paloalto TECHDOCS

GlobalProtect 앱 사용자 가이드

Version 6.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2021-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

August 19, 2022

Table of Contents

Windows용 GlobalProtect 앱 5

Windows용 GlobalProtect 앱 다운로드 및 설치하기 6
로그온 전 연결 사용하기 10
스마트 카드 인증을 사용하여 로그온 전 연결하기 10
SAML 인증을 사용하여 로그온 전 연결하기 15
사용자 이름/암호 기반 인증을 사용하여 로그온 전 연결하기 19
스마트 카드 인증에 Single Sign-On 사용하기 24
Windows용 GlobalProtect 앱 사용하기 26
Windows용 GlobalProtect 앱에서 문제 보고하기 39
Windows용 GlobalProtect 앱 연결 해제 43
Windows용 GlobalProtect 앱 제거 46
Microsoft 설치 관리자 충돌 해결 47

맥OS용 GlobalProtect 앱 49

macOS용 GlobalProtect 앱 다운로드 및 설치 50
macOS용 GlobalProtect 앱 사용하기 58
macOS용 GlobalProtect 앱에서 문제 보고하기 73
macOS용 GlobalProtect 앱 연결 해제 77
macOS용 GlobalProtect 앱 제거 79
GlobalProtect 인포서 커널 확장 프로그램 삭제 84
인증을 위해 클라이언트 인증서를 사용하도록 macOS용 GlobalProtect 앱 활성화 85

iOS용 GlobalProtect 앱 87

iOS용 GlobalProtect 앱 다운로드 및 설치하기 88
iOS용 GlobalProtect 앱 사용하기 89
iOS용 GlobalProtect 앱에서 문제 보고하기 102
iOS용 GlobalProtect 앱 제거 109

Android용 GlobalProtect 앱 111

Android용 GlobalProtect 앱 다운로드 및 설치하기 112
Chromebook에 Android용 GlobalProtect 앱 다운로드 및 설치하기 113
Android용 GlobalProtect 앱 사용하기 114
Android용 GlobalProtect 앱에서 문제 보고하기 123
Android용 GlobalProtect 앱 연결 해제 130
Android용 GlobalProtect 앱 제거 132
Chromebook에서 Android용 GlobalProtect 앱 제거 133

Linux용 GlobalProtect 앱 135

©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱 다운로드 및 설치하기 136
Linux용 GlobalProtect의 GUI 버전 다운로드 및 설치하기 136
Linux용 GlobalProtect의 CLI 버전을 다운로드하고 설치합니다 139
Linux용 GlobalProtect 앱 사용하기 143
Linux용 GlobalProtect 앱의 GUI 버전 사용하기 143
Linux용 GlobalProtect 앱의 CLI 버전 사용하기 152
Linux용 GlobalProtect 앱에서 문제 보고하기 156
Linux용 GlobalProtect 앱 연결 해제 161
GUI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 끊기 161
CLI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 해제 163
Linux용 GlobalProtect 앱 제거 165

IoT 디바이스용 GlobalProtect 167

 ©2023 Palo Alto Networks, Inc.

Windows용 GlobalProtect 앱

GlobalProtect™는 엔드포인트(데스크톱 컴퓨터, 노트북, 태블릿 또는 스마트폰)에서 실행되는 애플리케이션으로, 회사 네트워크의 중요한 리소스를 보호하는 것과 동일한 보안 정책을 사용하여 사용자를 보호합니다. GlobalProtect™는 데이터 센터, 사설 클라우드, 공용 클라우드 및 인터넷 트래픽을 보호하고 전 세계 어디에서나 회사 리소스에 액세스할 수 있도록 합니다.

다음 주제에서는 Windows용 GlobalProtect 앱을 설치하고 사용하는 방법을 설명합니다.

> Windows용 GlobalProtect 앱 다운로드 및 설치하기
> 로그온 전 연결 사용하기
> 스마트 카드 인증에 Single Sign-On 사용하기
> Windows용 GlobalProtect 앱 사용하기
> Windows용 GlobalProtect 앱에서 문제 보고하기
> Windows용 GlobalProtect 앱 연결 해제
> Windows용 GlobalProtect 앱 제거
> Microsoft 설치 관리자 충돌 해결

Windows용 GlobalProtect 앱 다운로드 및 설치하기

GlobalProtect 네트워크에 연결하기 전에 윈도우 엔드포인트에 GlobalProtect 앱을 다운로드하여 설치해야 합니다. 조직의 GlobalProtect 또는 Prisma Access 배포에 적합한 앱을 구입하려면 조직 내 GlobalProtect 포털에서 직접 앱을 다운로드해야 합니다. 이러한 이유로 Palo Alto Networks 사이트에는 직접 GP 앱을 다운로드할 수 있는 링크가 없습니다.

GP 앱을 다운로드하여 설치하려면 먼저 GP 관리자로부터 GlobalProtect 포털의 IP 주소 또는 정규화된 도메인 이름(FQDN)을 얻어야 합니다. 또한 관리자는 포털 및 게이트웨이에 연결하는 데 사용할 수 있는 사용자 이름 및 암호 정보를 확인해야 합니다. 대부분의 경우 사용자 이름과 암호는 회사 네트워크에 연결하는 데 사용하는 사용자 이름과 암호와 동일합니다. 필요한 정보를 수집한 후 다음 단계에 따라 앱을 다운로드하고 설치합니다.

***GlobalProtect** 앱 **5.0** 이상을 실행하려면 **Windows** 엔드포인트에 **Visual Studio 2013**용 **Visual C++** 재배포 가능 패키지 **12.0.3**이 필요합니다. 엔드포인트에 재배포 가능 패키지를 아직 설치하지 않은 경우 **GlobalProtect** 앱은 **Visual C++** 재배포 가능 패키지 **12.0.3**을 자동으로 설치합니다. **Visual C++** 재배포 가능 패키지 **12.0.2** 또는 이전 릴리스를 이미 설치한 경우 **GlobalProtect** 앱을 설치하기 전에 엔드포인트에서 기존 재배포 가능 패키지를 제거하거나 **Visual C++** 재배포 가능 패키지 **12.0.3**으로 업그레이드해야 합니다.*

 ©2023 Palo Alto Networks, Inc.

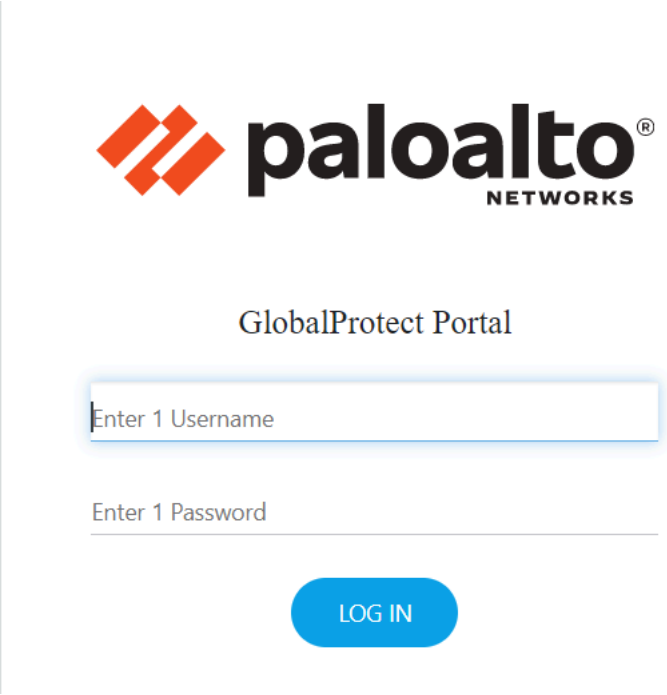
STEP 1 | GlobalProtect 포털에 로그인합니다.

1. 웹 브라우저를 시작하고 다음 URL로 이동합니다.

   `https://<portal IP address or FQDN>`

   예: **`http://gp.acme.com`**

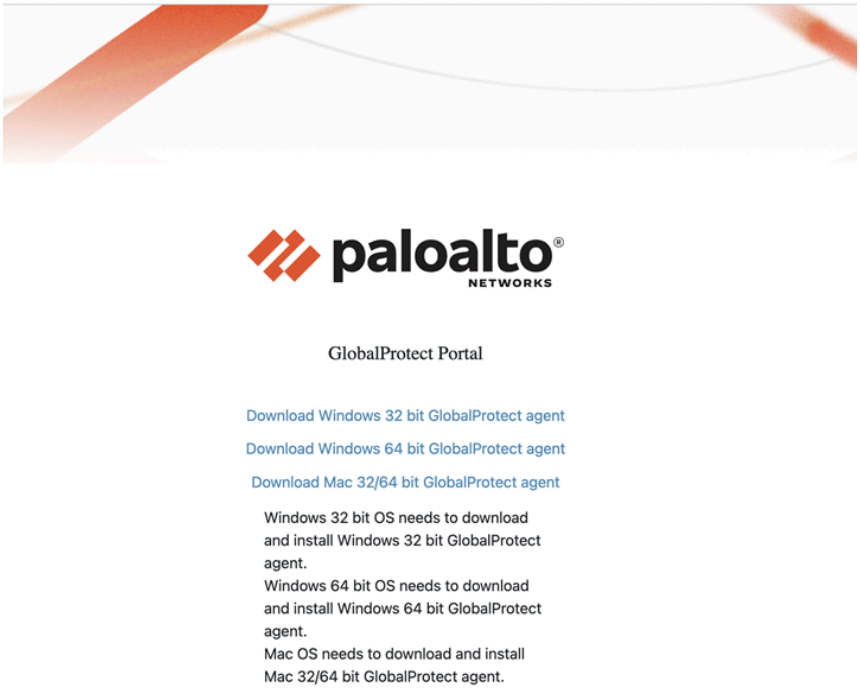
2. 포털 로그인 페이지에서 이름(사용자 이름)과 암호를 입력하고 로그인을 클릭합니다. 대부분의 경우 회사 네트워크에 연결할 때 사용하는 것과 동일한 사용자 이름과 암호를 사용할 수 있습니다.



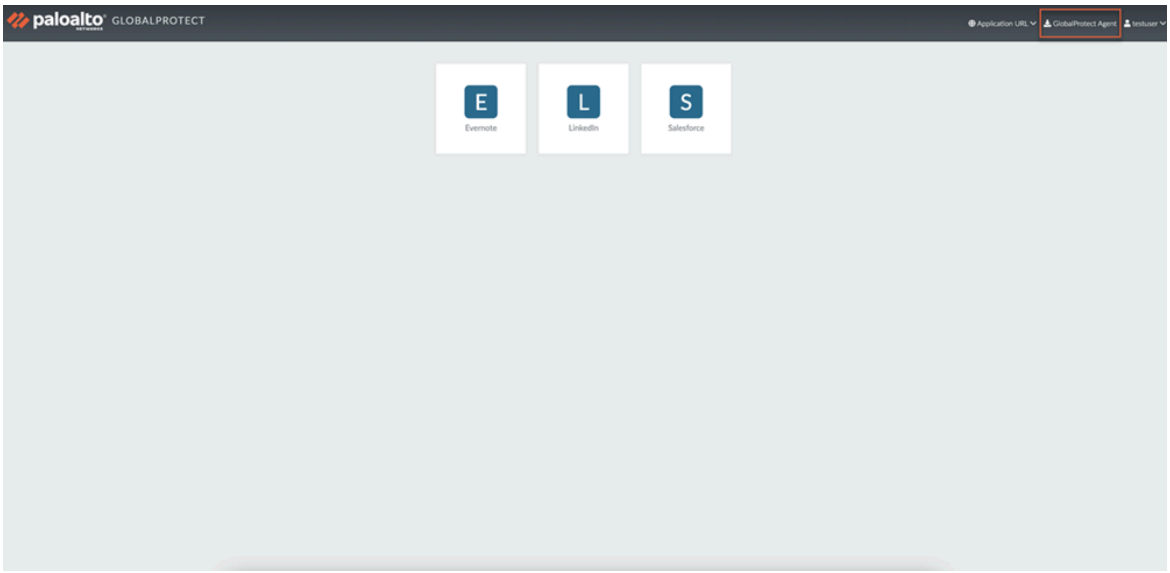
 ©2023 Palo Alto Networks, Inc.

STEP 2 | 앱 다운로드 페이지로 이동합니다.

대부분의 경우 앱 다운로드 페이지는 포털에 로그인한 직후에 표시됩니다. 이 페이지에서 최신 앱 소프트웨어 패키지를 다운로드할 수 있습니다.



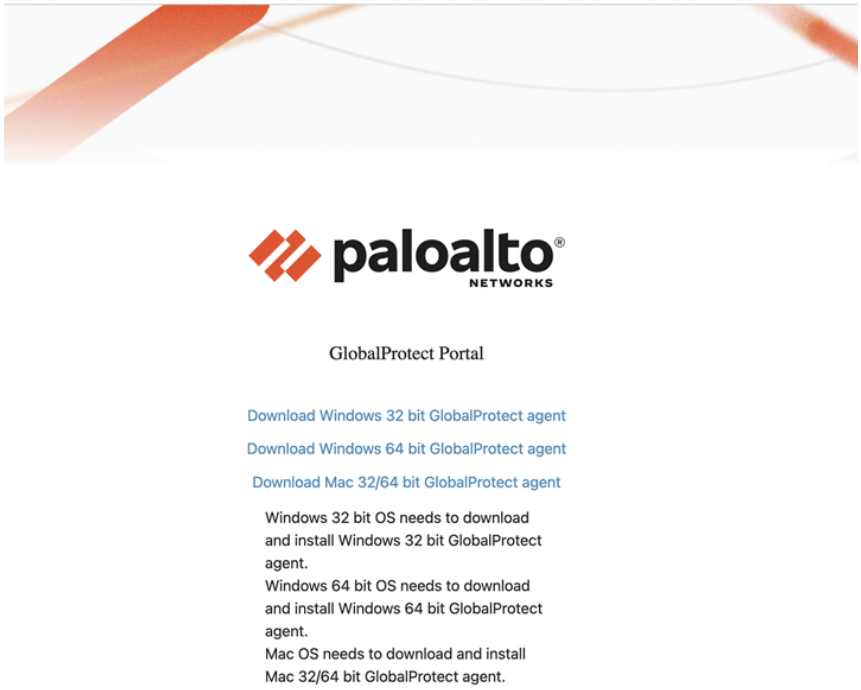
시스템 관리자가 GlobalProtect Clientless VPN 액세스를 활성화한 경우 포털에 로그인하면 앱 다운로드 페이지 대신 애플리케이션 페이지가 열립니다. **GlobalProtect** 에이전트를 선택하여 다운로드 페이지를 엽니다.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | 앱을 다운로드합니다.

1. 다운로드를 시작하려면 컴퓨터에서 실행 중인 운영 체제에 해당하는 소프트웨어 링크를 클릭합니다. 운영 체제가 32비트인지 64비트인지 확실하지 않으면 계속하기 전에 시스템 관리자에게 문의하십시오.



2. 소프트웨어 설치 파일을 엽니다.
3. 메시지가 표시되면 소프트웨어를 실행합니다.
4. 메시지가 다시 나타나면 GlobalProtect 설치 마법사를 실행합니다.

STEP 4 | GlobalProtect 앱 설정을 완료합니다.

1. GlobalProtect 설치 마법사에서 다음을 클릭합니다.
2. 다음을 클릭하여 기본 설치 폴더(C:\Program Files\Palo Alto Networks\GlobalProtect)를 적용한 후 다음을 두 번 클릭합니다.

   찾아보기를 통해 ***GlobalProtect*** 앱을 설치할 다른 위치를 선택할 수 있지만 기본 위치에 설치하는 것이 제일 좋습니다. 기본 설치 위치는 권한이 없는 사용자의 경우 읽기 전용이므로 이 위치에 설치하면 앱에 대한 악의적인 액세스로부터 보호됩니다.

3. 설치가 완료되면 마법사를 닫습니다.

 ©2023 Palo Alto Networks, Inc.

로그온 전 연결 사용하기

사전 로그온 및 사전 로그온 후 주문형 연결 방법은 로그온 전 연결과 동시에 지원되지 않습니다.

로그온 전 연결은 내부 게이트웨이 구성에 대해 지원되지 않습니다.

로그인 프로세스를 간소화하고 사용자 환경을 개선하기 위해 GlobalProtect는 스마트 카드, LDAP, RADIUS 또는 보안 보장 마크업 언어(SAML)과 같은 인증 서비스, 사용자 이름/암호 기반 인증 또는 일회용 암호(OTP) 인증을 사용하여 Windows 10 엔드포인트에 로그인하기 전에 회사 네트워크에 대한 VPN 연결을 설정할 수 있도록 로그온 전 연결을 제공합니다. 관리자는 사용자의 로컬 프로필 또는 계정으로 설정되지 않은 엔드포인트에서 새 GlobalProtect 사용자를 온보딩할 때 로그온 전 연결을 활성화하는 이점을 누릴 수 있습니다. 로그온 전 연결은 기본적으로 비활성화되어 있습니다. 관리자가 로그온 전 연결을 활성화하면 Windows 엔드포인트에 로그인하기 전에 GlobalProtect 앱 자격 증명 공급자를 시작하고 회사 네트워크에 연결할 수 있습니다. 로그온 전 연결에서 VPN 연결을 설정한 후 Windows 로그온 화면을 사용하여 Windows 엔드포인트에 로그인할 수 있습니다. GlobalProtect는 사전 로그인 액세스 공급자(PLAP) 자격 증명 공급자 역할을 하여 Windows에 로그인하기 전에 조직에 대한 액세스를 제공할 수 있습니다.

로그온 전 연결은 ***Windows*** 엔드포인트에 처음 로그인할 때 포털 및 게이트웨이에서 두 번 인증하라는 메시지를 표시하기 때문에 인증 재정의 쿠키가 예상대로 작동하지 않습니다.

로그온하기 전에 연결을 사용하려면 관리자가 Windows 레지스트리에 설정을 배포하고 인증 방법을 선택해야 합니다.

- 스마트 카드 인증을 사용하여 로그온 전 연결하기
- SAML 인증을 사용하여 로그온 전 연결하기
- 사용자 이름/암호 기반 인증을 사용하여 로그온 전 연결하기

스마트 카드 인증을 사용하여 로그온 전 연결하기

로그온 전 연결은 스마트 카드 인증을 지원합니다. 관리자는 스마트 카드에 포함된 인증서를 발급한 루트 CA 인증서를 포털 및 게이트웨이로 가져와야 합니다. 관리자는 인증서 프로필과 해당 루트 CA를 포털 또는 게이트웨이 구성에 적용하여 인증 프로세스에서 스마트 카드를 사용하도록 설정할 수 있습니다. 스마트 카드를 사용하여 Windows 엔드포인트에 로그인하기 전에 GlobalProtect에 인증할 수 있습니다. 메시지가 표시되면 스마트 카드를 삽입하여 스마트 카드 인증이 성공했는지 확인합니다. 스마트 카드 인증에 성공하면 GlobalProtect는 구성에 지정된 포털 또는 게이트웨이에 연결합니다.

STEP 1 | 로그온하기 전에 연결을 사용하려면 관리자가 다음 작업을 완료해야 합니다.

1. Windows 레지스트리에 로그온 전 연결 설정을 배포합니다.
2. 2단계 인증을 위해 스마트 카드를 설정합니다.
3. 인증서 프로필을 GlobalProtect 포털에 할당합니다.
4. 스마트 카드를 기반으로 최종 사용자를 인증하도록 게이트웨이를 구성합니다.

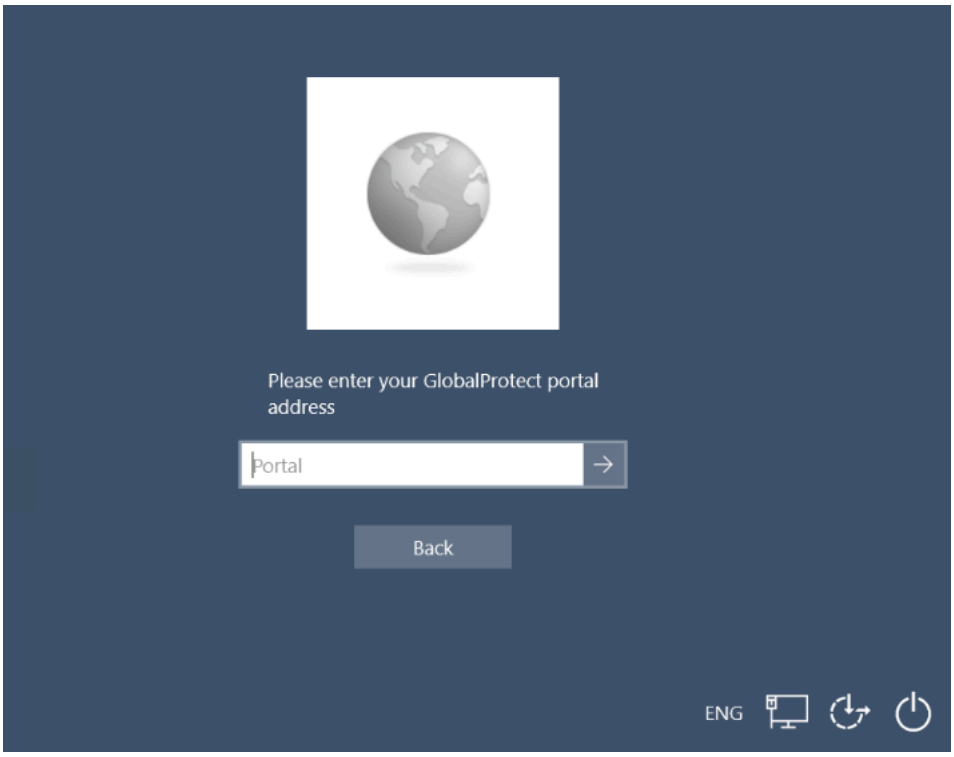
STEP 2 | 로그온 전 연결을 사용하여 Windows 엔드포인트에 로그인합니다.

1. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

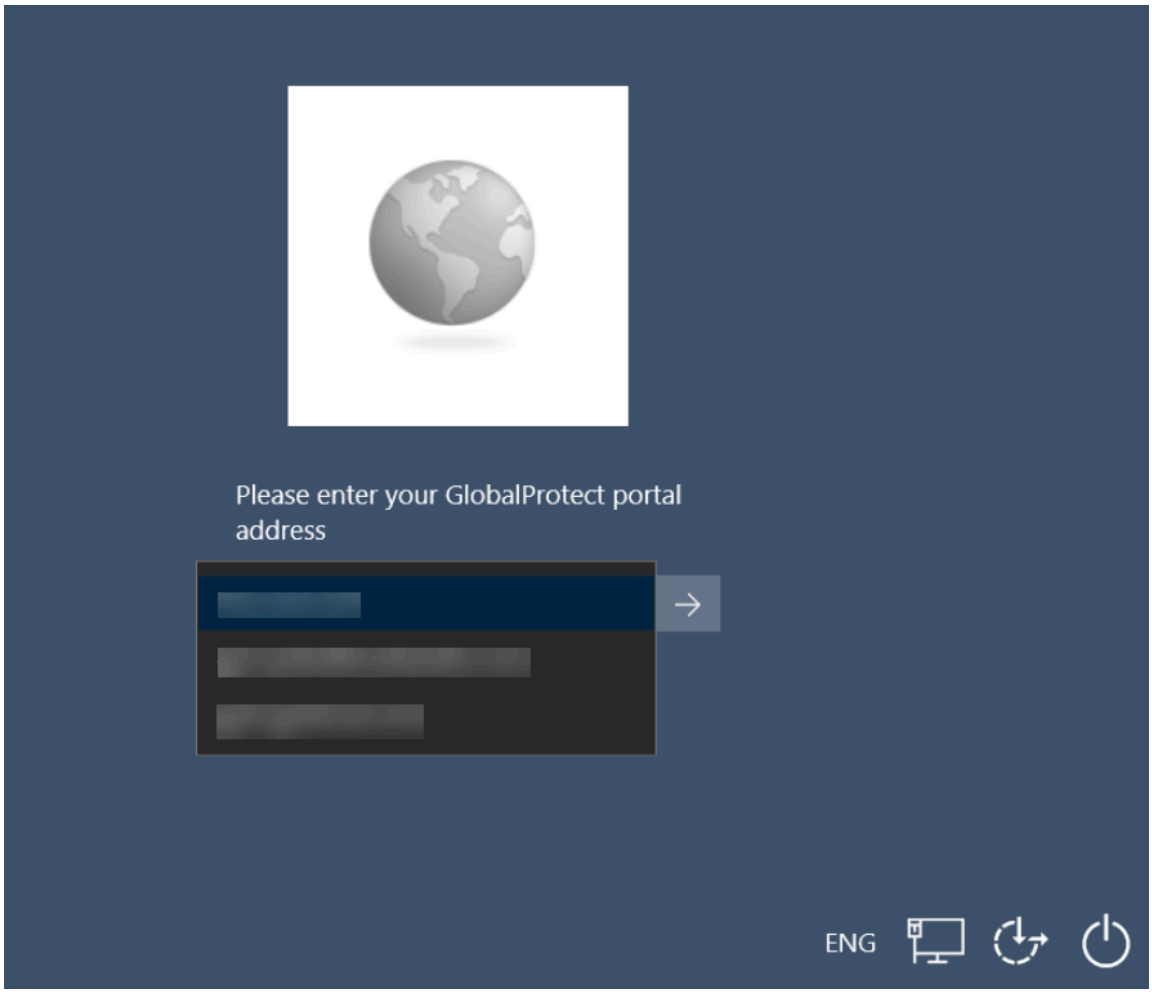
VPN 연결에 성공하면 Windows 로그온 화면의 네트워크 로그인 버튼 옆에 연결 해제( ) 버튼이 표시됩니다. 구성된 기간 내에 엔드포인트에 아직 로그인하지 않은 경우 VPN에서 로그아웃됩니다. 이로 인해 VPN 터널의 연결이 끊어집니다.

2. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의하지 않은 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력하고 제출합니다.



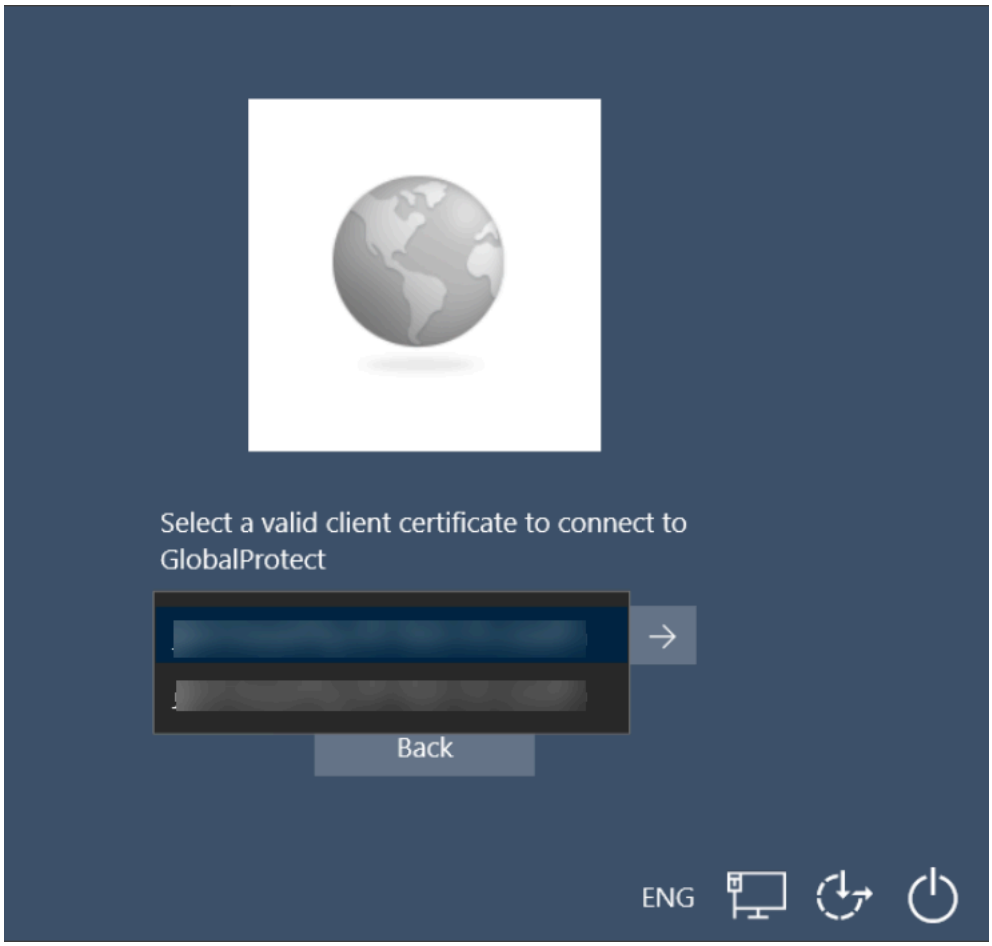
3. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의한 경우 포털 드롭다운에서 포털을 선택하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.



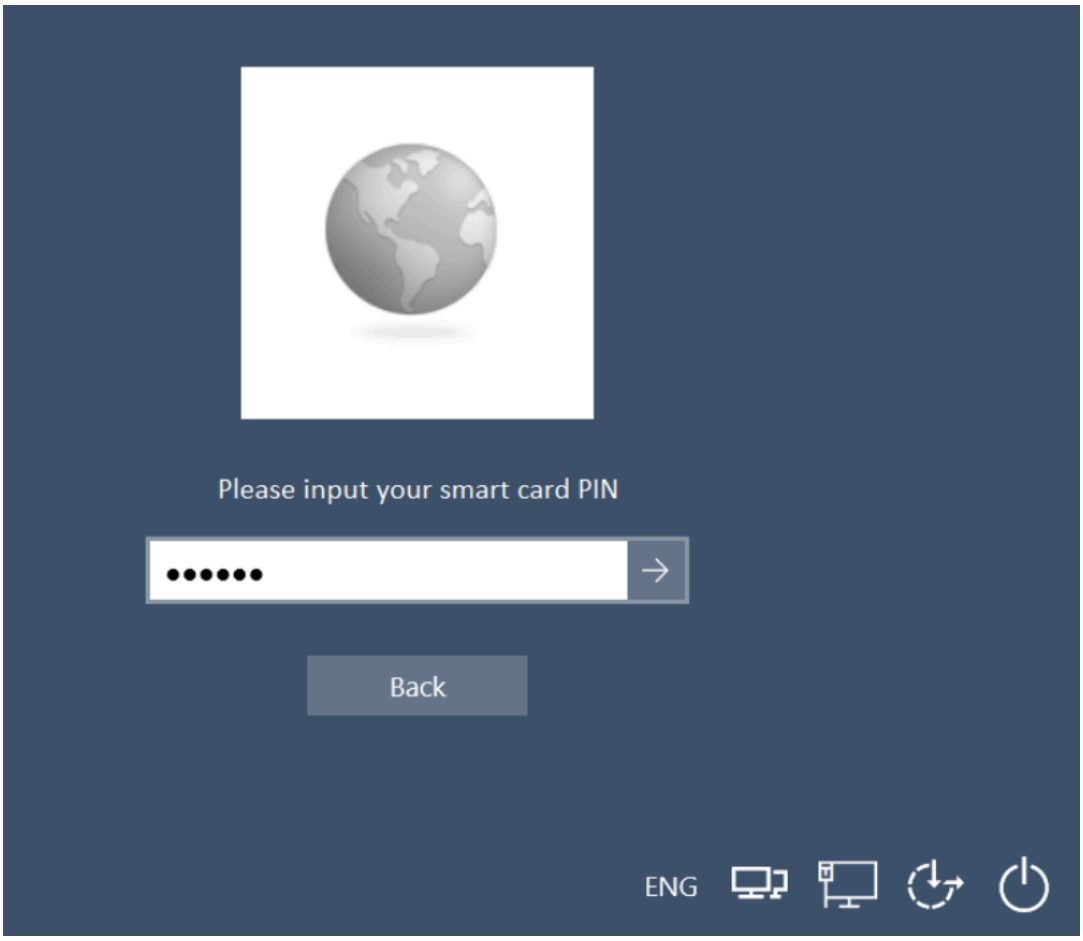
4. 엔드포인트의 유효한 인증서 목록에서 포털 또는 게이트웨이로 인증할 클라이언트 인증서를 선택하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.



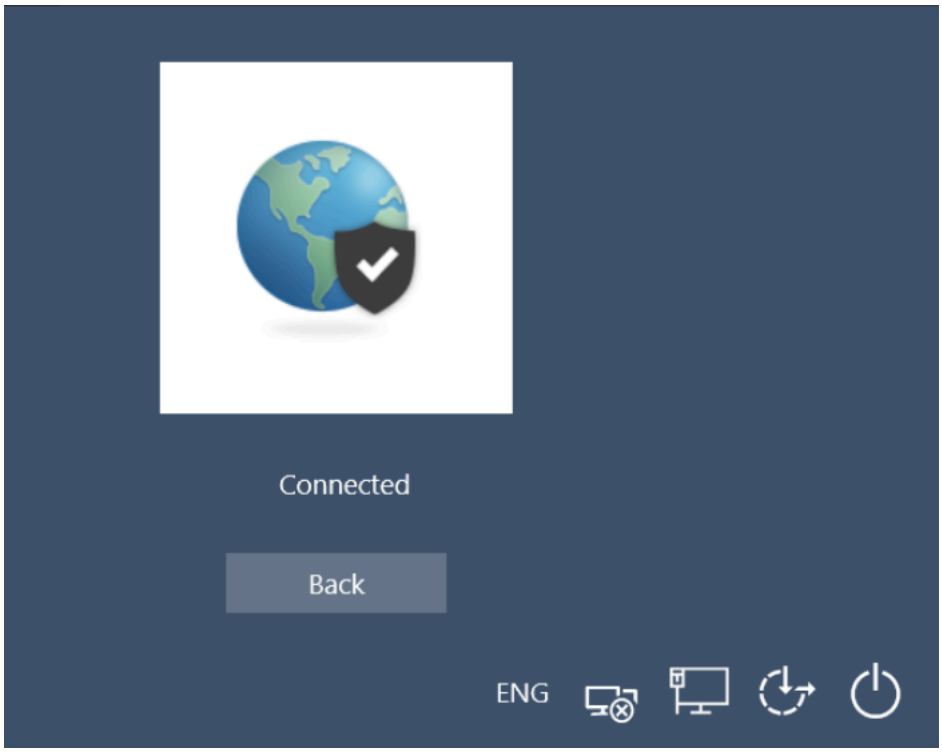
5. 스마트 카드의 개인 ID 번호(PIN)을 입력하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.



6. 인증에 성공하면 연결 상태가 VPN 연결 성공 시 연결됨으로 표시됩니다. 뒤로를 클릭하여 Windows 로그온 화면을 표시합니다.

 ©2023 Palo Alto Networks, Inc.



STEP 3 | GlobalProtect 게이트웨이에 연결되어 있는지 확인합니다.

1. Windows 엔드포인트에 다시 로그인합니다. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.
2. 상태 패널이 열립니다. 기본적으로 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다.

SAML 인증을 사용하여 로그온 전 연결하기

로그온 전 연결은 사용자 로그인에 대한 SAML 인증을 지원합니다. Onelogin 또는 Okta와 같이 구성된 SAML ID 공급자(IdP)를 사용하여 Windows 엔드포인트에 로그인하기 전에 GlobalProtect에 인증할 수 있습니다. SAML 인증에 성공하면 GlobalProtect는 구성에 지정된 포털 또는 게이트웨이에 연결합니다.

STEP 1 | 로그온하기 전에 연결을 사용하려면 관리자가 다음 작업을 완료해야 합니다.

1. Windows 레지스트리에 로그온 전 연결 설정을 배포합니다.
2. SAML 인증을 설정하여 최종 사용자를 인증합니다.
   - SAML 인증 서비스에 대한 설정을 사용하여 서버 프로파일을 생성합니다.
   - SAML 서버 프로파일을 참조하는 인증 프로파일을 생성합니다.
3. GlobalProtect 게이트웨이에 대한 SAML 인증을 지정합니다.
4. 클라이언트에 대한 SAML 인증을 지정합니다(GlobalProtect 클라이언트 인증 구성 정의 참조).

