MacOS/Cisco
```

Start Service

```
open -a "/opt/cisco/secureclient/zta/bin/Cisco Secure Client - Zero Trust Access.app"
```

附註：如果由於缺少管理訪問許可權而無法執行命令或ZTA服務無法重新啟動，則下一個選項是完整的系統重新啟動。

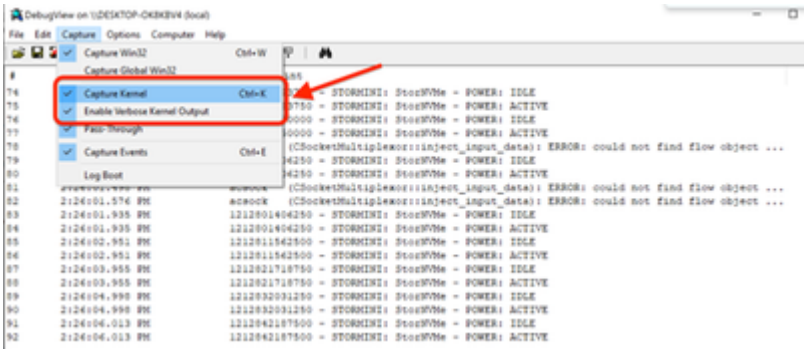
啟用KDF記錄、資料包捕獲、Duo調試模式和Dart套件

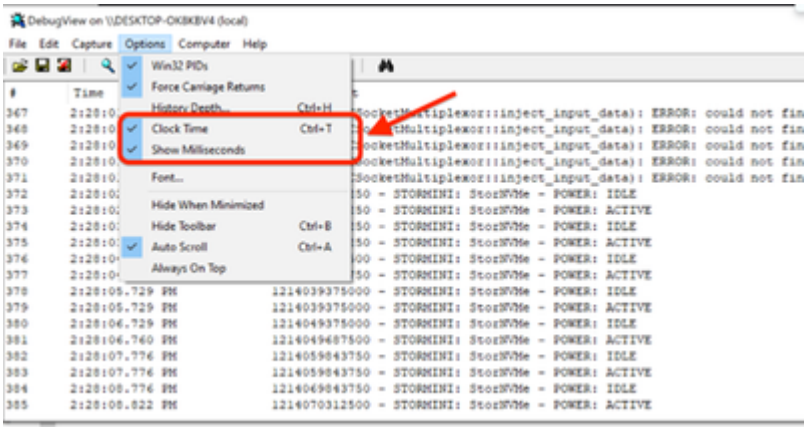
Windows

開啟具有管理員許可權的CMD並運行下一個命令：

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x400080152
```

- 從SysInternal下載DebugView以捕獲KDF日誌
- 運行DebugViewadministrator as 並啟用下一個選單選項：
- 按一下Capture（捕獲）
  - 複選標籤 Capture Kernel
  - 複選標籤 Enable Verbose Kernel Output
- 選項
  - 複選標籤 Clock Time
  - 複選標籤 Show Milliseconds

