

收集Windows裝置安全終結點中的調試日誌檔案

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[在Cisco Secure Endpoint for Windows中收集調試日誌檔案](#)

[版本7.5.5及更低版本](#)

[8.0.1及更高版本 \(思科安全客戶端 \)](#)

簡介

本檔案介紹從思科安全終端聯結器產生偵錯套件組合檔案的步驟。

作者：Javi Martinez，思科TAC工程師。

必要條件

需求

思科建議您瞭解Cisco Secure Endpoint Connector。

採用元件

文中使用的資訊是根據以下軟體版本：

- Microsoft Windows作業系統
- 思科安全終端聯結器6.3.7及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

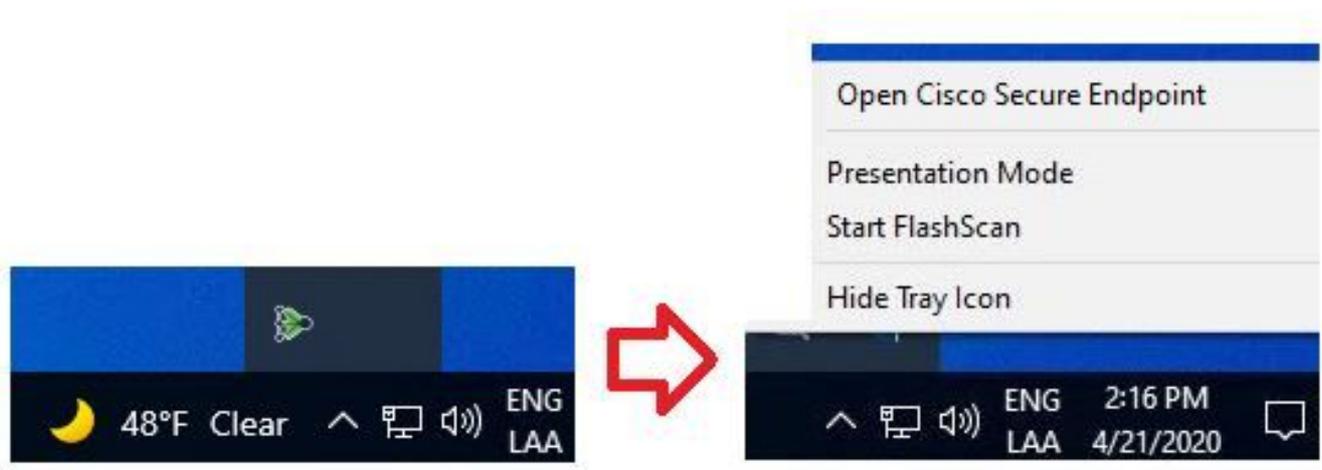
如果您在Microsoft Windows作業系統中遇到思科安全終結點聯結器的效能問題，請聯絡思科技術支援中心(TAC)。思科技術支援工程師繼續分析調試捆綁檔案中可用的日誌，以查詢根本問題。

附註： 如果重新啟動裝置，則從IP托盤介面啟用調試模式將無法經受重新啟動。在重新啟動的情況下，可以通過安全終端控制檯中的策略配置啟用調試模式。

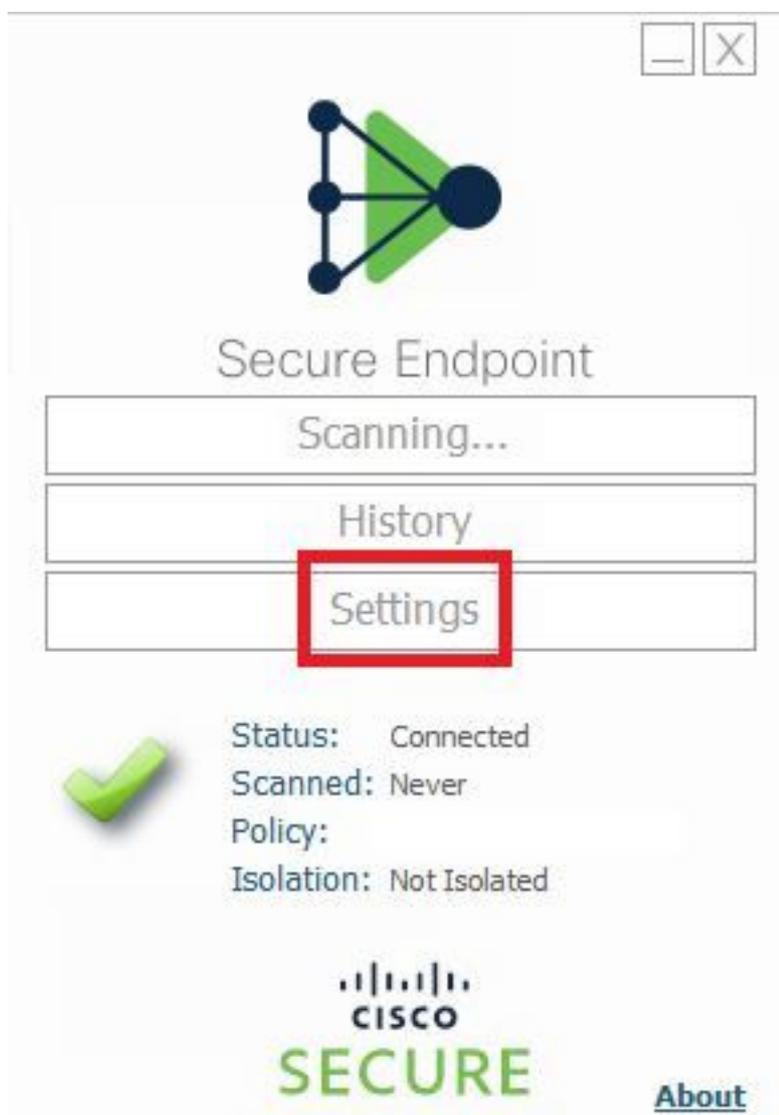
在Cisco Secure Endpoint for Windows中收集調試日誌檔案

