SOPHOS

Cybersecurity made simple.

Sophos Connect

도움말

목차

1 Sophos Connect 정보

Sophos Connect는 Windows 및 Mac에 설치할 수 있는 VPN 클라이언트로서, 원격 위치에서 XG로 보호되는 네트워크(예: 회사 네트워크)에 연결할 수 있게 해줍니다. 방화벽 관리자는 XG에 연결 세부 정보를 구성한 다음 사용자에게 설치 패키지 및 연결 구성 파일을 제공합니다.

이 설명서는 Sophos Connect를 사용하는 방법에 대한 정보를 제공합니다.

- Sophos Connect를 설치 및 제거하는 방법에 대한 지침은 Sophos Connect 설치 (페이지 1)를 참조하십시오.
- 연결 파일을 가져오고 연결을 관리하는 방법에 대한 지침은 연결 (페이지 2)을 참조하십시오.
- 이벤트에 대한 정보와 이벤트 오류 문제를 해결하는 방법은 이벤트 (페이지 11)를 참조하십시오.
- 이벤트 섹션에 표시되지 않는 문제를 해결하는 방법은 일반 문제 해결 (페이지 17)을 참조하십시오.

1.1 Sophos Connect 설치

Windows에 Sophos Connect 설치

- 설치 프로그램을 엽니다.
- 사용권 계약에 동의하고 설치를 클릭합니다.
- 설치가 완료되면 마침을 클릭합니다. 종료 후 Sophos Connect를 시작할 수 있습니다.

Mac에 Sophos Connect 설치

- 설치 프로그램을 엽니다.
- 설치 대상을 선택합니다. 선택한 대상(예: 시스템 드라이브)에 충분한 여유 공간이 있는지 확인합니다.
- 설치를 클릭합니다.
- 설치가 완료되면 마침을 클릭합니다.

1.2 Sophos Connect 제거

Windows에서 Sophos Connect 제거

- 제어판으로 이동하고 프로그램에서 프로그램 제거를 클릭합니다.
- Sophos Connect를 마우스 오른쪽 단추로 클릭하고 설치 제거를 선택합니다.

Mac에서 Sophos Connect 제거

- 터미널을 엽니다.
- 루트 수준으로 승격시키고 Sophos Connect가 설치된 위치에서 설치 제거 스크립트를 실행합니다.

  sudo /Library/Sophos Connect/uninstall.sh

제거가 성공한 경우 다음과 같은 메시지가 표시됩니다.

Sophos Connect has been uninstalled

1.3 연결

연결을 가져오고 연결을 설정하며 연결을 보고 편집할 수 있습니다.

Sophos Connect는 SSL VPN 및 IPsec VPN을 지원합니다.

1.3.1 연결 가져오기

Sophos Connect 클라이언트는 SSL 또는 IPsec VPN 연결을 사용하여 XG Firewall에 연결할 수 있습니다. Sophos Connect 클라이언트로 연결을 가져올 수 있습니다.

소개

Sophos Connect 클라이언트의 버전 2.0에서는 SSL 및 IPsec VPN 연결을 모두 가져올 수 있습니다. Sophos Connect 클라이언트의 이전 버전을 사용하는 경우 IPsec 연결만 가져올 수 있습니다.

이 페이지에서 다음 작업을 수행하는 방법을 알려줍니다.

- 관리자가 제공한 파일을 사용하여 IPsec 연결을 가져옵니다.
- 관리자가 제공한 파일을 사용하여 SSL 연결을 가져옵니다.
- 사용자 포털에서 파일을 다운로드하여 SSL 연결을 가져옵니다.

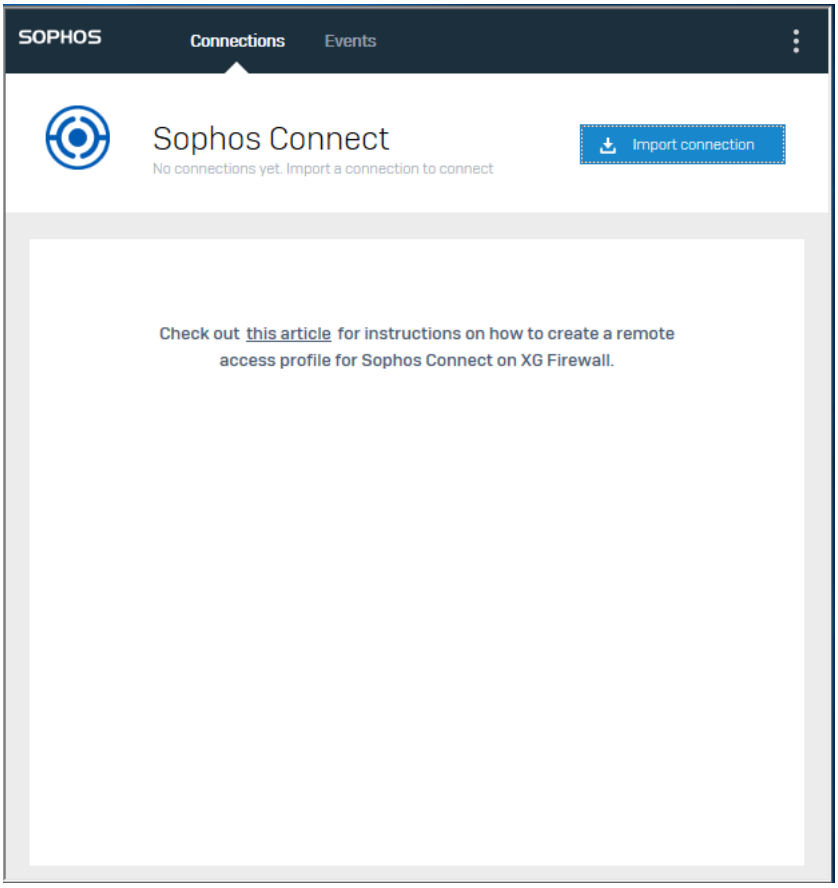
IPsec 연결 가져오기

연결 파일이 제공되었습니다. 이 파일은 tgb 확장자를 가집니다(예: Company_connection.tgb).