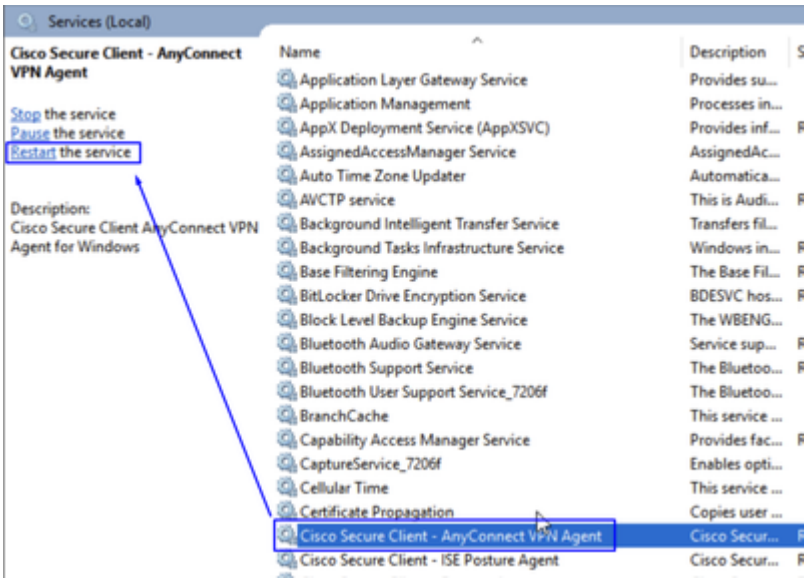




- 通過管理員提示重新啟動客戶端服務：

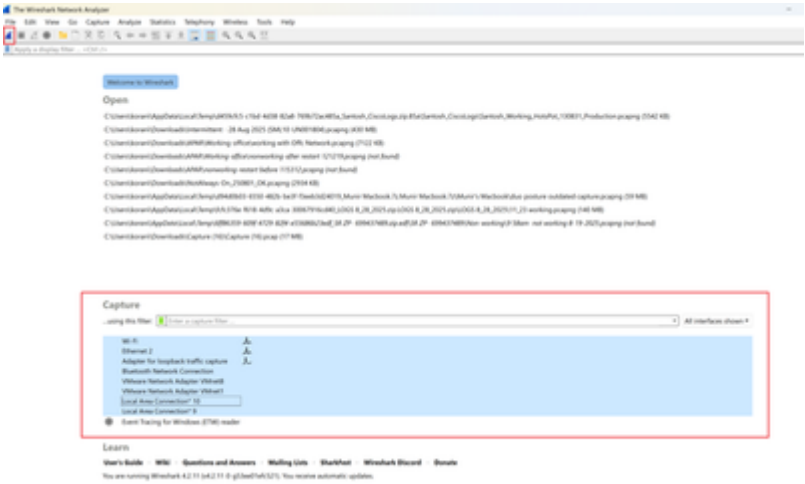
```
net stop csc_vpnagent && net start csc_vpnagent
```

- 如果net stop csc_vpnagent && net start csc_vpnagent不起作用，請從Cisco Secure Clientservices.msc重新啟動服務