版本7.5.5及更低版本

步驟1.使用工作列上的工作列圖示，選擇**開啟**思科安全終端，如下圖所示。



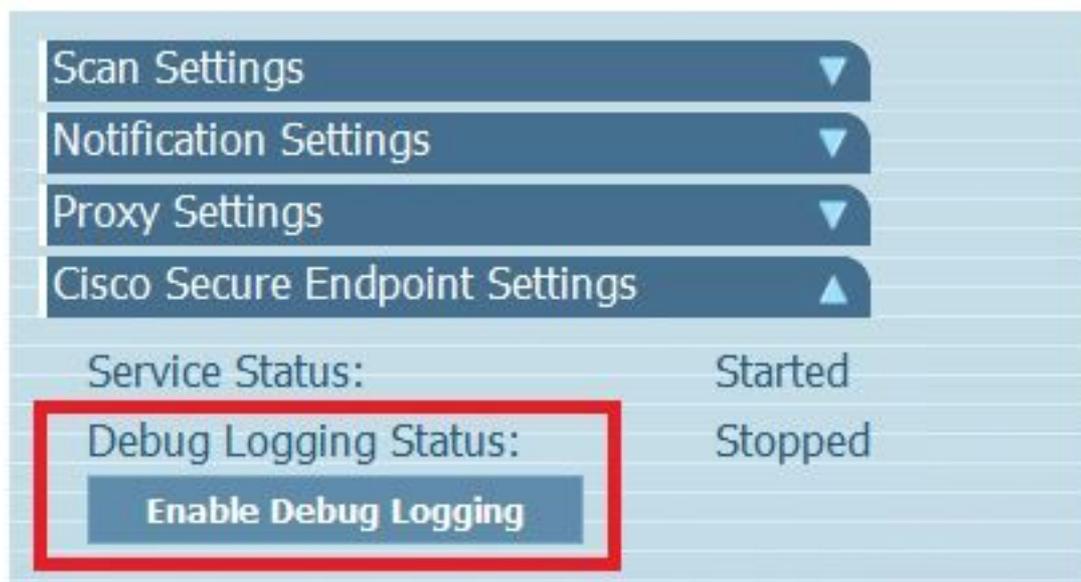
步驟2.選擇Secure Endpoint Connector中的**Settings**選項，如下圖所示。



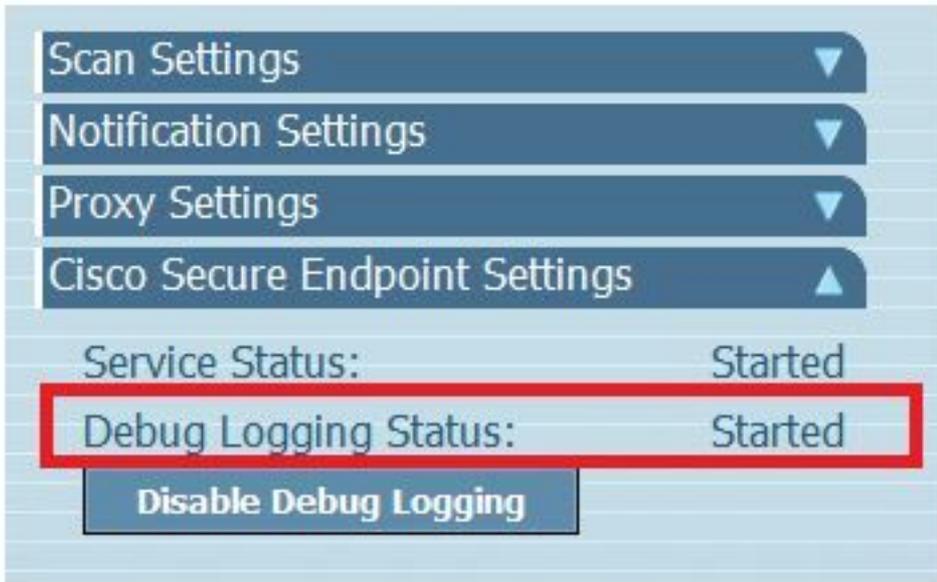
步驟3.導覽至**Settings**，然後選擇**Cisco Secure Endpoint Connector Settings**選單，如下圖所示。