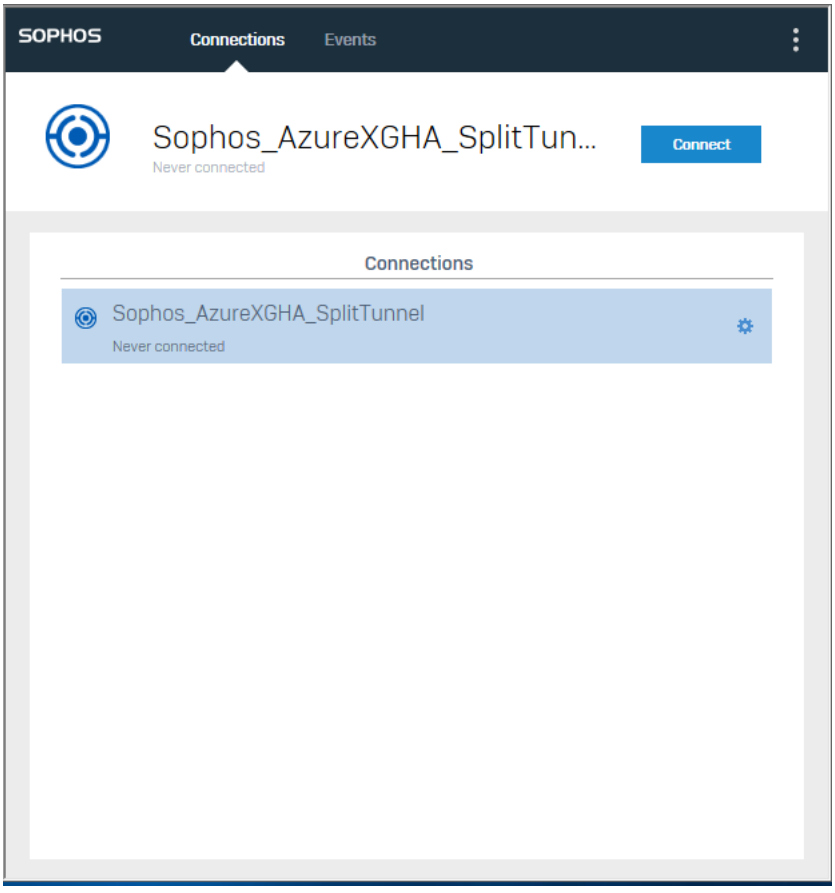
연결을 가져오려면 다음을 수행합니다.

1. 연결 페이지에서 연결 가져오기를 클릭합니다.

   기존 연결이 있는 경우 메뉴 단추를 클릭하고 드롭다운 메뉴에서 연결 가져오기를 선택합니다.



2. .tgb 파일을 탐색하여 해당 파일을 두 번 클릭합니다.
연결은 연결 아래에 표시됩니다.



이제 연결을 설정할 수 있습니다.

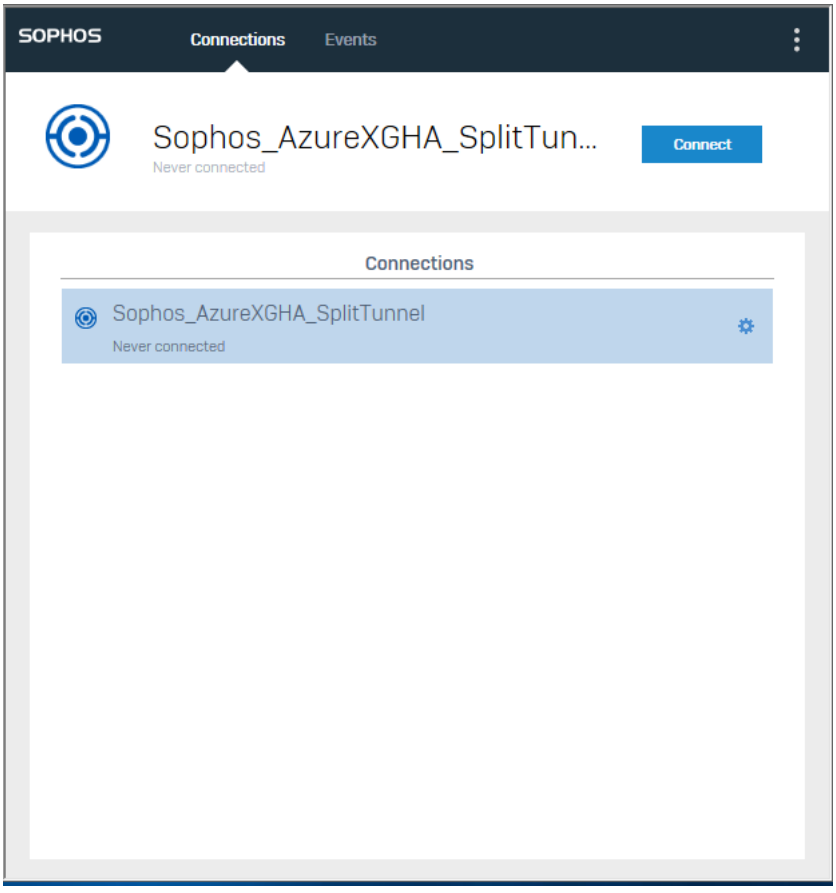
참고
여러 연결을 가져올 수 있습니다.

SSL 연결 가져오기

연결 파일이 제공되었습니다. 이 파일은 pro 확장자를 가집니다(예: Company_connection.pro).

연결을 가져오려면 다음을 수행합니다.

.pro 파일을 탐색하여 해당 파일을 두 번 클릭합니다.
연결이 자동으로 가져오기 되고 Sophos Connect가 열립니다. 연결은 연결 아래에 표시됩니다.



이제 연결을 설정할 수 있습니다.

참고
여러 연결을 가져올 수 있습니다.

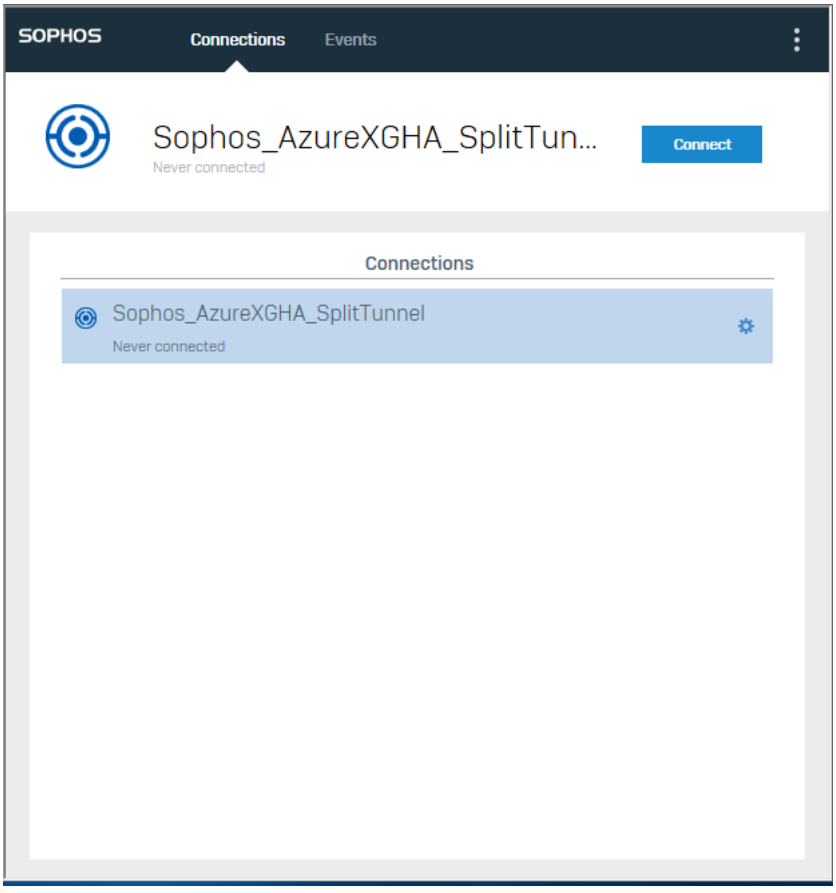
사용자 포털에서 SSL 연결 가져오기

연결을 가져오려면 다음을 수행합니다.