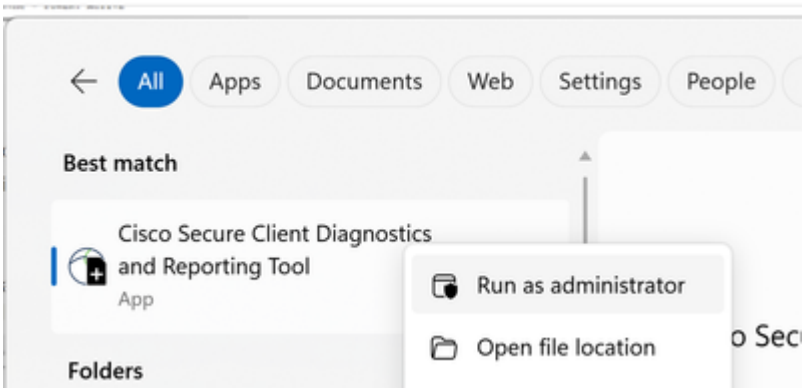


- 在偵錯模式下啟用Duo
- 開始 Wireshark Capture

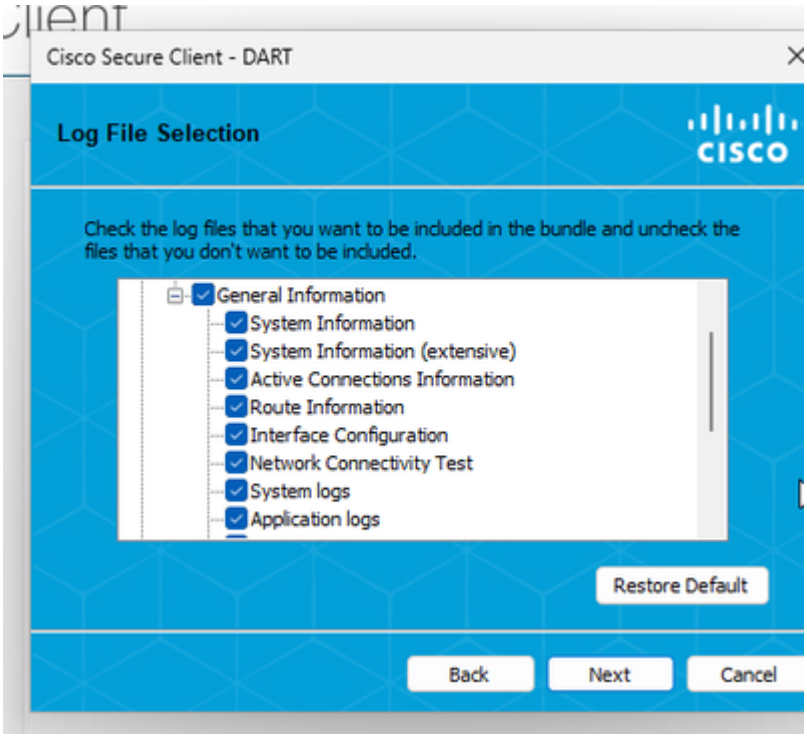
- 選擇所有介面，然後開始資料包捕獲



- 重現問題，然後儲存KDF Logs和Wireshark Capture，然後按照步驟進行捕獲 DART Bundle
- 以管理員Cisco Secure Client Diagnostics & Reporting Tool (DART)許可權開啟



- 按一下 Custom
  - 包括System Information Extensive和 Network Connectivity Test



- 要停止Windows上的KDF日誌記錄，請使用以下命令：

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

附註：將所有日誌、KDF日誌、Wireshark捕獲和DART捆綁包收集到TAC案例。

MacOS

開啟terminal，然後按照下一個命令鏈在MacOS上啟用KDF日誌記錄：

- Stop Service

```
sudo "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app/Contents/MacOS/Cisco
```

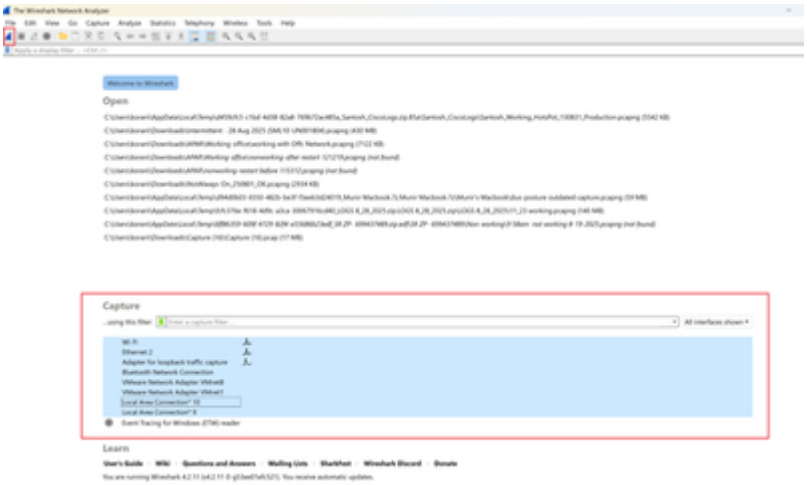
- Enable Flag

```
echo debug=0x400080152 | sudo tee /opt/cisco/secureclient/kdf/acsock.cfg
```