步驟4.選擇Enable Debug Logging按鈕，如下圖所示。

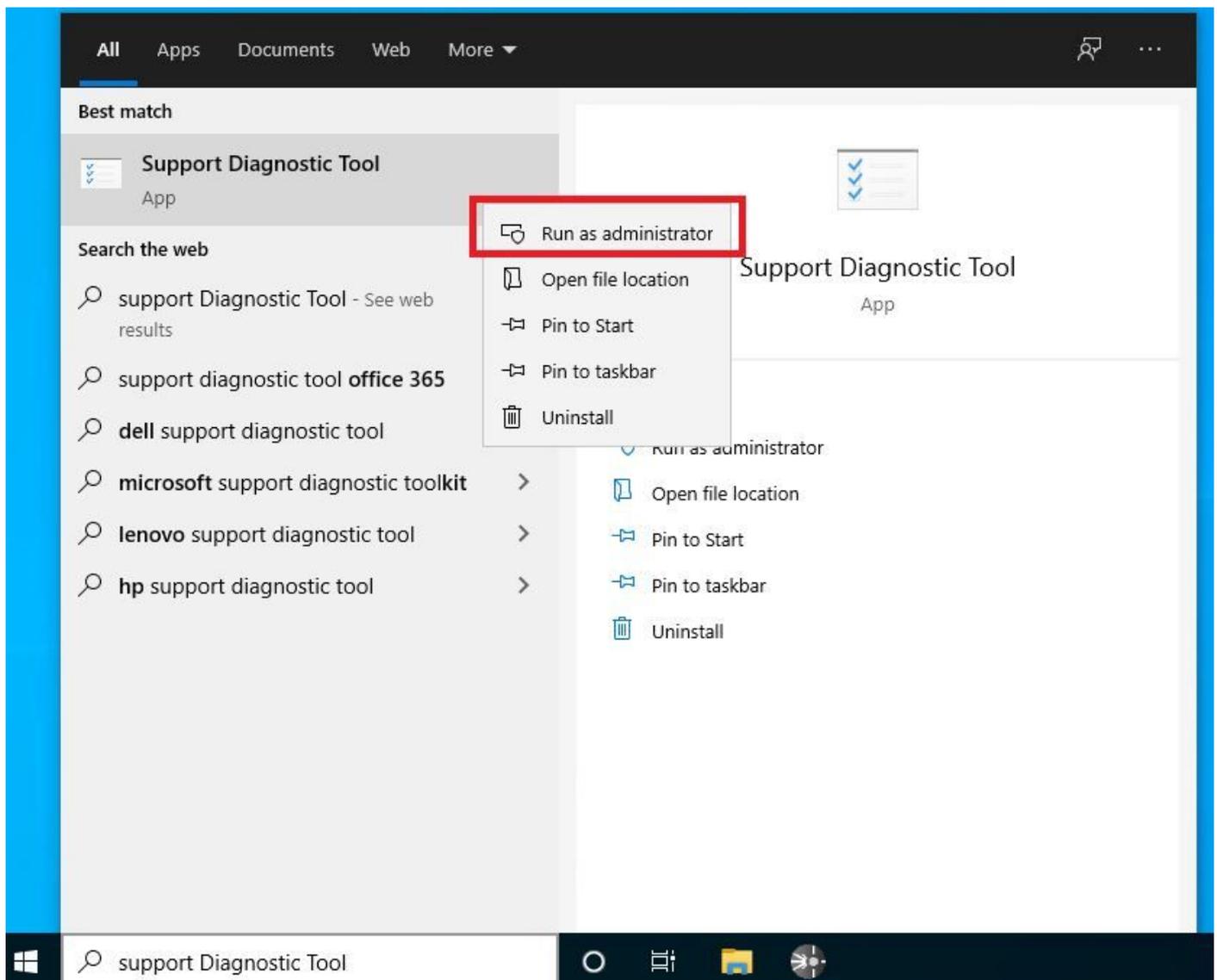


步驟4.1.按鈕名稱更改為Disable Debug Logging。現在您處於偵錯模式，如下圖所示。



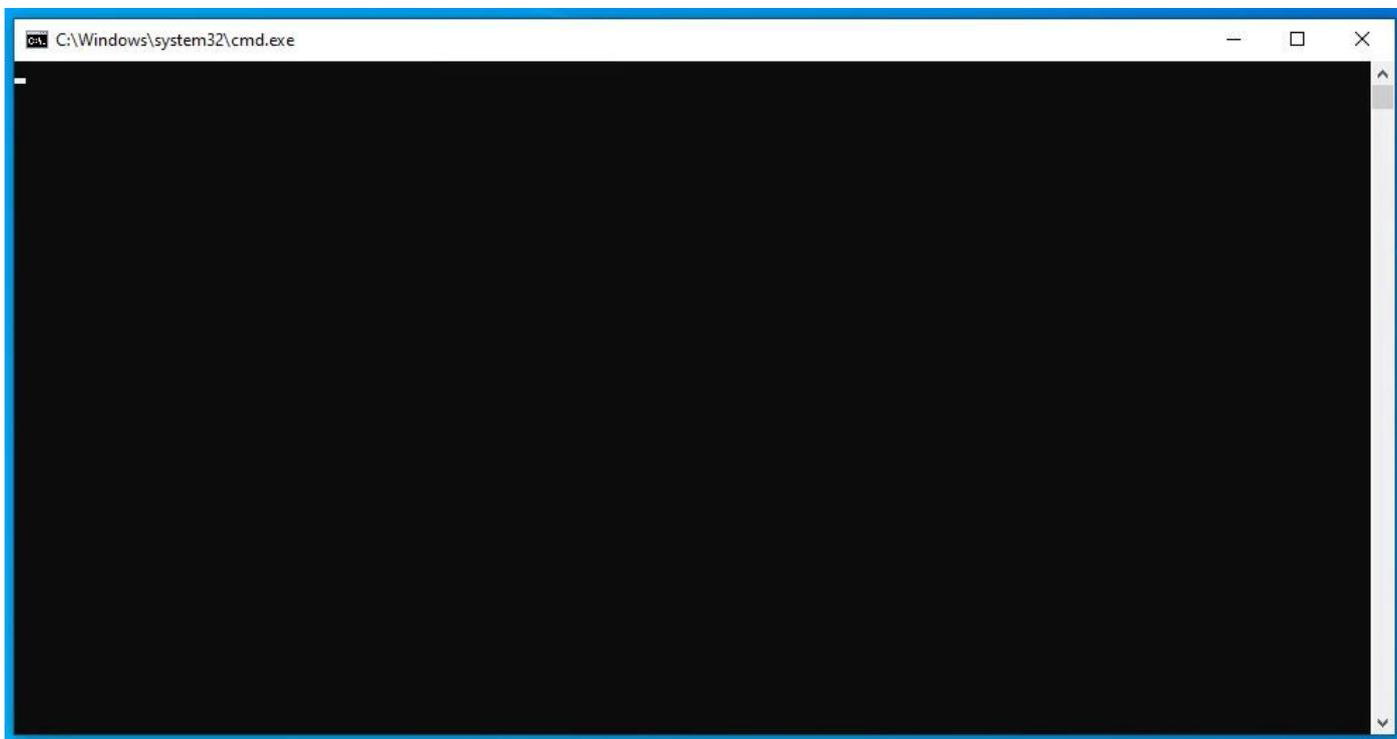
步驟5.重新建立問題並讓裝置運行至少30分鐘。

步驟6.在30分鐘後，開啟Windows搜尋，然後寫入**支援診斷工具**，此時將顯示診斷工具。請以管理員許可權執行該工具，如下圖所示。