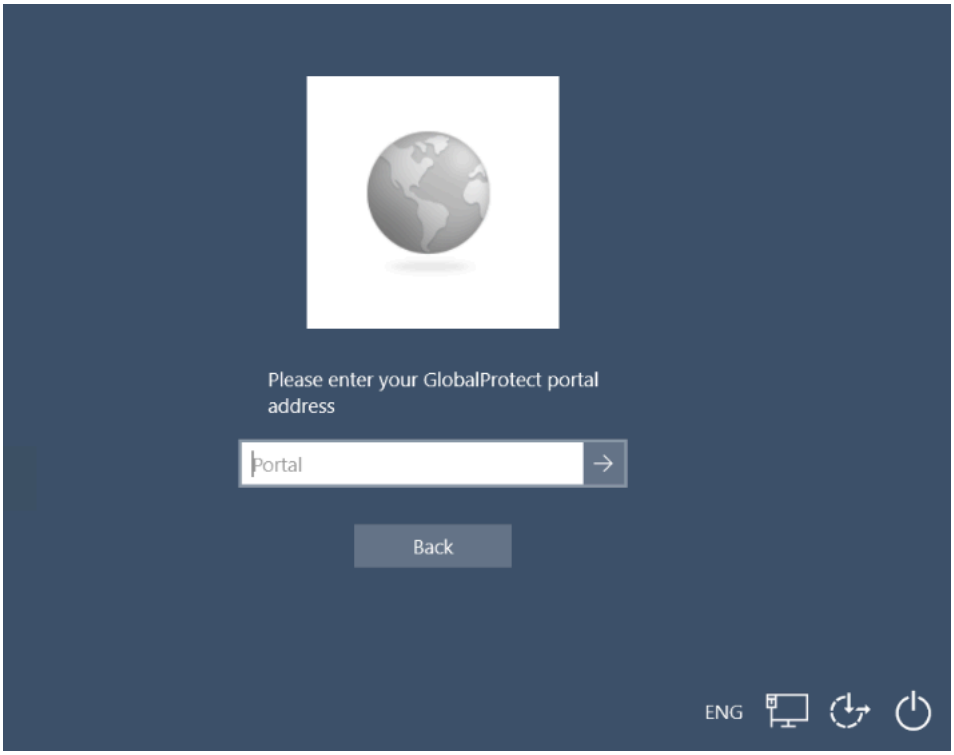
 ©2023 Palo Alto Networks, Inc.

STEP 2 | 로그온 전 연결을 사용하여 Windows 엔드포인트에 로그인합니다.

1. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.

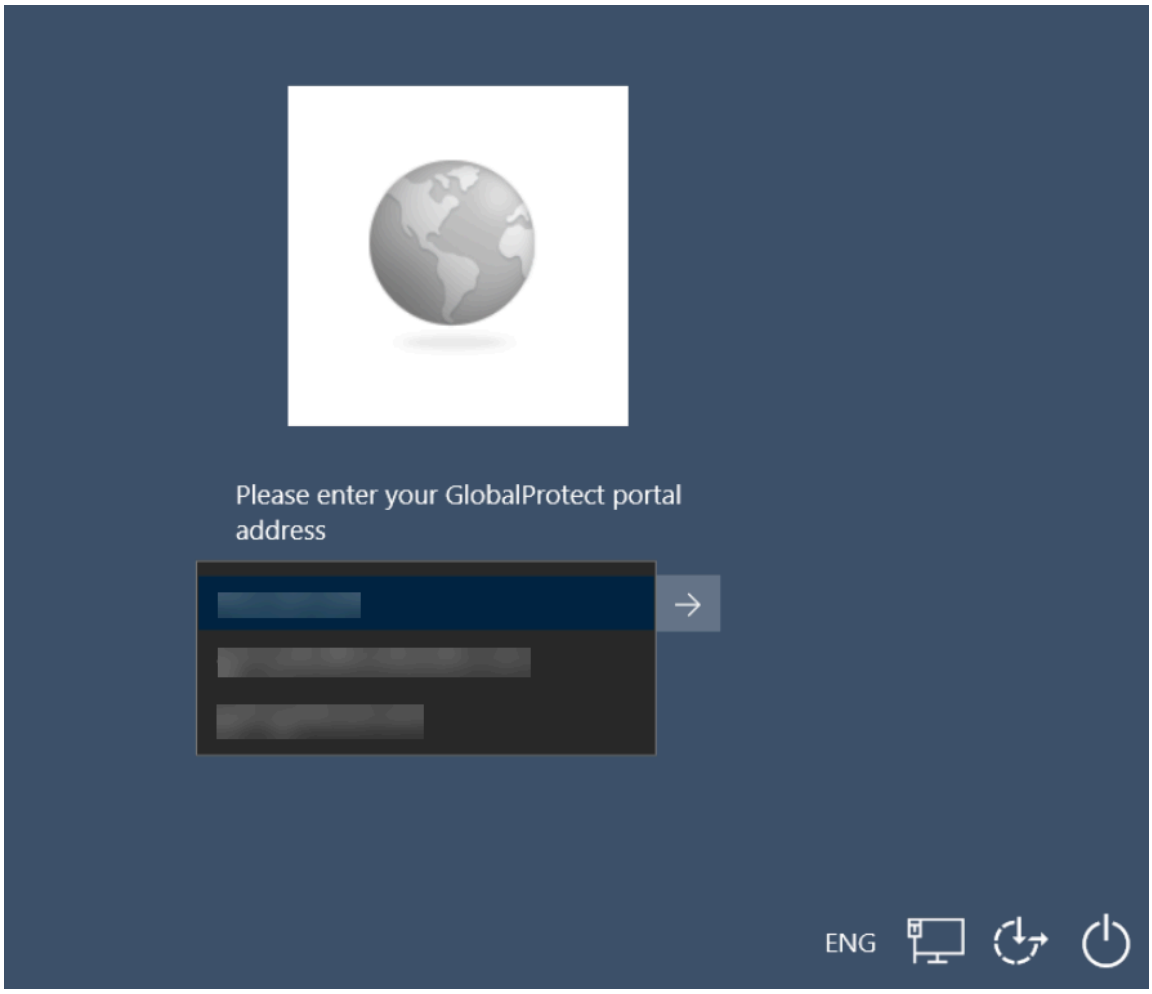
   VPN 연결에 성공하면 Windows 로그온 화면의 네트워크 로그인 버튼 옆에 연결 해제( ) 버튼이 표시됩니다. 구성된 기간 내에 엔드포인트에 아직 로그인하지 않은 경우 VPN에서 로그아웃됩니다. 이로 인해 VPN 터널의 연결이 끊어집니다.

2. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의하지 않은 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력하고 화살표를 클릭하여 제출합니다.



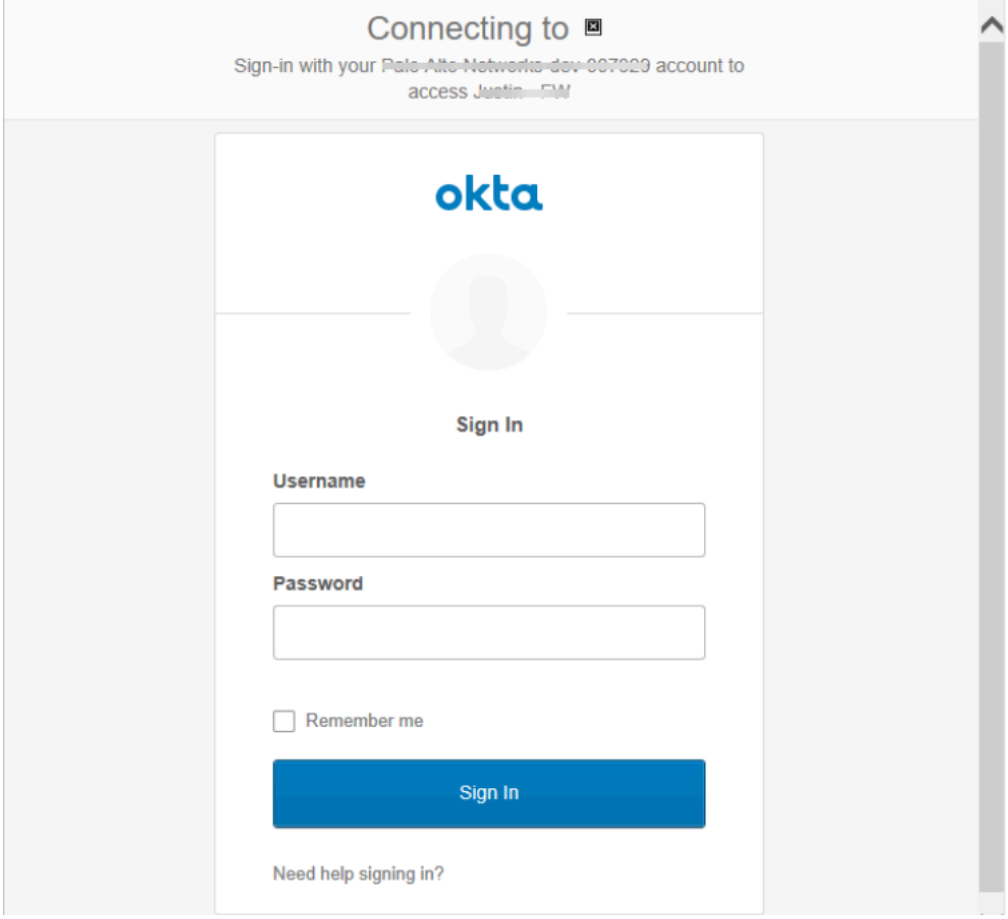
3. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의한 경우 포털 드롭다운에서 포털을 선택하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.



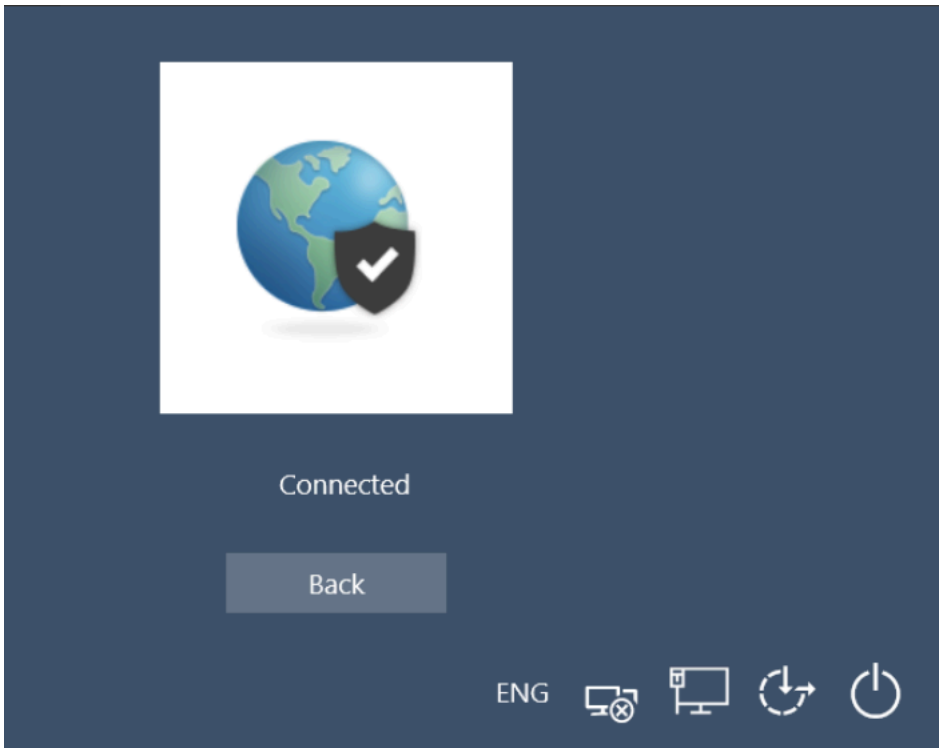
4. 사용자 이름과 암호를 입력하여 IdP에 인증한 다음 로그인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.



5. 인증에 성공하면 연결 상태가 VPN 연결 성공 시 연결됨으로 표시됩니다. 뒤로를 클릭하여 Windows 로그온 화면을 표시합니다.

 ©2023 Palo Alto Networks, Inc.



STEP 3 | GlobalProtect 게이트웨이에 연결되어 있는지 확인합니다.

1. Windows 엔드포인트에 다시 로그인합니다. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.
2. 상태 패널이 열립니다. 기본적으로 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다.

사용자 이름/암호 기반 인증을 사용하여 로그온 전 연결하기

로그온 전 연결은 LDAP, RADIUS 또는 OTP와 같은 인증 서비스를 사용하여 사용자 로그인의 사용자 이름/암호 기반 인증을 지원합니다. 사용자 이름 및 암호 자격 증명을 사용하여 Windows 엔드포인트에 로그인하기 전에 GlobalProtect에 인증할 수 있습니다. 사용자 이름/암호 기반 인증에 성공하면 GlobalProtect는 구성에 지정된 포털 또는 게이트웨이에 연결합니다.

STEP 1 | 로그온하기 전에 연결을 사용하려면 관리자가 다음 작업을 완료해야 합니다.

1. Windows 레지스트리에 로그온 전 연결 설정을 배포합니다.
2. 자격 증명을 사용하여 포털에 대한 최종 사용자를 인증하도록 GlobalProtect 포털에 대한 액세스를 설정합니다.
3. 자격 증명을 사용하여 게이트웨이에 최종 사용자를 인증하도록 GlobalProtect 게이트웨이를 구성합니다.

로그온 전 연결은 사용자 지정 인증 메시지를 지원하지 않습니다.

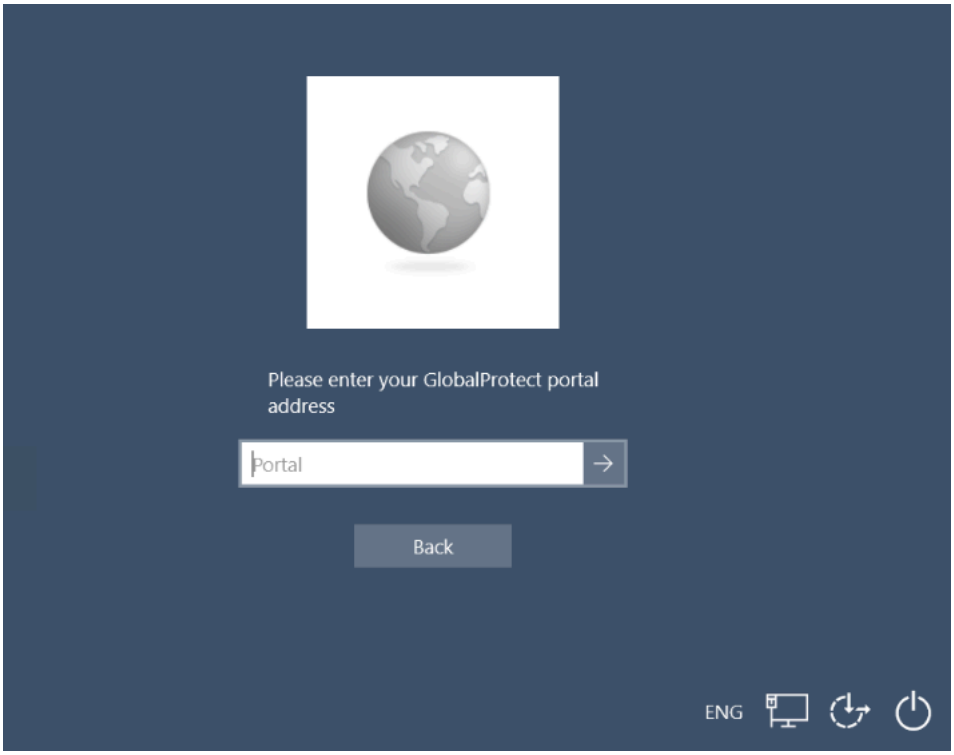
 ©2023 Palo Alto Networks, Inc.

STEP 2 | 로그온 전 연결을 사용하여 Windows 엔드포인트에 로그인합니다.

1. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.

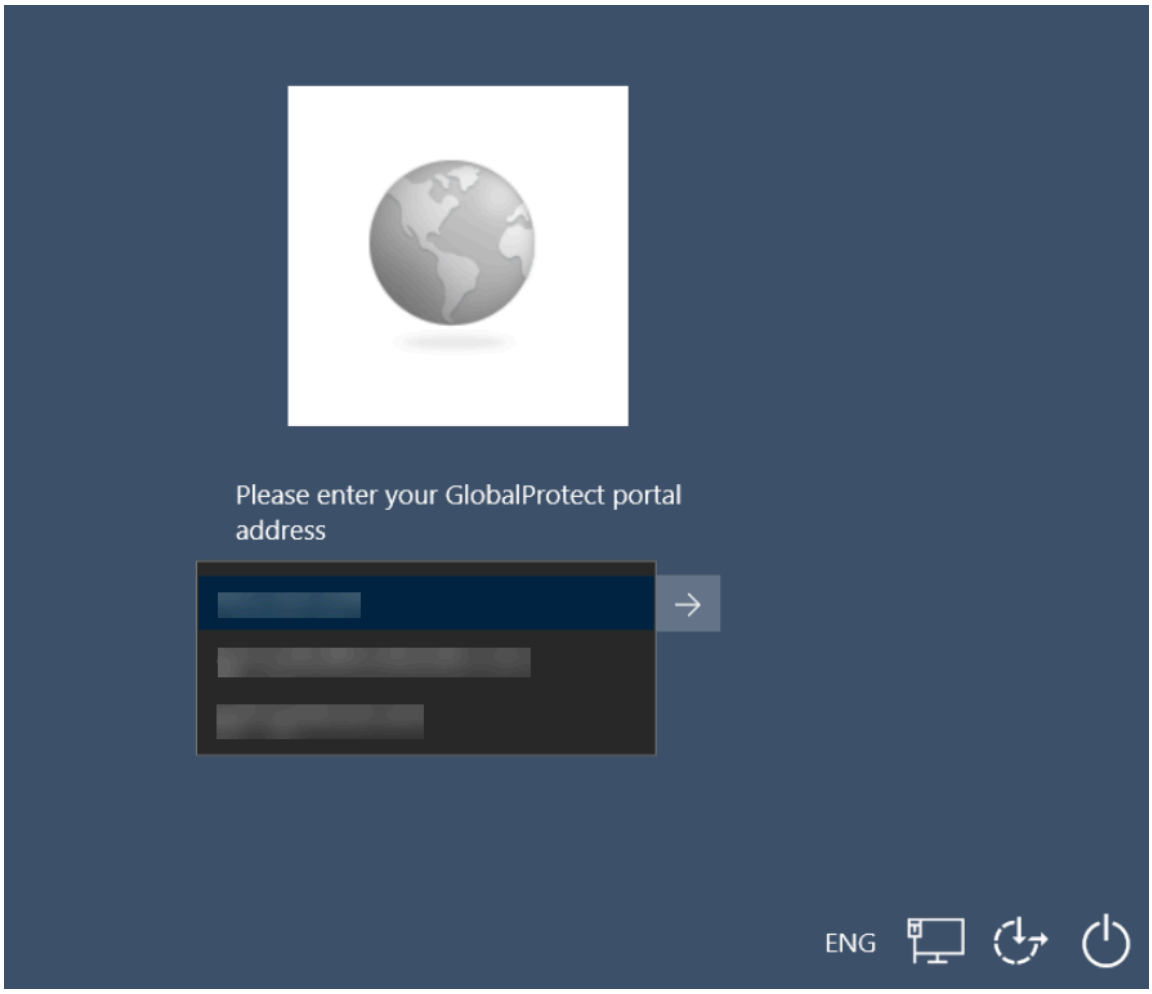
   VPN 연결에 성공하면 Windows 로그온 화면의 네트워크 로그인 버튼 옆에 연결 해제( ) 버튼이 표시됩니다. 구성된 기간 내에 엔드포인트에 아직 로그인하지 않은 경우 VPN에서 로그아웃됩니다. 이로 인해 VPN 터널의 연결이 끊어집니다.

2. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의하지 않은 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력하고 화살표를 클릭하여 제출합니다.



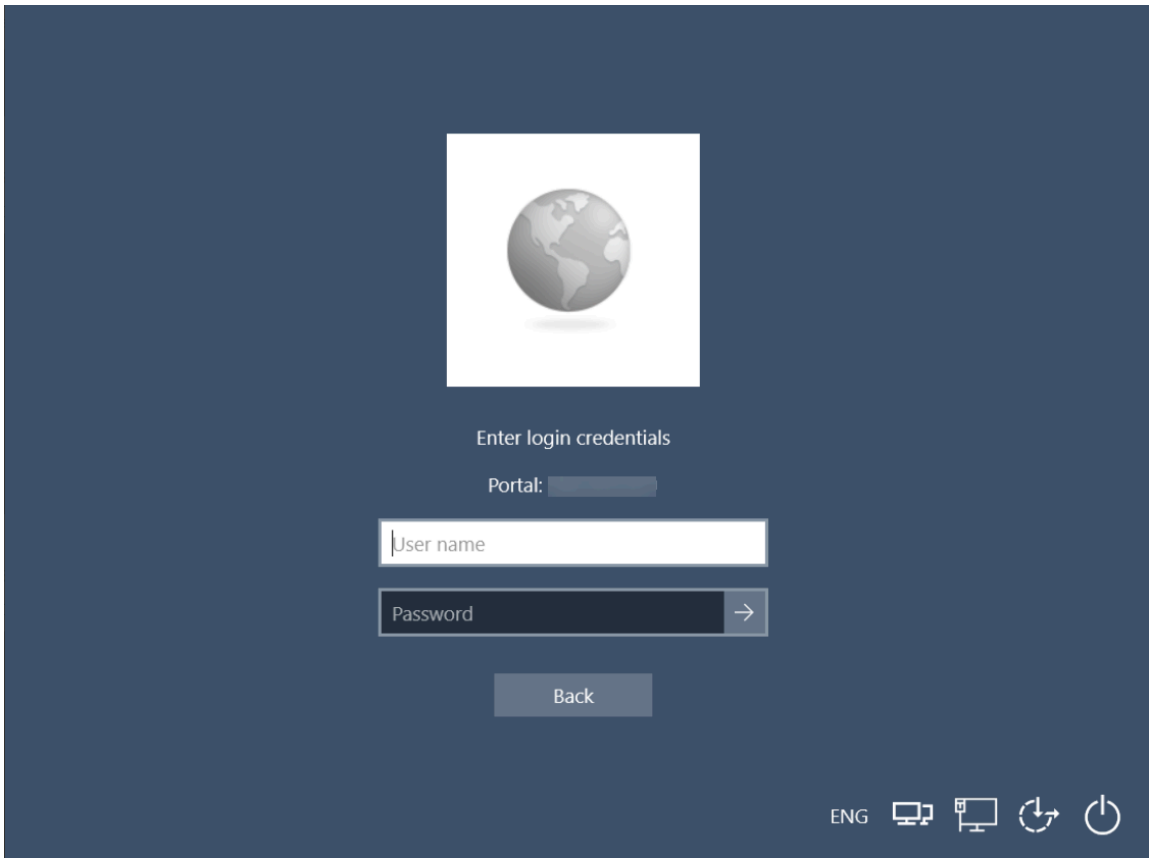
3. (선택 사항) 엔드포인트에 처음 로그인하고 관리자가 포털을 미리 정의한 경우 포털 드롭다운에서 포털을 선택하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.

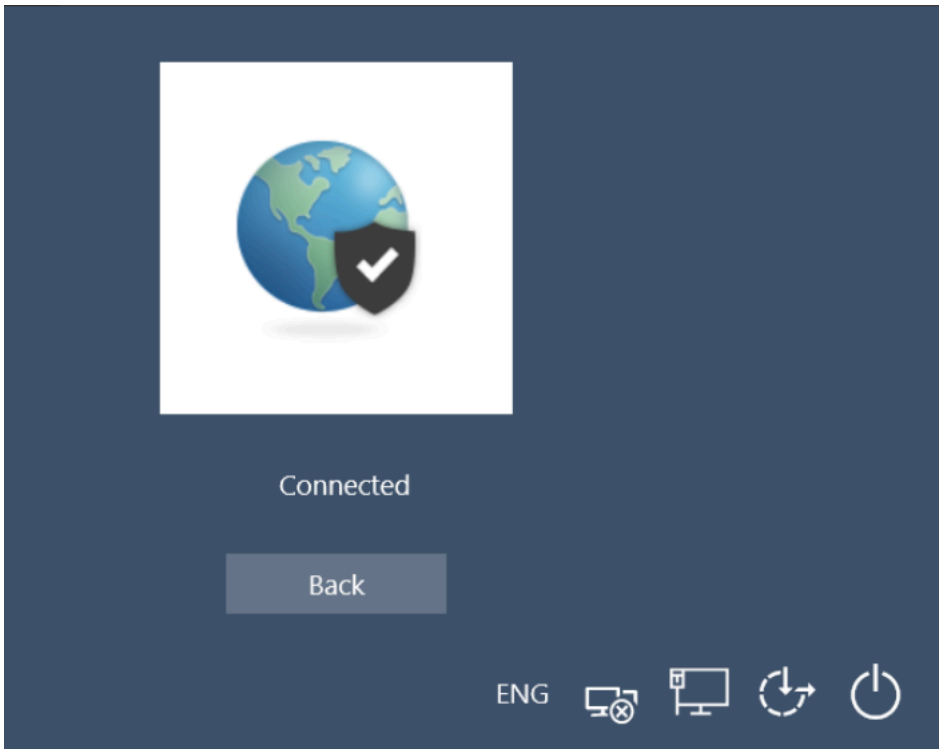


4. 사용자 이름과 암호를 입력하고 화살표를 클릭하여 제출합니다.

 ©2023 Palo Alto Networks, Inc.



5. 인증에 성공하면 연결 상태가 VPN 연결 성공 시 연결됨으로 표시됩니다. 뒤로를 클릭하여 Windows 로그온 화면을 표시합니다.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | GlobalProtect 게이트웨이에 연결되어 있는지 확인합니다.

1. Windows 엔드포인트에 다시 로그인합니다. Windows 로그온 화면의 오른쪽 하단 모서리에 있는 네트워크 로그인( ) 버튼을 클릭합니다.
2. 상태 패널이 열립니다. 기본적으로 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다.

 ©2023 Palo Alto Networks, Inc.

스마트 카드 인증에 Single Sign-On 사용하기

관리자가 스마트 카드 인증을 사용하여 Single Sign-On(SSO)을 통해 인증할 수 있도록 GlobalProtect 포털을 구성한 경우 원활한 SSO 환경을 위해 GlobalProtect 앱에 스마트 카드 개인 식별 번호(PIN)를 다시 입력하지 않고도 연결할 수 있습니다. Windows 엔드포인트에서 GlobalProtect에 대해 동일한 스마트 카드 PIN을 활용할 수 있습니다. 로그인할 때 스마트 카드 PIN을 입력해야 하는 횟수를 줄여 스마트 카드 인증에 SSO를 사용하면 이점을 얻을 수 있습니다. Windows 엔드포인트에 로그인하면 GlobalProtect 앱은 스마트 카드 PIN을 획득하고 기억하여 GlobalProtect 포털 및 게이트웨이로 인증합니다.

관리자는 스마트 카드 공급자의 ***PIN***과 연결된 ***Windows***의 PIN 캐싱 정책 유형을 정의할 수 있습니다. ***PIN***은 스마트 카드 공급자에서 허용한 경우에만 캐시됩니다. ***GlobalProtect***는 사용자가 ***GlobalProtect*** 앱에서 수동으로 로그아웃하거나 ***Windows***에서 로그아웃하거나 ***PIN***이 변경된 경우 캐시에서 ***PIN***을 지웁니다.

STEP 1 | 스마트 카드 인증에 SSO를 사용하려면 관리자가 다음 작업을 완료해야 합니다.

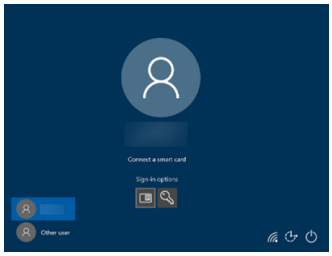
1. 스마트 카드 인증에 SSO를 사용하도록 Windows 엔드포인트에 미리 배포된 설정을 지정합니다.

   관리자는 스마트 카드 PIN에 SSO를 사용하도록 설정하기 전에 Windows 엔드포인트에서 미리 배포된 설정을 지정해야 합니다. GlobalProtect는 GlobalProtect 앱이 초기화될 때 이 항목을 한 번만 검색합니다.
2. 2단계 인증을 위해 스마트 카드를 설정합니다.
3. 인증서 프로필을 GlobalProtect 포털에 할당합니다.
4. 스마트 카드를 사용하여 인증할 수 있도록 게이트웨이를 구성합니다.
5. GlobalProtect 앱이 GlobalProtect 포털에서 스마트 카드 PIN에 SSO를 사용하도록 설정하여 Windows 엔드포인트에서 GlobalProtect에 대해 동일한 스마트 카드 PIN을 사용할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

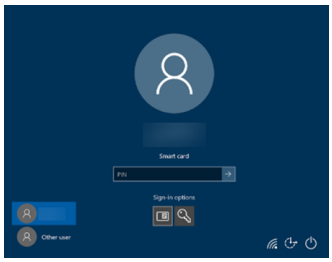
STEP 2 | 스마트 카드 PIN을 사용하여 Windows 엔드포인트에 로그인합니다.

1. 로그인 옵션을, 클릭하고 스마트 카드( ) 버튼을 클릭합니다 .
2. 메시지가 표시되면 스마트 카드를 삽입하여 스마트 카드 인증이 성공했는지 확인합니다.



3. 스마트 카드의 PIN을 입력하고 화살표를 클릭하여 제출합니다.

   스마트 카드 인증에 성공하면 스마트 카드 PIN을 다시 입력할 필요 없이 구성에 지정된 포털 또는 게이트웨이에 연결합니다.

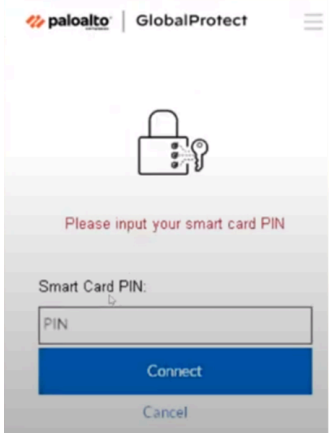


STEP 3 | (선택 사항) 동일한 스마트 카드 PIN을 사용하여 GlobalProtect에 로그인합니다.

Windows 엔드포인트에 로그인하는 데 사용한 것과 동일한 스마트 카드 PIN을 활용할 수 있습니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 햄버거 메뉴를 클릭하여 설정 패널을 엽니다.
3. 설정 패널에서 로그아웃하여 GlobalProtect 앱에서 저장된 사용자 자격 증명을 지웁니다.
4. 동일한 스마트 카드 PIN을 사용하여 GlobalProtect에 다시 연결합니다.

   PIN이 유효하지 않은 경우 GlobalProtect 앱에 스마트 카드 PIN 오류가 표시됩니다.



 ©2023 Palo Alto Networks, Inc.

Windows용 GlobalProtect 앱 사용하기

이 장은 설정에서 엔드포인트에 로그인한 후 GlobalProtect 로그인 자격 증명을 입력해야 하는 경우에만 적용됩니다(Single Sign-On은 비활성화됨).

일반적으로 조직에서는 GlobalProtect 사용자가 앱 설치 후 투명하게 로그인할 수 있도록 허용하는 것이 좋습니다. 투명한 GlobalProtect 로그인으로 엔드포인트에 로그인하면 GlobalProtect 앱이 자동으로 시작되어 추가 사용자 개입 없이 기업 네트워크에 연결됩니다.

설정에 GlobalProtect 자격 증명을 입력해야 하는 경우 아래에서 해당 단계를 따르십시오.

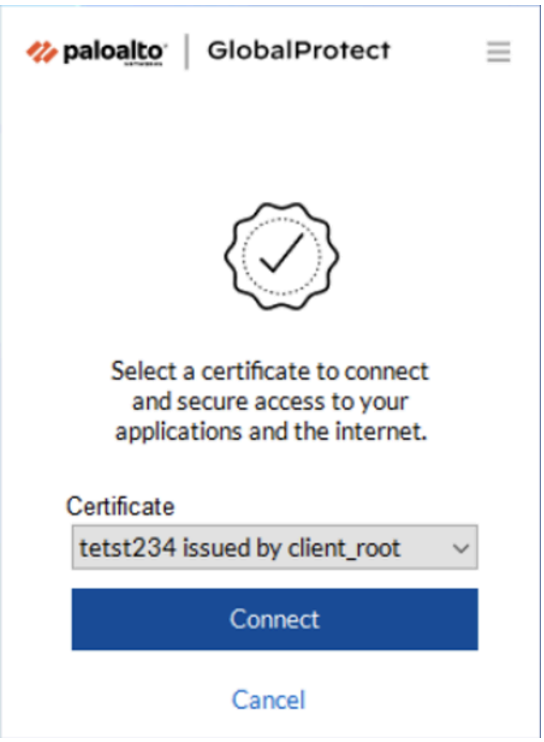
 ©2023 Palo Alto Networks, Inc.

STEP 1 | GlobalProtect에 로그인합니다.

엔드포인트에 처음 로그인하는 경우 GlobalProtect 앱은 로그인 시 친절한 환영 페이지를 표시합니다. 시작하기를 클릭합니다.

1. (선택 사항) 관리자가 온디맨드 연결 방법으로 GlobalProtect를 구성하고 처음으로 GlobalProtect에 로그인하는 경우 인증서 드롭다운의 유효한 인증서 목록에서 클라이언트 인증서를 선택하여 포털 또는 게이트웨이에 인증합니다.
2. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.

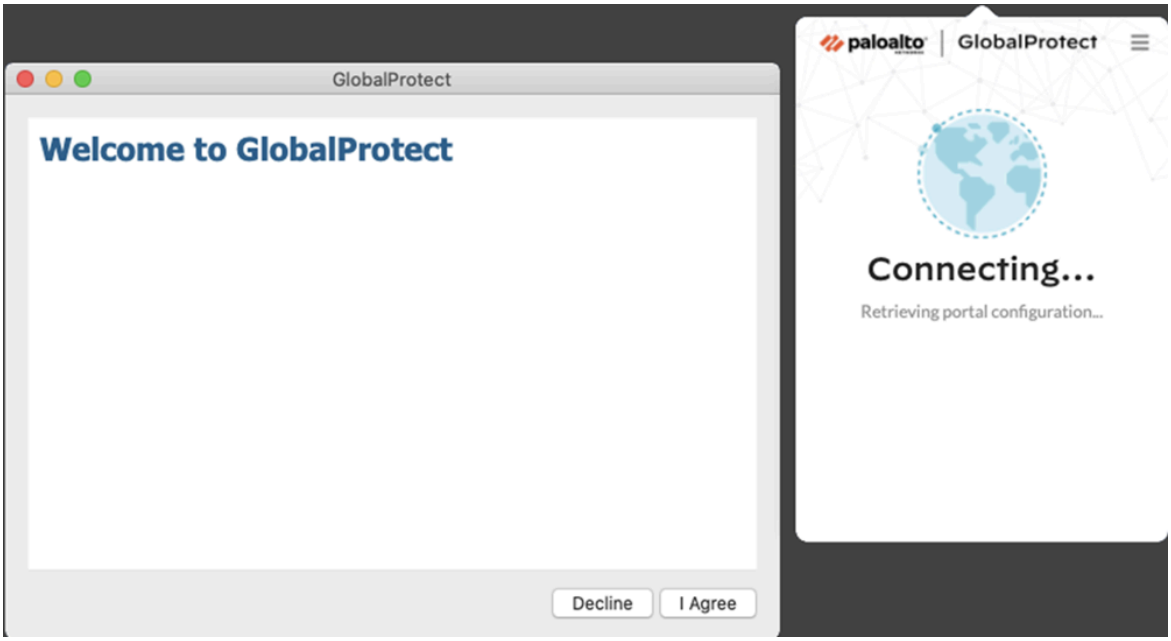
 ©2023 Palo Alto Networks, Inc.



3. (선택 사항) 관리자가 내부 리소스에 액세스하기 위해 페이지를 보도록 요구하는 경우 GlobalProtect에 연결하기 전에 회사의 서비스 약관을 검토하십시오.