1. 사용자 포털에 로그인합니다.
2. SSLVPN으로 이동하여 기타 OS용 구성 다운로드를 클릭합니다.
3. Sophos Connect 클라이언트를 엽니다.
4. 연결 페이지에서 연결 가져오기를 클릭합니다.

   기존 연결이 있는 경우 메뉴 단추를 클릭하고 드롭다운 메뉴에서 연결 가져오기를 선택합니다.
5. .ovpn 파일을 탐색하여 해당 파일을 엽니다.

연결은 연결 아래에 표시됩니다.



이제 연결을 설정할 수 있습니다.

참고
여러 연결을 가져올 수 있습니다.

1.3.2 연결

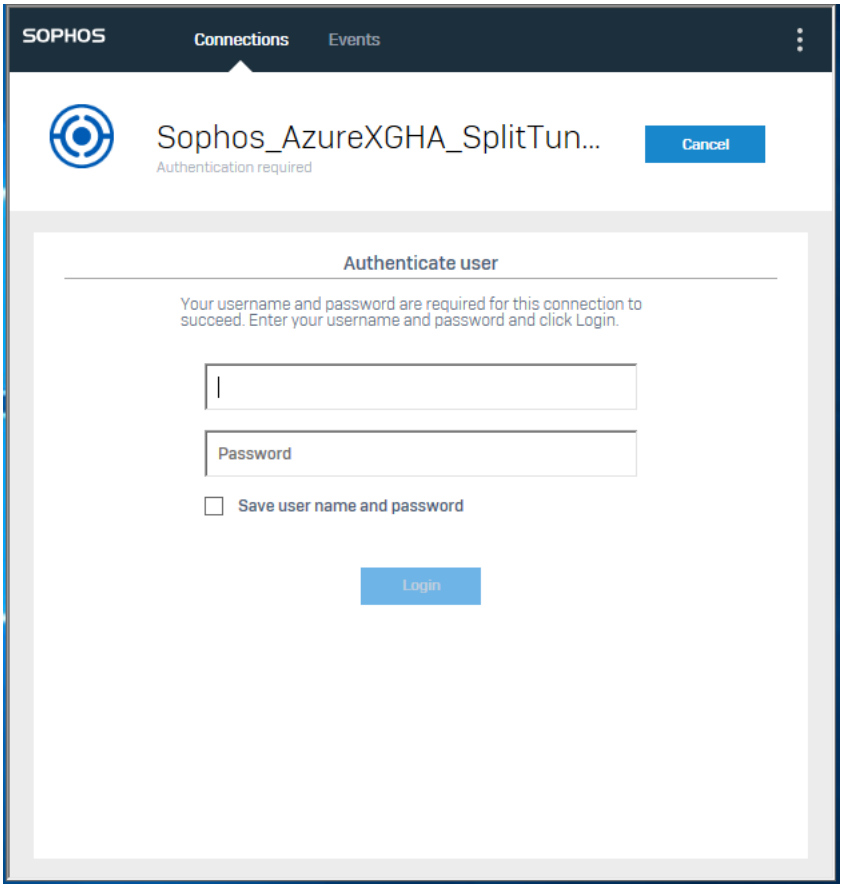
하나 이상의 가져온 연결을 사용할 수 있으며 필요한 자격 증명이 있는지 확인하십시오.

연결을 설정하려면 다음을 수행합니다.

1. 연결 페이지에서 연결을 선택합니다.
2. 선택한 연결을 두 번 클릭합니다.

   연결을 클릭해도 됩니다.

   로그인 화면이 나타납니다.

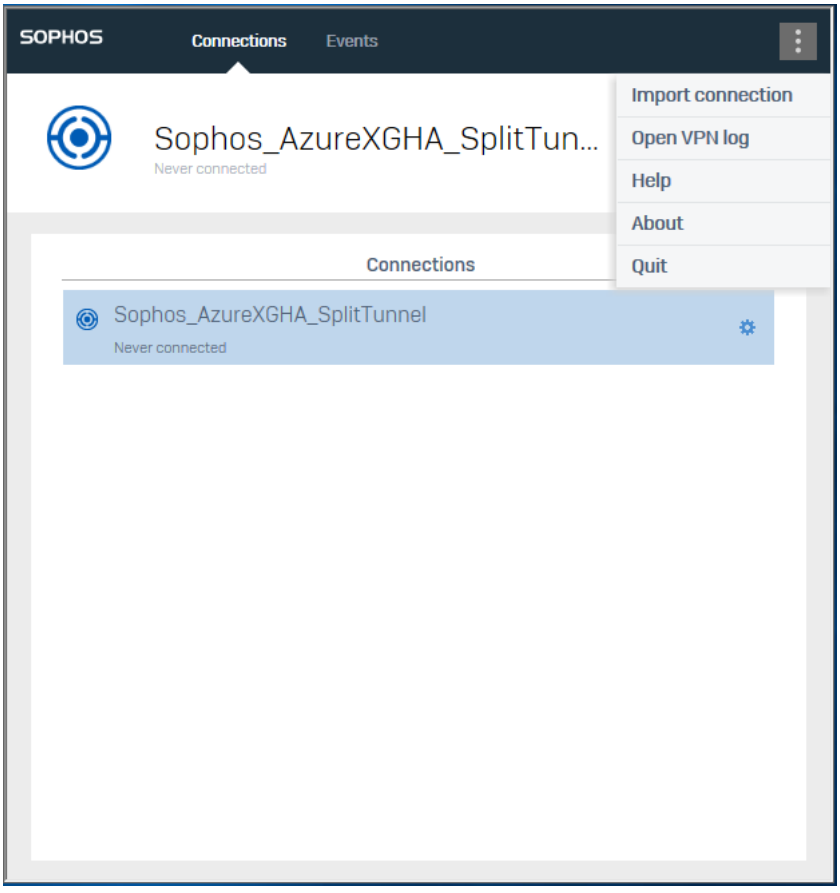


3. 사용자 이름 및 암호를 입력하고 로그인을 클릭합니다.
   관리자가 2단계 인증을 구성했을 수 있습니다.
   - 관리자가 OTP를 구성한 경우 사용자 이름과 암호를 입력하는 것 외에도 6자리 OTP 암호를 입력해야 합니다.
   - 관리자가 DUO 인증을 구성한 경우 연결 프로세스 중에 하나 또는 두 개의 DUO 프롬프트가 표시될 수 있습니다.