注意：在Secure Endpoint Connector v7.5.5中，不需要具有管理員許可權的Windows帳戶來開啟支援診斷工具以收集調試日誌。[發行說明](#)：「已更新支援診斷工具，因此它不需要提升的許可權」。

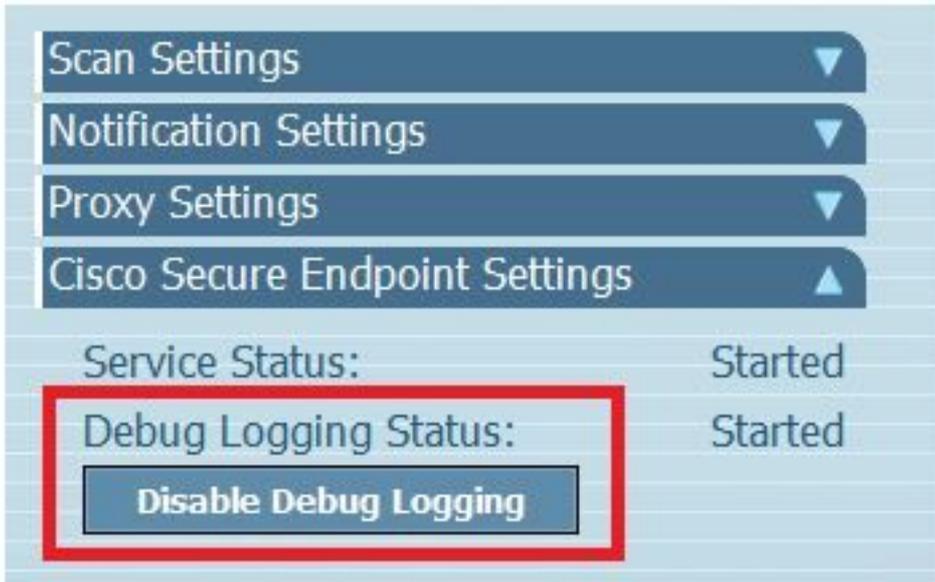
步驟7.顯示臨時Windows黑屏，如下圖所示。
(請等待幾秒鐘，Windows黑屏將自行關閉)。