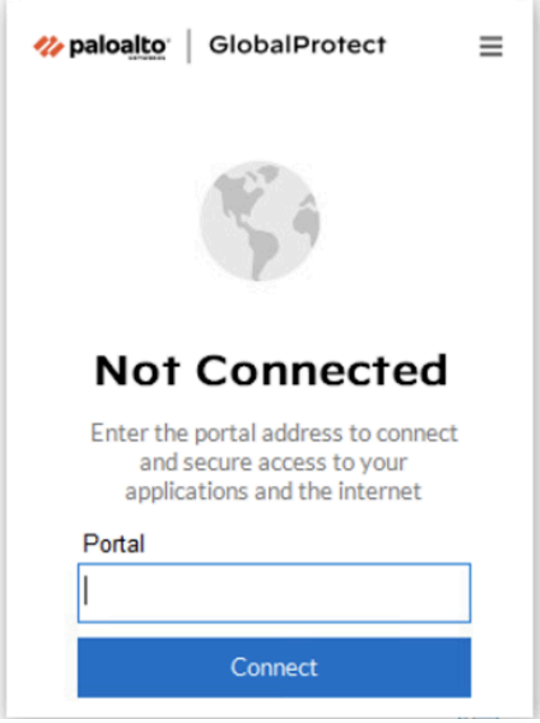
   이용 약관에 동의하지 않으면 GlobalProtect에 연결할 수 없습니다.

   선택적으로 취소를 클릭하면 GlobalProtect 포털의 IP 주소(또는 도메인)를 입력한 다음 연결을 클릭하여 연결을 시작해야 합니다.



4. GlobalProtect 관리자가 제공한 포털의 IP 주소 또는 도메인을 입력한 다음 연결을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.



5. (선택 사항) 기본적으로 관리자가 정의하는 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 변경 드롭다운에서 게이트웨이를 선택합니다(외부 게이트웨이에만 해당).

   이 옵션은 관리자가 수동 게이트웨이 선택을 활성화한 경우에만 사용할 수 있습니다.

6. (선택 사항) 연결 모드에 따라 연결을 클릭하여 연결을 시작합니다.
7. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력하고 로그인을 클릭합니다.

   관리자가 생체 인식(지문) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호를 사용하여 두 번 로그인해야 합니다(저장하기 위해 한 번, 인증하기 위해 한 번 더). 그 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

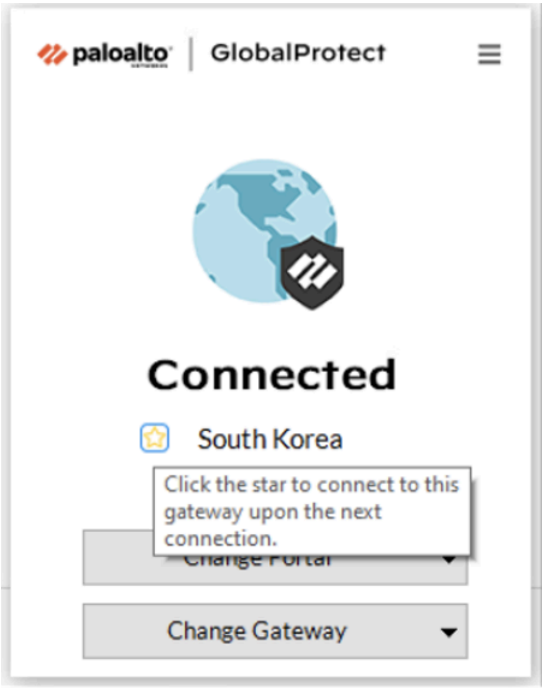
   인증에 성공하면 회사 네트워크에 연결되고 상태 패널에 연결됨 또는 연결됨 - 내부 상태가 표시됩니다. 관리자가 GlobalProtect 시작 페이지를 설정한 경우 로그인한 후 표시됩니다.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

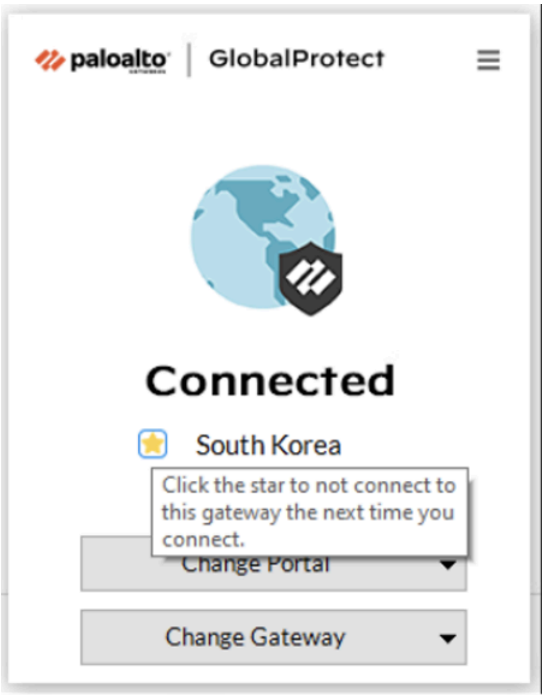
GlobalProtect 시스템 트레이 아이콘을 확인하여 연결 여부를 확인할 수 있습니다. 연결되지 않은 경우 아이콘은 회색( )이고 아이콘 위로 마우스를 가져가면 연결되지 않음이 표시됩니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. (선택 사항) GlobalProtect 앱에 처음 로그인하는 경우 GlobalProtect 포털의 IP 주소 또는 도메인을 입력한 다음 연결을 클릭합니다.
3. (선택 사항) 앱에 여러 포털이 저장된 경우 포털 변경 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 변경 드롭다운에서 미리 선택됩니다.
4. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 변경 드롭다운을 클릭하고 다음 옵션 중 하나를 사용합니다.
   - 게이트웨이를 수동으로 선택합니다(외부 게이트웨이만 해당). 이 옵션은 관리자가 수동 게이트웨이 선택을 활성화한 경우에만 사용할 수 있습니다.
   - 기본 게이트웨이 할당 및 자동 연결:
     1. 기본 게이트웨이를 지정하려면 별표 아이콘(☆)을 클릭합니다. 다음에 연결하면 지정된 기본 설정 게이트웨이에 자동으로 연결됩니다.



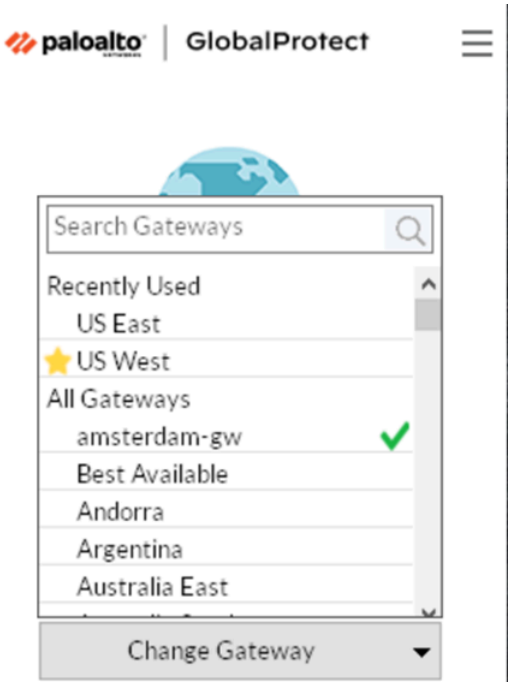
나중에 이 게이트웨이를 더 이상 기본 게이트웨이로 사용하지 않기로 결정한 경우 별표 아이콘을 지울 수 있습니다. 다음에 연결하면 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다.

 ©2023 Palo Alto Networks, Inc.



2. 기본적으로 게이트웨이 변경 드롭다운에서 확인 표시로 식별되는 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 기본 게이트웨이를 설정하면 게이트웨이 변경 드롭다운에서 별표 표시된 게이트웨이 옆에 별표가 표시됩니다.

   관리자가 포털 에이전트 구성에서 수동 외부 게이트웨이를 구성한 경우 게이트웨이 검색 필드를 사용하여 특정 게이트웨이를 선택할 수 있습니다.



5. (선택 사항) 연결 모드에 따라 연결을 클릭하여 연결을 시작합니다.
6. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 연결합니다.

 ©2023 Palo Alto Networks, Inc.

관리자가 생체 인식(지문) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호를 사용하여 두 번 로그인해야 합니다(저장하기 위해 한 번, 인증하기 위해 한 번 더). 그 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

앱이 외부 모드에서 연결되면 GlobalProtect 시스템 트레이 아이콘에 방패( ) 아이콘 위로 마우스를 가져가면 연결됨이 표시됩니다. 앱이 내부 모드로 연결되면 GlobalProtect 시스템 트레이 아이콘에 집( ) 아이콘 위로 마우스를 가져가면 내부 네트워크가 표시됩니다.

STEP 3 | GlobalProtect 앱을 엽니다.

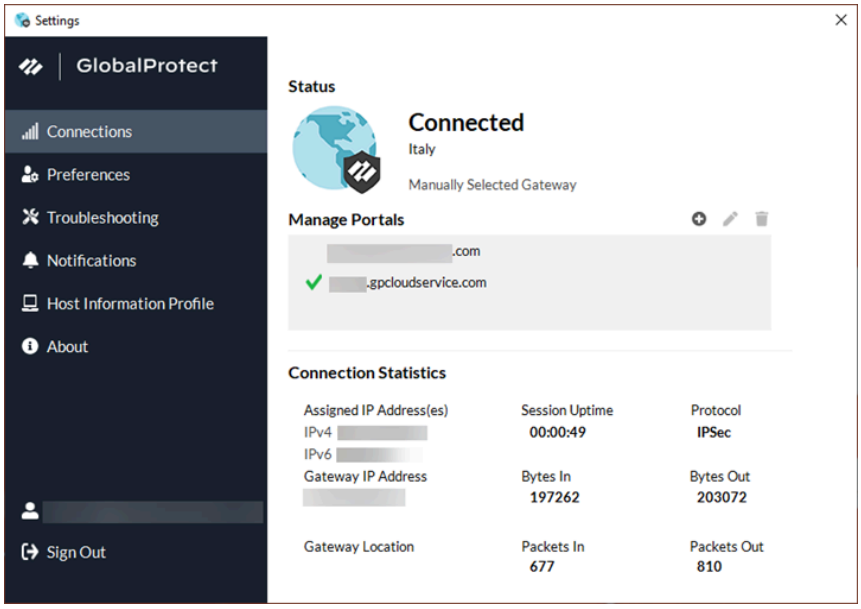
GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

관리자가 GlobalProtect 앱 설치 중에 Autonomous DEM(ADEM) 엔드포인트 에이전트를 설치하도록 포털을 구성하고 테스트 활성화를 허용하거나 허용하지 않은 경우 알림이 표시됩니다. 관리자가 이미 ADEM 엔드포인트 에이전트를 설치하고 나중에 ADEM 엔드포인트 에이전트를 제거하도록 포털을 구성한 경우 다음 로그인 시 알림이 표시됩니다.

STEP 4 | 네트워크 연결에 대한 정보를 봅니다.

앱을 실행한 후 상태 패널에서 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다. 설정을 선택하여 **GlobalProtect** 설정 패널을 연 후 다음 설정 중 하나를 선택하여 GlobalProtect 앱을 보고 수정합니다.

- 연결—연결 탭에는 GlobalProtect 계정과 연결된 포털이 표시됩니다. 이 탭에서 포털을 추가, 편집 또는 삭제할 수 있습니다. 이 탭에는 연결된 게이트웨이도 표시됩니다. 관리자가 GlobalProtect 포털 에이전트 구성에서 고급 보기 활성화를 예로 설정하면 게이트웨이에 대한 연결 통계(예: 게이트웨이 IP 주소, 위치 및 VPN 세션 가동 시간)를 볼 수 있습니다.

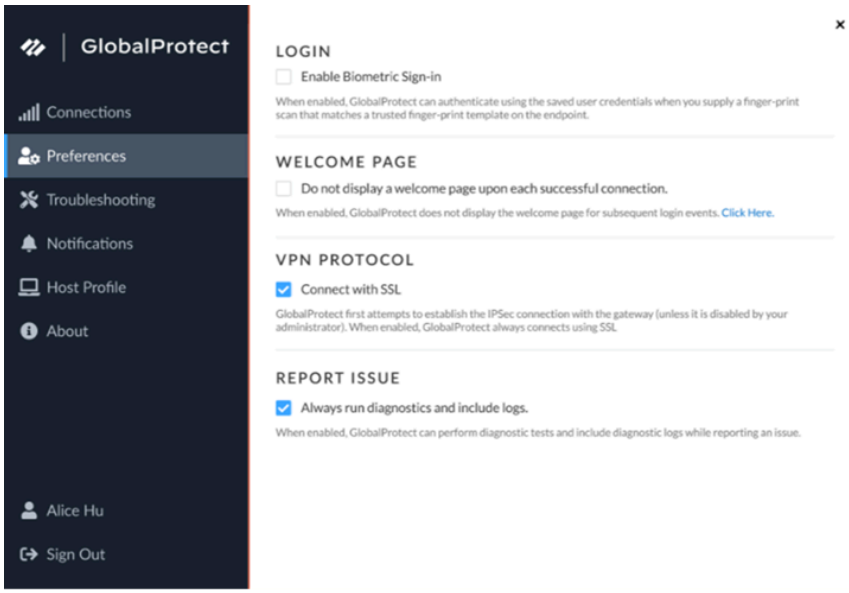


- 기본 설정—이제 관리자가 다음 옵션 중 하나 이상을 구성한 경우에만 기본 설정 탭을 사용할 수 있습니다.
  - 생체 인식 로그인 활성화—생체 인식(지문) 정보를 사용하여 로그인하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 에이전트 구성에서 사용자 자격 증명 저장을 사용자 지문으로만으로 구성하는 경우에만 사용할 수 있습니다. 엔드포인트의 신뢰할 수 있는 지문 템플릿과

 ©2023 Palo Alto Networks, Inc.

일치하는 지문을 제공하여 GlobalProtect 포털 및 게이트웨이에 대한 인증에 저장된 암호를 사용해야 합니다.

- 연결할 때마다 환영 페이지를 표시하지 않음—로그인에 성공하면 환영 페이지를 표시하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털 에이전트 구성에서 환영 페이지를 공장 기본값으로 설정한 경우에만 사용할 수 있습니다.
- **SSL**을 사용하여 연결—SSL을 사용하거나 IPSec을 유지하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털 에이전트 구성에서**SSL**로만 연결을 사용자가 변경할 수 있음으로 설정한 경우에만 사용할 수 있습니다.
- 항상 진단 테스트 실행 및 로그 포함—GlobalProtect 앱이 진단 테스트를 실행하고 진단 로그를 포함하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화한 경우에만 사용할 수 있습니다.

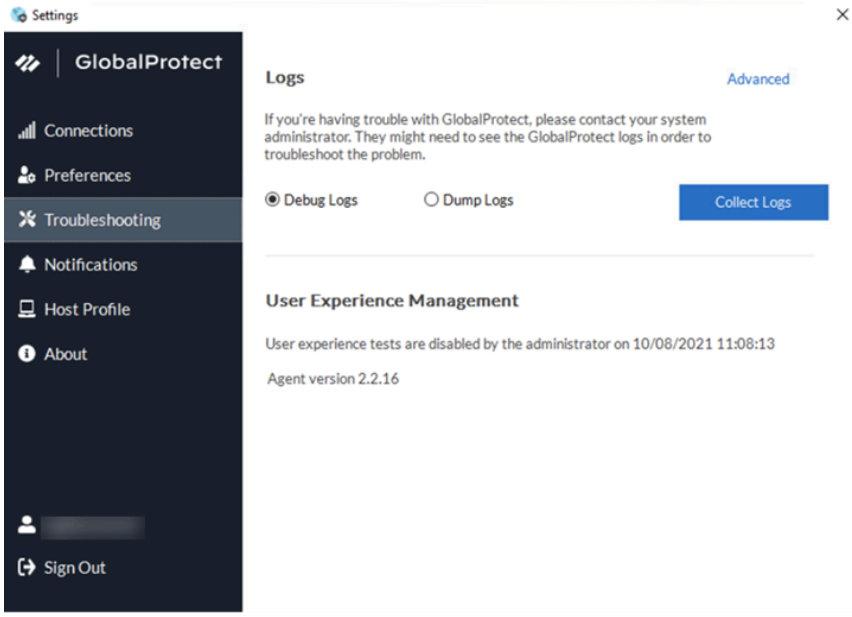


 ©2023 Palo Alto Networks, Inc.

- 문제 해결—문제 해결 탭에서는 로그를 수집하고 로깅 수준을 디버그 로그 또는 덤프 로그로 설정하고 선택적으로 사용자 환경 테스트를 활성화하도록 설정할 수 있습니다.

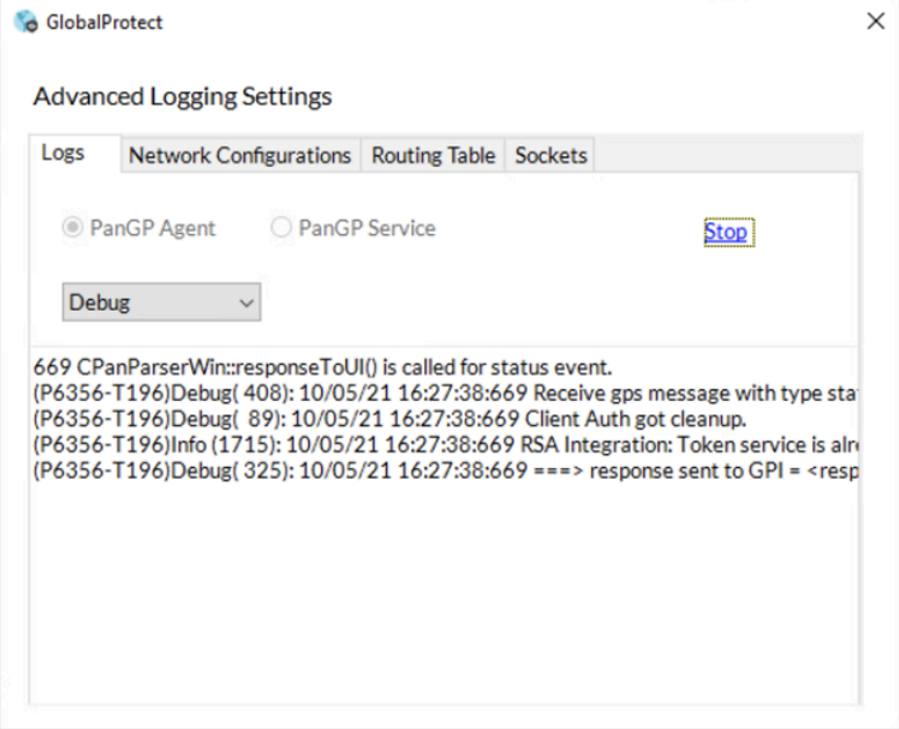
  GlobalProtect 앱이 추가 분석을 위해 문제 해결 로그, 진단 로그 또는 둘 모두를 Cortex Data Lake로 보내려면 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화하도록 *GlobalProtect* 포털을 구성해야 합니다. 또한 프로브하려는 웹 서버/리소스의 *IP* 주소 또는 정규화된 도메인 이름을 포함할 수 있는 HTTPS 기반 대상 URL을 구성하고 최종 사용자 엔드포인트에서 대기 시간 또는 네트워크 성능과 같은 문제를 확인할 수 있습니다.

  고급을 클릭하여 엔드포인트에 대한 자세한 정보를 볼 수 있습니다.



  고급 로깅 설정 창에는 네트워크 구성, 경로 설정 활성 연결 및 로그에 대한 정보가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



GlobalProtect가 연결되면 사용자 경험 테스트 활성화 확인란이 GlobalProtect 앱에 표시될 경우 자율 DEM(ADEM) 엔드포인트 에이전트가 사용자 경험 테스트를 수행할 수 있는지 확인하십시오. 또는 관리자가 GlobalProtect 앱 설치 중에 ADEM 엔드포인트 에이전트를 설치했지만 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화하도록 허용하지 않은 경우 메시지가 표시되는지 확인할 수 있습니다. 기본적으로 하트비트 알림은 GlobalProtect가 비활성화되거나 연결이 끊어진 경우에도 여전히 ADEM으로 전달됩니다.

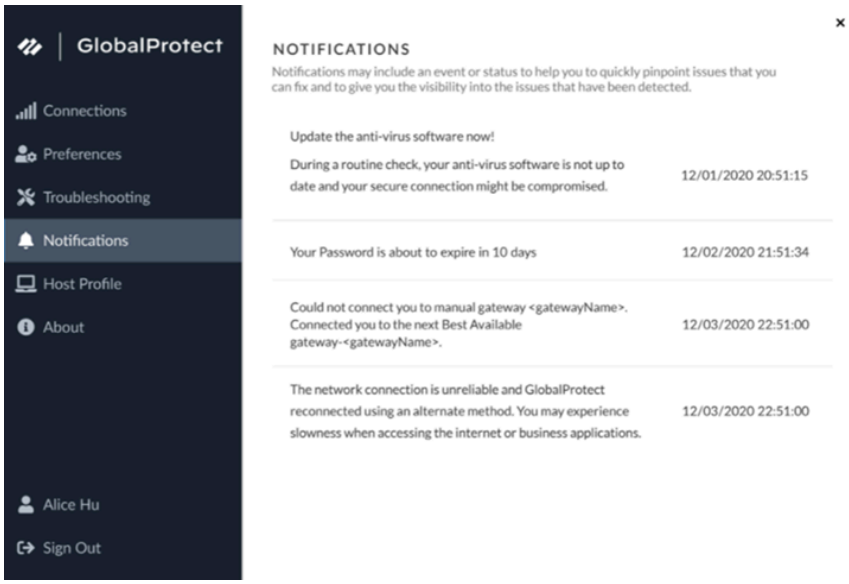
관리자가 GlobalProtect 앱 설치 중에 자율 DEM 엔드포인트 에이전트를 설치하도록 포털을 구성하고 테스트를 활성화하도록 허용한 경우 GlobalProtect 앱에서 사용자 경험 테스트 활성화 확인란을 선택합니다. 관리자가 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화하도록

 ©2023 Palo Alto Networks, Inc.

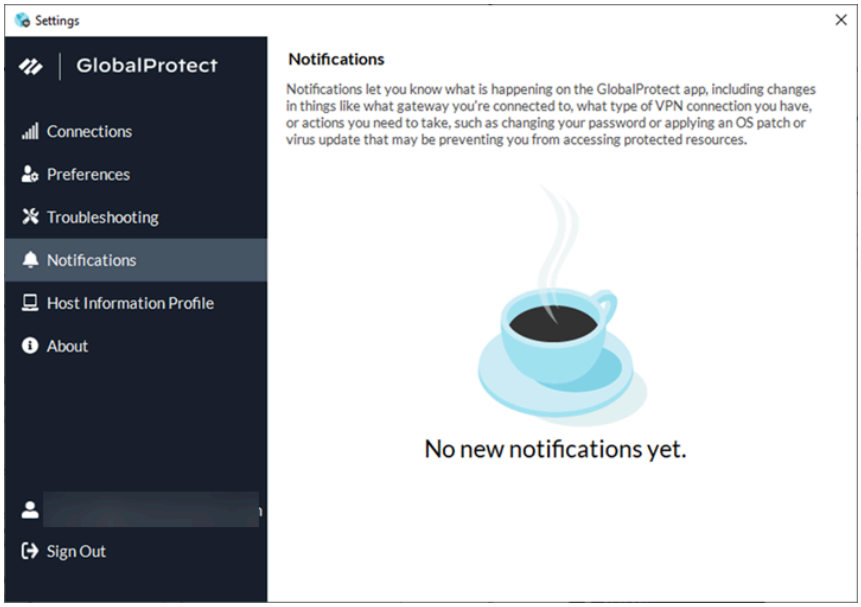
허용하지 않는 경우 이 확인란은 나타나지 않습니다. 대신 앱이 사용자 경험 테스트를 실행할 수 있음을 확인하는 메시지가 표시됩니다.

사용자 경험 테스트 활성화 확인란을 선택하지 않으면 하트비트 알림이 여전히 ADEM으로 전달됩니다.

- 알림—알림 탭에는 GlobalProtect 앱에서 트리거된 특정 알림에 대한 자세한 정보가 표시됩니다.

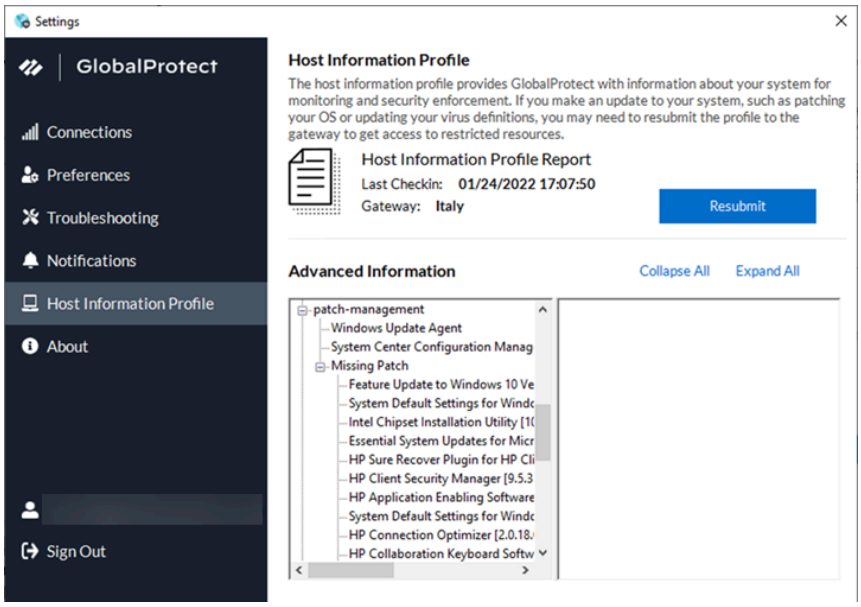


GlobalProtect 앱에서 트리거된 새 알림이 없는 경우에도 알림을 받습니다.

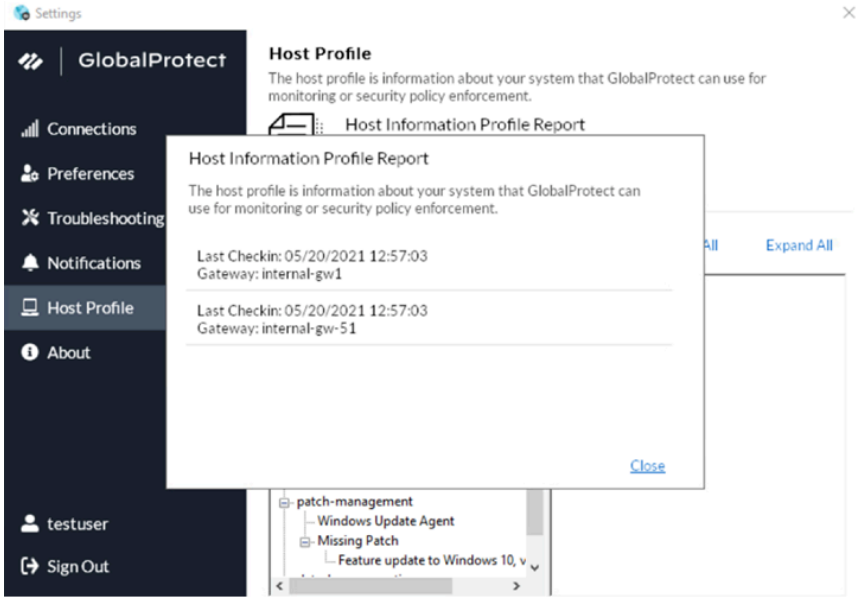


- 호스트 정보 프로파일—호스트 정보 프로파일 탭에는 GlobalProtect가 호스트 정보 프로파일을 사용하여 보안 정책을 모니터링하고 적용하는 데 사용하는 엔드포인트 데이터가 표시됩니다. 다시 제출하여 HIP 데이터를 게이트웨이에 수동으로 다시 제출할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

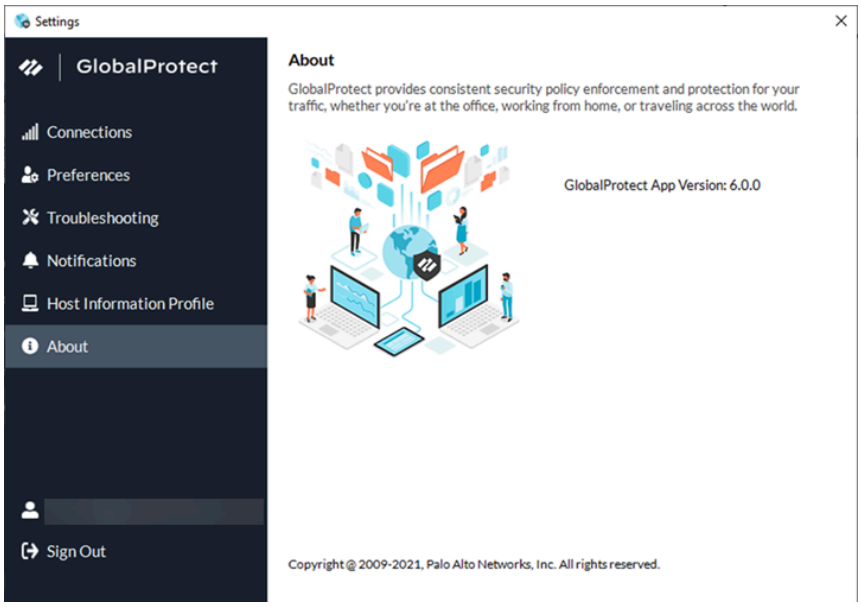


관리자가 비터널 모드 및 내부 호스트 감지에서 여러 내부 게이트웨이를 구성한 경우 추가 세부 정보를 클릭하여 호스트 정보 프로필(HIP) 관련 문제를 신속하게 해결하는 데 도움이 되도록 중앙 위치에서 각 게이트웨이에 대한 HIP 보고서 제출을 모니터링할 수 있습니다.



- 정보—정보 탭에는 엔드포인트에 현재 설치된 GlobalProtect 버전이 표시되며 업데이트를 확인할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



STEP 5 | (선택 사항) 새 암호를 사용하여 로그인합니다.

> ***GlobalProtect*** 관리자가 ***GlobalProtect*** 포털 에이전트가 사용자 자격 증명을 저장하도록 구성하면 자격 증명이 ***GlobalProtect*** 앱에 자동으로 저장됩니다. 회사 네트워크에 액세스하기 위한 암호가 변경되면 새 암호를 사용하여 ***GlobalProtect***에 로그인해야 합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다.
3. 설정을 선택하여 **GlobalProtect** 설정 패널을 엽니다.
4. **GlobalProtect** 설정 패널에서 로그아웃하여 GlobalProtect 앱에서 저장된 사용자 자격 증명을 지웁니다.
5. 사용자 자격 증명을 지운 후 새 사용자 이름과 암호를 사용하여 GlobalProtect에 다시 연결할 수 있습니다.

STEP 6 | (선택 사항) GlobalProtect와의 연결을 끊습니다.

관리자가 주문형 연결 방법으로 GlobalProtect를 구성한 경우 상태 패널에서 연결 해제를 클릭하여 GlobalProtect에서 연결을 끊을 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

Windows용 GlobalProtect 앱에서 문제 보고하기

네트워크 성능이 저하되거나 포털 및 게이트웨이와의 연결이 설정되지 않는 등의 비정상적인 동작이 발생하는 경우 관리자가 액세스할 수 있는 Cortex Data Lake에 직접 문제를 보고할 수 있습니다. 더 이상 이메일을 통해 GlobalProtect 앱 로그를 수동으로 수집 및 전송하거나 클라우드 드라이브에 저장할 필요가 없습니다.

GlobalProtect 앱에 문제 보고 옵션을 표시하려면 관리자가 ***GlobalProtect*** 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화해야 합니다.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. (선택 사항) GlobalProtect 앱에 처음 로그인하는 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력한 다음 연결을 클릭합니다.
3. (선택 사항) 앱에 여러 포털이 저장되어 있는 경우 포털 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 드롭다운에서 미리 선택됩니다.
4. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 드롭다운을 클릭합니다.

STEP 2 | GlobalProtect 앱을 엽니다.

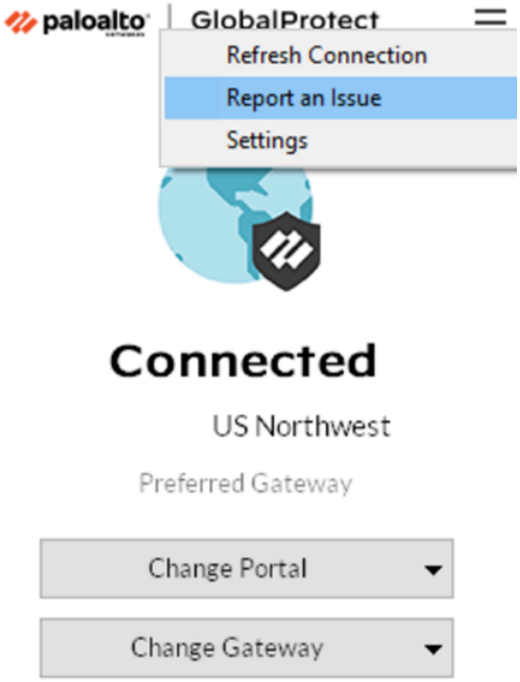
GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 엔드포인트에서 GlobalProtect 앱의 문제를 보고합니다.

앱을 실행한 후 상태 패널에서 햄버거 메뉴를 클릭하여 관리자에게 문제를 보고합니다.

1. 문제 신고를 선택합니다.



2. 진단 테스트를 실행하고 진단 로그를 포함하도록 GlobalProtect 앱을 활성화합니다. 진단 및 문제 해결 로그가 모두 수집되어 간결한 문제 해결 보고서로 Cortex Data Lake에 전송됩니다.

   진단 테스트가 완료되면 GlobalProtect 디버그 로그 파일이 엔드포인트에서 Cortex Data Lake로 업로드됩니다.

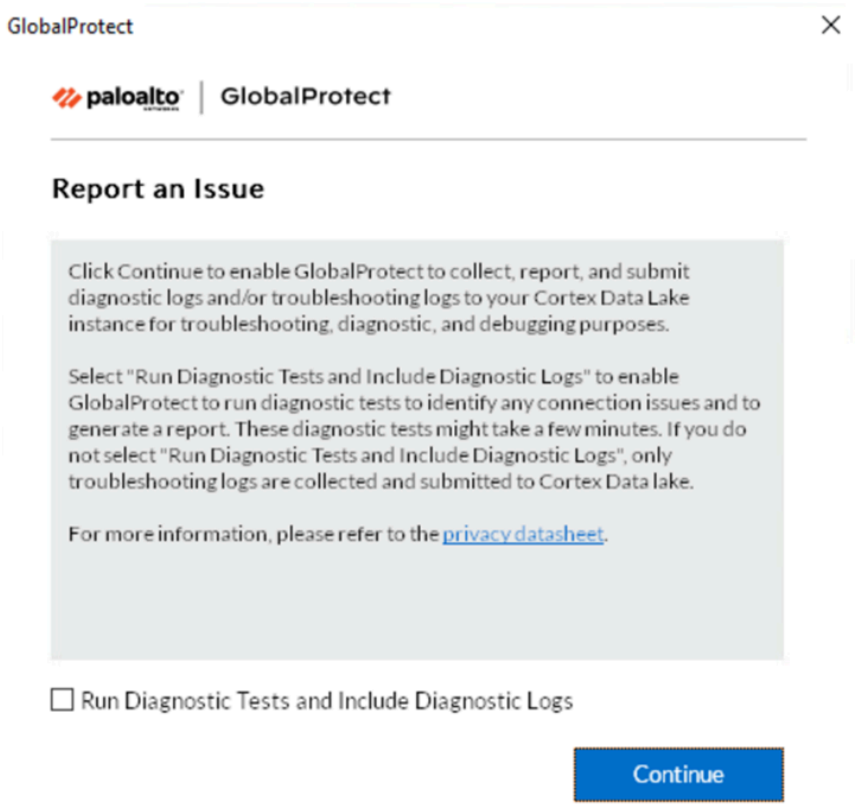
   앱에서 진단 테스트를 실행하고 진단 로그를 포함하도록 설정하지 않으면 문제 해결 로그만 수집되어 압축 문제 해결 보고서로 ***Cortex Data Lake***에 전송됩니다. ***GlobalProtect*** 앱은 `.json` 형식으로 자동 생성되는 보고서 파일(***pan_gp.trb.log*** 또는 ***pan_gp_trbl.log***)을 확인합니다. 문제 해결 로그에서 문제가 발견되지 않은 경우 알림 메시지가 표시됩니다. 다시 시도를 클릭하여 ***pan_gp.trb*.log*** 파일이 있는지 확인합니다.