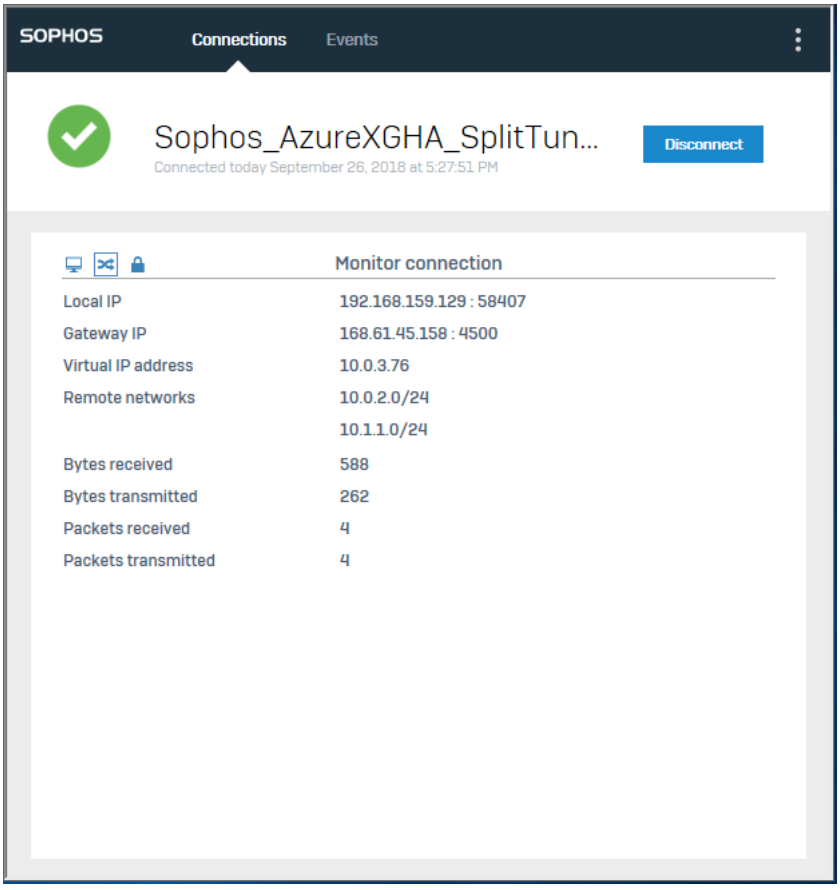
   참고
   프로비저닝 파일을 사용하여 연결을 가져온 경우 서버 인증서를 확인할 수 없다는 경고가 표시됩니다. 확인을 클릭하여 계속 진행할 수 있습니다. 메시지를 표시하지 않으려면 관리자에게 문의하십시오.

   Sophos Connect이 연결을 설정하고 사용자 인증을 시도합니다.

   참고
   연결 문제가 발생하는 경우 이벤트 페이지를 검토하고 IT에 문의하십시오. 메뉴 아이콘을 클릭하고 선택하여 VPN 로그를 확인할 수도 있습니다.



원격 서버에 대한 연결이 설정됩니다.



연결에 성공하는 경우 작업 표시줄에

아이콘이 표시됩니다.

연결에 실패하는 경우 작업 표시줄에

아이콘이 표시됩니다.

참고

연결 이름을 변경한 경우 방화벽 관리자가 제공한 원래 이름이 연결 세부 정보에 계속 표시됩니다. 이 이름을 변경하는 방법에 대한 지침은 연결 옵션 (페이지 9)을 참조하십시오.

1.3.3 연결 옵션

연결의 오른쪽에 있는 설정 아이콘을 클릭하면 Sophos Connect의 연결을 다양하게 변경할 수 있습니다.

1. 자동 연결은 Sophos Connect가 시작될 때 연결을 시도합니다.
2. 삭제는 연결을 삭제하므로 해당 연결을 재활성화하려면 다시 가져와야 합니다.
3. 이름 바꾸기는 연결 이름을 바꿀 수 있는 옵션을 제공합니다.
4. 자격 증명 지우기는 이전에 저장한 자격 증명을 지웁니다.
5. 업데이트 정책(프로비저닝 파일을 사용하여 연결을 생성한 경우에만 사용할 수 있음) 이를 통해 요청 시 XG 방화벽에서 최신 정책을 가져올 수 있습니다.

팁
여러 번 다시 시도한 후 연결에 실패한 경우 정책 업데이트를 시작하고 다시 연결을 시도합니다.

1.4 이벤트

Sophos Connect 내의 모든 작업과 해당 작업의 결과를 확인합니다. 여기에는 사용자 작업으로 인한 실패뿐 아니라 IKE 협상 실패도 포함됩니다. 이벤트 오류 문제를 해결하려면 이벤트 문제 해결 (페이지 12)을 참조하십시오.

- 상세한 오류 정보가 필요한 경우 VPN 로그 열기를 클릭합니다.
- 목록에서 이벤트를 제거하려면 이벤트 지우기를 클릭합니다.