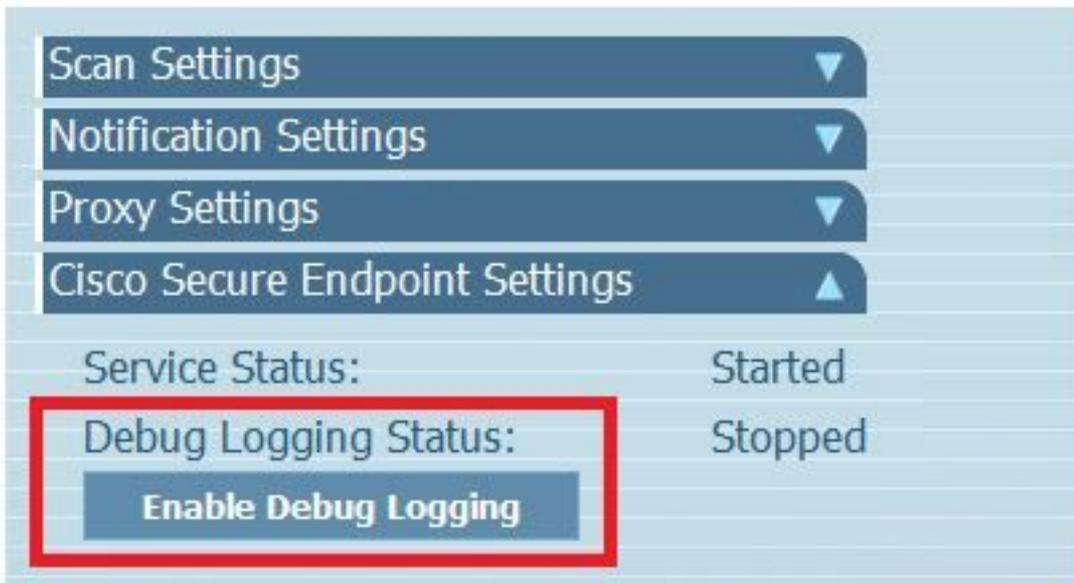
步驟8.幾分鐘後，案頭上會顯示Debug Bundle檔案，如下圖所示。



步驟9.產生偵錯套件組合檔案後，即可停用偵錯模式。選擇Disable Debug Logging按鈕，如下圖所示。



步驟9.1. 按鈕名稱變更為Enable Debug Logging，如下圖所示。



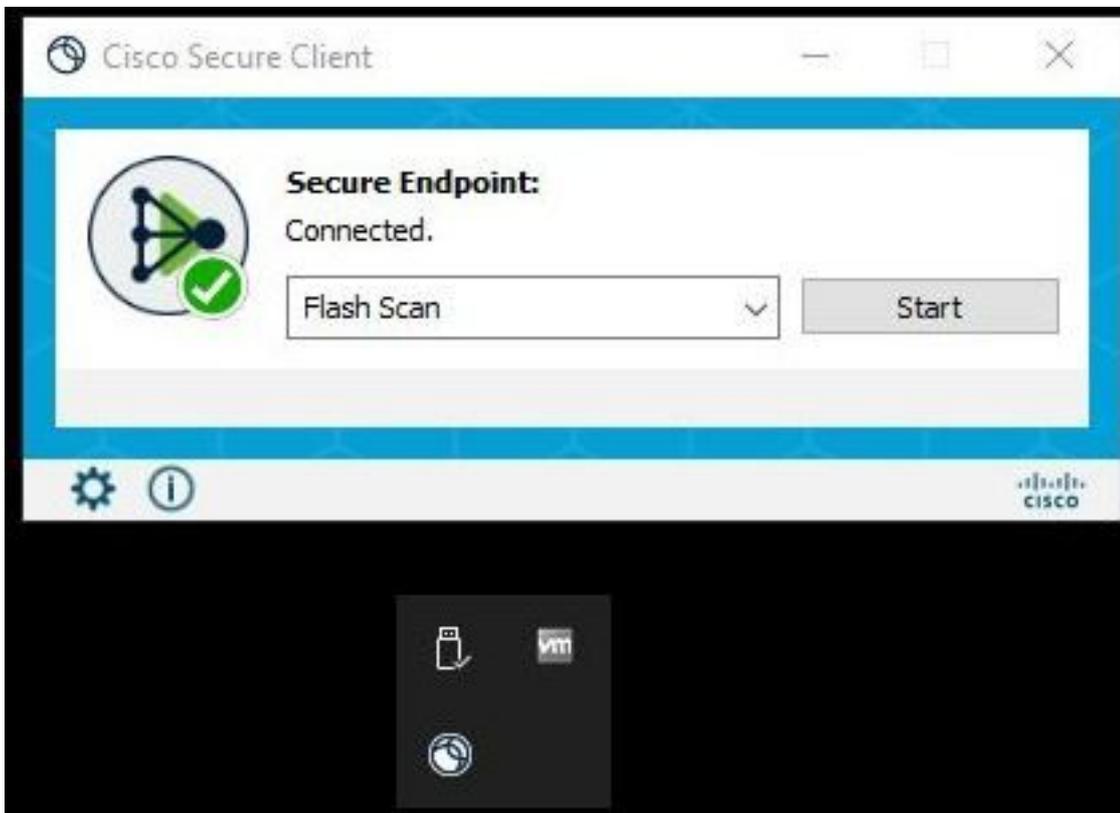
注意：必須啟用調試模式才能收集調試捆綁檔案。啟用更長時間調試模式會佔用磁碟空間。