3. 진단 테스트 실행 및 진단 로그 포함 확인란을 선택합니다.
4. 계속을 클릭하면 앱이 문제 해결 로그를 생성하고 관리자의 Cortex Data Lake 인스턴스로 보고서를 전송할 수 있습니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다. GlobalProtect 앱은 터널을 사용하거나 터널 없이 진단 테스트를 실행할 수 있습니다. 예를 들어

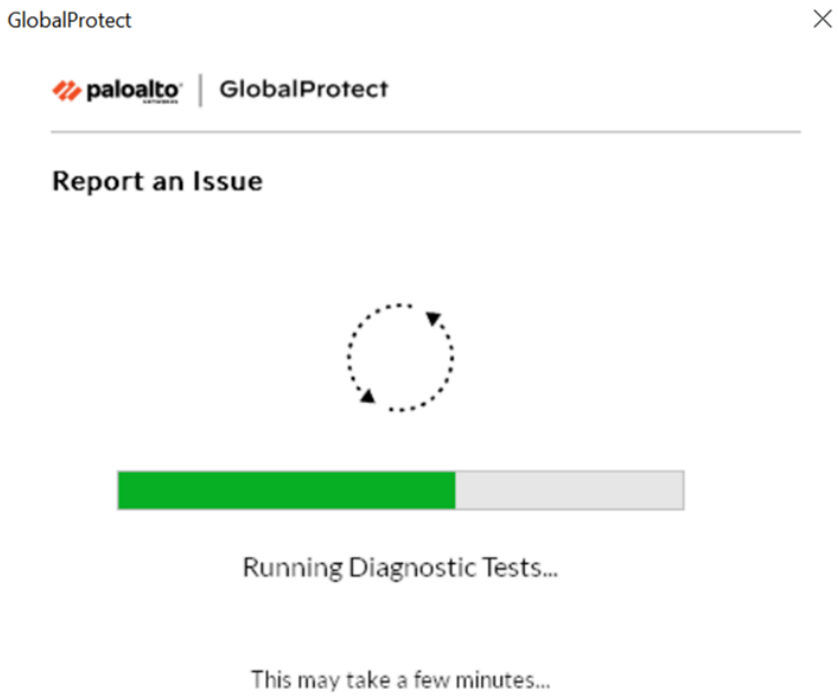
 ©2023 Palo Alto Networks, Inc.

앱이 터널을 통해 진단 테스트를 연결하고 실행하기 전에 GlobalProtect 로그인 자격 증명을 입력할 수 있습니다.

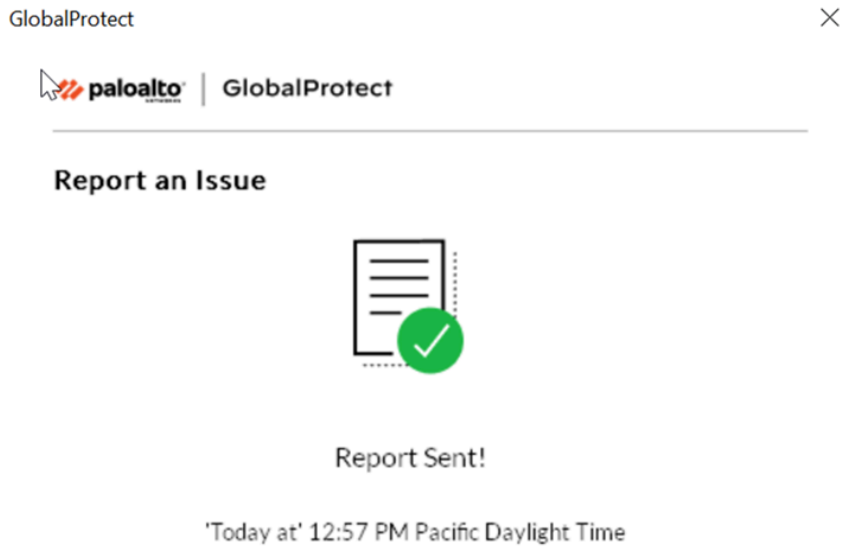


진단 테스트 실행 및 진단 로그 포함 확인란을 선택한 경우에만 앱이 진단 테스트를 실행하고 있음을 확인하는 메시지가 팝업됩니다.

 ©2023 Palo Alto Networks, Inc.



5. 닫기를 클릭하여 앱이 Cortex Data Lake로 보고서를 전송했는지 확인합니다. 이 확인 메시지에는 보고서가 처리되고 전송된 날짜 및 시간이 표시됩니다.



 ©2023 Palo Alto Networks, Inc.

Windows용 GlobalProtect 앱 연결 해제

관리자가 GlobalProtect 연결 방법을 항상 켬으로 구성한 경우 적절한 이유가 있다면 GlobalProtect 앱의 연결을 끊을 수 있습니다. 예를 들어 호텔에서 GlobalProtect 가상 사설망(VPN)이 작동하지 않고 VPN 오류로 인해 인터넷에 연결할 수 없는 경우 앱 연결을 끊을 수 있습니다. GlobalProtect 앱의 연결을 끊은 후 보안되지 않은 통신(VPN 없이)을 사용하여 인터넷에 연결할 수 있습니다.

GlobalProtect 앱의 연결을 끊을 수 있는 방법, 시간 및 횟수는 관리자가 GlobalProtect 서비스(PanGPS)를 구성하는 방법에 따라 다릅니다. 이 구성을 사용하면 앱 연결을 완전히 끊지 못하거나 챌린지에 올바르게 응답한 후에만 앱 연결을 끊을 수 있습니다.

구성에 챌린지가 포함된 경우 GlobalProtect 앱은 다음 중 하나를 묻는 메시지를 표시합니다.

- 앱 연결을 해제하려는 이유
- 인터넷 속도가 느리거나 앱이 작동하지 않는 것과 같은 하나 이상의 이유에 응답(필요한 경우)
- 암호
- 티켓 번호

챌린지에 암호 또는 티켓 번호가 필요한 경우 전화로 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 문의하는 것이 좋습니다.

관리자는 일반적으로 이메일(신규 GlobalProtect 사용자의 경우)을 통하거나 조직의 웹 사이트에 게시하여 암호를 미리 제공합니다. 중단 또는 시스템 문제에 대한 응답으로 관리자는 전화로 암호를 제공할 수도 있습니다.

유효한 티켓 번호를 받기 전에 엔드포인트에 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 전달해야 하는 티켓 요청 번호가 표시됩니다. 연결 해제 요청이 승인되면 GlobalProtect를 연결 해제하는 데 사용할 수 있는 유효한 티켓 번호를 받게 됩니다.

다음 단계에서는 앱 연결을 끊고 챌린지를 통과하는 방법을 설명합니다.

STEP 1 | GlobalProtect 앱의 연결을 끊습니다.

1. GlobalProtect 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다.
3. 연결 해제를 선택합니다.

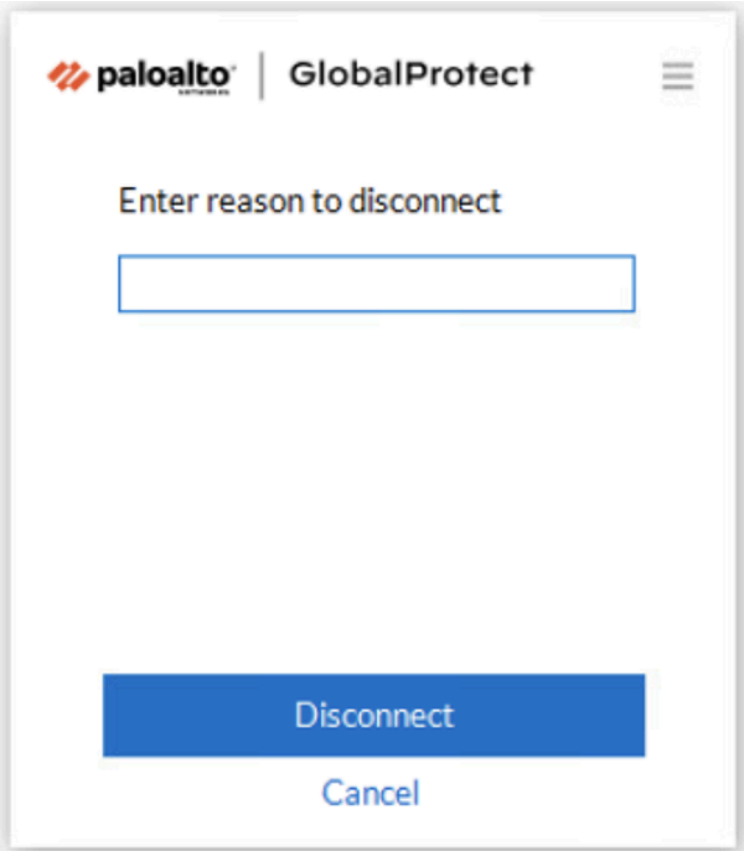
연결 해제 옵션은 ***GlobalProtect*** 에이전트 구성에서 앱 연결을 끊을 수 있는 경우에만 표시됩니다. 구성을 통해 챌린지에 응답할 필요 없이 ***GlobalProtect*** 앱의 연결을 끊을 수 있는 경우 추가 조치 없이 ***GlobalProtect*** 앱이 닫힙니다.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | 필요한 경우 하나 이상의 챌린지에 대응합니다.

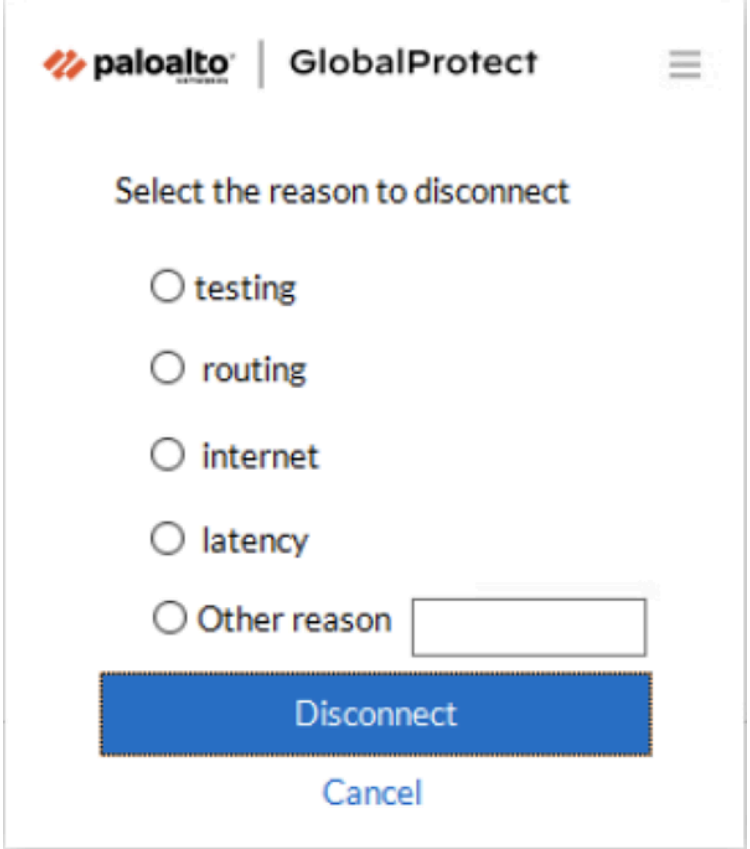
메시지가 표시되면 다음 정보를 제공합니다.

- 연결 해제 원인—GlobalProtect 앱 연결을 해제하는 이유입니다.



- 연결 해제 이유 선택—구성에 하나 이상의 이유로 응답하거나 다른 이유를 입력해야 하는 경우 연결 해제를 선택하는 즉시 GlobalProtect 앱에 이유가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



- 암호—앱을 비활성화해야 하는 알려진 문제 또는 이벤트에 따라 관리자가 일반적으로 미리 제공하는 암호입니다.
- 티켓—구성에 티켓 번호를 제공해야 하는 경우 연결 해제를 선택하는 즉시 GlobalProtect 앱에 8자리 16진수 티켓 요청 번호가 표시됩니다. 티켓 번호로 앱 연결을 해제하려면 관리자 또는 헬프 데스크 담당자(전화)에게 연락하여 티켓 요청 번호를 제공하십시오. 요청을 승인하면 관리자 또는 지원 센터 담당자가 8자리 16진수 티켓 번호를 제공합니다. 티켓 필드에 티켓 번호를 입력하고 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

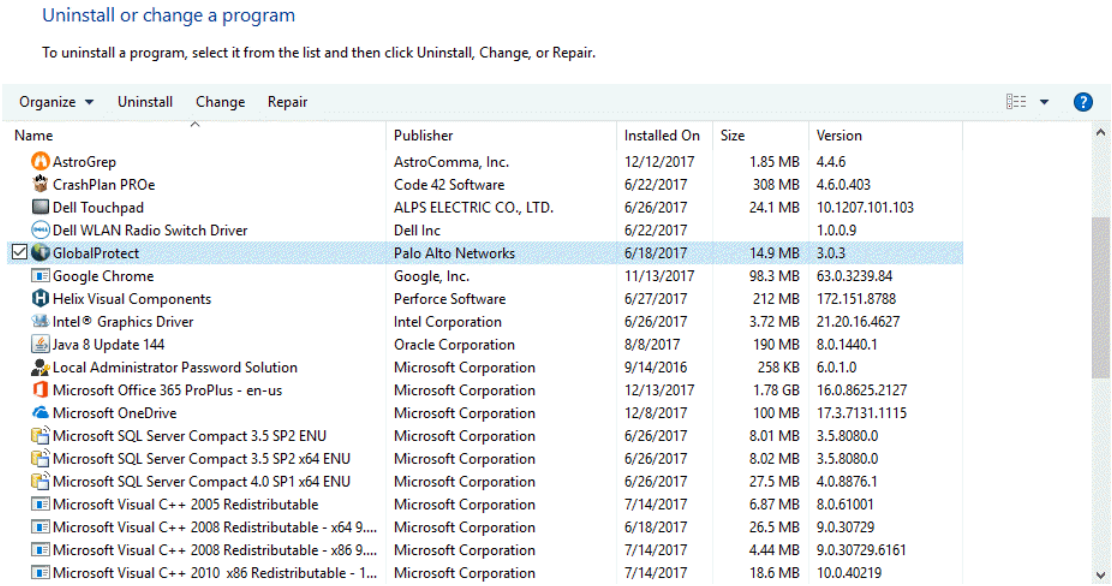
Windows용 GlobalProtect 앱 제거

다음 단계를 사용하여 Windows 엔드포인트에서 GlobalProtect 앱을 제거합니다. 앱을 제거하면 더 이상 기업 네트워크에 VPN으로 액세스할 수 없으며 엔드포인트가 회사의 보안 정책에 의해 보호되지 않는다는 점에 유의하십시오.

관리자 권한이 있는 사용자만 ***Windows*** 엔드포인트에서 ***GlobalProtect*** 앱을 제거할 수 있습니다.

STEP 1 | 시작 > 제어판 > 프로그램 > 프로그램 및 기능을 선택합니다.

STEP 2 | 목록에서**GlobalProtect**를 선택한 다음 제거를 클릭합니다.



Name	Publisher	Installed On	Size	Version
AstroGrep	AstroComma, Inc.	12/12/2017	1.85 MB	4.4.6
CrashPlan PROe	Code 42 Software	6/22/2017	308 MB	4.6.0.403
Dell Touchpad	ALPS ELECTRIC CO., LTD.	6/26/2017	24.1 MB	10.1207.101.103
Dell WLAN Radio Switch Driver	Dell Inc	6/22/2017		1.0.0.9
GlobalProtect	Palo Alto Networks	6/18/2017	14.9 MB	3.0.3
Google Chrome	Google, Inc.	11/13/2017	98.3 MB	63.0.3239.84
Helix Visual Components	Perforce Software	6/27/2017	212 MB	172.151.8788
Intel® Graphics Driver	Intel Corporation	6/26/2017	3.72 MB	21.20.16.4627
Java 8 Update 144	Oracle Corporation	8/8/2017	190 MB	8.0.1440.1
Local Administrator Password Solution	Microsoft Corporation	9/14/2016	258 KB	6.0.1.0
Microsoft Office 365 ProPlus - en-us	Microsoft Corporation	12/13/2017	1.78 GB	16.0.8625.2127
Microsoft OneDrive	Microsoft Corporation	12/8/2017	100 MB	17.3.7131.1115
Microsoft SQL Server Compact 3.5 SP2 ENU	Microsoft Corporation	6/26/2017	8.01 MB	3.5.8080.0
Microsoft SQL Server Compact 3.5 SP2 x64 ENU	Microsoft Corporation	6/26/2017	8.02 MB	3.5.8080.0
Microsoft SQL Server Compact 4.0 SP1 x64 ENU	Microsoft Corporation	6/26/2017	27.5 MB	4.0.8876.1
Microsoft Visual C++ 2005 Redistributable	Microsoft Corporation	7/14/2017	6.87 MB	8.0.61001
Microsoft Visual C++ 2008 Redistributable - x64 9....	Microsoft Corporation	6/18/2017	26.5 MB	9.0.30729
Microsoft Visual C++ 2008 Redistributable - x86 9....	Microsoft Corporation	7/14/2017	4.44 MB	9.0.30729.6161
Microsoft Visual C++ 2010 x86 Redistributable - 1...	Microsoft Corporation	7/14/2017	18.6 MB	10.0.40219

STEP 3 | 제거를 계속할지 묻는 메시지가 표시되면 예를 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

Microsoft 설치 관리자 충돌 해결

GlobalProtect 포털 에이전트 구성에서 네트워크 액세스를 위해 **GlobalProtect**를 적용한 다음 Windows 엔드포인트를 GlobalProtect 앱의 최신 버전으로 업그레이드하면 설치가 실패하고 적용 구성이 모든 트래픽을 차단할 수 있습니다.

이 문제는 Windows 엔드포인트에서 여러 Microsoft 설치 프로그램(`msiexec.exe`) 인스턴스가 동시에 실행될 때 발생하는 OS 제한으로 인해 발생합니다. Microsoft 설치 프로그램 충돌을 해결하려면 다음 절차를 사용해야 합니다.

STEP 1 | 엔드포인트를 다시 시작합니다.

STEP 2 | 백그라운드에서 실행 중인 모든 타사 설치 프로그램을 중지합니다.

1. **Ctrl+Alt+Delete**를 누른 다음 작업 관리자를 클릭합니다.
2. 작업 관리자에서 현재 실행 중인 타사 `msiexec` 프로그램을 모두 찾습니다 (예: **`msiexec` 명령줄 - Google** 검색).
3. 타사 설치 프로그램을 선택한 다음 작업 종료를 클릭하여 설치 프로그램을 중지합니다.

STEP 3 | GlobalProtect의 기존 버전을 복원한 다음 새 버전의 앱으로 업그레이드합니다.

1. (선택 사항) 필요한 경우 GlobalProtect의 기존(이전) 버전을 다시 설치하여 복구합니다. 업그레이드가 계속 실패하는 경우 이 단계가 필요합니다.
2. 업그레이드가 예상대로 진행되도록 합니다.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

맥OS용 GlobalProtect 앱

GlobalProtect™는 엔드포인트(데스크톱 컴퓨터, 노트북, 태블릿 또는 스마트폰)에서 실행되는 애플리케이션으로, 회사 네트워크의 중요한 리소스를 보호하는 것과 동일한 보안 정책을 사용하여 사용자를 보호합니다. GlobalProtect™는 인트라넷, 사설 클라우드, 공용 클라우드 및 인터넷 트래픽을 보호하고 전 세계 어디에서나 회사 리소스에 액세스할 수 있도록 합니다.

다음 주제에서는 macOS용 GlobalProtect 앱을 설치하고 사용하는 방법을 설명합니다.

> macOS용 GlobalProtect 앱 다운로드 및 설치하기
> macOS용 GlobalProtect 앱 사용하기
> macOS용 GlobalProtect 앱에서 문제 보고하기
> macOS용 GlobalProtect 앱 비활성화하기
> macOS용 GlobalProtect 앱 제거
> GlobalProtect 인포서 커널 확장 프로그램 삭제
> 인증을 위해 클라이언트 인증서를 사용하도록 macOS용 GlobalProtect 앱 활성화

macOS용 GlobalProtect 앱 다운로드 및 설치

GlobalProtect 네트워크에 연결하기 전에 macOS 엔드포인트에 GlobalProtect 앱을 다운로드하여 설치해야 합니다. 조직의 GlobalProtect 또는 Prisma Access 배포에 적합한 앱을 구입하려면 조직 내 GlobalProtect 포털에서 직접 앱을 다운로드해야 합니다. 이러한 이유로 Palo Alto Networks 사이트에는 직접 GP 앱을 다운로드할 수 있는 링크가 없습니다.

GlobalProtect 앱을 다운로드하고 설치하려면 먼저 관리자로부터 GlobalProtect 포털의 IP 주소 또는 FQDN을 받아야 합니다. 또한 관리자는 포털 및 게이트웨이에 연결하는 데 사용할 수 있는 사용자 이름과 암호를 확인해야 합니다. 이것은 일반적으로 회사 네트워크에 연결하는 데 사용하는 것과 동일한 사용자 이름 및 암호입니다.

macOS Catalina 10.15.4, macOS Big Sur 11 이상을 실행하는 macOS 디바이스에 GlobalProtect 앱을 처음으로 설치하거나 GlobalProtect 앱 5.1.4로 업그레이드하는 경우 특정 GlobalProtect 기능에 사용되는 시스템 확장 프로그램을 활성화해야 합니다. 관리자가 대상 도메인 이름 및 애플리케이션 프로세스 이름을 기반으로 GlobalProtect 게이트웨이에서 분할 터널을 구성하거나 GlobalProtect 포털에서 네트워크 액세스를 위해 GlobalProtect 연결을 적용한 경우(GlobalProtect 앱 사용자 지정 참조) 설치 중에 GlobalProtect 앱에 시스템 확장 프로그램 차단됨 알림 메시지가 표시됩니다. 이 메시지는 사용자에게 로딩이 차단된 macOS의 시스템 확장 프로그램을 활성화하고 허용하여 분할 터널과 네트워크 액세스용 GlobalProtect 적용 기능을 사용하도록 설정하라는 메시지를 표시합니다.

 ©2023 Palo Alto Networks, Inc.

시스템 확장 프로그램을 사용할 때는 다음 지침을 따르십시오.

- 관리자 권한이 있는 사용자만 *macOS* 엔드포인트용 *GlobalProtect* 앱에서 시스템 확장 프로그램을 활성화할 수 있습니다.
- 타사 애플리케이션을 사용하는 동안 데이터를 보호할 수 있도록 *macOS Catalina 10.15* 및 *macOS Big Sur 11*의 보안이 강화되었으므로 *GlobalProtect*는 문서, 데스크탑 및 다운로드 폴더와 네트워크 드라이브에 저장된 파일 및 폴더에 접근하기 전에 사용자의 권한을 요청해야 합니다. 관리자가 *HIP* 검사를 활성화한 경우 *GlobalProtect*가 파일 시스템에 저장된 특정 파일 및 폴더에 대한 액세스를 요청할 때 *macOS* 엔드포인트에 새 권한 팝업이 표시됩니다.
- *macOS* 카탈리나 *10.15.4*, *macOS Big Sur 11* 이상에서 실행되는 *GlobalProtect* 앱 *5.1.4*는 커널 확장 프로그램을 사용하지 않으며 시스템 확장 프로그램을 사용합니다.
- *macOS* 카탈리나 *10.15.4*, *macOS Big Sur 11* 이상에서 실행되는 *GlobalProtect* 앱 *5.1.4*는 커널 확장 프로그램(***com.paloaltonetworks.kext.pangpd***)을 사용하지 않으며 대신 *macOS*에서 제공하는 사용 가능한 utun 인터페이스를 가상 어댑터로 사용합니다.
- 이전 릴리스에서 *macOS* 카탈리나 *10.15.4*, *macOS Big Sur 11* 이상에서 실행되는 *GlobalProtect* 앱 *5.1.4*로 업그레이드하는 경우 커널 확장 프로그램이 더 이상 필요하지 않습니다. 업그레이드 후에는 *GlobalProtect* 앱에 시스템 확장 프로그램이 차단됨 알림 메시지가 표시되어 로드가 차단된 *macOS*의 시스템 확장 프로그램을 활성화하고 허용할지 묻는 메시지가 사용자에게 표시됩니다. 기본적으로 앱은 시스템 확장 프로그램을 설치하지 않으며 동일한 기본 설정이 적용됩니다.

필요한 정보를 수집한 후 다음 단계에 따라 앱을 다운로드하고 설치합니다.

 ©2023 Palo Alto Networks, Inc.

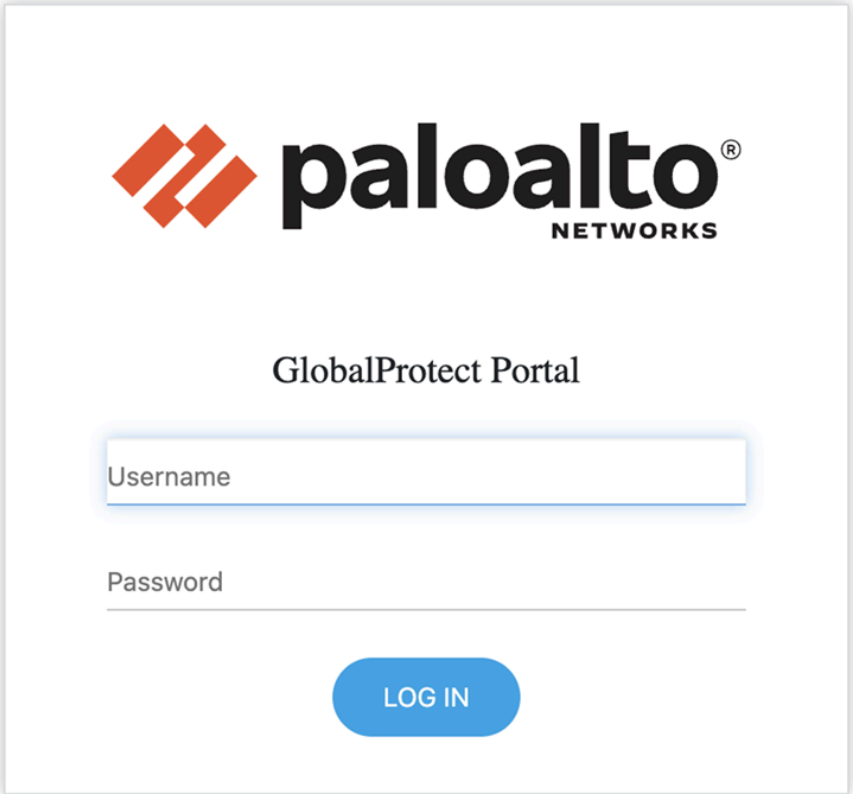
STEP 1 | GlobalProtect 포털에 로그인합니다.

1. 웹 브라우저를 시작하고 다음 URL로 이동합니다.

   `https://<portal IP address or FQDN>`

   예: **`http://gp.acme.com`**

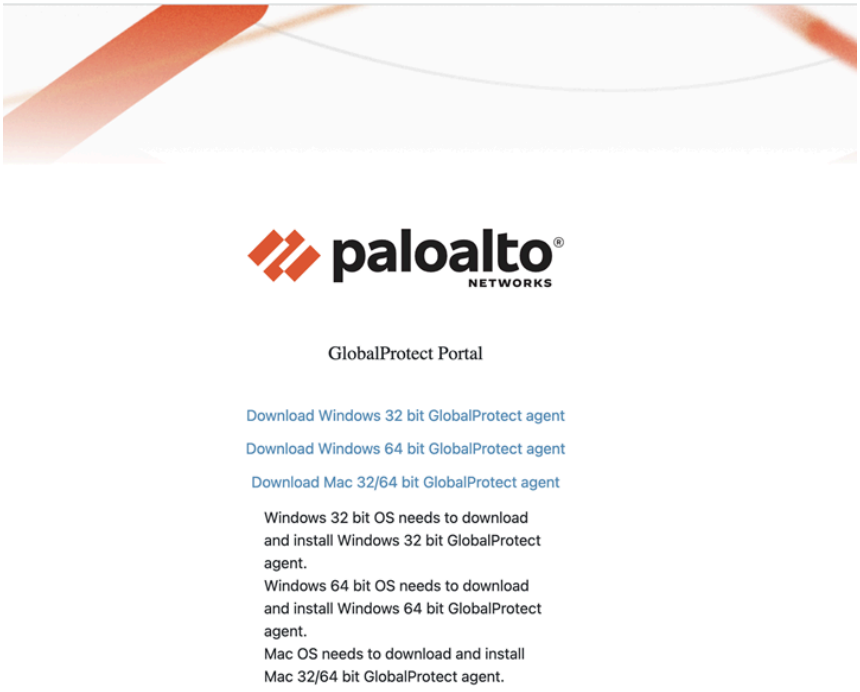
2. 포털 로그인 페이지에서 이름(사용자 이름)과 암호를 입력한 다음 로그인을 클릭합니다. 대부분의 경우 회사 네트워크에 연결할 때 사용하는 것과 동일한 사용자 이름과 암호를 사용할 수 있습니다.



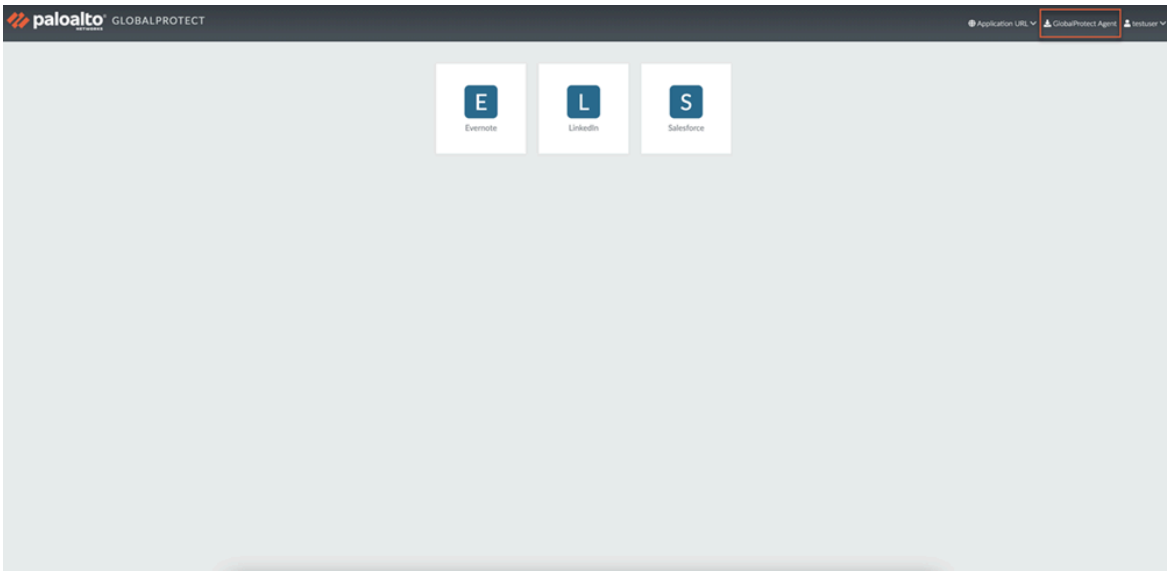
 ©2023 Palo Alto Networks, Inc.

STEP 2 | 앱 다운로드 페이지로 이동합니다.

대부분의 경우 앱 다운로드 페이지는 포털에 로그인한 직후에 표시됩니다. 이 페이지에서 최신 앱 소프트웨어 패키지를 다운로드할 수 있습니다.



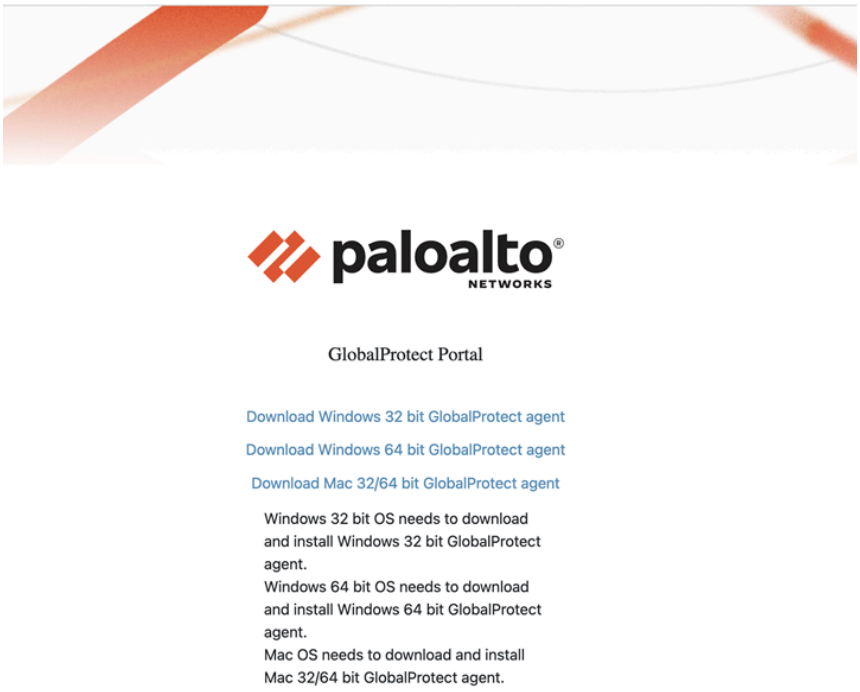
시스템 관리자가 GlobalProtect Clientless VPN 액세스를 활성화한 경우 포털에 로그인하면 앱 다운로드 페이지 대신 애플리케이션 페이지가 열립니다. **GlobalProtect** 에이전트를 선택하여 다운로드 페이지를 엽니다.



 ©2023 Palo Alto Networks, Inc.

STEP 3 | 앱을 다운로드합니다.

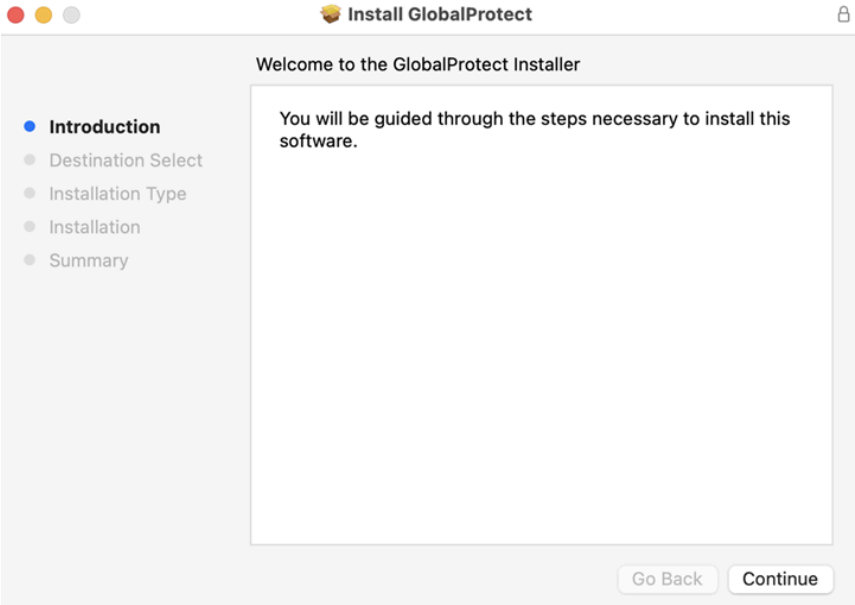
1. **Mac 32/64**비트 **GlobalProtect** 에이전트 다운로드를 클릭합니다.



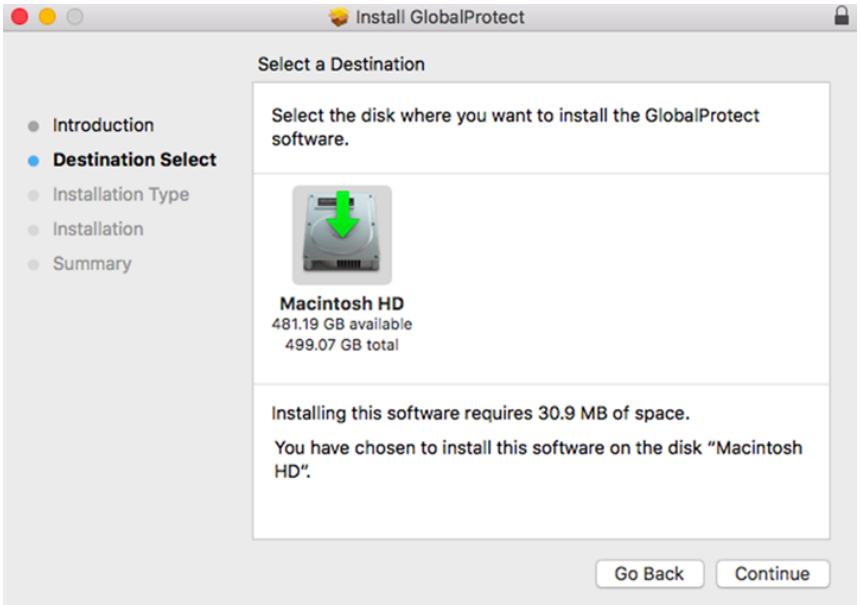
2. 메시지가 표시되면 소프트웨어를 실행합니다.
3. 메시지가 다시 표시되면 GlobalProtect 설치 프로그램을 실행합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | GlobalProtect 설치 프로그램을 사용하여 GlobalProtect 앱 설정을 완료합니다.



