

在安全客戶端中禁用VPN模組

目錄

[簡介](#)

[安全客戶端中VPN模組的要求](#)

[禁用VPN功能的方法](#)

[在安裝期間禁用VPN模組](#)

[Windows](#)

[macOS](#)

[安裝後禁用VPN模組](#)

[驗證](#)

簡介

本文檔介紹如何在確保DNS流量攔截繼續正常運行的同時禁用安全客戶端中的VPN模組。

安全客戶端中VPN模組的要求

即使AnyConnect不用於VPN訪問，VPN模組也是安全客戶端的必要元件。Umbrella依靠共用的安全客戶端驅動程式來攔截和管理DNS流量。雖然必須安裝VPN模組，但您可以完全禁用VPN功能。

禁用VPN功能的方法

您可以通過禁用以下功能來禁用安全客戶端中的VPN功能：

- 在安裝期間使用安裝引數(Windows)或修改安裝包(OSX)。
- 安裝後，將配置檔案部署到終端（可以通過程式設計方式部署）。

在安裝期間禁用VPN模組

Windows

1. 在安裝期間，使PRE_DEPLOY_DISABLE_VPN=1用MSI引數禁用VPN功能。
2. 有關詳細資訊，請參閱[自定義Cisco安全客戶端的Windows安裝](#)。

macOS

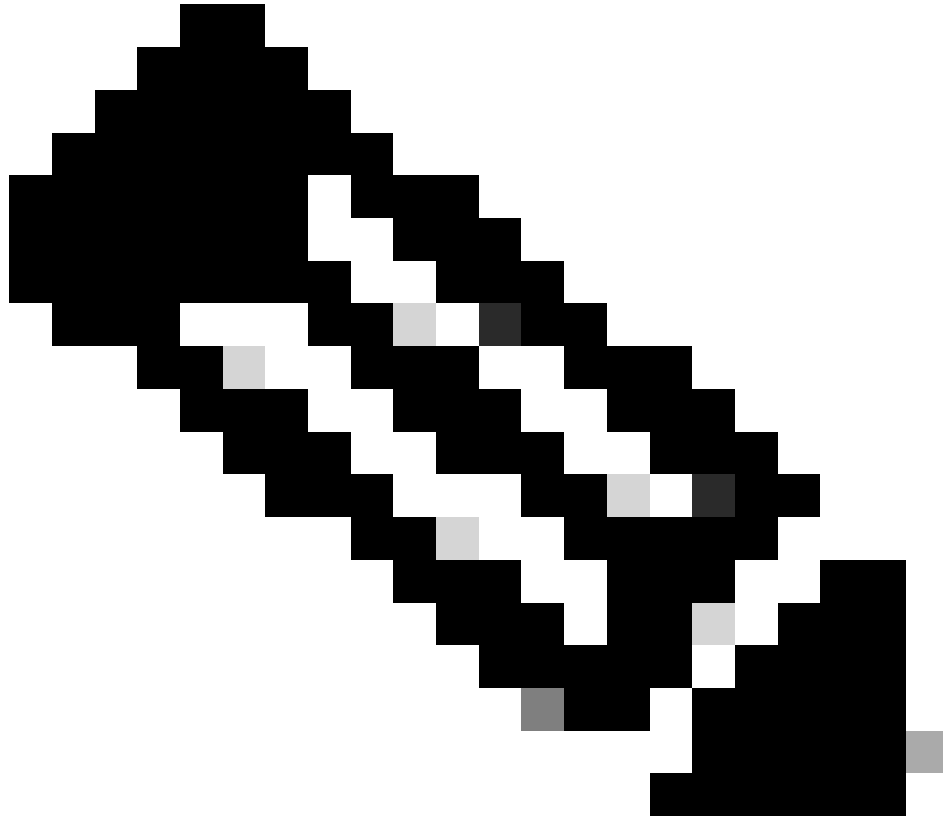
1. 使用控制VPN功能啟用的檔案ACTransforms.xml，自定義安裝包(.DMG)。
2. 有關詳細資訊，請參閱[自定義Cisco安全客戶端的MacOS安裝](#)。

安裝後禁用VPN模組

1. 導航到終端上的配置檔案目錄：

- Windows:

C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile\



附註：ProgramData資料夾在Windows中預設處於隱藏狀態。如果需要，請直接在Windows資源管理器中鍵入路徑。

- macOS:

/opt/cisco/secureclient/vpn/profile/

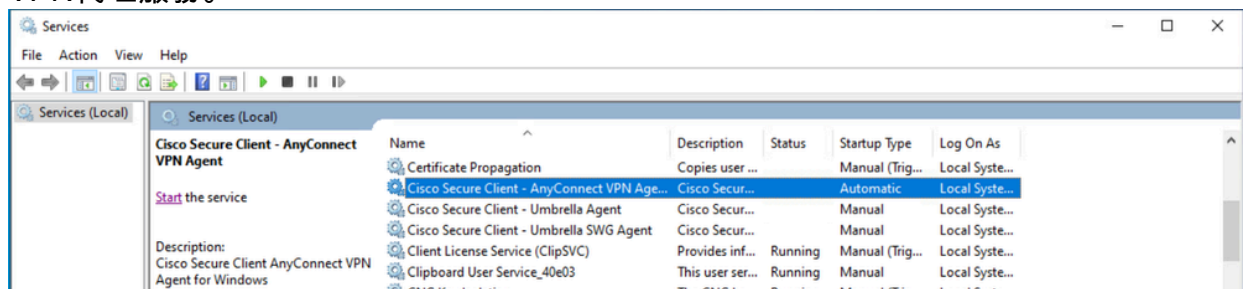
2. 建立新的空白文本文檔。

3. 將提供的XML內容複製到文檔中，並將其儲存為VPNDisable_ServiceProfile.xmlProfile文件夾：

true

4. 在配置檔案文VPNDisable_ServiceProfile.xml 件夾中儲存檔案後，重新啟動電腦。

- 在Windows上，也可以使用Windows服務重新啟動Cisco Secure Client - AnyConnect VPN代理服務。



18212956792980

驗證

重新啟動後，啟動Secure Client圖形使用者介面(GUI)以驗證VPN模組是否已禁用。



18212229472020

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）。