步驟10. 收集偵錯套件組合檔案後，請將其上傳到<https://cway.cisco.com/csc/>。

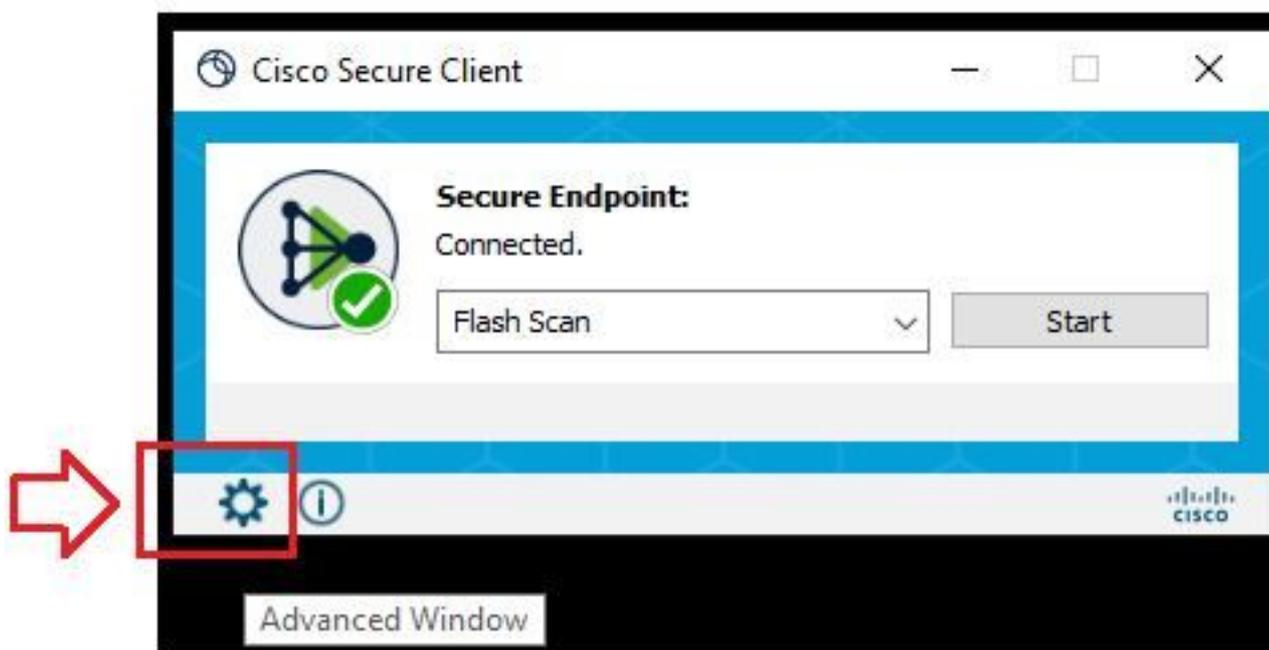
注意：請確保參考服務請求編號。

8.0.1及更高版本（思科安全客戶端）