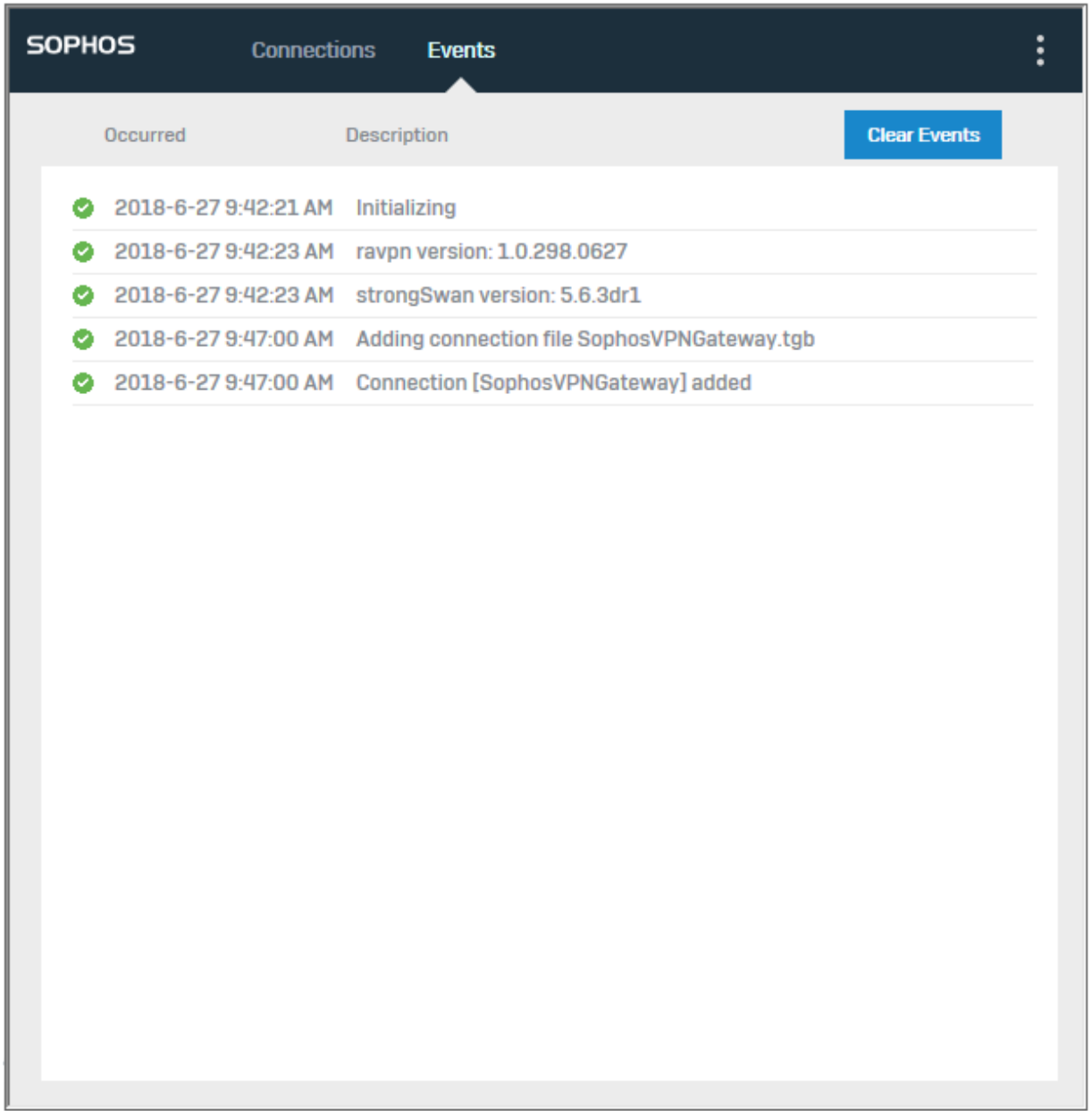


그림 1: 이벤트

1.4.1 이벤트 문제 해결

연결 문제가 있는 경우 이벤트를 클릭하고 연결을 시도한 시점의 타임스탬프를 찾아 관련 오류를 확인합니다.

이 섹션에서는 오류 메시지, 가능한 오류 원인 및 해결 방법에 대한 정보를 볼 수 있습니다. 아래에 나열되지 않은 문제가 발생한 경우 일반 문제 해결 항목을 확인하십시오.

추가 지원이 필요한 경우 Sophos 지원에 문의하십시오.

네트워크 연결 없음

원인: 네트워크 어댑터(이더넷 또는 Wi-Fi)에 IP 주소가 없습니다.

해결 방법: 유효한 IP 주소를 사용 중이며 기존 네트워크 연결이 작동하고 있는지 확인합니다.

DNS 확인 실패

원인: 클라이언트가 게이트웨이 호스트 이름을 해석할 수 없습니다.

해결 방법: DNS 서버가 네트워크 인터페이스에 할당되어 있는지 확인합니다. 명령 프롬프트(Windows) 또는 공용 호스트(예: www.sophos.com)의 터미널(Mac)에서 nslookup을 실행하고 IP 주소로 확인되는지 확인합니다. 확인되지 않는 경우 ISP에 문의하십시오.

UDP 포트 500/4500 차단됨

원인: 방화벽 또는 라우터가 UDP 포트 500 및 4500을 차단하고 있습니다.

해결 방법: 로컬 방화벽 또는 라우터 구성을 확인하고 이러한 포트에 대한 트래픽을 허용합니다. 방화벽 또는 라우터에 액세스할 수 없는 경우(예: 호텔) 모바일 핫스팟을 통해 연결하고 다시 연결을 시도합니다.

게이트웨이에서 응답이 없음: <연결에 지정된 게이트웨이 FQDN 또는 IP>

원인: 게이트웨이가 IKE 협상 메시지에 응답하지 않습니다. 다음과 같은 상태가 원인일 수 있습니다.

- 원격 게이트웨이(방화벽 또는 라우터)가 종료되었습니다.
- 원격 게이트웨이의 WAN 주소가 인터넷에 직접 연결되어 있지 않습니다.

해결 방법: 방화벽 관리자에게 연락하여 문제를 보고하고 해결 조치를 상담합니다.

게이트웨이로부터 NO_PROPOSAL_CHOSEN 알림 수신

원인: Sophos Connect의 IKE 협상에 대해 원격 게이트웨이가 이 오류 알림으로 응답했습니다. 다음과 같은 상태가 원인일 수 있습니다.

- 방화벽에 Sophos Connect 정책이 정의되어 있지 않거나 활성화되어 있지 않습니다.

- 방화벽 관리자가 방화벽에서 Sophos Connect 정책에 사용되는 IKE 1단계 제안을 변경했으며 새 구성을 내보내 클라이언트에 업로드하지 않았습니다.

해결 방법: 방화벽 관리자에게 연락하여 문제를 보고하고 해결 조치를 상담합니다.

서버에 원격 ID <예상 ID 값>이 필요하지만 <실제 ID 값>이 있음

원인: 방화벽의 Sophos Connect 정책에 구성된 로컬 ID 유형 또는 값이 이 연결에 사용되는 값과 다릅니다. 이는 방화벽 관리자가 방화벽에서 로컬 ID를 변경했으며 새 구성 파일을 Sophos Connect로 가져오지 않았기 때문일 수 있습니다.

해결 방법: 방화벽 관리자에게 연락하여 문제를 보고하고 해결 조치를 상담합니다.

사전 공유 키가 <연결 이름>과 일치하지 않을 수 있음

원인: 방화벽의 사전 공유 키가 이 연결에 사용된 키와 일치하지 않습니다. 이는 방화벽 관리자가 방화벽에서 해당 키를 변경했으며 새 구성 파일을 Sophos Connect로 업로드하지 않았기 때문일 수 있습니다.

해결 방법: 방화벽 관리자에게 연락하여 문제를 보고하고 해결 조치를 상담합니다.

<입력한 사용자 이름>의 사용자 인증 실패

원인: 사용자 이름 또는 암호가 일치하지 않습니다.

해결 방법: 다시 시도하여 입력하는 동안 사용자 오류로 인한 것인지 확인합니다. 여러 번 다시 시도했지만 동일한 오류가 발생하는 경우 암호가 변경되었거나 방화벽에서 비활성화되었을 수 있습니다. 이 경우 방화벽 관리자에게 연락하여 문제를 보고하고 해결 조치를 상담합니다.

[네트워크/마스크] 경로 추가 실패로 인해 2단계를 완료할 수 없음

참고
아래 문제 해결 단계는 Windows에만 해당합니다.

원인: 2단계 SA가 설정된 후 원격 네트워크에 대한 route add에 실패했습니다. 이는 터널이 활성화되어 있는 동안 strongSwan 서비스가 충돌했기 때문일 수 있습니다.

