

보안 클라이언트에서 VPN 모듈 비활성화

목차

[소개](#)

[보안 클라이언트의 VPN 모듈 요구 사항](#)

[VPN 기능을 비활성화하는 방법](#)

[설치하는 동안 VPN 모듈 비활성화](#)

[참](#)

[맥OS](#)

[VPN 모듈 사후 설치 비활성화](#)

[확인](#)

소개

이 문서에서는 DNS 트래픽 가로채기가 계속 작동하도록 하면서 Secure Client에서 VPN 모듈을 비활성화하는 방법에 대해 설명합니다.

보안 클라이언트의 VPN 모듈 요구 사항

VPN 모듈은 AnyConnect가 VPN 액세스에 사용되지 않는 경우에도 Secure Client의 필수 구성 요소입니다. Umbrella는 공유 Secure Client 드라이버를 사용하여 DNS 트래픽을 가로채고 관리합니다. VPN 모듈의 설치가 필수적이지만 VPN 기능을 완전히 비활성화할 수 있습니다.

VPN 기능을 비활성화하는 방법

Secure Client에서 VPN 기능을 비활성화하려면 다음을 수행합니다.

- 설치 인수(Windows)를 사용하여 설치하거나 설치 패키지(OSX)를 수정하는 동안
- 설치 후 엔드포인트에 컨피그레이션 프로파일을 구축합니다(프로그래밍 방식으로 구축 가능).

설치하는 동안 VPN 모듈 비활성화

참

1. 설치하는 동안 VPN 기능을 `PRE_DEPLOY_DISABLE_VPN=1` 비활성화하려면 MSI 인수를 사용합니다.
2. 자세한 내용은 [Cisco Secure Client의 Windows 설치 사용자 정의를 참조하십시오](#).

맥OS

1. VPN 기능의 활성화를 제어하는 파일로 설치 패키지(.DMG)를 `ACTransforms.xml` 사용자 지정합니다.

2. 자세한 내용은 [Cisco Secure Client의 MacOS 설치 사용자 정의를 참조하십시오.](#)

VPN 모듈 사후 설치 비활성화

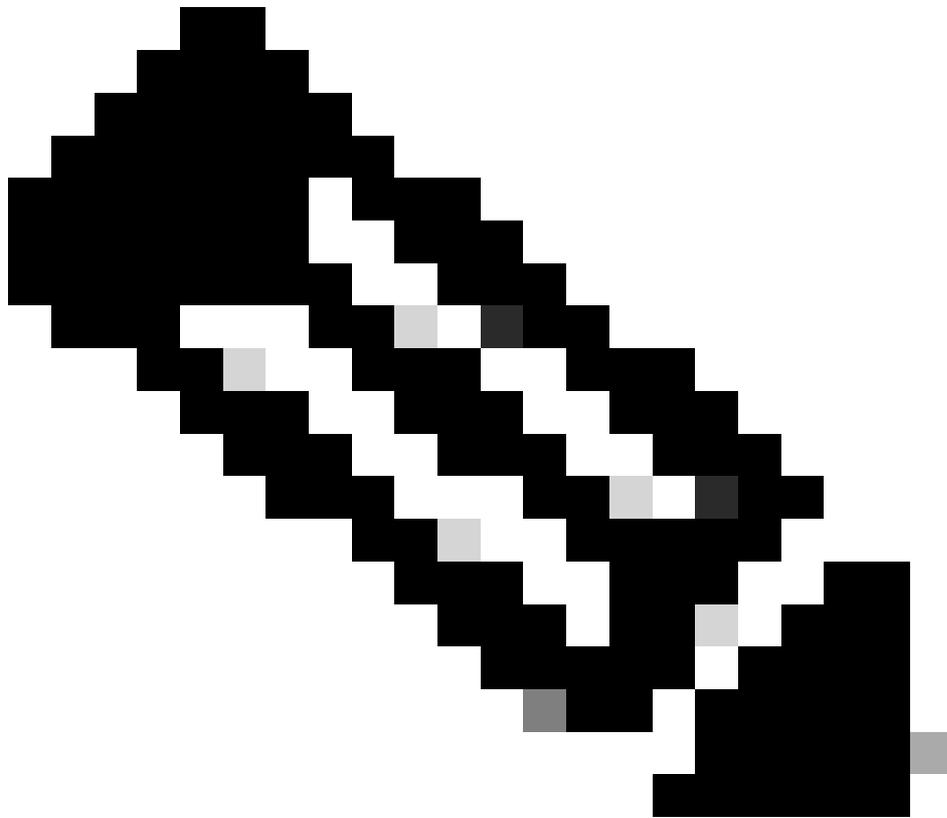
1. 엔드포인트에서 프로파일 디렉토리로 이동합니다.