1. GlobalProtect 설치 프로그램에서 계속을 클릭합니다.
2. 대상 선택 화면에서 GlobalProtect 앱의 설치 폴더를 선택한 다음 계속을 클릭합니다.

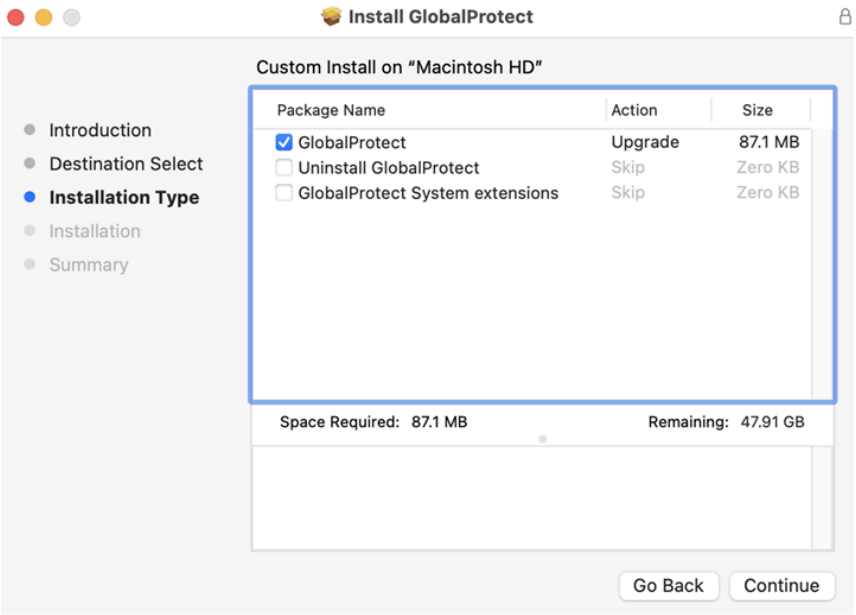


3. 설치 유형 화면에서 **GlobalProtect** 설치 패키지 확인란을 선택합니다.

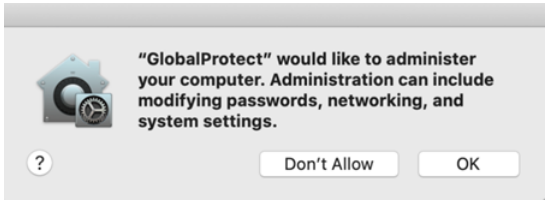
   시스템 관리자가 게이트웨이에서 분할 터널을 구성했거나 포털의 네트워크 접근을 위해 GlobalProtect 연결을 적용한 경우 **GlobalProtect** 시스템 확장 프로그램 확인란을 선택합니다(기본적으로 비활성화됨).

   계속을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

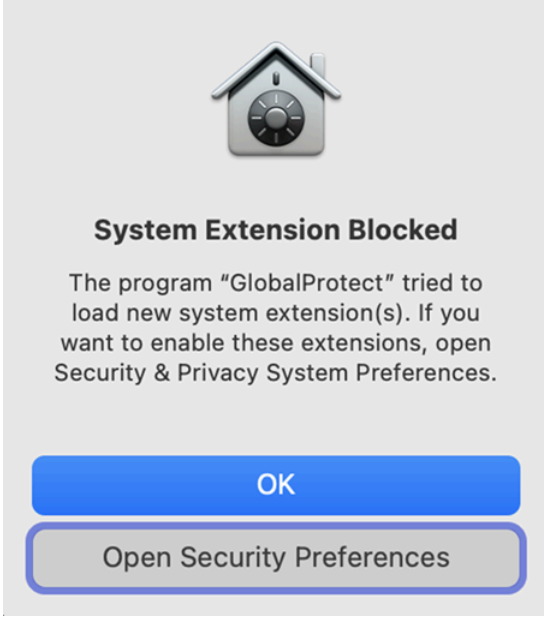


4. 설치를 클릭하여 GlobalProtect를 설치할 것인지 확인합니다.
5. 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 소프트웨어 설치를 클릭하여 설치를 시작합니다.
6. 설치가 완료되면 설치 프로그램을 닫습니다.
7. 관리자가 GlobalProtect 앱을 처음 설치하는 동안 Autonomous DEM (ADEM) 엔드포인트 에이전트를 설치하도록 포털을 구성한 경우, 다음 팝업 메시지에서 확인을 선택하여 해당 에이전트가 다시 나타나지 않도록 합니다.



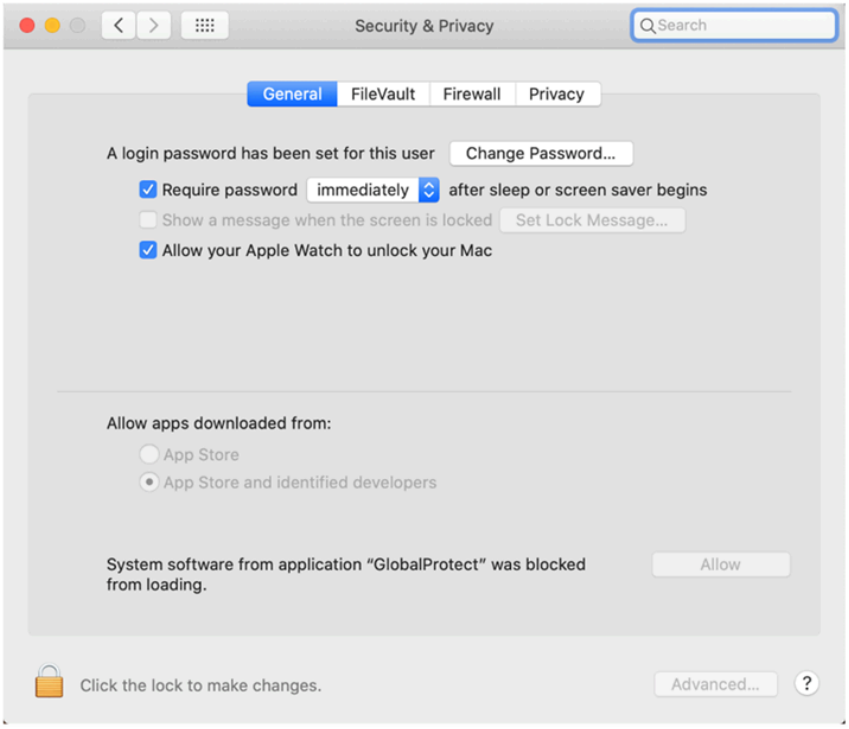
8. **GlobalProtect** 시스템 확장 프로그램을 활성화한 경우 보안 환경설정 열기를 선택하여 다음 시스템 확장 프로그램 차단됨 알림에서 로드되지 않도록 차단된 macOS의 시스템 확장 프로그램을 활성화합니다.

 ©2023 Palo Alto Networks, Inc.



관리자가 Workspace ONE과 같은 지원되는 모바일 디바이스 관리(MDM) 시스템을 사용하여 이 알림을 표시하지 않은 경우 이 알림을 받지 않고도 시스템 확장 프로그램을 자동으로 로드할 수 있습니다.

9. 보안 및 개인정보 보호 대화 상자에서 자물쇠 아이콘을 클릭하여 변경한 다음 앱 다운로드 허용 영역에서 **App Store** 및 식별된 개발자를 선택합니다. 허용을 클릭합니다.



 ©2023 Palo Alto Networks, Inc.

macOS용 GlobalProtect 앱 사용하기

이 항목은 설정에서 엔드포인트에 로그인한 후 GlobalProtect 로그인 자격 증명을 입력해야 하는 경우에만 적용됩니다(Single Sign-On은 비활성화됨).

일반적으로 조직에서는 GlobalProtect 사용자가 앱 설치 후 투명하게 로그인할 수 있도록 허용하는 것이 좋습니다. 투명한 GlobalProtect 로그인으로 엔드포인트에 로그인하면 GlobalProtect 앱이 자동으로 시작되어 추가 사용자 개입 없이 기업 네트워크에 연결됩니다.

설치가 완료되면 로드가 차단된 시스템 확장 프로그램을 macOS에서 활성화하라는시스템 확장 프로그램 차단됨 알림 메시지가 표시됩니다. 설치 중에 **GlobalProtect** 시스템 확장 프로그램 옵션을 선택하지 않은 경우 사용자가 게이트웨이에 연결하면 이 알림 메시지가 표시됩니다. 이 알림은 관리자가 GlobalProtect 게이트웨이에서 분할 터널, GlobalProtect 포털에서 네트워크 액세스를 위한 강제 GlobalProtect 연결(GlobalProtect 앱 사용자 지정 참조) 또는 둘 모두를 구성한 경우 표시됩니다. 두 기능 모두 사용자가 시스템 확장 프로그램을 활성화해야 합니다.

설정에 GlobalProtect 자격 증명을 입력해야 하는 경우 아래에서 해당 단계를 따르십시오.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | GlobalProtect에 로그인합니다.

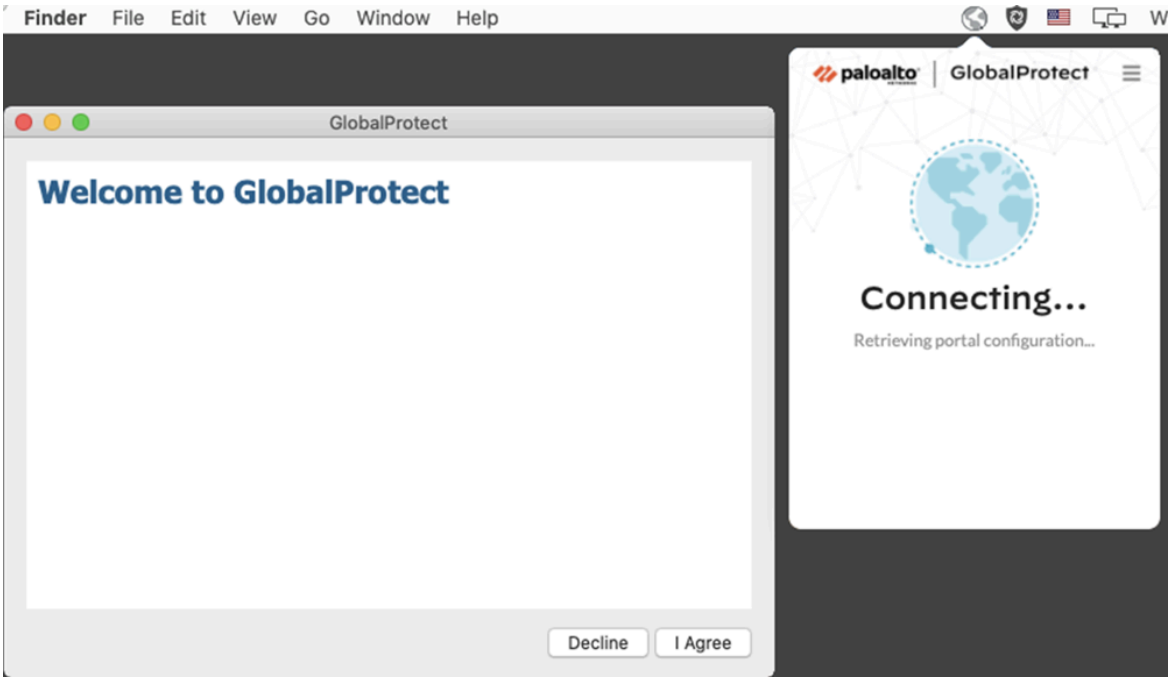
엔드포인트에 처음 로그인하는 경우 GlobalProtect 앱은 로그인 시 친절한 환영 페이지를 표시합니다. 시작하기를 클릭합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. (선택 사항) 관리자가 내부 리소스에 액세스하기 위해 페이지를 보도록 요구하는 경우 GlobalProtect에 연결하기 전에 회사의 서비스 약관을 검토하십시오.

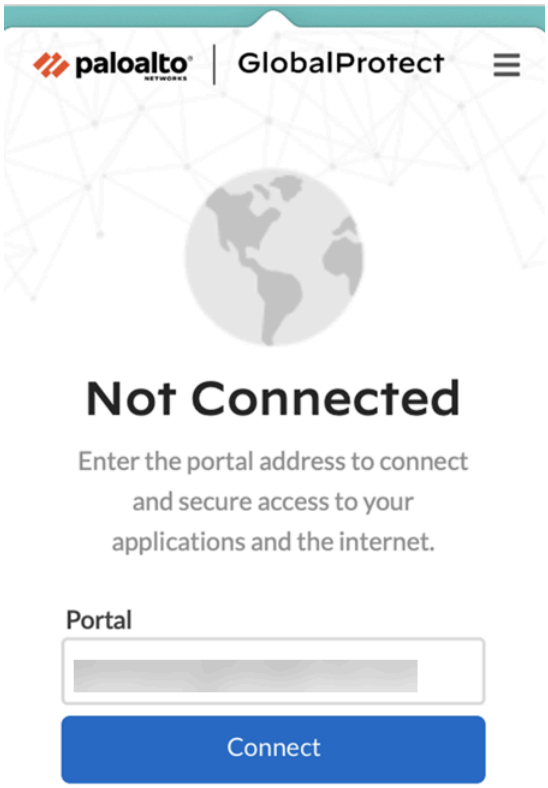
   이용 약관에 동의하지 않으면 GlobalProtect에 연결할 수 없습니다.

   선택적으로 취소를 클릭하면 GlobalProtect 포털의 IP 주소(또는 도메인)를 입력한 다음 연결을 클릭하여 연결을 시작해야 합니다.

 ©2023 Palo Alto Networks, Inc.



3. GlobalProtect 관리자가 제공한 포털의 IP 주소 또는 도메인을 입력한 다음 연결을 클릭합니다.



 ©2023 Palo Alto Networks, Inc.

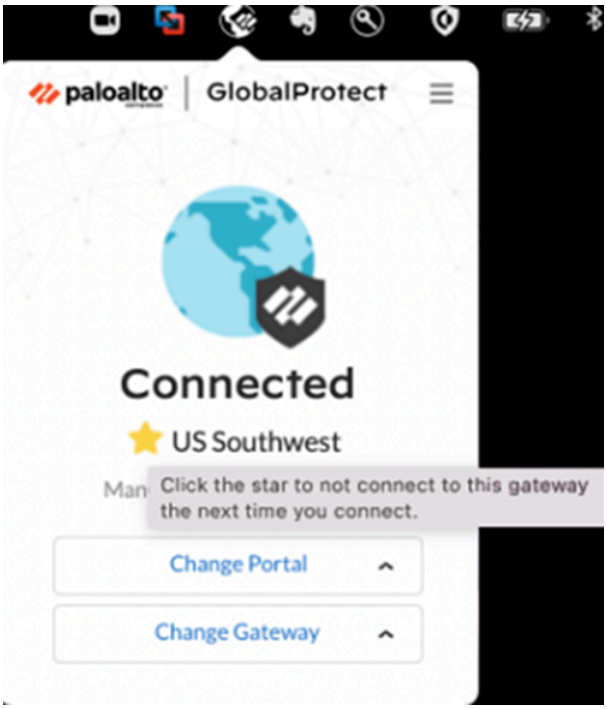
STEP 2 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

GlobalProtect 시스템 트레이 아이콘을 확인하여 연결 여부를 확인할 수 있습니다. 연결되어 있지 않으면 아이콘이 회색( ) 아이콘 위로 마우스를 가져가면 연결되지 않음이 표시됩니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. (선택 사항) GlobalProtect 앱에 처음 로그인하는 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력한 다음 연결을 클릭합니다.
3. (선택 사항) 앱에 여러 포털이 저장된 경우 포털 변경 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 변경 드롭다운에서 미리 선택됩니다.
4. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 변경 드롭다운을 클릭하고 다음 옵션 중 하나를 사용합니다.
   - 게이트웨이를 수동으로 선택합니다(외부 게이트웨이만 해당). 이 옵션은 관리자가 수동 게이트웨이 선택을 활성화한 경우에만 사용할 수 있습니다.
   - 기본 게이트웨이 할당 및 자동 연결:
     1. 게이트웨이를 기본 설정으로 지정하려면 별표 아이콘( )을 클릭합니다. 다음에 연결할 때 이 기본 게이트웨이에 자동으로 연결됩니다.

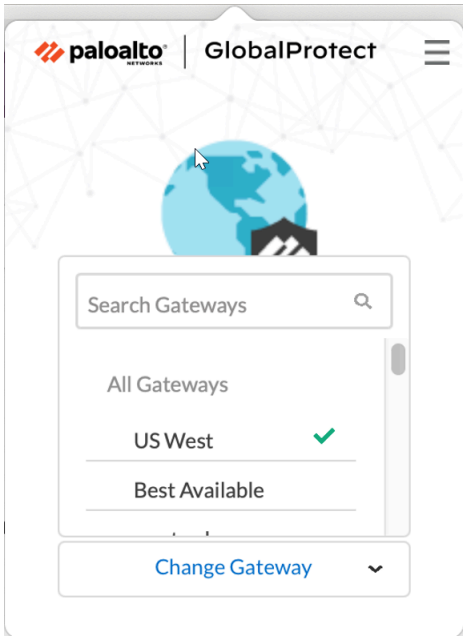
나중에 게이트웨이를 더 이상 기본 게이트웨이로 사용하지 않으려면 별표 아이콘을 지우면 기본 연결에서 이 게이트웨이를 삭제할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



2. 기본적으로 게이트웨이 변경 드롭다운에서 확인 표시로 식별되는 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 기본 게이트웨이를 설정하면 게이트웨이 변경 드롭다운에서 별표 표시된 게이트웨이 옆에 별표가 표시됩니다.

   관리자가 포털 에이전트 구성에서 수동 외부 게이트웨이를 구성한 경우 게이트웨이 검색 필드를 사용하여 특정 게이트웨이를 선택할 수 있습니다.



5. (선택 사항) 연결 모드에 따라 연결을 클릭하여 연결을 시작합니다.
6. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 로그인합니다.

 ©2023 Palo Alto Networks, Inc.

관리자가 생체 인식(지문) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호를 사용하여 두 번 로그인해야 합니다(저장하기 위해 한 번, 인증하기 위해 한 번 더). 그 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

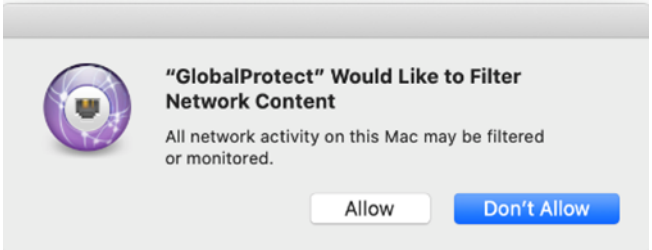
시스템 관리자가 **GlobalProtect** 시스템 확장 프로그램을 활성화한 경우 분할 터널 및 네트워크 액세스를 위해 GlobalProtect 적용 기능을 사용하려면 로드가 차단된 macOS에서 시스템 확장 프로그램을 활성화해야 합니다.

사용자는 네트워크 확장 프로그램 구성 팝업 메시지를 모두 허용하기 위해 관리자 권한이 필요하지 않습니다. 관리자는 *Jamf Pro*와 같은 모바일 디바이스 관리*(MDM)* 시스템을 사용하여 이러한 메시지를 받지 않고 네트워크 확장 프로그램을 자동으로 로드함으로써 이러한 메시지가 표시되는 것을 억제할 수 있습니다. Jamf Pro를 사용하여 시스템 및 네트워크 확장 프로그램을 활성화하는 방법에 대한 정보는https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8의 기술 자료 문서를 참조하십시오.

1. (macOS Catalina 10.15.4 이상에만 해당) 시스템 관리자가 GlobalProtect 게이트웨이의 도메인 및 애플리케이션을 기반으로 분할 터널을 구성한 경우 다음 팝업 메시지에서 허용을 선택합니다.

허용하지 않음을 선택하면 GlobalProtect 앱에서 분할 터널 기능을 사용할 수 없습니다. 이 팝업 메시지는 다음에 포털이나 게이트웨이에 연결할 때 표시됩니다.

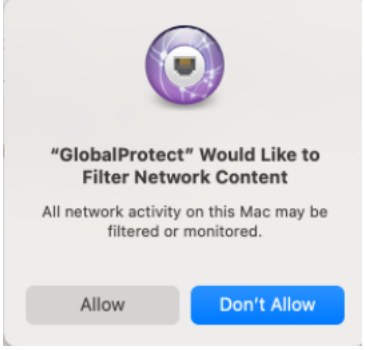
2. (macOS Catalina 10.15.4 이상에만 해당) 시스템 관리자가 네트워크 액세스를 위해 GlobalProtect 연결 적용 기능을 활성화한 경우 다음 팝업 메시지에서 허용을 선택합니다.



허용하지 않음을 선택하면 네트워크 액세스를 위해 GlobalProtect 연결 적용 기능이 작동하지 않고 네트워크 액세스에 대한 GlobalProtect 연결을 적용할 수 없습니다. 이 팝업 메시지는 허용을 선택할 때까지 표시됩니다.

3. (macOS Big Sur 11 이상에만 해당) 시스템 관리자가 GlobalProtect 게이트웨이의 도메인 및 애플리케이션을 기반으로 분할 터널을 구성하고 네트워크 액세스를 위해 GlobalProtect 연결 적용 기능을 활성화한 경우 다음 팝업 메시지에서 허용을 선택합니다.

 ©2023 Palo Alto Networks, Inc.



허용하지 않음을 선택하면 GlobalProtect 앱에서 분할 터널 기능을 사용할 수 없으며 네트워크 액세스를 위해 GlobalProtect 연결 적용 기능이 작동하지 않고 네트워크 액세스에 대한 GlobalProtect 연결을 적용할 수 없습니다. 이 팝업 메시지는 다음에 포털이나 게이트웨이에 연결할 때 또는 허용을 선택할 때까지 표시됩니다.

앱이 외부 모드에서 연결되면 GlobalProtect 시스템 트레이 아이콘에 방패( ) 아이콘 위로 마우스를 가져가면 연결됨이 표시됩니다. 앱이 내부 모드로 연결되면 GlobalProtect 시스템 트레이 아이콘에 집( ) 아이콘 위로 마우스를 가져가면 내부 네트워크가 표시됩니다.

STEP 3 | GlobalProtect 앱을 엽니다.

GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

관리자가 GlobalProtect 앱 설치 중에 Autonomous DEM(ADEM) 엔드포인트 에이전트를 설치하도록 포털을 구성하고 테스트 활성화를 허용하거나 허용하지 않은 경우 알림이 표시됩니다. 관리자가 이미 ADEM 엔드포인트 에이전트를 설치하고 나중에 ADEM 엔드포인트 에이전트를 제거하도록 포털을 구성한 경우 다음 로그인 시 알림이 표시됩니다.

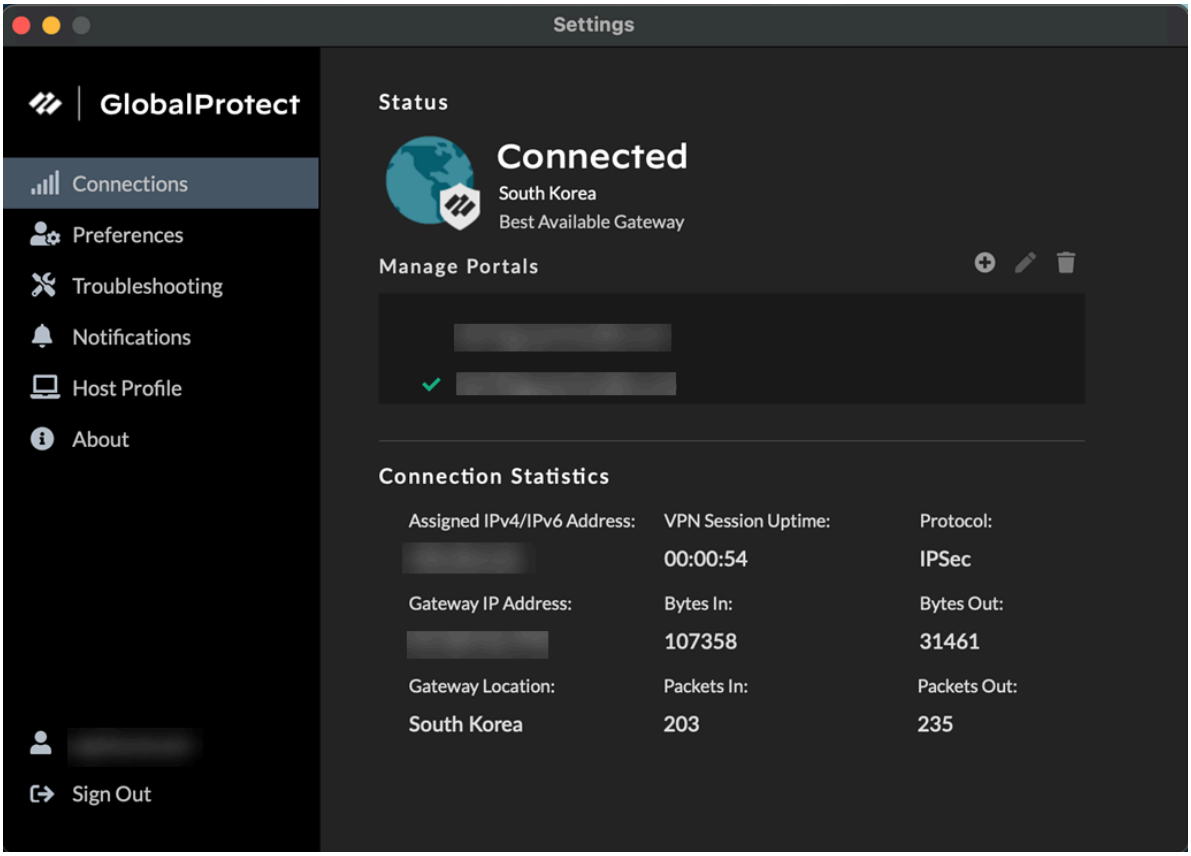
STEP 4 | 네트워크 연결에 대한 정보를 봅니다.

앱을 실행한 후 상태 패널에서 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다. 설정을 선택하여 **GlobalProtect** 설정 패널을 연 후 다음 설정 중 하나를 선택하여 GlobalProtect 앱을 보고 수정합니다.

- 연결—연결 탭에는 GlobalProtect 계정과 연결된 포털이 표시됩니다. 이 탭에서 포털을 추가, 편집 또는 삭제할 수 있습니다. 이 탭에는 연결된 게이트웨이도 표시됩니다. 관리자가 GlobalProtect 포

 ©2023 Palo Alto Networks, Inc.

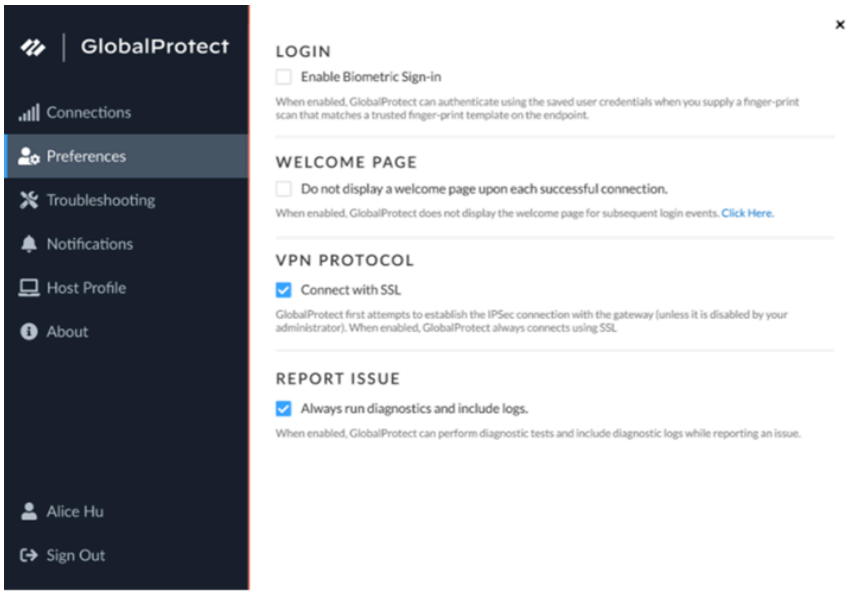
털 에이전트 구성에서 고급 보기 활성화를 예로 설정하면 게이트웨이에 대한 연결 통계(예: 게이트웨이 IP 주소, 위치 및 VPN 세션 가동 시간)를 볼 수 있습니다.



- 기본 설정—이제 관리자가 다음 옵션 중 하나 이상을 구성한 경우에만 기본 설정 탭을 사용할 수 있습니다.
  - 생체 인식 로그인 활성화—생체 인식(지문) 정보를 사용하여 로그인하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 에이전트 구성에서 사용자 자격 증명 저장을 사용자 지문으로만으로 구성하는 경우에만 사용할 수 있습니다. 엔드포인트의 신뢰할 수 있는 지문 템플릿과 일치하는 지문을 제공하여 GlobalProtect 포털 및 게이트웨이에 대한 인증에 저장된 암호를 사용해야 합니다.
  - 연결할 때마다 환영 페이지를 표시하지 않음—로그인에 성공하면 환영 페이지를 표시하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털 에이전트 구성에서 환영 페이지를 공장 기본값으로 설정한 경우에만 사용할 수 있습니다.
  - **SSL**을 사용하여 연결—SSL을 사용하거나 IPSec을 유지하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털 에이전트 구성에서**SSL**로만 연결을 사용자가 변경할 수 있음으로 설정한 경우에만 사용할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

- 항상 진단 테스트 실행 및 로그 포함—GlobalProtect 앱이 진단 테스트를 실행하고 진단 로그를 포함하도록 선택할 수 있습니다. 이 옵션은 관리자가 GlobalProtect 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화한 경우에만 사용할 수 있습니다.

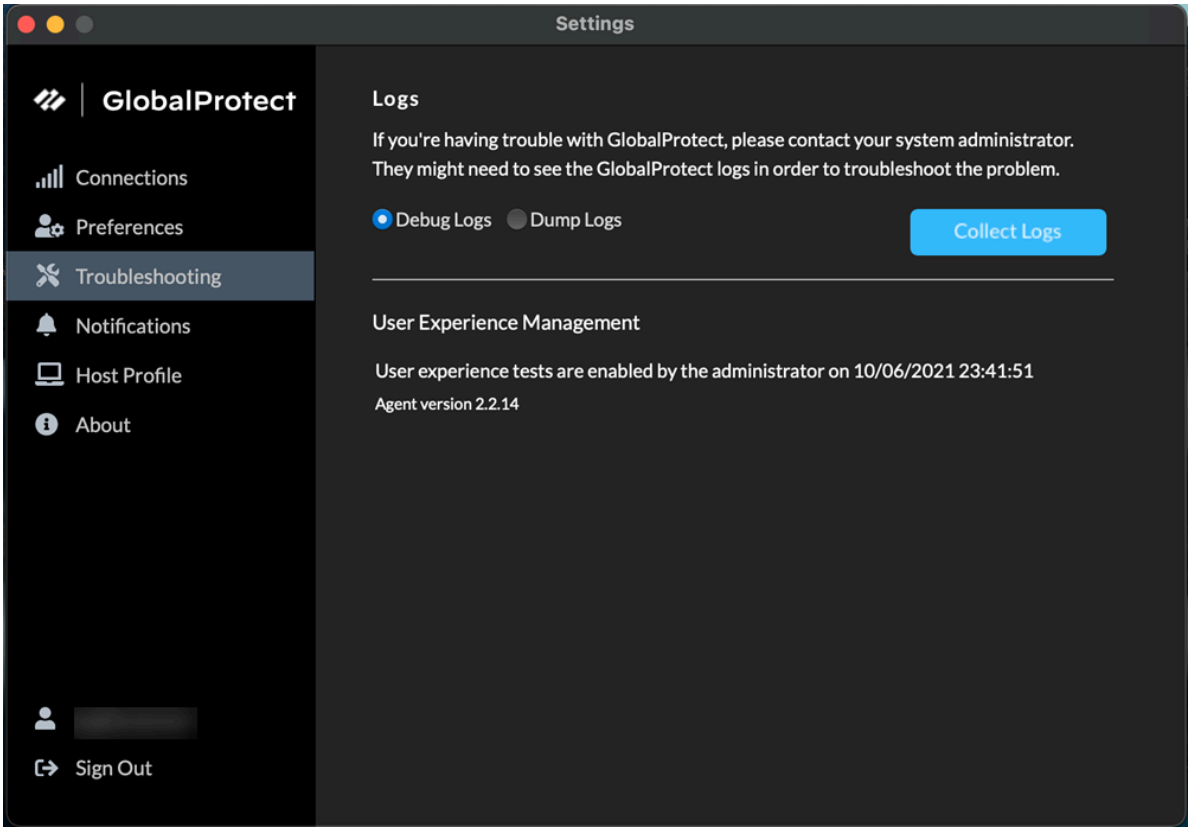


 ©2023 Palo Alto Networks, Inc.

- 문제 해결—문제 해결 탭에서는 로그를 수집하고 로깅 수준을 디버그 로그 또는 덤프 로그로 설정하고 선택적으로 사용자 환경 테스트를 활성화하도록 설정할 수 있습니다.

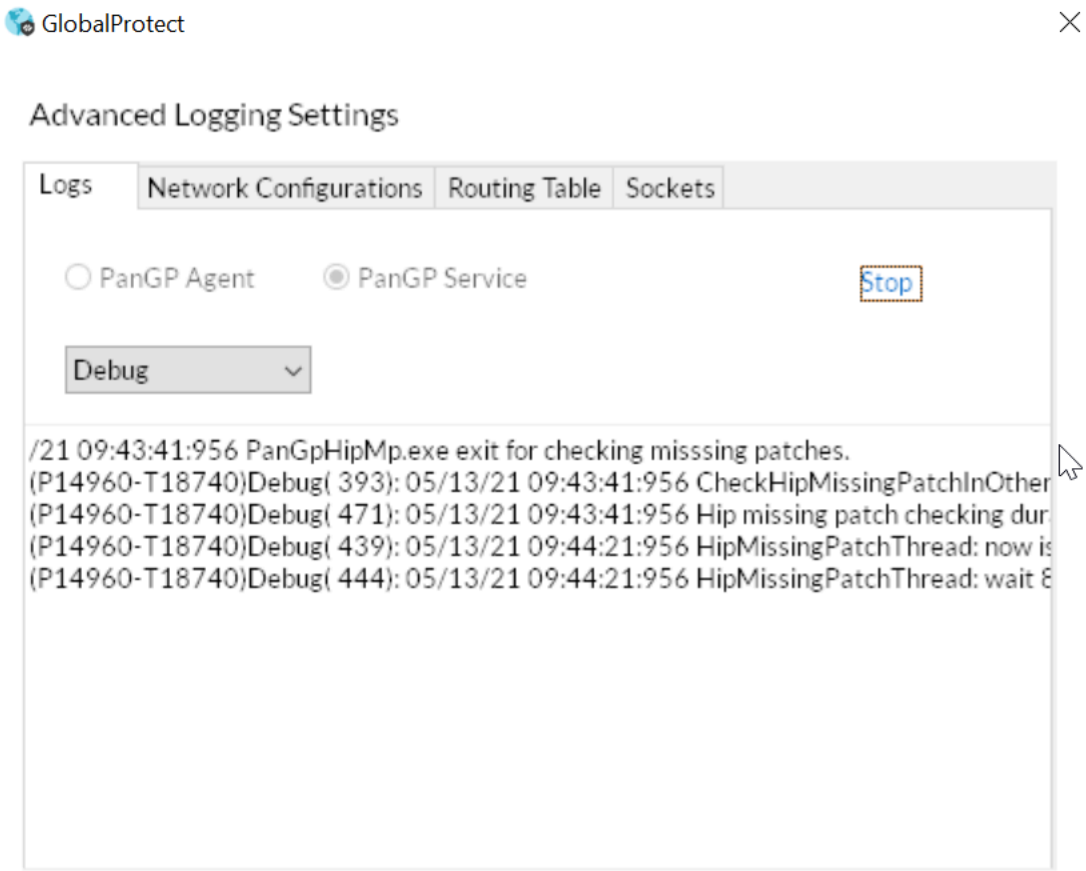
  GlobalProtect 앱이 추가 분석을 위해 문제 해결 로그, 진단 로그 또는 둘 모두를 Cortex Data Lake로 보내려면 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화하도록 *GlobalProtect* 포털을 구성해야 합니다. 또한 프로브하려는 웹 서버/리소스의 *IP* 주소 또는 정규화된 도메인 이름을 포함할 수 있는 HTTPS 기반 대상 URL을 구성하고 최종 사용자 엔드포인트에서 대기 시간 또는 네트워크 성능과 같은 문제를 확인할 수 있습니다.