해결 방법: TAP 어댑터를 비활성화했다가 다시 활성화합니다. 관리자 권한으로 명령 프롬프트를 열고 다음 명령을 입력합니다.

net stop scvpn

net start scvpn

연결 데이터를 추가할 수 없습니다. <연결 이름> 이름을 가진 연결이 이미 존재함

원인: 같은 이름의 연결을 이미 가져왔습니다.

해결 방법: Sophos Connect에서 기존 연결을 삭제합니다. 기존 연결을 삭제하기 전에 정말로 삭제할 것인지 확인합니다. 그렇지 않으면 관리자에게 연락하여 해결 조치를 상담합니다.

서비스를 사용할 수 없음

참고
아래 문제 해결 단계는 Windows에만 해당합니다.

원인: Sophos Connect 서비스(scvpn)가 실행 중이 아닙니다.

해결 방법: 관리자 권한으로 명령 프롬프트를 열고 다음 명령을 입력합니다.

net start scvpn

연결 정보를 strongSwan에 로드하지 못함

참고
아래 문제 해결 단계는 Windows에만 해당합니다.

원인: strongSwan 서비스(서비스 이름:charon-svc.exe)가 실행 중이 아닙니다.

해결 방법: 관리자 권한으로 명령 프롬프트를 열고 다음 명령을 입력합니다.

net start strongswan

게이트웨이가 SA를 비활성화하거나 삭제함

원인: 게이트웨이에서 IKE 삭제 요청을 전송한 다음 터널이 삭제되었습니다. 다음과 같은 상태가 원인일 수 있습니다.

- 방화벽 관리자가 방화벽의 정책을 변경했습니다. 이로 인해 IKE 삭제 요청이 방화벽의 모든 활성 SA로 전송됩니다.
- 방화벽 관리자가 방화벽에서 이 사용자에 대한 모든 IPsec 연결을 수동으로 삭제했습니다.

해결 방법: 연결을 다시 시도합니다. 그래도 작동하지 않으면 관리자에게 연락하여 해결 조치를 상담합니다.

게이트웨이에 대한 DNS 해석 실패: <게이트웨이 이름:포트>

원인: 이 오류는 잘못된 호스트 이름으로 인해 발생합니다.

해결 방법:

- 프로비저닝 파일을 사용하여 연결을 추가한 경우 제공된 호스트 이름을 확인합니다.
- ovpn 파일을 가져와서 연결을 추가한 경우 XG Firewall에서 SSL VPN 설정을 확인합니다.

서버 인증서를 확인할 수 없음: <게이트웨이 이름>. 계속하시겠습니까?

원인: Sophos Connect 클라이언트는 프로비저닝 파일의 속성을 사용해 XG Firewall 사용자 포털에 연결하여 SSL VPN 구성을 가져옵니다. 사용자 포털은 Sophos Connect 클라이언트에서 확인할 수 없는 자체 서명된 인증서를 사용합니다.

해결 방법: 보안 경고를 수락하여 사용자 포털에서 ovpn 구성 파일을 연결 및 다운로드합니다. 나중에 메시지가 표시되지 않도록 하려면 다음 옵션 중 하나를 사용합니다.

- 공개 CA에서 서명한 XG Firewall에 대한 새 인증서를 발급합니다. XG Firewall에서 인증서를 가져온 다음 관리자 설정에서 인증서를 선택하여 웹 관리 콘솔에 로그인합니다.
- XG Firewall에서 원격 컴퓨터의 신뢰할 수 있는 저장소로 기본 CA 인증서를 푸시합니다.

신뢰할 수 없는 서버에 연결할 수 없음: <게이트웨이>

원인: 인증서 경고 프롬프트를 취소했으며 연결이 종료되었습니다.

해결 방법: 보안 경고를 수락하여 XG Firewall에서 SSL VPN 정책을 연결 및 다운로드합니다. SSL VPN 정책을 다운로드할 때 메시지가 표시되지 않도록 하려면 다음 옵션 중 하나를 사용합니다.

- 공개 CA에서 서명한 XG Firewall에 대한 새 인증서를 발급합니다. XG Firewall에서 인증서를 가져온 다음 관리자 설정에서 인증서를 선택하여 웹 관리 콘솔에 로그인합니다.
- XG Firewall에서 원격 컴퓨터의 신뢰할 수 있는 저장소로 기본 CA 인증서를 푸시합니다.

가져오기 파일에 중복된 연결이 포함되어 있음: <연결 이름>

원인: 프로비저닝 파일에서 가져온 연결에 중복된 표시 이름이 있습니다.

해결 방법: 프로비저닝 파일에서 display_name 속성을 확인하고 중복된 이름을 변경합니다.

정책 게이트웨이에 연결할 수 없음: <게이트웨이 이름>

원인: 프로비저닝 파일이 잘못 구성되었습니다. 이는 다음과 같은 이유로 인해 발생할 수 있습니다.

1. 게이트웨이 호스트 이름 또는 IP 주소가 잘못되었습니다.
2. 포트가 잘못되었거나 차단된 발신 포트입니다.
3. 정책 게이트웨이가 꺼져 있어 연결할 수 없습니다.

해결 방법:

프로비저닝 파일에서 다음을 확인합니다.

1. 게이트웨이 속성에 할당된 값이 올바른지 확인합니다.
2. user_portal_port 속성에 할당된 값이 XG Firewall의 사용자 포털 HTTPS 포트 설정과 일치하는지 확인합니다.
3. 프로비저닝 파일이 올바르게 구성된 경우 관리자에게 연락하여 해결 조치를 상담합니다.

이 사용자에 대해 정의된 SSL VPN 정책이 없음: <사용자 이름>

원인: XG Firewall의 SSL VPN(원격 액세스) 정책에 정책 구성원이 포함되어 있지 않습니다.

해결 방법: 관리자에게 연락합니다.

압축 불일치 오류입니다. 연결을 다시 시도합니다.

원인: XG Firewall에서 처음으로 SSL VPN 정책이 다운로드되고 이를 통해 SSL VPN 터널이 설정되었습니다.

해결 방법: 이 오류는 연결 구성 방법에 따라 해결됩니다.

- 프로비저닝 파일 사용: Sophos Connect가 자동으로 연결을 다시 시도합니다.

- ovpn 파일 사용: 수동으로 다시 연결합니다.

정책 불일치 오류입니다. 정책을 다운로드하고 연결을 다시 시도합니다.

원인: Sophos Connect 클라이언트가 이 연결에 대해 저장한 기존 정책을 사용하여 SSL VPN 연결을 설정하려고 했습니다.

Sophos Connect에서 SSL VPN 연결을 설정하고 저장한 후 관리자가 XG Firewall에서 SSL VPN 설정을 변경했습니다.

해결 방법: 프로비저닝 파일을 사용하여 연결을 만들었습니다. Sophos Connect는 자동으로 새 정책을 다운로드하고 SSL VPN 터널을 다시 설정합니다.