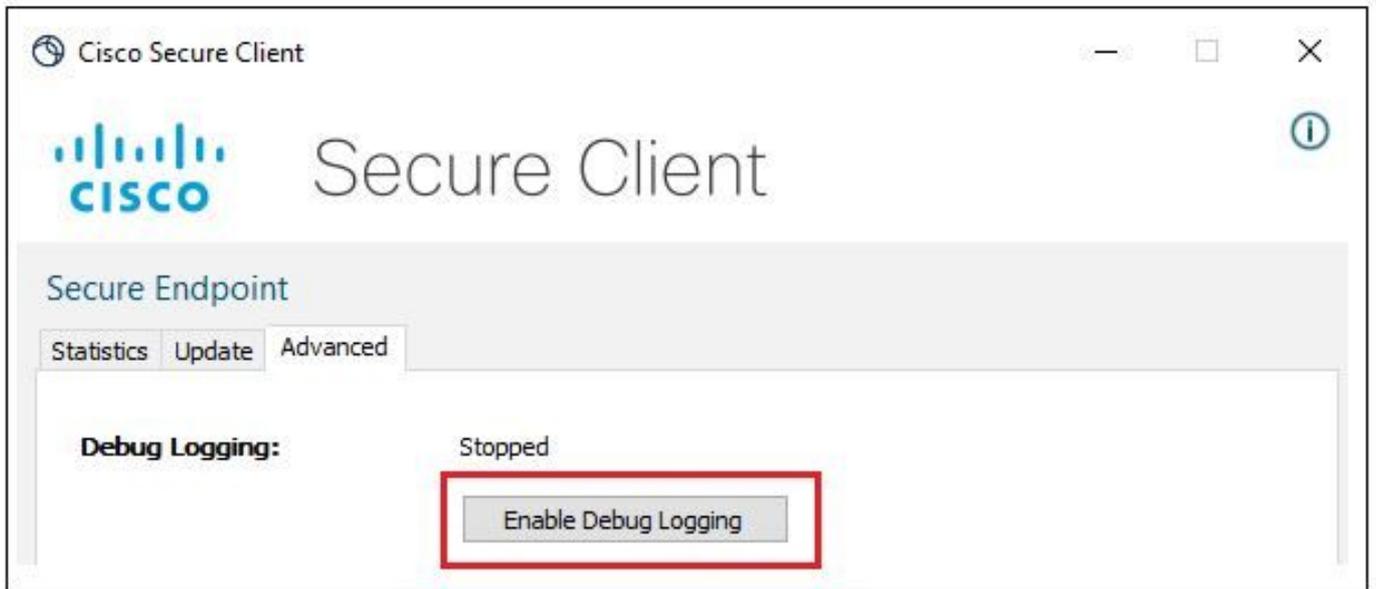
步驟1. 在工作列上**啟動**工作列圖示，如下圖所示。



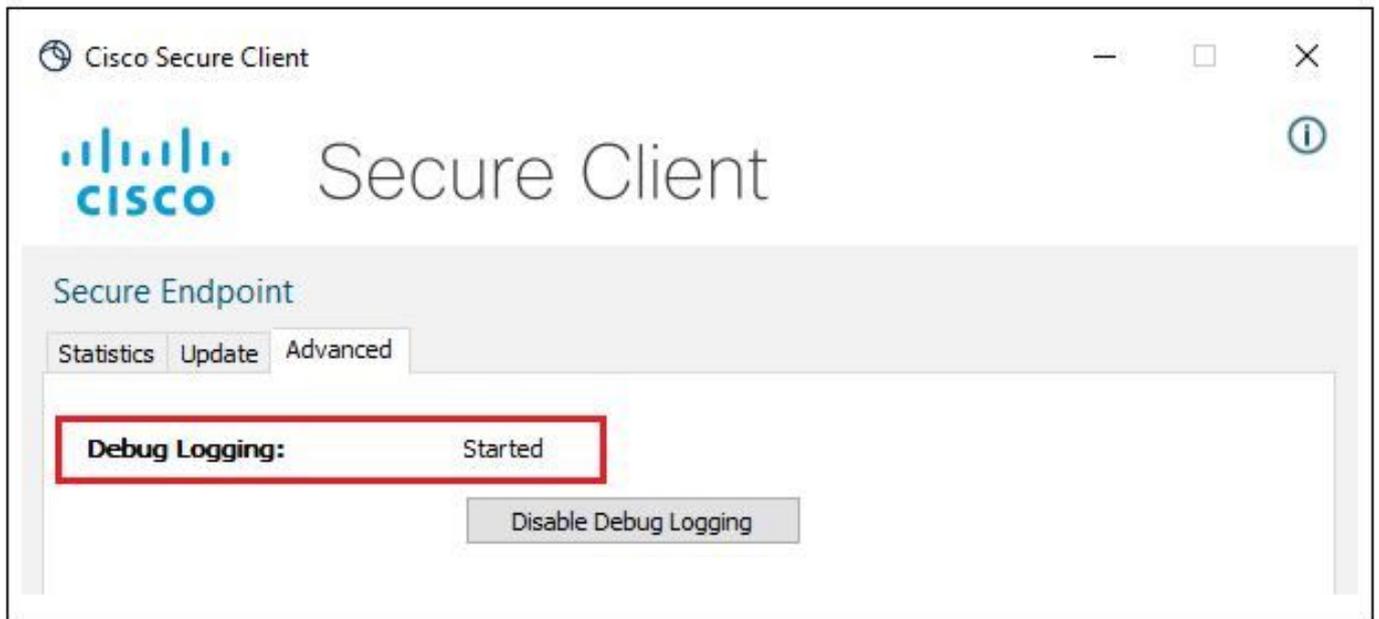
步驟2.在Secure Endpoint Connector中選擇Advanced Window選項，如下圖所示。