  고급을 클릭하여 엔드포인트에 대한 자세한 정보를 볼 수 있습니다.



  고급 로깅 설정 창에는 네트워크 구성, 경로 설정 활성 연결 및 로그에 대한 정보가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



GlobalProtect가 연결되면 사용자 경험 테스트 활성화 확인란이 GlobalProtect 앱에 표시될 경우 ADEM 엔드포인트 에이전트가 사용자 경험 테스트를 수행할 수 있는지 확인하십시오. 또는 관리자가 GlobalProtect 앱 설치 중에 ADEM 엔드포인트 에이전트를 설치했지만 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화하도록 허용하지 않은 경우 메시지가 표시되는지 확인할 수 있습니다. 기본적으로 하트비트 알림은 GlobalProtect가 비활성화되거나 연결이 끊어진 경우에도 여전히 ADEM으로 전달됩니다.

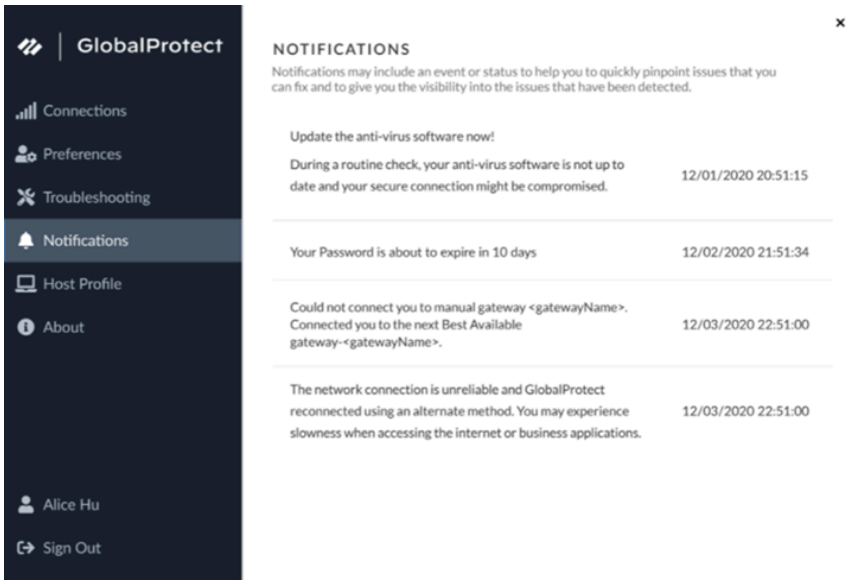
관리자가 GlobalProtect 앱 설치 중에 자율 DEM 엔드포인트 에이전트를 설치하도록 포털을 구성하고 테스트를 활성화하도록 허용한 경우 GlobalProtect 앱에서 사용자 경험 테스트 활성화 확인란을 선택합니다. 관리자가 GlobalProtect 앱에서 사용자 경험 테스트를 활성화 또는 비활성화하도록

 ©2023 Palo Alto Networks, Inc.

허용하지 않는 경우 이 확인란은 나타나지 않습니다. 대신 앱이 사용자 경험 테스트를 실행할 수 있음을 확인하는 메시지가 표시됩니다.

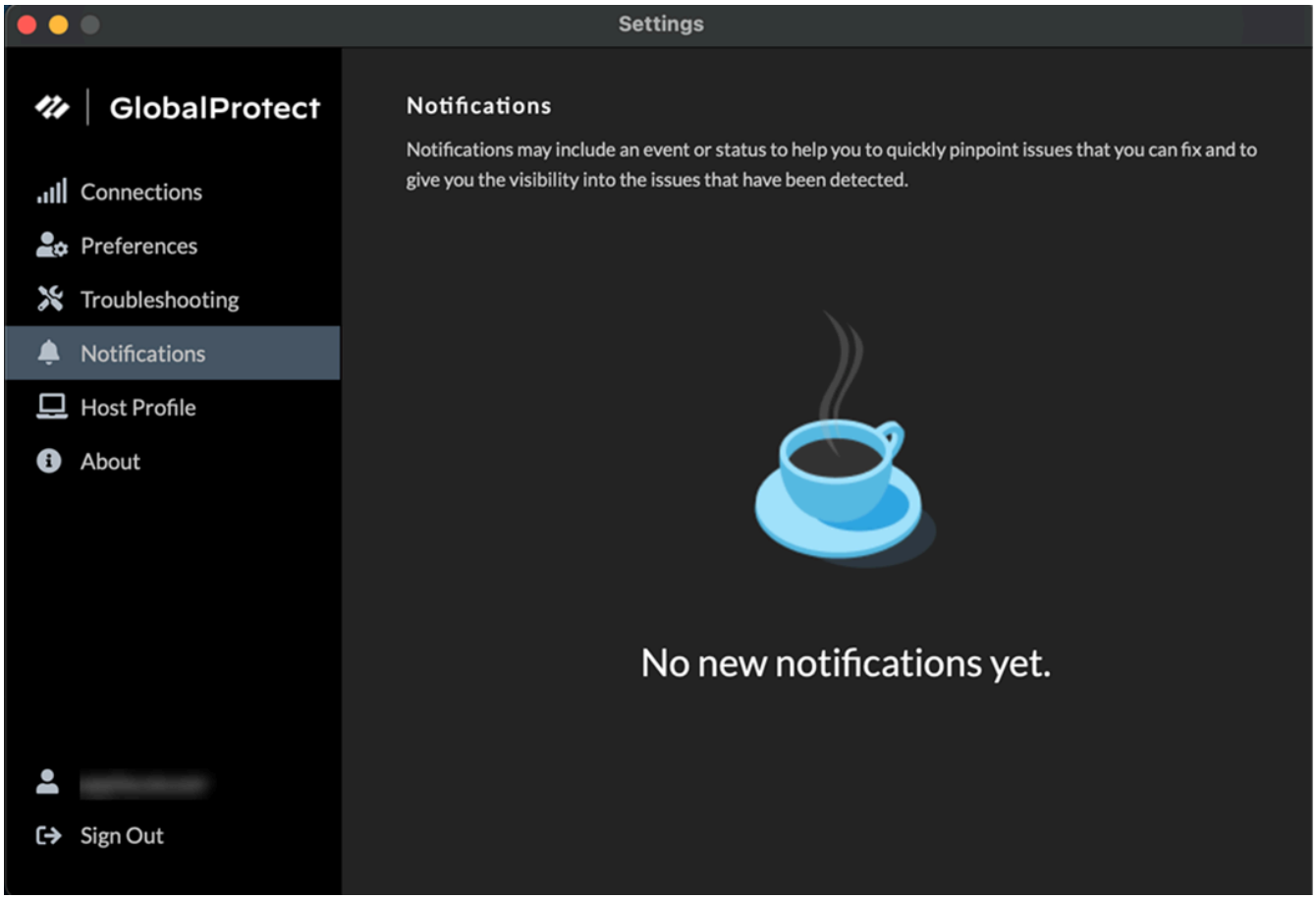
사용자 경험 테스트 활성화 확인란을 선택하지 않으면 하트비트 알림이 여전히 ADEM으로 전달됩니다.

- 알림—알림 탭에는 GlobalProtect 앱에서 트리거된 특정 알림에 대한 자세한 정보가 표시됩니다.



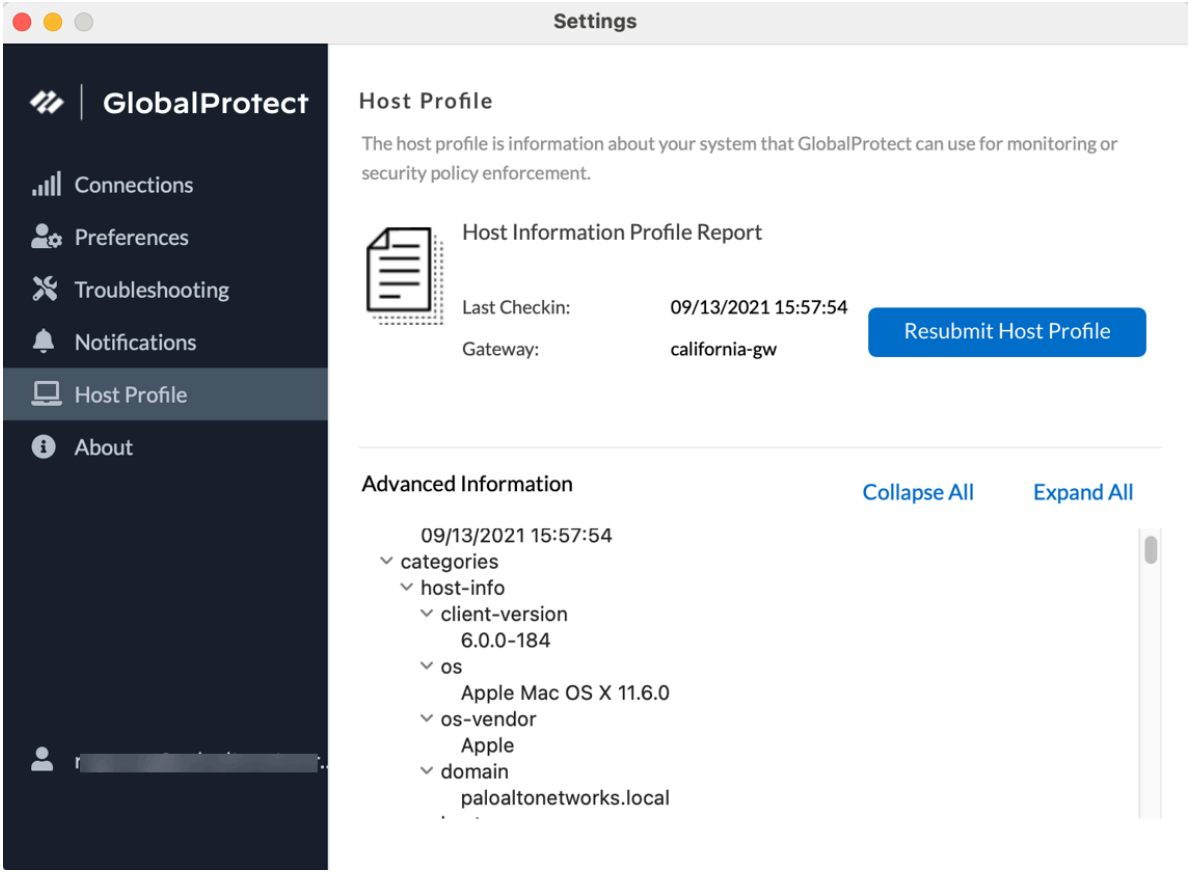
GlobalProtect 앱에서 트리거된 새 알림이 없는 경우에도 알림을 받습니다.

 ©2023 Palo Alto Networks, Inc.

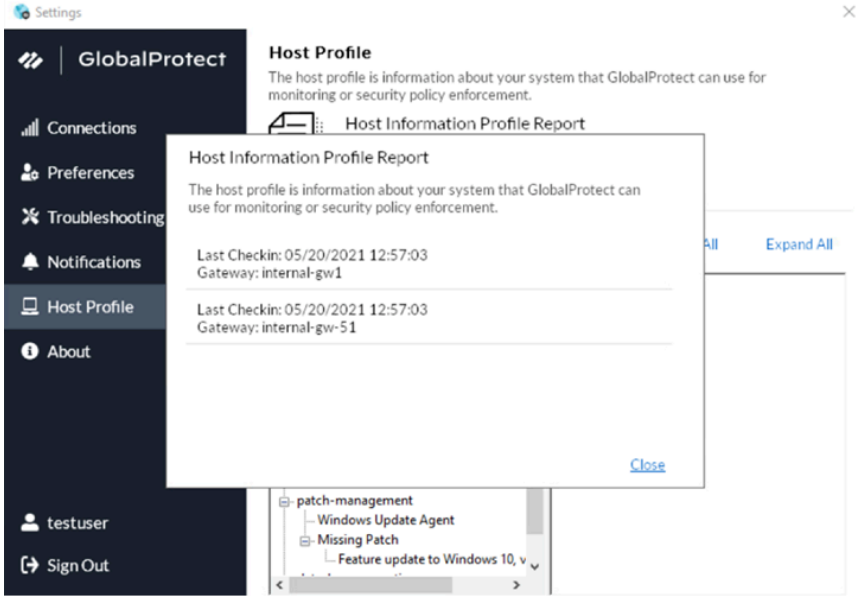


- 호스트 프로파일—호스트 프로파일 탭은 GlobalProtect가 호스트 정보 프로파일을 통해 보안 정책을 모니터링하고 시행하는 데 사용하는 엔드포인트 데이터를 표시합니다. 게이트웨이에 HIP 데이터를 수동으로 다시 제출하기 위해 호스트 프로파일을 다시 제출할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

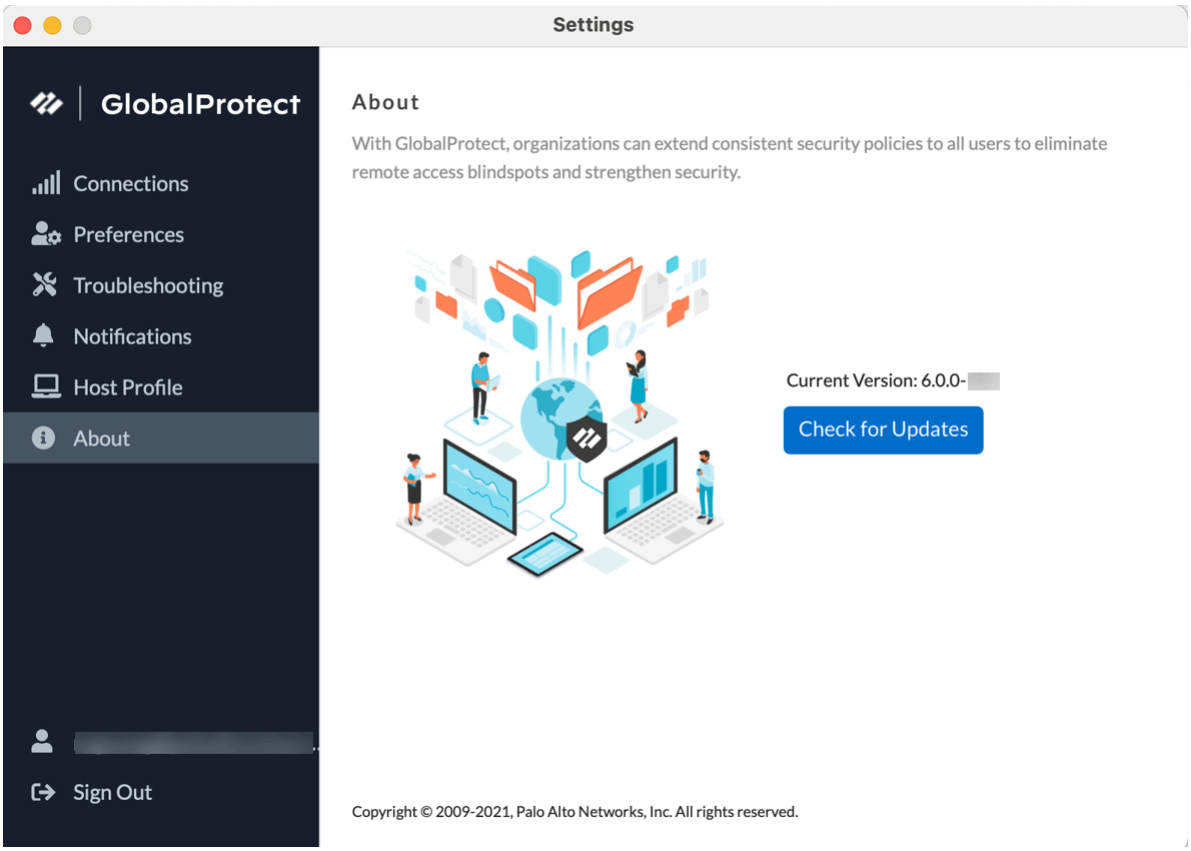


관리자가 비터널 모드 및 내부 호스트 감지에서 여러 내부 게이트웨이를 구성한 경우 추가 세부 정보를 클릭하여 호스트 정보 프로필(HIP) 관련 문제를 신속하게 해결하는 데 도움이 되도록 중앙 위치에서 각 게이트웨이에 대한 HIP 보고서 제출을 모니터링할 수 있습니다.



- 정보—정보 탭은 엔드포인트에 현재 설치된 GlobalProtect 버전을 표시하고 최종 사용자가 업데이트를 확인할 수 있도록 합니다.

 ©2023 Palo Alto Networks, Inc.



STEP 5 | (선택 사항) 새 암호를 사용하여 로그인합니다.

> *GlobalProtect* 관리자가 *GlobalProtect* 포털 에이전트가 사용자 자격 증명을 저장하도록 구성하면 자격 증명이 *GlobalProtect* 앱에 자동으로 저장됩니다. 회사 네트워크에 액세스하기 위한 암호가 변경되면 새 암호를 사용하여 *GlobalProtect*에 로그인해야 합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다.
3. 설정을 선택하여**GlobalProtect** 설정 패널을 엽니다.
4. **GlobalProtect** 설정 패널에서로그아웃하여 GlobalProtect 앱에서 저장된 사용자 자격 증명을 지웁니다.
5. 사용자 자격 증명을 지운 후 새 사용자 이름과 암호를 사용하여 GlobalProtect에 다시 연결할 수 있습니다.

STEP 6 | (선택 사항) GlobalProtect와의 연결을 끊습니다.

관리자가 주문형 연결 방법으로 GlobalProtect를 구성한 경우 상태 패널에서 연결 해제를 클릭하여 GlobalProtect에서 연결을 끊을 수 있습니다.

macOS용 GlobalProtect 앱에서 문제 보고하기

네트워크 성능이 저하되거나 포털 및 게이트웨이와의 연결이 설정되지 않는 등의 비정상적인 동작이 발생하는 경우 관리자가 액세스할 수 있는 Cortex Data Lake에 직접 문제를 보고할 수 있습니다. 더 이상 이메일을 통해 GlobalProtect 앱 로그를 수동으로 수집 및 전송하거나 클라우드 드라이브에 저장할 필요가 없습니다.

GlobalProtect 앱에 문제 보고 옵션을 표시하려면 관리자가 ***GlobalProtect*** 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화해야 합니다.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. (선택 사항) GlobalProtect 앱에 처음 로그인하는 경우 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력한 다음 연결을 클릭합니다.
3. (선택 사항) 앱에 여러 포털이 저장되어 있는 경우 포털 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 드롭다운에서 미리 선택됩니다.
4. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 드롭다운을 클릭합니다.

STEP 2 | GlobalProtect 앱을 엽니다.

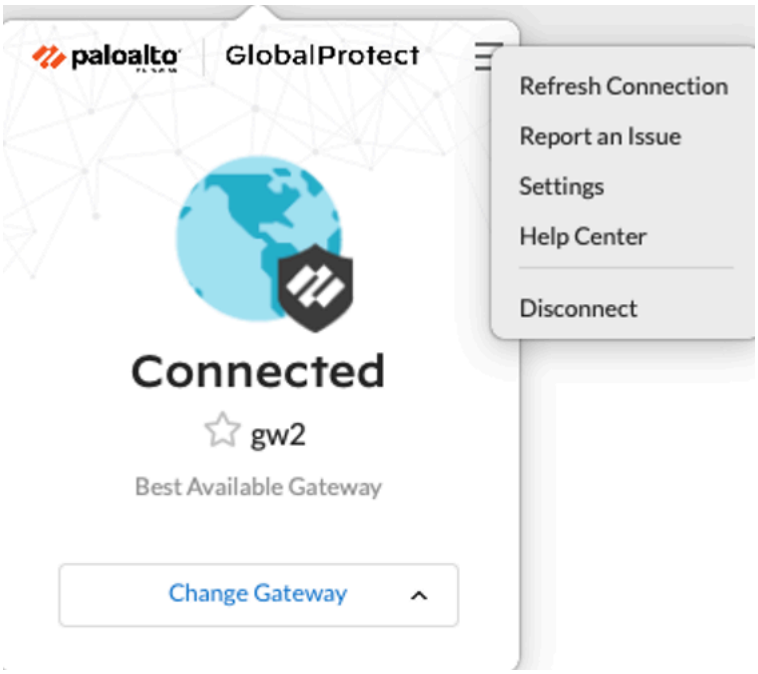
GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 엔드포인트에서 GlobalProtect 앱의 문제를 보고합니다.

앱을 실행한 후 상태 패널에서 햄버거 메뉴를 클릭하여 관리자에게 문제를 보고합니다.

1. 문제 신고를 선택합니다.



2. 진단 테스트를 실행하고 진단 로그를 포함하도록 GlobalProtect 앱을 활성화합니다. 진단 및 문제 해결 로그가 모두 수집되어 간결한 문제 해결 보고서로 Cortex Data Lake에 전송됩니다.

   진단 테스트가 완료되면 GlobalProtect 디버그 로그 파일이 엔드포인트에서 Cortex Data Lake로 업로드됩니다.

   앱에서 진단 테스트를 실행하고 진단 로그를 포함하도록 설정하지 않으면 문제 해결 로그만 수집되어 압축 문제 해결 보고서로 ***Cortex Data Lake***에 전송됩니다. ***GlobalProtect*** 앱은 `.json` 형식으로 자동 생성되는 보고서 파일(***pan_gp.trb.log*** 또는 ***pan_gp_trbl.log***)을 확인합니다. 문제 해결 로그에서 문제가 발견되지 않은 경우 알림 메시지가 표시됩니다. 다시 시도를 클릭하여 ***pan_gp.trb*.log*** 파일이 있는지 확인합니다.

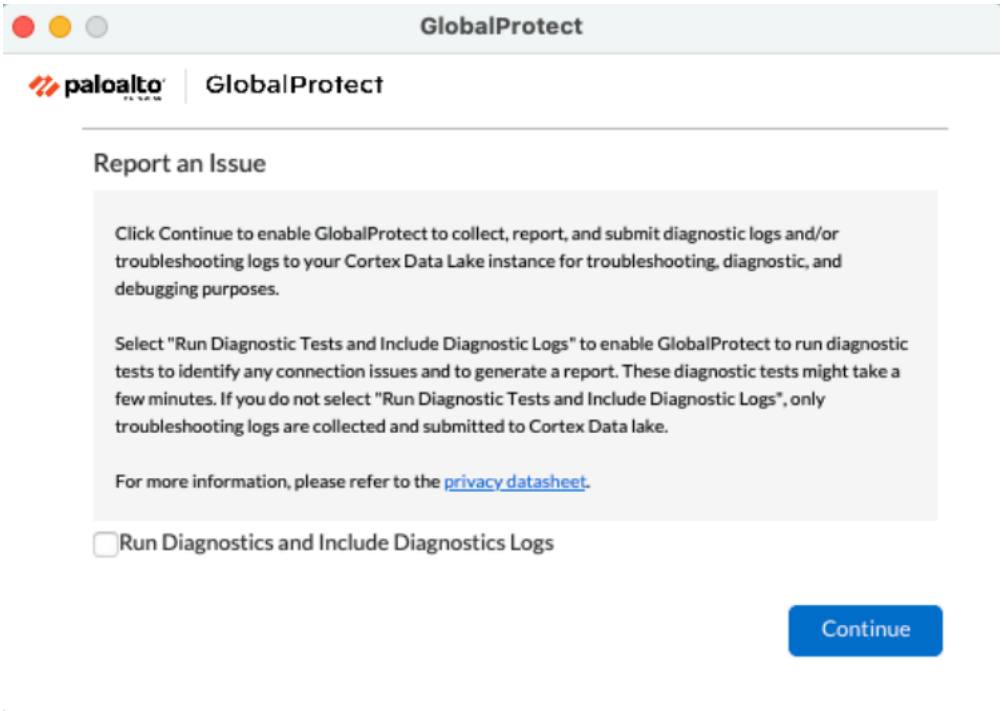
3. 진단 테스트 실행 및 진단 로그 포함 확인란을 선택합니다.
4. 계속을 클릭하면 앱이 문제 해결 로그를 생성하고 관리자의 Cortex Data Lake 인스턴스로 보고서를 전송할 수 있습니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다.

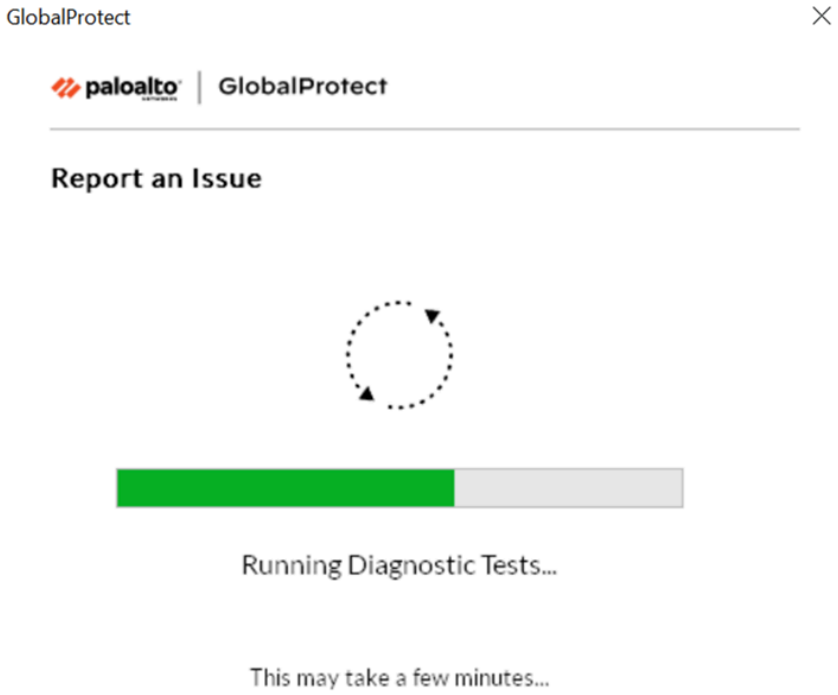
   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다. GlobalProtect 앱은 터널을 사용하거나 터널 없이 진단 테스트를 실행할 수 있습니다. 예를 들어

 ©2023 Palo Alto Networks, Inc.

앱이 터널을 통해 진단 테스트를 연결하고 실행하기 전에 GlobalProtect 로그인 자격 증명을 입력할 수 있습니다.

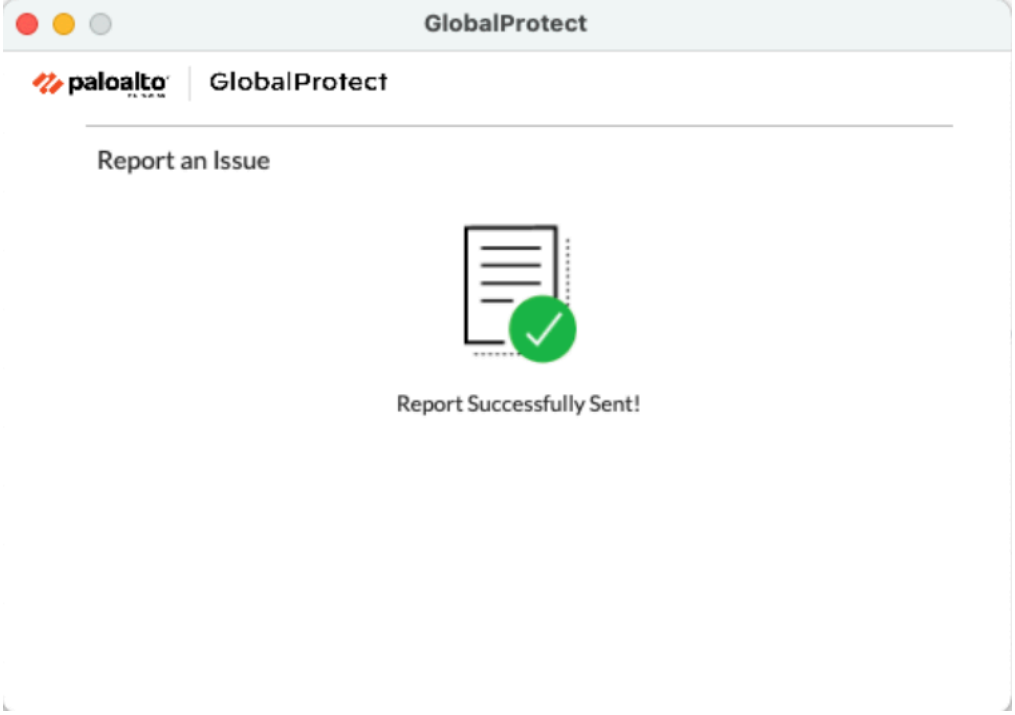


진단 테스트 실행 및 진단 로그 포함 확인란을 선택한 경우에만 앱이 진단 테스트를 실행하고 있음을 확인하는 메시지가 팝업됩니다.



 ©2023 Palo Alto Networks, Inc.

5. 닫기를 클릭하여 앱이 Cortex Data Lake로 보고서를 전송했는지 확인합니다. 이 확인 메시지에는 보고서가 처리되고 전송된 날짜 및 시간이 표시됩니다.



 ©2023 Palo Alto Networks, Inc.

macOS용 GlobalProtect 앱 연결 해제

관리자가 GlobalProtect 연결 방법을 항상 켬으로 구성한 경우 GlobalProtect 앱의 연결을 끊을 수 있습니다. 예를 들어 호텔에서 GlobalProtect 가상 사설망(VPN)이 작동하지 않고 VPN 오류로 인해 인터넷에 연결할 수 없는 경우 앱 연결을 끊을 수 있습니다. GlobalProtect 앱의 연결을 끊은 후 보안되지 않은 통신(VPN 없이)을 사용하여 인터넷에 연결할 수 있습니다.

GlobalProtect 앱의 연결을 끊을 수 있는 방법, 시간 및 횟수는 관리자가 GlobalProtect 서비스(PanGPS)를 구성하는 방법에 따라 다릅니다. 이 구성을 사용하면 앱 연결을 완전히 끊지 못하거나 챌린지에 올바르게 응답한 후에만 앱 연결을 끊을 수 있습니다.

구성에 챌린지가 포함된 경우 GlobalProtect 앱은 다음 중 하나를 묻는 메시지를 표시합니다.

- 앱 연결을 해제하려는 이유
- 인터넷 속도가 느리거나 앱이 작동하지 않는 것과 같은 하나 이상의 이유에 응답(필요한 경우)
- 암호
- 티켓 번호

챌린지에 암호 또는 티켓 번호가 포함된 경우 전화로 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 문의하는 것이 좋습니다.

관리자는 일반적으로 이메일(신규 GlobalProtect 사용자의 경우)을 통하거나 조직의 웹 사이트에 게시하여 암호를 미리 제공합니다. 중단 또는 시스템 문제에 대한 응답으로 관리자는 전화로 암호를 제공할 수도 있습니다.

유효한 티켓 번호를 받기 전에 엔드포인트에 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 전달해야 하는 티켓 요청 번호가 표시됩니다. 연결 해제 요청이 승인되면 GlobalProtect를 연결 해제하는 데 사용할 수 있는 유효한 티켓 번호를 받게 됩니다.

다음 단계에서는 앱 연결을 끊고 챌린지를 통과하는 방법을 설명합니다.

STEP 1 | GlobalProtect 앱의 연결을 끊습니다.

1. GlobalProtect 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 햄버거 메뉴를 클릭하여 설정 메뉴를 엽니다.
3. 연결 해제를 선택합니다.

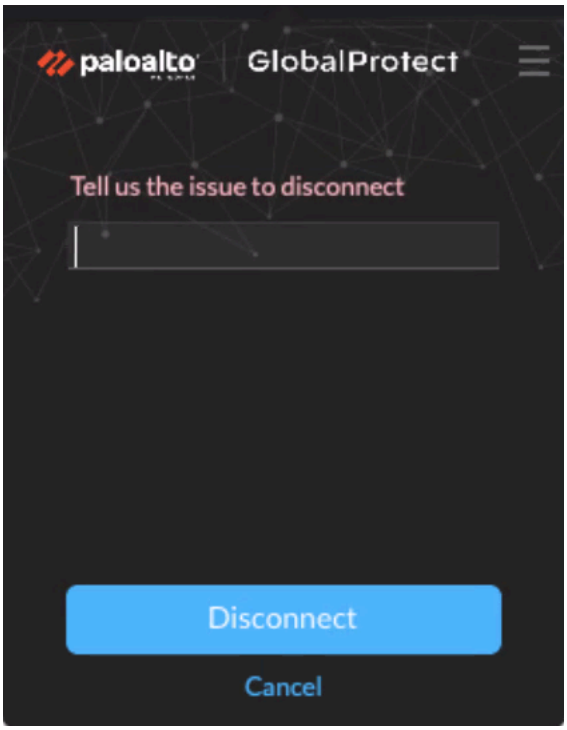
연결 해제 옵션은 ***GlobalProtect*** 에이전트 구성에서 앱 연결을 끊을 수 있는 경우에만 표시됩니다. 구성을 통해 챌린지에 응답할 필요 없이 ***GlobalProtect*** 앱의 연결을 끊을 수 있는 경우 추가 조치 없이 ***GlobalProtect*** 앱이 닫힙니다.

 ©2023 Palo Alto Networks, Inc.

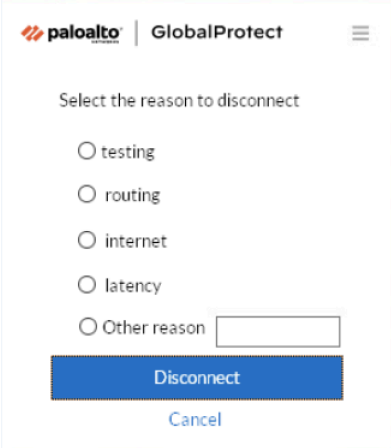
STEP 2 | 필요한 경우 하나 이상의 챌린지에 대응합니다.

메시지가 표시되면 다음 정보를 제공합니다.

- 연결 해제 원인—GlobalProtect 앱 연결을 해제하는 이유입니다.



- 연결 해제 이유 선택—구성에 하나 이상의 이유로 응답하거나 다른 이유를 입력해야 하는 경우 연결 해제를 선택하는 즉시 GlobalProtect 앱에 이유가 표시됩니다.



- 암호—앱 연결을 해제해야 하는 알려진 문제 또는 이벤트에 따라 관리자가 일반적으로 미리 제공하는 암호입니다.
- 티켓—구성에 티켓 번호를 제공해야 하는 경우 연결 해제를 선택하는 즉시 GlobalProtect 앱에 8자리 16진수 티켓 요청 번호가 표시됩니다. 티켓 번호로 앱 연결을 해제하려면 관리자 또는 헬프 데스크 담당자(전화)에게 연락하여 티켓 요청 번호를 제공하십시오. 요청을 승인하면 관리자 또는 지원 센터 담당자가 8자리 16진수 티켓 번호를 제공합니다. 티켓 필드에 티켓 번호를 입력하고 확인을 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

macOS용 GlobalProtect 앱 제거

다음 단계를 사용하여 macOS 엔드포인트에서 GlobalProtect 앱을 제거합니다. 앱을 제거하면 더 이상 기업 네트워크에 VPN으로 액세스할 수 없으며 엔드포인트가 회사의 보안 정책에 의해 보호되지 않는다는 점에 유의하십시오.