참고
터널이 연결된 상태에 있는 동안 관리자가 XG Firewall에서 SSL VPN 정책을 변경하고 TCP를 통한 SSL VPN인 경우 Sophos Connect 클라이언트가 새 정책을 즉시 감지하고 다운로드합니다. UDP 터널을 통한 SSL VPN인 경우 비활성 타이머가 터널을 삭제할 때까지 기다려야 합니다. 그러면 Sophos Connect는 새 정책을 다운로드하여 터널을 다시 설정합니다.

정책 불일치 오류입니다. 이 연결에 대한 새 정책을 가져옵니다.

원인: Sophos Connect 클라이언트가 이 연결에 대해 저장한 기존 정책을 사용하여 SSL VPN 연결을 설정하려고 했습니다.

Sophos Connect에서 SSL VPN 연결을 설정하고 저장한 후 관리자가 XG Firewall에서 SSL VPN 설정을 변경했습니다.

해결 방법: ovpn 파일을 가져와서 연결을 만들었습니다. SSL VPN 터널을 다시 설정하려면 사용자가 XG Firewall 사용자 포털에서 새 ovpn 파일을 다운로드하여 가져와야 합니다.

참고
터널이 연결된 상태에 있는 동안 관리자가 XG Firewall에서 SSL VPN 정책을 변경하고 TCP 터널을 통한 SSL VPN인 경우 Sophos Connect 클라이언트가 터널을 감지하고 오류가 있는 터널을 연결 해제합니다. UDP 터널을 통한 SSL VPN인 경우 비활성 타이머가 터널을 삭제할 때까지 기다려야 합니다. SSL VPN 터널을 성공적으로 다시 설정하려면 사용자가 XG Firewall 사용자 포털에서 새 ovpn 파일을 다운로드하여 가져와야 합니다.

서버 응답 대기 시간이 초과되었습니다.

원인: XG Firewall에서 SSL VPN 정책이 잘못 구성되었습니다. 가능한 실패 원인은 다음과 같습니다.

1. 호스트 이름 재정의가 구성되었지만 올바르거나 유효한 공용 IP 주소로 확인되지 않습니다.
2. DDNS가 구성되었지만 올바르거나 유효한 공용 IP 주소로 확인되지 않습니다.
3. 호스트 이름 재정의 및 DDNS가 모두 구성되지 않았으며 WAN 포트에 공용 IP 주소가 없습니다.

해결 방법: 프로비저닝 파일을 사용하여 연결을 가져온 경우 Sophos Connect 클라이언트에서 정책 연결 설정 메뉴를 업데이트합니다. ovpn 파일을 사용하여 연결을 만든 경우 사용자 포털에서 새 ovpn 파일을 내보내고 Sophos Connect 클라이언트에서 다시 가져옵니다.

1.5 일반 문제 해결

이 항목은 이벤트 페이지에 표시되지 않는 문제를 해결하는 방법을 다루고 있습니다.

추가 지원이 필요한 경우 Sophos 지원에 문의하십시오.

트래픽이 VPN 터널을 통과하지 않음

원인: v17.5 이전의 펌웨어 버전을 실행 중인 경우, 클라이언트가 1단계 키 다시 지정 후 새 가상 IP를 받았을 수 있습니다.

해결 방법: 연결을 해제했다가 다시 연결해야 합니다. 영구적인 해결책은 v17.5로 업그레이드하는 것입니다.

Sophos Connect 대시보드가 열리지 않음

원인: 트레이 아이콘을 클릭할 때 Sophos Connect 대시보드가 열리지 않거나 응답하지 않는 경우는 Sophos Connect GUI가 무한 루프에 멈춰 있거나 외부 입력에 응답할 수 없음을 의미합니다.

해결 방법(Windows): 작업 관리자를 열고 세부 정보 탭을 선택합니다. scgui.exe를 찾은 다음 오른쪽 클릭하여 작업을 종료합니다. 데스크톱 바로 가기에서 애플리케이션을 다시 시작합니다.

해결 방법(Mac): 작업 모니터를 열고 Sophos Connect 프로세스를 찾습니다. 해당 프로세스를 열고 강제 종료를 선택합니다. LaunchPad에서 애플리케이션을 다시 시작합니다.

터널의 연결이 끊기면 웹 탐색이 작동하지 않음

참고
이는 Mac에서 더 자주 발생합니다.

원인: 터널의 모든 연결이 끊어지면 DNS 서버가 물리적 네트워크 어댑터에서 복원되지 않습니다. 즉, VPN을 통해 연결되었을 때 사용된 내부 DNS 서버는 계속 사용됩니다. 터널이 더 이상 존재하지 않으므로 이름 확인이 작동하지 않습니다.

해결 방법: 로컬 네트워크의 연결을 끊은 다음 다시 연결합니다.

Sophos Connect GUI에 "서비스 사용 불가" 표시

참고
이는 Mac에서 더 자주 발생합니다.

원인: 터널 연결 해제 작업이 시작되면 strongSwan IPsec 데몬이 무한 루프에 멈춥니다. 이로 인해 GUI는 연결 해제에 대한 응답을 받을 수 없으며 결국 시간이 종료되어 "서비스 사용 불가" 오류가 표시됩니다.

해결 방법(Mac):

1. 작업 모니터를 열고 Sophos Connect GUI 프로세스를 종료합니다.
2. 터미널을 열고 다음 명령을 실행합니다.

sudo /bin/launchctl unload -w /Library/LaunchDaemons/com.sophos.connect.scvpn.plist

sudo /bin/launchctl load -w /Library/LaunchDaemons/com.sophos.connect.scvpn.plist

3. Sophos Connect를 열고 "서비스 사용 불가" 오류가 해결되었는지 확인합니다.

해결 방법(Windows):

1. cmd를 관리자로 열고 다음 명령을 실행합니다.

   net stop scvpn

   net start scvpn

2. Sophos Connect를 열고 "서비스 사용 불가" 오류가 해결되었는지 확인합니다.

Sophos Connect가 터널을 설정할 수 없음

원인: Sophos Connect 클라이언트를 먼저 설치한 다음 Sophos SSL VPN 클라이언트를 설치했을 수 있습니다.

해결 방법: 두 클라이언트를 모두 제거한 다음, Sophos SSL VPN 클라이언트를 다시 설치한 후 Sophos Connect 클라이언트를 설치합니다.

참고
반드시 이 순서로 설치해야 합니다.

게이트웨이에서 연결 재설정 수신: <게이트웨이 이름>

이 메시지는 scvpn.log 파일(설치 폴더)에 기록됩니다.

원인: XG Firewall에서 SSL VPN 설정이 변경되었거나 사용자가 수동으로 연결을 끊었거나 XG Firewall이 다시 시작됩니다. 연결에서 TCP를 통해 SSL VPN을 사용하는 경우 XG Firewall은 연결 재설정 요청을 보냅니다. 연결이 UDP를 통해 SSL VPN을 사용하는 경우 유휴 시간 제한 기간에 따라 연결이 자동으로 다시 연결될 수 있습니다.