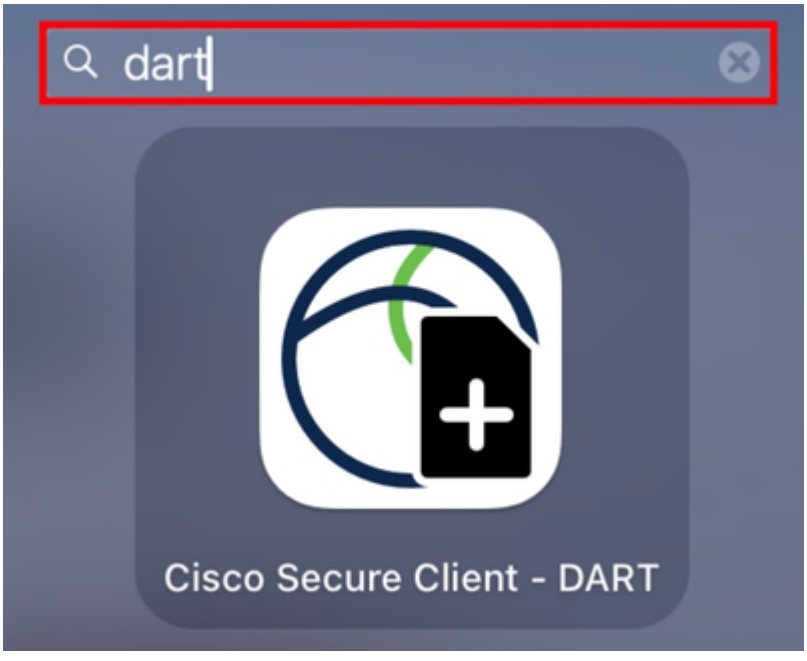
- Start Service

```
open -a "/opt/cisco/secureclient/bin/Cisco Secure Client - AnyConnect VPN Service.app"
```

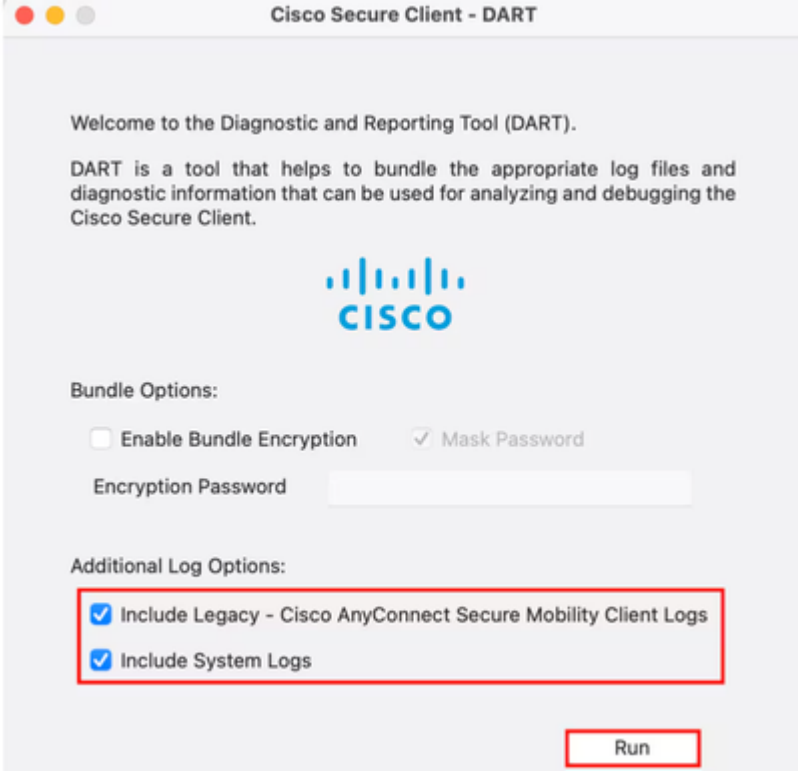
- 在偵錯模式下啟用Duo
- 開始 Wireshark Capture
- 選擇所有介面，然後開始資料包捕獲



- 重現問題，然後儲存KDF Logs和Wireshark Capture，然後按照步驟進行捕獲 DART Bundle
- 開啟 Cisco Secure Client - DART



- 選中下一個選項：
  - Include Legacy - Cisco AnyConnect Secure Mobility Client Logs
  - Include System Logs
- 按一下 Run



附註：將所有日誌、KDF日誌、Wireshark捕獲和DART捆綁包收集到TAC案例。

相關資訊

- 思科技術支援與下載
- Cisco Secure Access幫助中心
- Cisco SASE設計手冊
- 收集Windows和MacOS上安全客戶端的KDF日誌

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）。