관리자 권한이 있는 사용자만 ***macOS*** 엔드포인트에서 ***GlobalProtect*** 앱을 제거할 수 있습니다.

macOS 엔드포인트에서 macOS 설치 프로그램(이 경우 GlobalProtect 설치 관리자)을 사용하여 프로그램을 제거할 수 있습니다. 엔드포인트에서 GlobalProtect 앱을 제거하려면 GlobalProtect 소프트웨어 패키지를 설치한 다음 GlobalProtect 설치 관리자를 시작합니다. GlobalProtect 설치 관리자는 **GlobalProtect** 제거 패키지를 선택하라는 메시지를 표시합니다. 관리자가 GlobalProtect 앱을 설치하는 동안 macOS 엔드포인트용 GlobalProtect 앱에서 시스템 확장 프로그램을 활성화한 경우, GlobalProtect 앱은 GlobalProtect 제거 중에 시스템 확장 프로그램을 삭제하라는 메시지도 표시합니다. **GlobalProtect** 제거 패키지가 설치되면 GlobalProtect 앱이 엔드포인트에서 삭제됩니다.

macOS 엔드포인트에 더 이상 ***GlobalProtect*** 설치 프로그램이 없는 경우 명령줄에서 다음 명령을 실행하여 ***GlobalProtect***를 제거할 수 있습니다.

```
sudo /Applications/GlobalProtect.app/Contents/Resources/
uninstall_gp.sh
```

STEP 1 | GlobalProtect 포털에 로그인합니다.

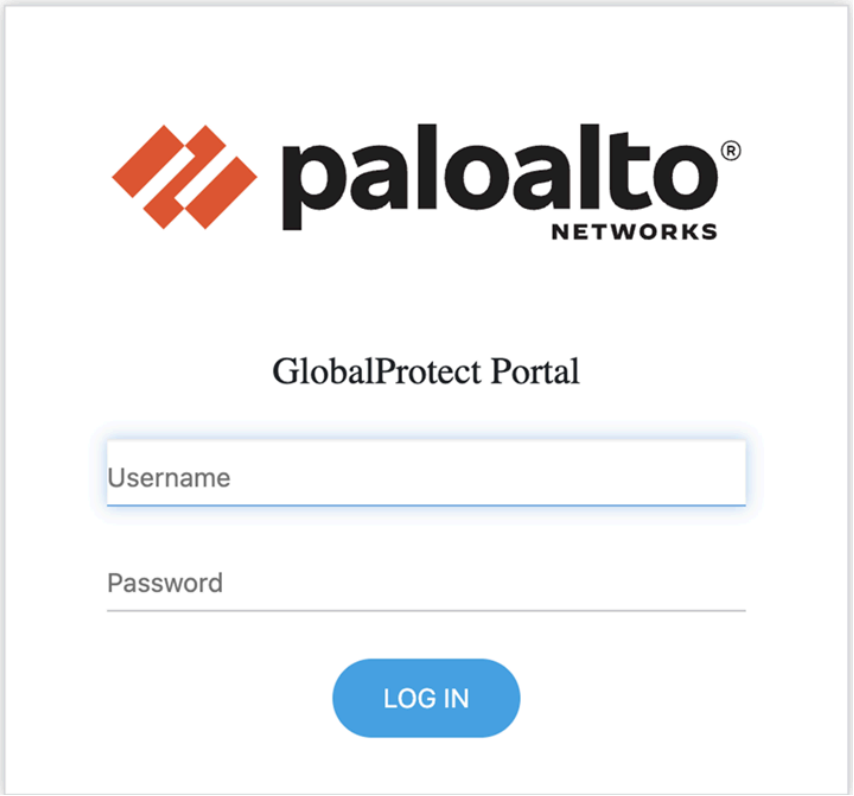
1. 웹 브라우저를 실행하고 다음 URL로 이동합니다.

   `https://<portal address or name>`

   예: **`http://gp.acme.com`**

2. 포털 로그인 페이지에서 이름(사용자 이름)과 암호를 입력하고 로그인을 클릭합니다. 대부분의 경우 회사 네트워크에 연결할 때 사용하는 것과 동일한 사용자 이름과 암호를 사용할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



STEP 2 | 앱 다운로드 페이지로 이동합니다.

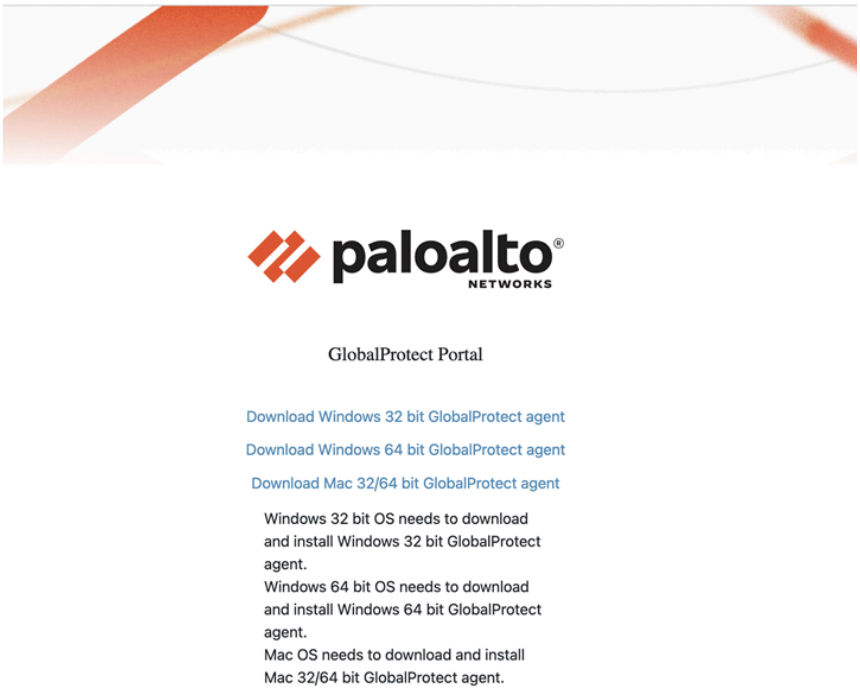
대부분의 경우 앱 다운로드 페이지는 포털에 로그인한 직후에 표시됩니다.

시스템 관리자가 *GlobalProtect Clientless VPN* 액세스를 활성화한 경우 포털에 로그인하면 앱 다운로드 페이지 대신 애플리케이션 페이지가 열립니다. ***GlobalProtect*** 에이전트를 선택하여 다운로드 페이지를 엽니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 앱을 다운로드합니다.

1. **Mac 32/64**비트 **GlobalProtect** 에이전트 다운로드를 클릭합니다.

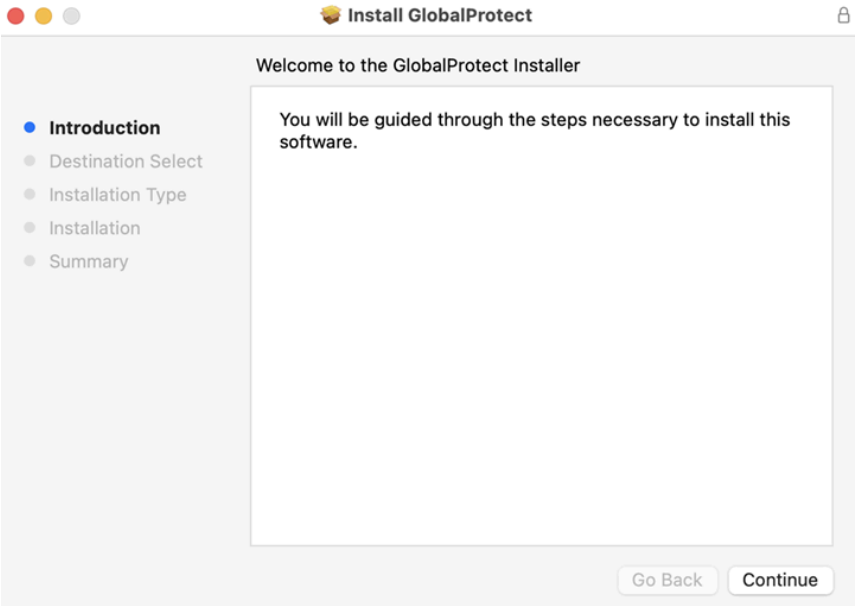


2. 메시지가 표시되면 소프트웨어를 실행합니다.
3. 메시지가 다시 표시되면 GlobalProtect 설치 프로그램을 실행합니다.

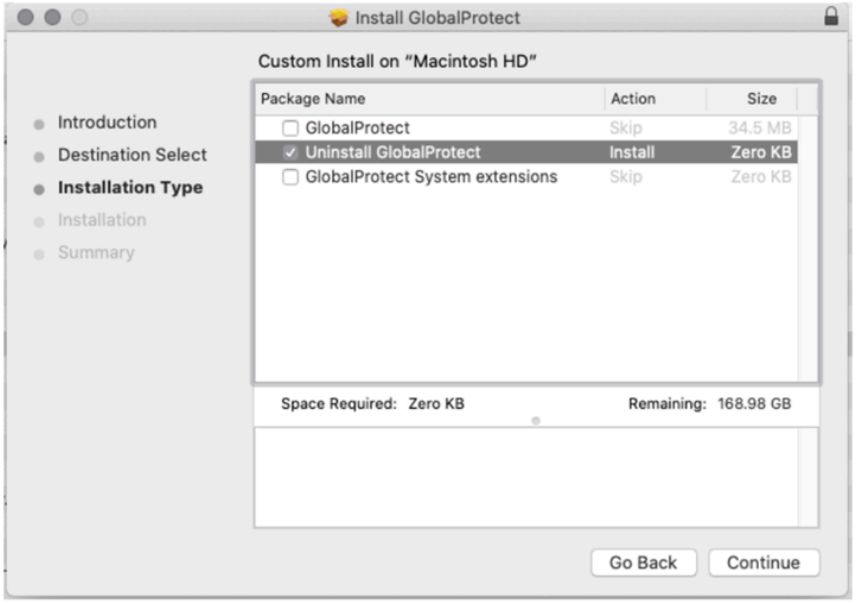
 ©2023 Palo Alto Networks, Inc.

STEP 4 | GlobalProtect를 제거합니다.

1. GlobalProtect 설치 프로그램에서 계속을 클릭합니다.

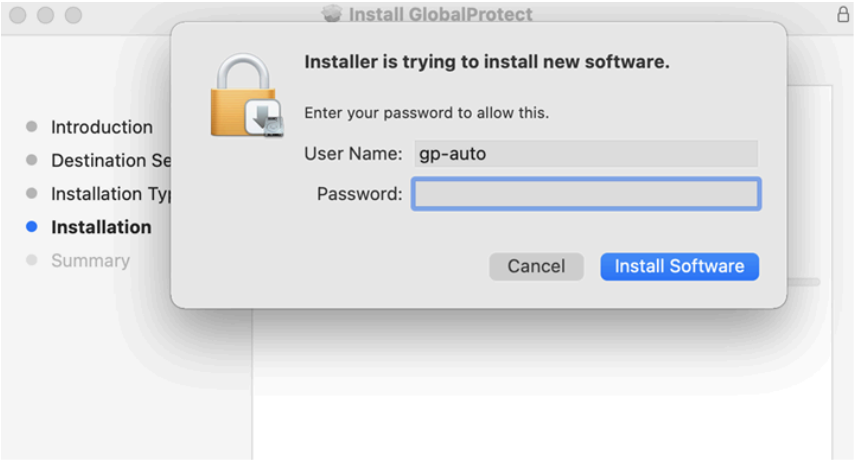


2. 대상 선택 화면에서 계속을 클릭합니다.
3. 설치 유형 화면에서 **GlobalProtect** 제거 확인란을 선택하고 계속을 클릭합니다.

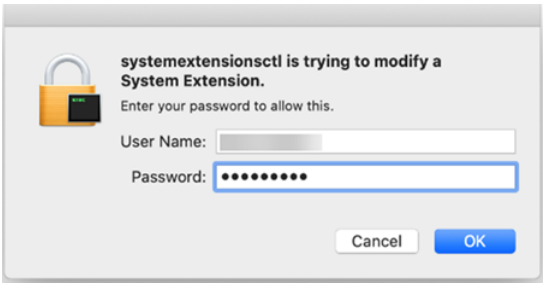


4. 설치를 클릭하여 GlobalProtect 앱을 삭제할 것임을 확인합니다.
5. 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 소프트웨어 설치를 클릭하여 GlobalProtect를 제거합니다.

 ©2023 Palo Alto Networks, Inc.

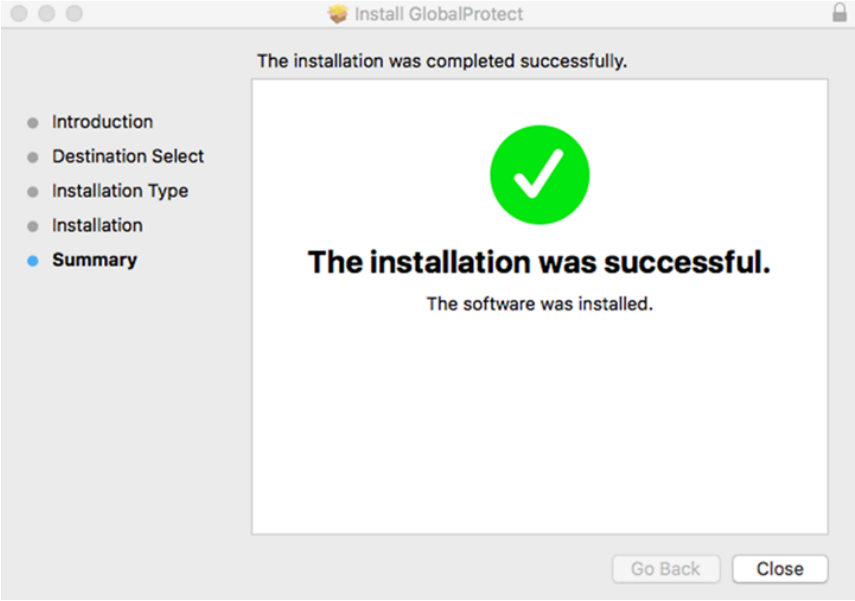


6. macOS Catalina 10.15.4 이상을 실행하는 GlobalProtect 앱 5.1.4 설치 중에 시스템 관리자가 macOS 시스템 확장 프로그램을 활성화한 경우 시스템 확장 프로그램을 제거하라는 팝업 메시지가 표시됩니다. 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 확인을 클릭하여 시스템 확장 프로그램을 삭제합니다.



STEP 5 | GlobalProtect 앱이 더 이상 설치되지 않았는지 확인합니다.

GlobalProtect 제거 패키지가 설치되었음을 확인하는 메시지가 표시됩니다. 이 확인은 엔드포인트에서 GlobalProtect 앱이 삭제되었음을 나타냅니다.



 ©2023 Palo Alto Networks, Inc.

GlobalProtect 인포서 커널 확장 프로그램 삭제

macOS용 GlobalProtect 앱을 제거한 다음 앱의 새 인스턴스를 설치할 때 GlobalProtect 인포서 커널 확장 프로그램이 올바르게 업데이트되지 않으면 연결 문제가 발생할 수 있습니다. 커널 확장 프로그램(`kext`)은 애플리케이션을 관리하는 macOS 운영 체제용 플러그인입니다. 앱의 새 인스턴스를 설치한 후 GlobalProtect에 연결할 수 없는 경우 다음 절차를 사용하여 GlobalProtect 인포서 커널 확장 프로그램을 찾아 삭제하십시오.

STEP 1 | Mac용 GlobalProtect 앱을 제거합니다.

STEP 2 | GlobalProtect 인포서 커널 확장 프로그램이 엔드포인트에 존재하는지 확인하십시오.

macOS 엔드포인트에서 애플리케이션 > 유틸리티 폴더에서 터미널 애플리케이션을 열고 다음 명령을 입력합니다.

```
kextstat | grep gplock
```

STEP 3 | 확장 프로그램이 존재하면 인포서를 언로드하십시오.

터미널 애플리케이션에서 다음 명령을 입력하여 인포서를 언로드합니다.

```
sudo kextunload -b com.paloaltonetworks.GlobalProtect.gplock
```

STEP 4 | 재부팅 후 인포서가 다시 로드되지 않도록 합니다.

터미널 애플리케이션에서 다음 명령을 입력하여 macOS 하드 디스크에서 인포서를 삭제합니다.

```
sudo rm -r "/System/Library/Extensions/gplock*.kext"
```

STEP 5 | Mac용 GlobalProtect 앱을 다운로드하고 설치합니다.

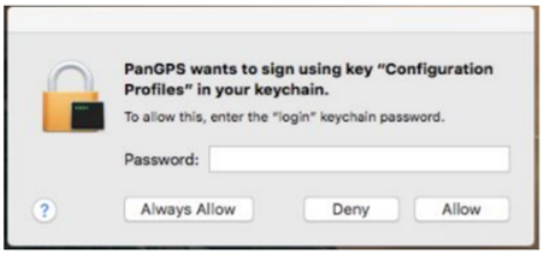
 ©2023 Palo Alto Networks, Inc.

인증을 위해 클라이언트 인증서를 사용하도록 macOS용 GlobalProtect 앱 활성화

GlobalProtect 앱이 처음으로 macOS 엔드포인트에 설치되고 클라이언트 인증서 인증이 포털 또는 게이트웨이에서 활성화되면 키체인 팝업 메시지가 나타나 사용자에게 GlobalProtect가 로그인 키체인의 클라이언트 인증서에 액세스하고 클라이언트 인증서를 사용할 수 있도록 암호를 입력하라는 메시지를 표시합니다. 키체인 팝업 메시지는 이전 인증서가 만료되어 새 인증서를 설치할 때도 나타날 수 있습니다.

인증을 위해 클라이언트 인증서를 사용하려면 다음 절차를 따라 macOS용 GlobalProtect 앱을 활성화해야 합니다.

STEP 1 | 다음 키체인 팝업 메시지에서 macOS 엔드포인트로 로그인 키체인 액세스를 허용하려면 암호를 입력하십시오.



STEP 2 | 항상 허용을 선택하여 GlobalProtect가 VPN 터널을 설정하도록 합니다. 키체인 팝업 메시지는 클라이언트 인증서가 만료될 때까지 나타나지 않습니다. 이 팝업 메시지는 클라이언트 인증서가 갱신될 때 다시 나타날 수 있습니다.

> 허용을 선택하면 사용자가 *GlobalProtect*에 연결할 때마다 키체인 팝업 메시지가 표시됩니다. 거부를 선택하면 *GlobalProtect*가 *VPN* 터널을 설정할 수 없으며 키체인 팝업 메시지가 표시됩니다. *GlobalProtect*는 로그인 키체인 액세스를 허용한 후에만 *VPN* 터널을 설정할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

iOS용 GlobalProtect 앱

GlobalProtect™는 엔드포인트(데스크톱 컴퓨터, 노트북, 태블릿 또는 스마트폰)에서 실행되는 애플리케이션으로, 회사 네트워크의 중요한 리소스를 보호하는 것과 동일한 보안 정책을 사용하여 사용자를 보호합니다. GlobalProtect™는 인트라넷, 사설 클라우드, 공용 클라우드 및 인터넷 트래픽을 보호하고 전 세계 어디에서나 회사 리소스에 액세스할 수 있도록 합니다.

다음 주제에서는 iOS용 글로벌프로텍트 앱을 설치하고 사용하는 방법을 설명합니다.

> iOS용 GlobalProtect 앱 다운로드 및 설치하기

> iOS용 GlobalProtect 앱 사용하기

> iOS용 GlobalProtect 앱에서 문제 보고하기

> iOS용 GlobalProtect 앱 제거

iOS용 GlobalProtect 앱 다운로드 및 설치하기

iOS 엔드포인트를 GlobalProtect 네트워크에 연결하려면 먼저 앱을 다운로드하고 설치해야 합니다. iOS 엔드포인트가 모바일 디바이스 관리(MDM) 시스템에서 관리되는 경우 관리자가 자동으로 GlobalProtect 앱을 엔드포인트에 푸시하고 VPN 설정을 구성했을 수 있습니다. iOS 엔드포인트에 GlobalProtect 앱이 아직 없는 경우 App Store에서 다운로드할 수 있습니다.

앱을 다운로드하기 전에 관리자로부터 GlobalProtect 포털의 IP 주소 또는 FQDN을 받아야 합니다. 또한 관리자는 포털 및 게이트웨이에 연결하는 데 사용할 수 있는 사용자 이름과 암호를 확인해야 합니다. 이것은 일반적으로 회사 네트워크에 연결하는 데 사용하는 것과 동일한 사용자 이름 및 암호입니다. 관리자가 생체 인식(지문 또는 macOS X 디바이스의 경우 Face ID) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호를 사용하여 두 번 로그인해야 합니다(저장하기 위해 한 번, 인증하기 위해 한 번 더). 그 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

필요한 정보를 수집한 후 다음과 같이 앱을 다운로드하고 설치할 수 있습니다.

STEP 1 | App Store를 실행합니다.

STEP 2 | **`GlobalProtect`**를 검색합니다.

STEP 3 | 검색 결과에서 **GlobalProtect™**를 선택합니다.

STEP 4 | GlobalProtect 앱 제품 페이지에서 **GET**을 누릅니다.

STEP 5 | 앱을 설치합니다.

STEP 6 | 메시지가 표시되면 Apple ID로 로그인합니다.

 ©2023 Palo Alto Networks, Inc.

iOS용 GlobalProtect 앱 사용하기

이 항목은 설정에서 엔드포인트에 로그인한 후 GlobalProtect 로그인 자격 증명을 입력해야 하는 경우에만 적용됩니다(Single Sign-On은 비활성화됨).

일반적으로 조직에서는 GlobalProtect 사용자가 앱 설치 후 투명하게 로그인할 수 있도록 허용하는 것이 좋습니다. 투명한 GlobalProtect 로그인으로 엔드포인트에 로그인하면 GlobalProtect 앱이 자동으로 시작되어 추가 사용자 개입 없이 기업 네트워크에 연결됩니다.

설정에 GlobalProtect 자격 증명을 입력해야 하는 경우 아래에서 해당 단계를 따르십시오.

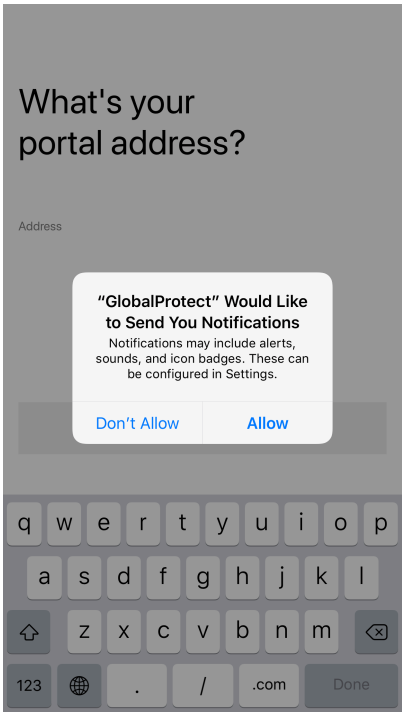
 ©2023 Palo Alto Networks, Inc.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

다음 워크플로 중 하나를 사용하여 GlobalProtect 포털 또는 게이트웨이에 연결하십시오.

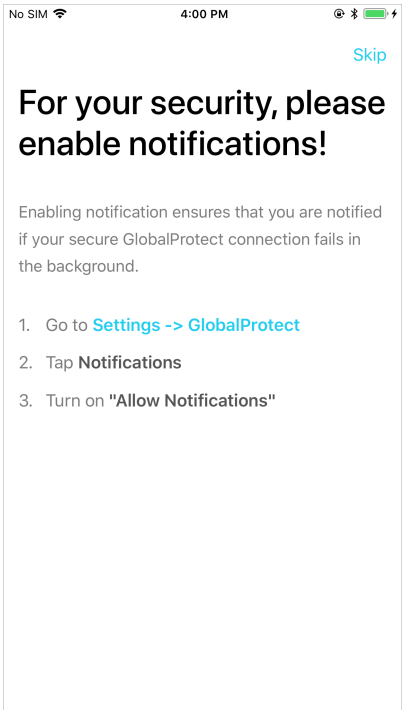
- 첫 번째 연결 경험:

  1. GlobalProtect 앱을 사용합니다.
  2. (선택 사항) 엔드포인트에서 GlobalProtect 알림을 활성화하지 않은 경우 알림 권한 대화 상자가 표시됩니다. GlobalProtect가 사용자에게 알림을 보내도록 허용합니다

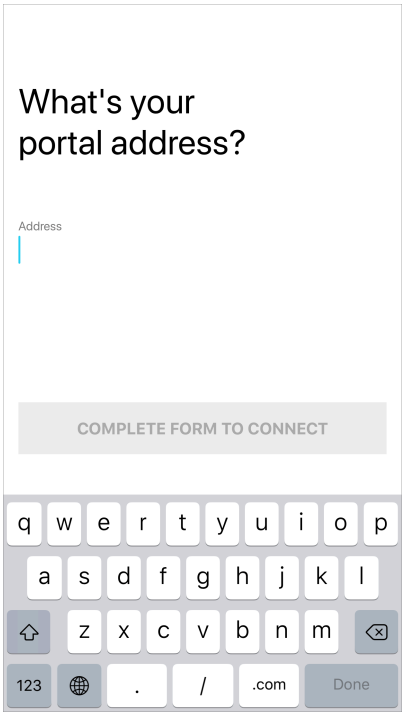


GlobalProtect에서 알림을 보내도록 허용하지 않으면 다음에 앱을 실행할 때 미리 알림이 표시됩니다. 설정 **-> GlobalProtect** 링크를 탭하여 알림을 활성화할 수 있는 알림 권한 화면으로 이동합니다. 그래도 알림을 활성화하지 않으려면 이 화면을 건너뜁니다.

 ©2023 Palo Alto Networks, Inc.

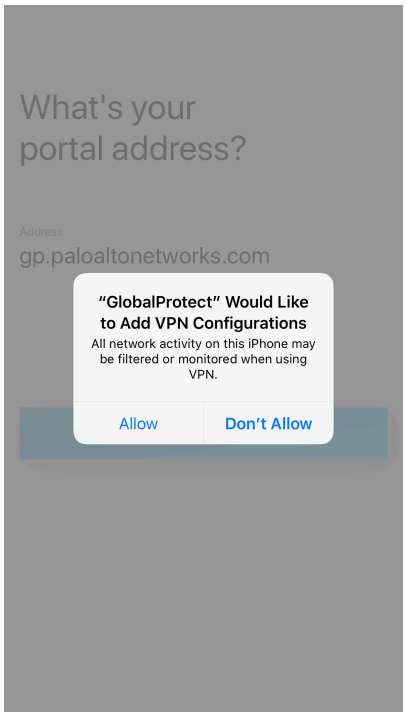


3. GlobalProtect 포털 주소를 입력합니다.

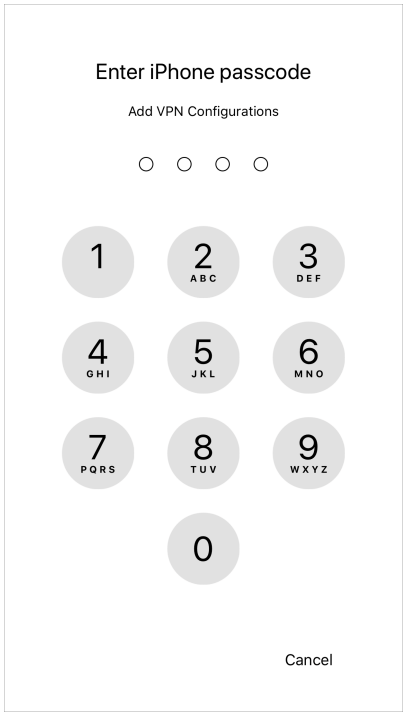


4. (선택 사항) 연결 모드에 따라 연결을 탭하여 연결을 시작합니다.
5. **'GlobalProtect' 가 VPN 구성을 추가하려 함** 메시지가 나타나면 다음 단계를 사용하여 엔드포인트에 VPN 구성을 추가합니다.
   1. GlobalProtect가 엔드포인트에 VPN 구성을 추가하도록 허용합니다. 이 설정을 사용하면 VPN을 사용할 때 GlobalProtect가 엔드포인트에서 네트워크 활동을 필터링하고 모니터링할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



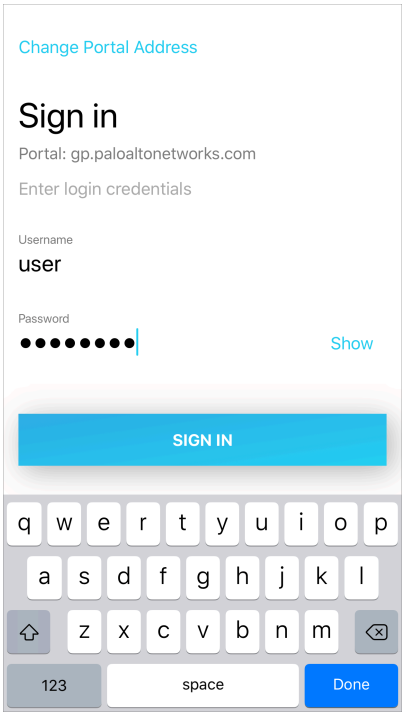
2. iPhone 또는 iPad 암호를 입력하여 엔드포인트에 VPN 구성을 추가할 것인지 확인합니다.



6. (선택 사항) 엔드포인트가 포털 서버 인증서를 사용하여 GlobalProtect 포털의 ID를 확인할 수 없는 경우 **서버 ID를 확인할 수 없음** 메시지가 표시됩니다. 인증서를 신뢰할 수 있는 경우 계속을 탭하여 연결을 계속하십시오.
7. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 로그인합니다.

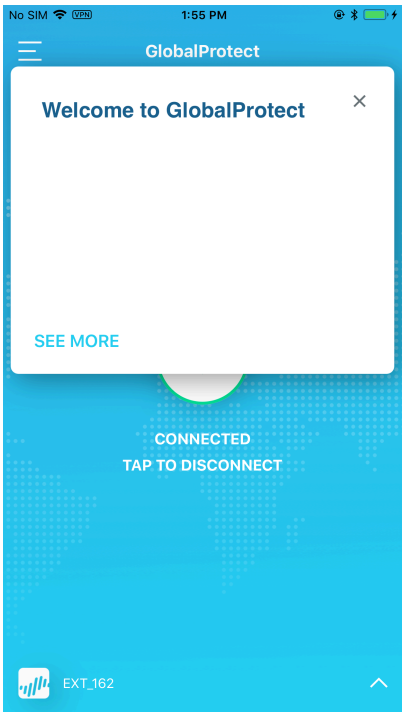
 ©2023 Palo Alto Networks, Inc.

관리자가 생체 인식(지문 또는 iOS X 디바이스의 경우 Face ID) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호를 사용하여 두 번 로그인해야 합니다(저장하기 위해 한 번, 인증하기 위해 한 번 더). 그 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

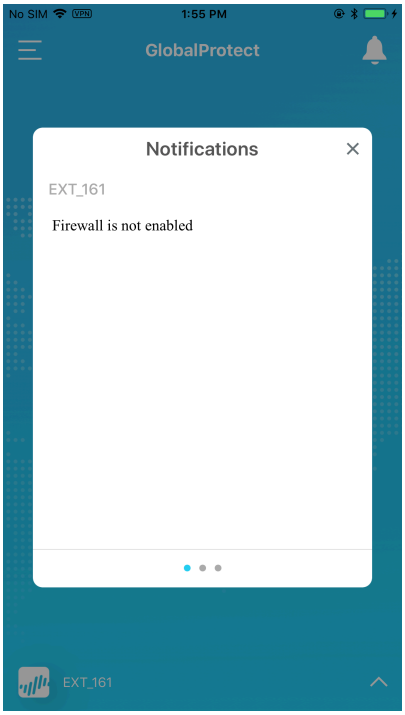


8. (선택 사항) 다단계 인증을 사용하는 경우 로그인한 후 엔드포인트로 전송되는 GlobalProtect 인증 코드를 입력한 다음 계속을 누릅니다.
9. (선택 사항) 관리자가 GlobalProtect 앱이 환영 메시지를 표시하도록 구성한 경우 연결하면 환영 메시지가 표시됩니다. 환영 메시지를 닫고 홈 화면으로 이동합니다.

 ©2023 Palo Alto Networks, Inc.

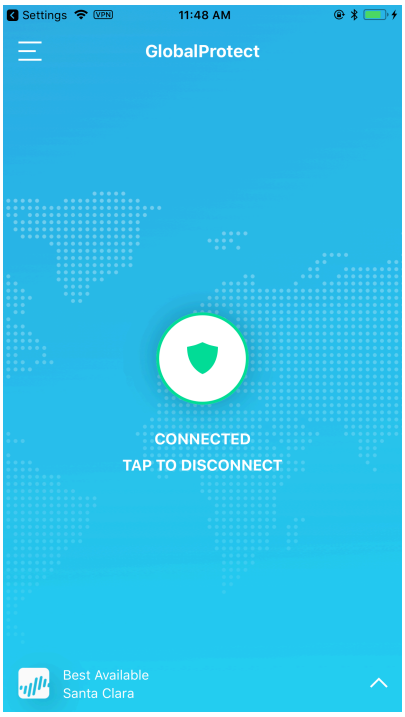


10. (선택 사항) 앱에 알림이 있는 경우 연결에 성공하면 알림 대화 상자가 표시됩니다. 알림 대화 상자를 닫아 홈 화면으로 이동합니다.



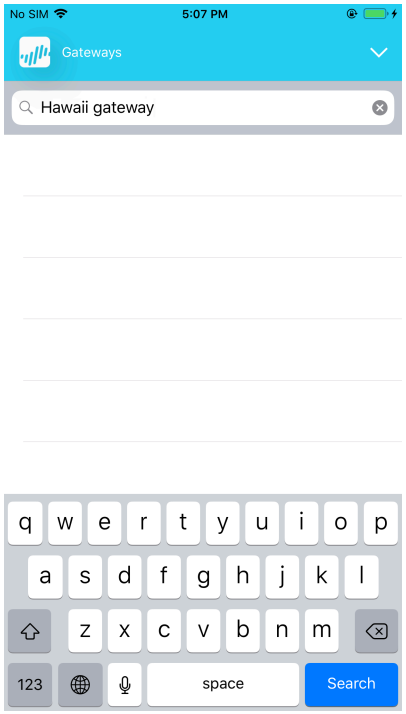
11. 홈 화면이 나타나면 연결이 설정되었는지 확인합니다. 연결에 성공하면 홈 화면에 연결됨 상태가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



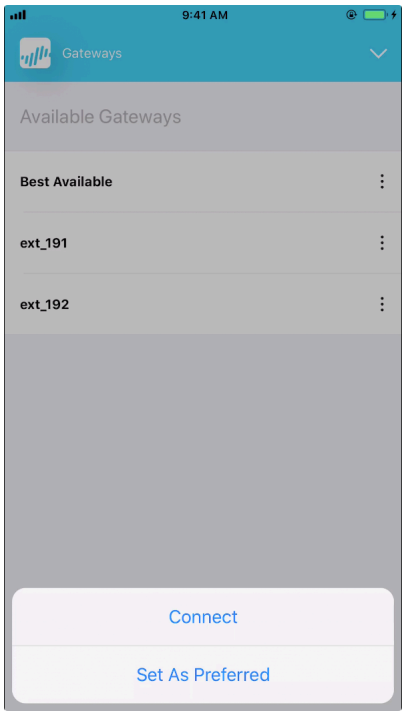
12. (선택 사항) 기본적으로 엔드포인트는 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 홈 화면 하단의 게이트웨이 드롭다운을 탭하고 다음 옵션 중 하나를 사용합니다.

- 게이트웨이를 수동으로 선택합니다(외부 게이트웨이만 해당). 관리자가 포털 에이전트 구성에서 10개 이상의 수동 외부 게이트웨이를 구성한 경우 게이트웨이 검색 옵션을 사용하여 특정 게이트웨이를 찾을 수도 있습니다.

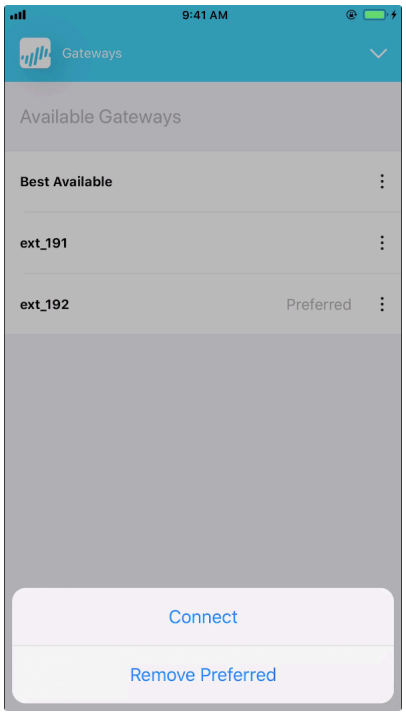


 ©2023 Palo Alto Networks, Inc.