해결 방법: 새 구성 파일을 Sophos Connect 클라이언트로 가져온 다음 다시 연결합니다. 관리자가 파일을 보내지 않은 경우 사용자 포털로 이동하여 다운로드합니다. 그렇지 않으면 사용자 포털로 이동하여 ovpn 파일을 다운로드합니다.

SSL VPN 연결에 자동 연결 및 업데이트 정책 메뉴 항목이 회색으로 표시됩니다.

원인: ovpn 파일을 가져와서 SSL VPN 연결을 생성하는 경우 이러한 옵션을 사용할 수 없습니다.

해결 방법: 이러한 옵션을 활성화하려면 프로비저닝 파일을 사용하여 연결을 생성해야 합니다. 프로비저닝 파일에 이러한 옵션을 추가합니다. 처음으로 연결한 후에는 업데이트 정책을 사용할 수 있습니다. 자동 연결을 활성화하려면 내부 네트워크에서만 액세스할 수 있는 auto_connect_host를 정의해야 합니다.

자동 연결을 활성화하기 위한 최소 요구 사항이 있는 프로비저닝 파일의 예:

```
[
 {
  "display_name": "<연결 이름 입력>",
  "gateway": "<게이트웨이 호스트 이름 또는 IP 입력>",
  "auto_connect_host":" <내부 네트워크 리소스의 호스트 이름 또는 IP 입력>"
```



```
}
]
```

SSL VPN 오류

원인: OpenVPN 서비스에서 생성된 오류입니다.

해결 방법: 연결을 다시 설정합니다. 작동하지 않으면 장치를 다시 시작하고 다시 시도합니다.

관리 포트를 사용할 수 없음

원인: Sophos Connect가 OpenVPN과 통신하는 데 필요한 TCP 포트 25340을 요구하지 못했습니다.

해결 방법: 이 포트를 사용하여 장치에서 다른 응용 프로그램이 실행되고 있는지 확인합니다. 가능한 경우 응용 프로그램을 종료합니다. 이 문제를 해결하지 않으면 Sophos Connect 2.0을 장치에서 실행할 수 없습니다. 이 포트를 사용하는 다른 응용 프로그램이 없는 경우 일시적인 문제일 수 있습니다. 연결을 다시 설정하면 문제가 해결됩니다.

임시 파일을 만들지 못함

원인: Sophos Connect는 임시 파일을 사용하여 OpenVPN 서비스에 연결 속성을 전달합니다. Sophos Connect가 이 장치에 파일을 만들지 못했습니다.

해결 방법: 장치를 다시 시작합니다.

OpenVPN 서비스를 사용할 수 없음

원인: OpenVPN 서비스가 시작되지 않았을 수 있습니다.

해결 방법: OpenVPN 서비스 시작 유형이 비활성화로 설정된 경우 이를 수동으로 변경하고 Sophos Connect 서비스도 다시 시작합니다.

파이프에 쓰지 못함

원인: Sophos Connect 클라이언트에서 생성된 오류입니다.

해결 방법: 연결을 다시 설정합니다. 작동하지 않으면 장치를 다시 시작하고 다시 시도합니다.

2 Sophos Connect Admin 정보

Sophos Connect Admin에서 구성(.tgb) 파일을 가져오고 VPN 설정에 대한 다양한 옵션을 구성할 수 있습니다.

참고
XG에서 .tgb 파일을 구성 및 내보내는 방법에 대한 자세한 내용은 XG 도움말 가이드의 Sophos Connect Client 섹션을 참조하십시오. Sophos Connect 클라이언트.

Sophos Connect Admin의 설치 및 제거 프로세스는 Sophos Connect의 프로세스와 동일합니다. 자세한 내용은 Sophos Connect 도움말 가이드의 설치를 참조하십시오.

2.1 구성 파일 편집

Sophos Connect Admin에서 구성(.tgb) 파일을 편집할 수 있습니다. 이 파일은 보다 세분화된 VPN 구성 옵션을 제공합니다.

Sophos Admin의 XG에서 내보낸 .tgb 파일을 엽니다. 다음과 같이 할 수 있습니다.

- VPN 연결을 통해 모든 트래픽을 전송하려면 모두 터널을 활성화합니다.
- Sophos Endpoint가 XG로 하트비트를 전송하도록 허용하려면 보안 하트비트 전송을 활성화합니다. 이 작업은 사용자의 컴퓨터에 Sophos Endpoint 클라이언트가 설치되어 있는 경우에만 작동합니다.
- 사용자가 자신의 컴퓨터에 사용자 이름과 암호를 저장하도록 허용하려면 암호 저장 허용을 활성화합니다. 사용자 자격 증명은 키 체인 서비스를 사용하여 안전하게 저장됩니다.
- XG에서 VPN 사용자에 대해 2단계 인증을 구성한 경우 2FA 프롬프트를 활성화합니다.
- 사용자가 컴퓨터에서 Sophos Connect에 로그온한 후 자동으로 연결을 활성화하려면 터널 자동 연결을 활성화합니다. Sophos Connect는 사용자가 이미 회사 네트워크에 연결되어 있는 경우 자동으로 연결을 시작하지 않습니다.

  자동 연결을 사용하려면 추가 구성 매개 변수가 필요합니다. DNS 접미사/모니터링 호스트(사용자의 로컬 시스템이 회사 네트워크 내부 또는 외부에 있는지 확인하는 데 사용 가능). 다음 값 중 하나를 사용합니다.

  — IP 주소.

  — FQDN(정규화된 도메인 이름)입니다. 호스트 이름은 내부 DNS 서버를 사용할 때만 확인해야 합니다.

  — DNS 접미사.

  참고
  IP 주소 또는 FQDN을 구성하는 경우 이 호스트에서 ICMP가 허용되어야 합니다.

- 사용자가 연결할 수 있는 네트워크를 추가, 수정 및 삭제합니다. 특정 네트워크를 목록에 추가하면 사용자가 VPN 연결을 통해 해당 네트워크의 리소스에 액세스하지만 원격 게이트웨이를 통해 인터넷 리소스에 직접 액세스하므로 분할 터널링이 가능합니다.

참고
모든 네트워크를 삭제하면 모두 터널 모드가 활성화되어 모든 트래픽이 VPN 연결을 통해 전달됩니다.

- 연결 이름 및 대상 호스트를 변경합니다.

  구성을 지우면 .tbg 파일을 다시 가져와야 합니다.

  구성을 저장하면 .scx 파일로 저장됩니다.

  참고
  .scx 파일을 가져와서 다시 편집할 수 있습니다.

구성 파일을 저장하면 사용자에게 해당 파일을 보낼 수 있으며 사용자는 이를 Sophos Connect로 가져옵니다. 자세한 내용은 Sophos Connect를 참조하십시오.

3 법적 고지