步驟3.導覽至Advanced索引標籤，然後選擇Enable Debug Logging按鈕，如下圖所示。



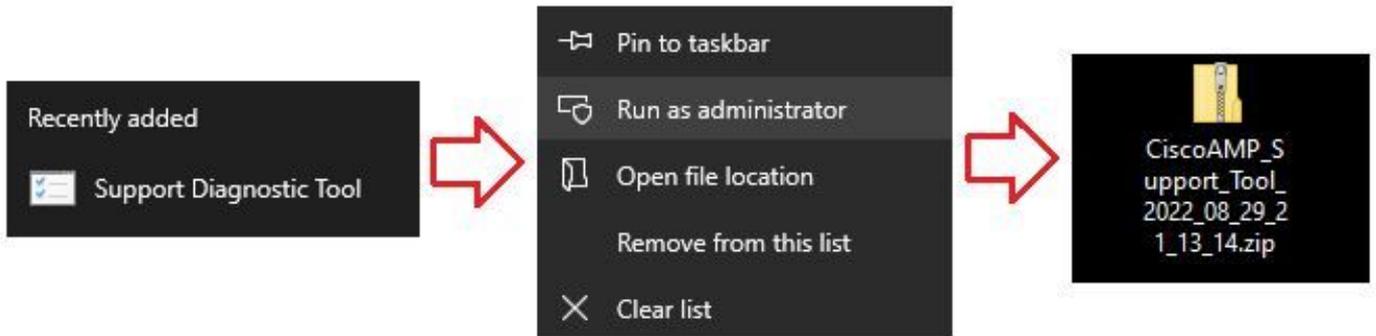
步驟4.調試日誌記錄按鈕名稱更改為「已啟動」。現在您處於偵錯模式，如下圖所示。



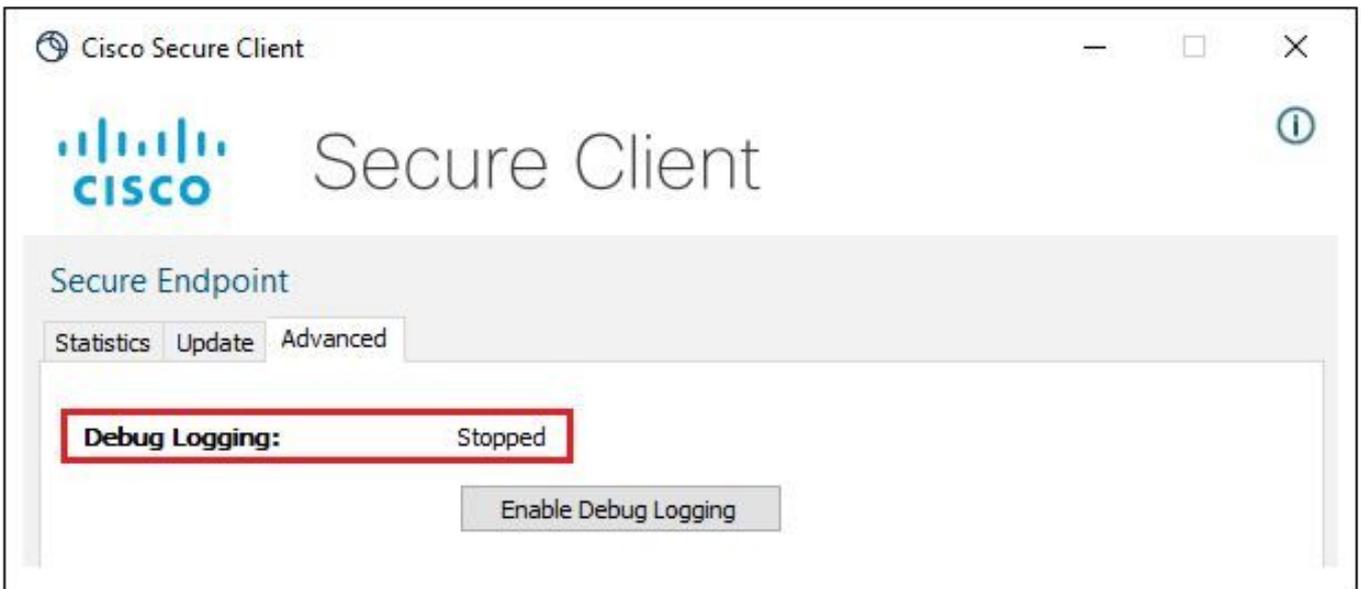
步驟5.重新建立問題並讓裝置運行至少30分鐘。

步驟6.在30分鐘後，開啟Windows搜尋和寫入支持診斷工具。

- 出現診斷工具。以管理員許可權執行工具。
(出現臨時Windows黑屏，等待幾秒鐘，Windows黑屏自行關閉)。
- 幾分鐘後，案頭上會顯示Debug Bundle檔案，如下圖所示。



步驟7.生成調試捆綁檔案後，您可以禁用調試模式。選擇**禁用調試日誌**按鈕。Debug logging button name更改為「**Stopped**」，如下圖所示。



注意：必須啟用調試模式才能收集調試捆綁檔案。啟用更長時間調試模式會佔用磁碟空間。

步驟8.收集偵錯套件組合檔案後，請將其上傳到<https://cway.cisco.com/csc/>。

注意：請確保參考服務請求編號。

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）。