- 창:

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


---


```



참고: ProgramData 폴더는 기본적으로 Windows에서 숨겨져 있습니다. 필요한 경우 Windows 탐색기에 경로를 직접 입력합니다.

- macOS:

```
/opt/cisco/secureclient/vpn/profile/  


---


```

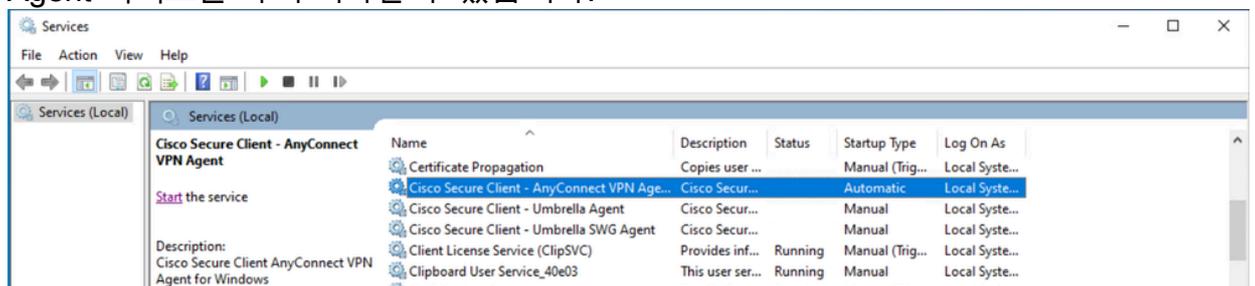
2. 빈 텍스트 문서를 새로 만듭니다.

3. 제공된 XML 내용을 문서로 복사하고 프로파일 폴더에 VPNDisable_ServiceProfile.xml 저장합니다.

true

4. 프로파일 폴더에 VPNDisable_ServiceProfile.xml 파일을 저장한 후 컴퓨터를 다시 시작합니다.

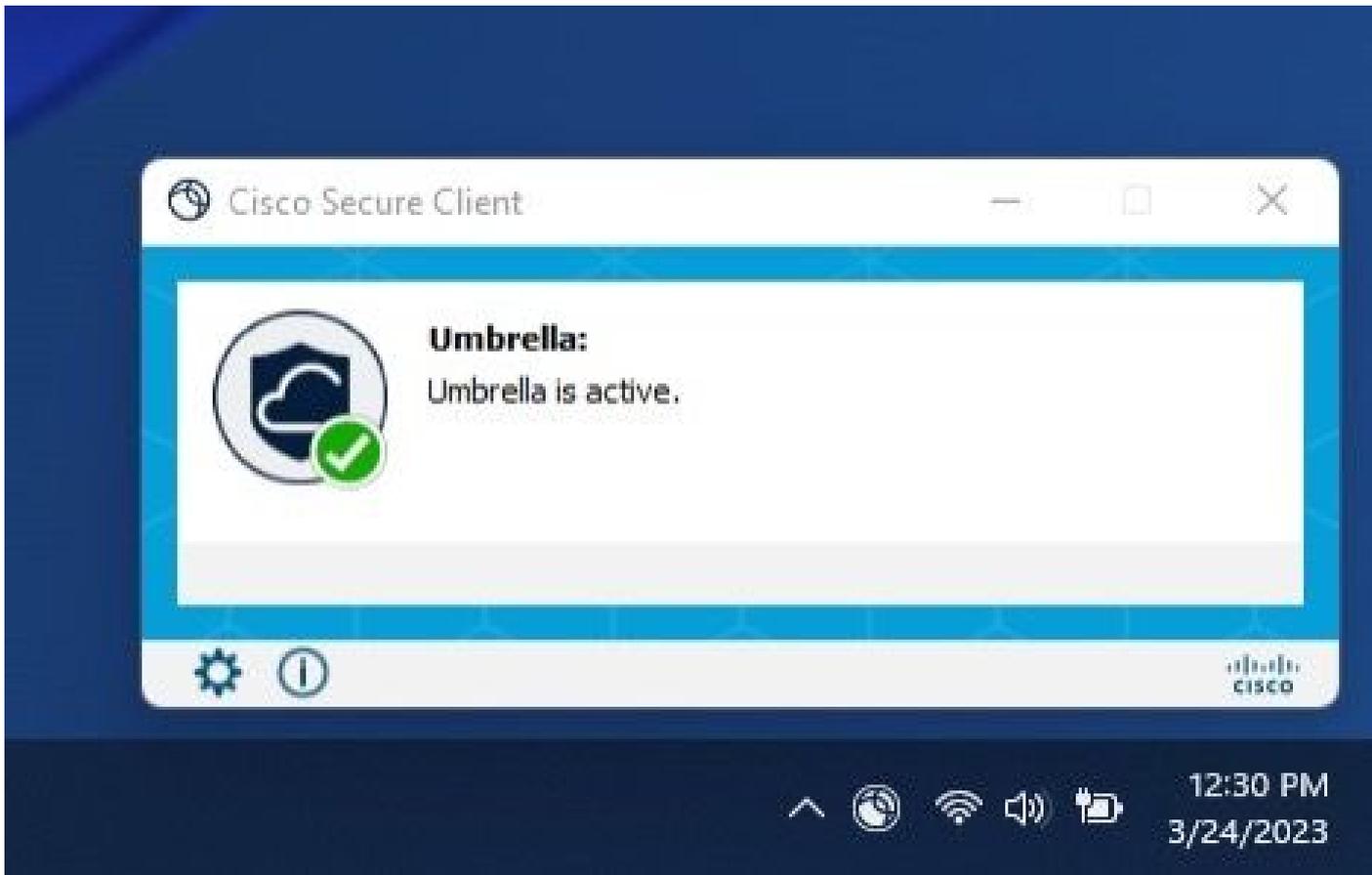
- Windows에서는 Windows 서비스를 사용하여 Cisco Secure Client - AnyConnect VPN Agent 서비스를 다시 시작할 수 있습니다.



18212956792980

확인

다시 시작한 후 Secure Client GUI(그래픽 사용자 인터페이스)를 실행하여 VPN 모듈이 비활성화되었는지 확인합니다.



18212229472020

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.