- 기본 게이트웨이로 설정하려는 게이트웨이의 추가 옵션(⋮) 아이콘을 누른 다음 기본 설정으로 설정을 탭하여 기본 게이트웨이를 할당하고 자동으로 연결합니다. 또는 게이트웨이를 길게 누르고(길게 탭) 다음 기본 설정으로 설정할 수 있습니다.



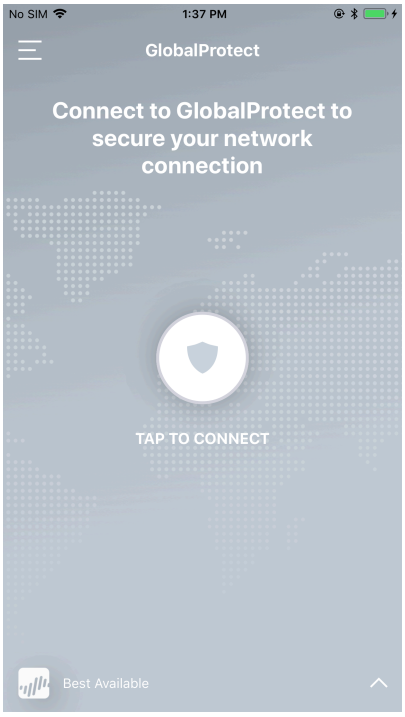
기본 게이트웨이 할당을 제거하려면 기본 게이트웨이에 대한 추가 옵션(⋮) 아이콘을 누른 다음 기본 게이트웨이 삭제를 누릅니다. 또는 게이트웨이를 길게 누르고 (길게 탭) 기본 설정 삭제를 할 수 있습니다.



 ©2023 Palo Alto Networks, Inc.

- 온디맨드(원격 액세스 VPN) 연결 경험:

  GlobalProtect 관리자가 온디맨드 연결 방법으로 GlobalProtect를 구성하는 경우 수동으로 연결을 시작하려면 GlobalProtect 앱을 실행해야 합니다. 연결이 시작된 후 탭하여 연결하여 GlobalProtect 연결을 설정할 수 있습니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하면 추가 사용자 상호 작용 없이 연결이 설정됩니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하지 않은 경우 로그인하여 연결을 설정해야 합니다.



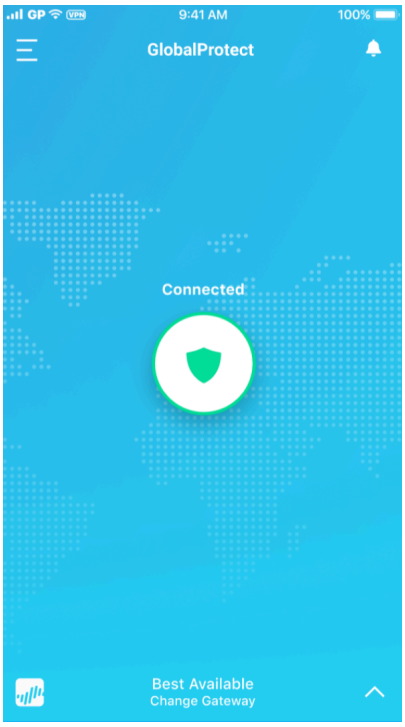
- 항상 켬 연결 환경

  GlobalProtect 관리자가 항상 켬 연결 방법을 사용하여 GlobalProtect를 구성하면 연결이 자동으로 시작됩니다. 관리자가 사용자 자격 증명을 저장하도록 GlobalProtect 앱을 구성했는지 여부에 따라 앱을 실행하지 않고도 GlobalProtect 연결을 설정할 수 있습니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하면 사용자 상호 작용 없이 연결이 자동으로 설정됩니다. 관리자가

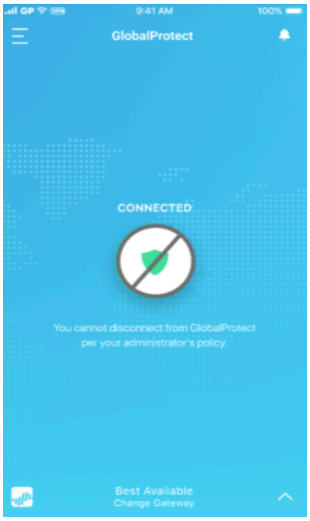
 ©2023 Palo Alto Networks, Inc.

GlobalProtect에서 사용자 자격 증명 저장을 활성화하지 않은 경우 앱을 통해 로그인하여 연결을 설정해야 합니다.

- (선택 사항) 관리자가 항상 켬 연결 방법을 사용하여 GlobalProtect를 구성한 경우 연결이 자동으로 시작됩니다. 홈 화면에 연결됨 상태가 표시됩니다.



항상 켬 연결 방식을 사용하면 연결 아이콘을 탭하려고 할 때 연결이 끊기지 않도록 홈 화면에 연결 해제 메시지가 표시된 연결됨 상태가 표시됩니다.

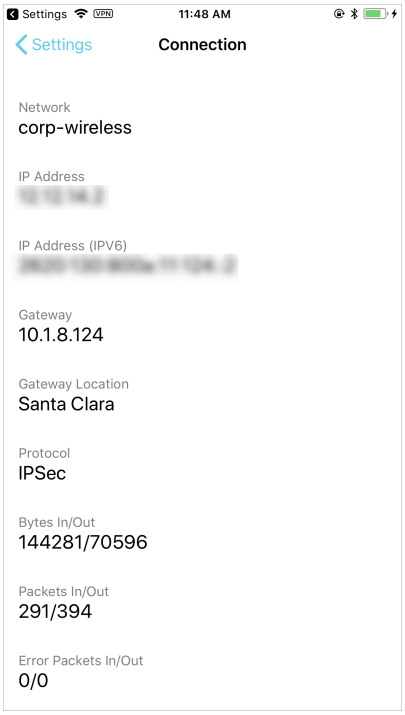


 ©2023 Palo Alto Networks, Inc.

STEP 2 | GlobalProtect 연결에 대한 정보를 봅니다.

GlobalProtect 연결을 설정한 후 GlobalProtect 앱을 실행합니다. 설정 아이콘을 탭하여 설정 메뉴를 엽니다. 설정 메뉴에서 설정을 탭하여 포털 주소 및 연결 상태를 포함하여 연결에 대한 정보를 봅니다.

- 다른 GlobalProtect 포털에 연결하려면 포털 주소를 누릅니다. 메시지가 표시되면 새 포털 주소를 입력한 다음 연결을 탭합니다.
- 외부 게이트웨이에 연결된 경우 연결 상태를 탭하여 연결에 대한 추가 세부 정보 (네트워크 SSID 및 게이트웨이 IP 주소/FQDN 포함) 를 볼 수 있습니다.



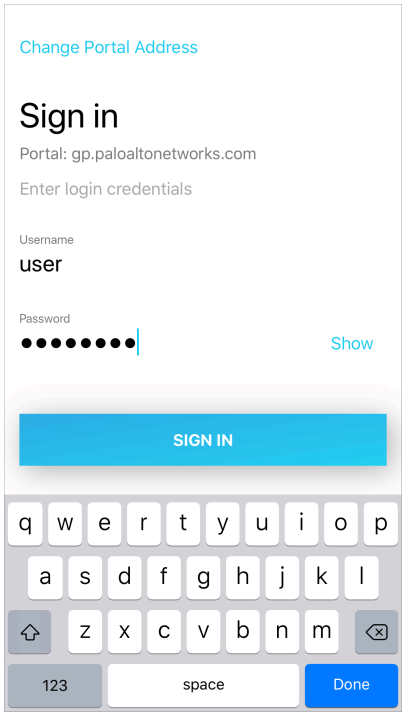
STEP 3 | (선택 사항) 저장된 암호를 변경합니다.

GlobalProtect 관리자가 GlobalProtect 포털 에이전트가 사용자 자격 증명을 저장하도록 구성하면 자격 증명이 GlobalProtect 앱에 자동으로 저장됩니다. 암호가 만료되거나 RADIUS 또는 AD 관리자가 다음 로그인 시 암호 변경을 요구하는 경우 앱에서 암호를 업데이트할 수 있습니다. 이 기능은 보호된 확장 프로그램 가능 인증 프로토콜 Microsoft 챌린지 핸드셰이크 인증 프로토콜 버전 2(PEAP-MSCHAPv2)를 사용하여 RADIUS 서버에서 인증된 경우에만 활성화됩니다.

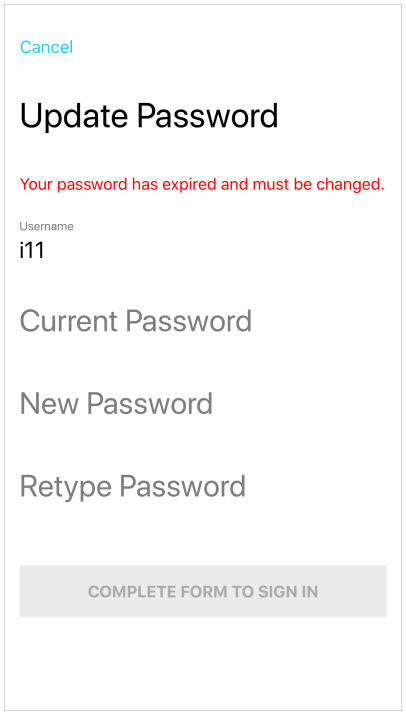
1. GlobalProtect 앱을 사용합니다.
2. 홈 화면에서 탭하여 연결합니다.

 ©2023 Palo Alto Networks, Inc.

3. (선택 사항) 메시지가 표시되면 이전 사용자 이름과 암호를 입력한 다음 로그인합니다.



4. GlobalProtect 앱에서 **암호를 업데이트**하라는 메시지가 표시되면 현재 암호와 새 암호를 차례로 입력합니다.

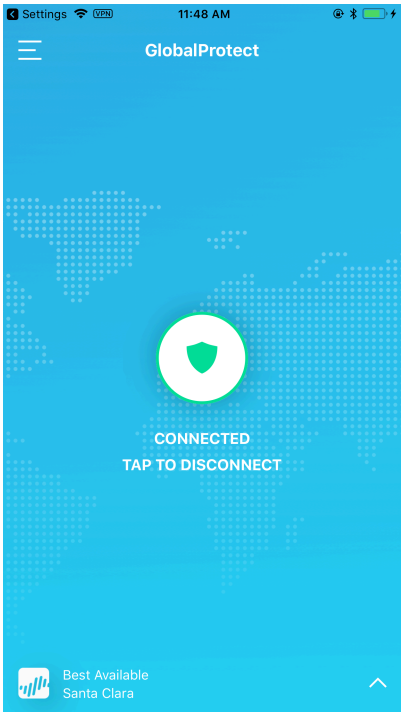


5. 암호를 다시 입력하여 새 암호를 확인합니다.
6. 로그인하여 새 암호로 GlobalProtect에 다시 연결합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (선택 사항) GlobalProtect와의 연결을 끊습니다.

관리자가 온디맨드 연결 방식으로 GlobalProtect를 구성한 경우 홈 화면에서 탭하여 연결을 끊을 수 있습니다.



 ©2023 Palo Alto Networks, Inc.

iOS용 GlobalProtect 앱에서 문제 보고하기

네트워크 성능이 저하되거나 포털 및 게이트웨이와의 연결이 설정되지 않는 등의 비정상적인 동작이 발생하는 경우 관리자가 액세스할 수 있는 Cortex Data Lake에 직접 문제를 보고할 수 있습니다. 더 이상 이메일을 통해 GlobalProtect 앱 로그를 수동으로 수집 및 전송하거나 클라우드 드라이브에 저장할 필요가 없습니다.

GlobalProtect 앱에 문제 보고 옵션을 표시하려면 관리자가 ***GlobalProtect*** 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화해야 합니다.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

1. GlobalProtect 앱을 사용합니다.
2. GlobalProtect 포털 주소를 입력합니다.
3. (선택 사항) 연결 모드에 따라 연결을 탭하여 연결을 시작합니다.
4. GlobalProtect가 엔드포인트에 VPN 구성을 추가하도록 허용합니다. 이 설정을 사용하면 VPN을 사용할 때 GlobalProtect가 엔드포인트에서 네트워크 활동을 필터링하고 모니터링할 수 있습니다.
5. iPhone 또는 iPad 암호를 입력하여 엔드포인트에 VPN 구성을 추가할 것인지 확인합니다.
6. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 로그인합니다.
7. 홈 화면이 나타나면 연결이 설정되었는지 확인합니다. 연결에 성공하면 홈 화면에 연결됨 상태가 표시됩니다 .
8. (선택 사항) 기본적으로 엔드포인트는 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 홈 화면 하단의 게이트웨이 드롭다운을 탭한 다음 목록에서 게이트웨이를 선택합니다(외부 게이트웨이만 해당).

STEP 2 | GlobalProtect 연결에 대한 정보를 봅니다.

GlobalProtect 연결을 설정한 후 GlobalProtect 앱을 실행합니다. 설정 아이콘을 탭하여 설정 메뉴를 엽니다. 설정 메뉴에서 설정을 탭하여 포털 주소 및 연결 상태를 포함하여 연결에 대한 정보를 봅니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 최종 사용자의 엔드포인트에서 GlobalProtect 앱의 문제를 보고합니다.

앱을 시작한 후 도움말을 탭하여 엔드포인트에서 문제를 보고합니다.

1. 문제 신고를 탭합니다.

2. 진단 테스트를 실행하고 진단 로그를 포함하도록 GlobalProtect 앱을 활성화합니다. 진단 및 문제 해결 로그가 모두 수집되어 간결한 문제 해결 보고서로 Cortex Data Lake에 전송됩니다.

   진단 테스트가 완료되면 GlobalProtect 디버그 로그 파일이 엔드포인트에서 Cortex Data Lake로 업로드됩니다.

 ©2023 Palo Alto Networks, Inc.

> 앱에서 진단 테스트를 실행하고 진단 로그를 포함하도록 설정하지 않으면 문제 해결 로그만 수집되어 압축 문제 해결 보고서로 ***Cortex Data Lake***에 전송됩니다. ***GlobalProtect*** 앱은 ***`.json`*** 형식으로 자동 생성되는 보고서 파일(***pan_gp.trb.log*** 또는 ***pan_gp_trbl.log***)을 확인합니다. 문제 해결 로그에서 문제가 발견되지 않은 경우 알림 메시지가 표시됩니다. 다시 시도를 클릭하여 ***pan_gp.trb*.log*** 파일이 있는지 확인합니다.

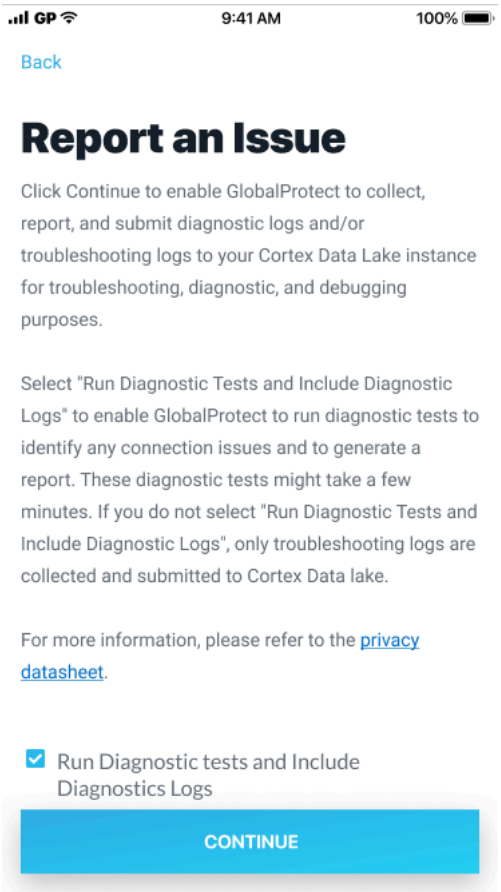
3. 진단 테스트 실행 및 진단 로그 포함 확인란을 선택합니다.
4. 앱이 문제 해결 로그를 만들고 관리자의 Cortex Data Lake 인스턴스로 보고서를 보낼 수 있도록 허용하려면 계속을 누릅니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다. GlobalProtect 앱은 터널을 사용하거나 터널 없이 진단 테스트를 실행할 수 있습니다. 예를 들어

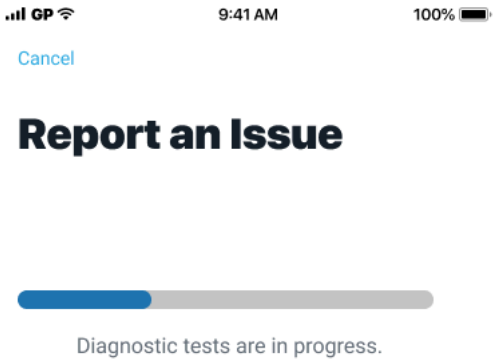
 ©2023 Palo Alto Networks, Inc.

앱이 터널을 통해 진단 테스트를 연결하고 실행하기 전에 GlobalProtect 로그인 자격 증명을 입력할 수 있습니다.



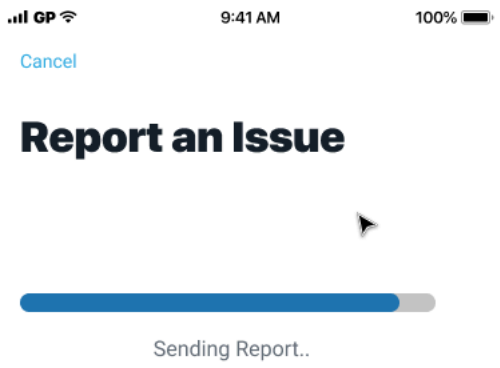
진단 테스트 실행 및 진단 로그 포함 확인란을 선택한 경우에만 앱이 진단 테스트를 실행하고 있음을 확인하는 메시지가 팝업됩니다.

 ©2023 Palo Alto Networks, Inc.



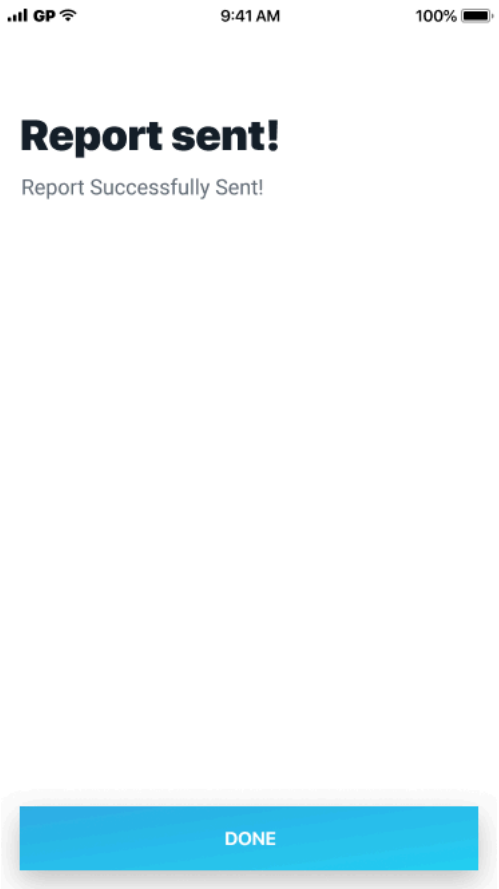
앱이 Cortex Data Lake로 보고서를 보내고 있음을 확인하는 메시지가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



5. 완료를 탭하여 앱이 보고서를 Cortex Data Lake로 전송했는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

iOS용 GlobalProtect 앱 제거

다음 단계를 사용하여 iOS 엔드포인트에서 GlobalProtect 앱을 제거하십시오. 앱을 제거하면 더 이상 기업 네트워크에 VPN으로 액세스할 수 없으며 엔드포인트가 회사의 보안 정책에 의해 보호되지 않는다는 점에 유의하십시오.

STEP 1 | GlobalProtect 앱 아이콘이 흔들릴 때까지 길게 탭합니다.

STEP 2 | 아이콘의 왼쪽 상단 모서리에 있는 **X**를 탭합니다.

STEP 3 | 메시지가 표시되면 GlobalProtect를 삭제합니다.

STEP 4 | 완료를 탭하거나 홈 버튼을 탭하여 홈 화면으로 돌아갑니다.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Android용 GlobalProtect 앱

GlobalProtect™는 엔드포인트(데스크톱 컴퓨터, 노트북, 태블릿 또는 스마트폰)에서 실행되는 애플리케이션으로, 회사 네트워크의 중요한 리소스를 보호하는 것과 동일한 보안 정책을 사용하여 사용자를 보호합니다. GlobalProtect™는 인트라넷, 사설 클라우드, 공용 클라우드 및 인터넷 트래픽을 보호하고 전 세계 어디에서나 회사 리소스에 액세스할 수 있도록 합니다.

다음 주제에서는 Android용 GlobalProtect 앱을 설치하고 사용하는 방법을 설명합니다.

> Android용 GlobalProtect 앱 다운로드 및 설치하기
> Chromebook에 Android용 GlobalProtect 앱 다운로드 및 설치하기
> Android용 GlobalProtect 앱 사용하기
> Android용 GlobalProtect 앱에서 문제 보고하기
> Android용 GlobalProtect 앱 연결 해제
> Android용 GlobalProtect 앱 제거
> Chromebook에서 Android용 GlobalProtect 앱 제거

Android용 GlobalProtect 앱 다운로드 및 설치하기

Android 엔드포인트를 GlobalProtect 네트워크에 연결하려면 먼저 앱을 다운로드하고 설치해야 합니다. Android 엔드포인트가 모바일 디바이스 관리(MDM) 시스템에서 관리되는 경우 관리자가 자동으로 GlobalProtect 앱을 엔드포인트에 푸시하고 VPN 설정을 구성했을 수 있습니다. Android 엔드포인트에 GlobalProtect 앱이 아직 없는 경우 Google Play에서 다운로드할 수 있습니다.

앱을 다운로드하기 전에 관리자로부터 GlobalProtect 포털의 IP 주소 또는 FQDN을 받아야 합니다. 또한 관리자는 포털 및 게이트웨이에 연결하는 데 사용할 수 있는 사용자 이름과 암호를 확인해야 합니다. 이것은 일반적으로 회사 네트워크에 연결하는 데 사용하는 것과 동일한 사용자 이름 및 암호입니다.

필요한 정보를 수집한 후 다음과 같이 앱을 다운로드하고 설치할 수 있습니다.

STEP 1 | Google Play를 실행합니다.

STEP 2 | **`GlobalProtect`**를 검색합니다.

STEP 3 | 검색 결과에서 **GlobalProtect**를 선택합니다.

STEP 4 | GlobalProtect 앱 제품 페이지에서 설치를 탭합니다.

STEP 5 | 메시지가 표시되면 GlobalProtect가 액세스해야 하는 정보를 검토하고 수락합니다.

 ©2023 Palo Alto Networks, Inc.

Chromebook에 Android용 GlobalProtect 앱 다운로드 및 설치하기

Chromebook에서 Android용 GlobalProtect 앱을 사용하려면 앱을 다운로드하고 설치해야 합니다. Chromebook이 Workspace ONE 또는 Google 관리 콘솔에서 관리되는 경우 관리자가 자동으로 GlobalProtect 앱을 엔드포인트에 푸시하고 VPN 설정을 구성했을 수 있습니다. Chromebook에 Android용 GlobalProtect 앱이 아직 설치되어 있지 않다면 Google Play 스토어에서 다운로드할 수 있습니다.

앱을 다운로드하기 전에 관리자로부터 GlobalProtect 포털의 IP 주소 또는 FQDN을 받아야 합니다. 또한 관리자는 포털 및 게이트웨이에 연결하는 데 사용할 수 있는 사용자 이름과 암호를 확인해야 합니다. 이것은 일반적으로 회사 네트워크에 연결하는 데 사용하는 것과 동일한 사용자 이름 및 암호입니다.

필요한 정보를 수집한 후 다음과 같이 앱을 다운로드하고 설치할 수 있습니다.

> ***Android*용 *GlobalProtect* 앱은** 일부 Chromebook에서만 지원됩니다. ***Chrome OS*용 *GlobalProtect* 앱 버전 *4.1.x*를 사용 중이었다면 해당 앱을 더 이상 사용할 수 없습니다. *Android* 앱을 지원하는 *Chrome OS* 시스템으로 업그레이드하고 *Android*용 *GlobalProtect* 앱을 사용하는 것이 좋습니다.**

STEP 1 | Chromebook에서 Google Play 스토어 앱을 활성화합니다.

1. (선택사항) Chromebook에서 Chrome OS 버전 52 이하를 실행하는 경우 Chromebook 운영체제를 업데이트하십시오.
2. Chromebook 화면의 오른쪽 하단 모서리에 있는 계정 사진을 클릭합니다.
3. 설정을 선택합니다.
4. Google Play 스토어 영역에서 **Chromebook**에서 **Google Play** 스토어를 활성화합니다.

   > 이 옵션을 사용할 수 없다면 ***Chromebook***에서 ***Android*** 앱을 지원하지 않는 것입니다.

5. 메시지가 표시되면 시작하기를 클릭하여 Google Play 스토어를 시작합니다.
6. 서비스 약관에 동의합니다.
7. 환영 페이지에서 Google Play 스토어에 로그인합니다.
8. 구글 플레이 서비스 약관에 동의합니다.

STEP 2 | Chromebook에 Android용 GlobalProtect 앱 엔드포인트를 다운로드하여 설치합니다.

1. Google Play 스토어 앱을 엽니다.
2. **`GlobalProtect`** 앱을 검색합니다.
3. GlobalProtect 앱 아이콘을 클릭합니다.
4. 설치를 클릭한 다음 화면의 지시에 따라 앱 설치를 완료합니다.

 ©2023 Palo Alto Networks, Inc.

Android용 GlobalProtect 앱 사용하기

이 항목은 설정에서 엔드포인트에 로그인한 후 GlobalProtect 로그인 자격 증명을 입력해야 하는 경우에만 적용됩니다(Single Sign-On은 비활성화됨).

일반적으로 조직에서는 GlobalProtect 사용자가 앱 설치 후 투명하게 로그인할 수 있도록 허용하는 것이 좋습니다. 투명한 GlobalProtect 로그인으로 엔드포인트에 로그인하면 GlobalProtect 앱이 자동으로 시작되어 추가 사용자 개입 없이 기업 네트워크에 연결됩니다.

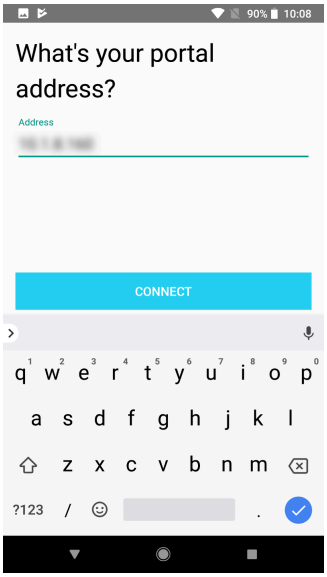
설정에 GlobalProtect 자격 증명을 입력해야 하는 경우 아래에서 해당 단계를 따르십시오.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

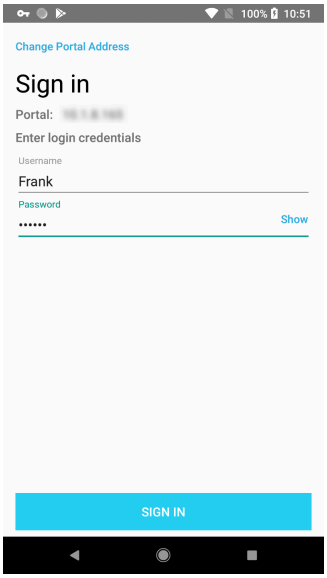
다음 워크플로 중 하나를 사용하여 GlobalProtect 포털 또는 게이트웨이에 연결하십시오.

- 첫 번째 연결 경험:
  1. GlobalProtect 앱을 사용합니다.
  2. GlobalProtect 포털 주소를 입력합니다.



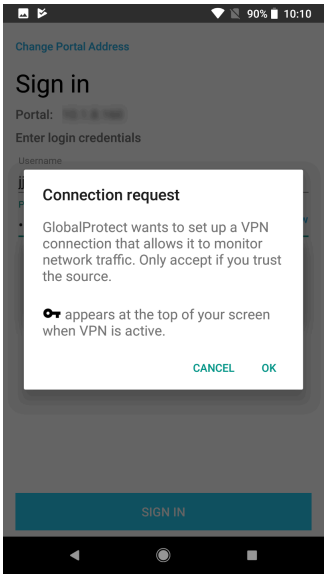
  3. (선택 사항) 연결 모드에 따라 연결을 탭하여 연결을 시작합니다.
  4. (선택 사항) 엔드포인트가 포털 서버 인증서를 사용하여 GlobalProtect 포털의 ID를 확인할 수 없는 경우 **서버 ID를 확인할 수 없음** 메시지가 표시됩니다. 인증서를 신뢰할 수 있는 경우 계속을 탭하여 연결을 계속하십시오.
  5. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 로그인합니다.

     관리자가 생체 인식(지문) 정보를 사용한 로그인을 허용한 경우 먼저 사용자 이름과 암호로 로그인한 다음 생체 인식 정보를 사용하여 로그인할 수 있습니다.

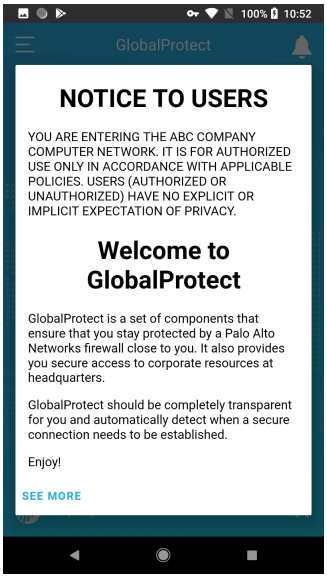


 ©2023 Palo Alto Networks, Inc.

6. **연결 요청** 메시지가 나타나면 확인을 탭하여 GlobalProtect가 엔드포인트에서 VPN 연결을 설정하도록 허용합니다.

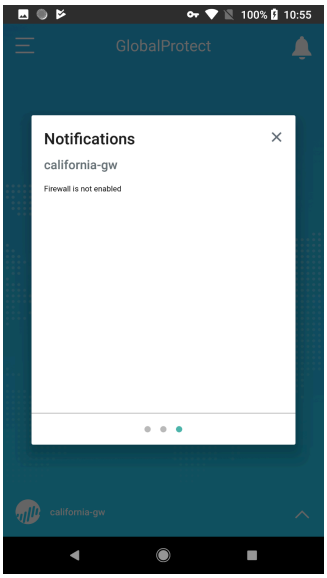


7. (선택 사항) 다단계 인증을 사용하는 경우 로그인한 후 엔드포인트로 전송되는 GlobalProtect 인증 코드를 입력한 다음 계속을 누릅니다.
8. (선택 사항) 관리자가 GlobalProtect 앱이 환영 메시지를 표시하도록 구성한 경우 연결하면 환영 메시지가 표시됩니다. 환영 메시지 바깥쪽을 탭하여 홈 화면으로 이동합니다.

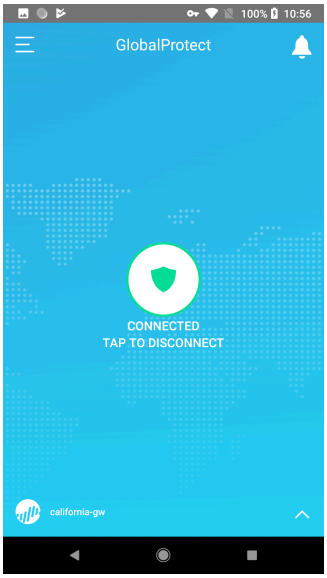


9. (선택 사항) 앱에 알림이 있는 경우 연결에 성공하면 알림 대화 상자가 표시됩니다. 알림 대화 상자를 닫아 홈 화면으로 이동합니다.

 ©2023 Palo Alto Networks, Inc.

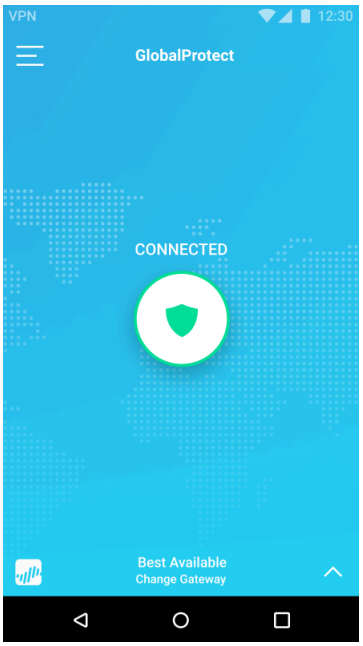


10. 홈 화면이 나타나면 연결이 설정되었는지 확인합니다. 연결에 성공하면 홈 화면에 연결됨 상태가 표시됩니다.

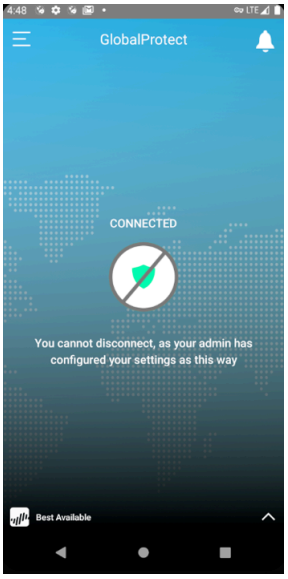


11. (선택 사항) 관리자가 항상 켬 연결 방법을 사용하여 GlobalProtect를 구성한 경우 연결이 자동으로 시작됩니다. 홈 화면에 연결됨 상태가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



항상 켬 연결 방식을 사용하면 연결 아이콘을 탭하려고 할 때 연결이 끊기지 않도록 홈 화면에 연결 해제 메시지가 표시된 연결됨 상태가 표시됩니다.



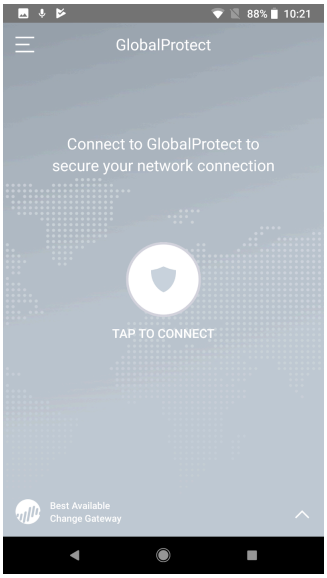
12. (선택 사항) 기본적으로 엔드포인트는 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 홈 화면 하단에서 게이트웨이 드롭다운을 탭한 다음 목록에서 게이트웨이를 선택합니다(외부 게이트웨이만 해당).

- 온디맨드(원격 액세스 VPN) 연결 경험:

  GlobalProtect 관리자가 온디맨드 연결 방법을 사용하여 GlobalProtect를 구성하는 경우 GlobalProtect 앱을 실행하여 연결을 수동으로 시작해야 합니다. 연결이 시작된 후 탭하여 연결하여 GlobalProtect 연결을 설정할 수 있습니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을

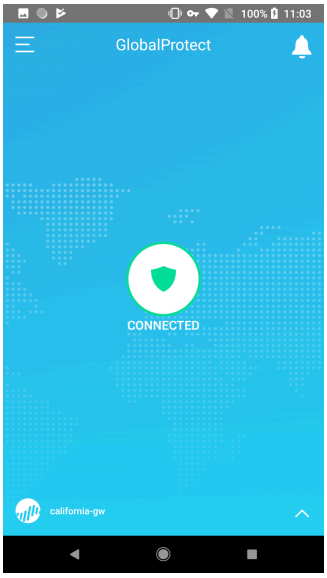
 ©2023 Palo Alto Networks, Inc.

활성화하면 추가 사용자 상호 작용 없이 연결이 설정됩니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하지 않은 경우 로그인하여 연결을 설정해야 합니다.



- 항상 켬 연결 경험:

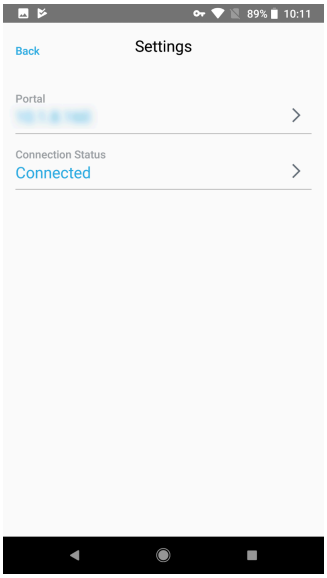
  GlobalProtect 관리자가 항상 켬 연결 방법을 사용하여 GlobalProtect를 구성하면 연결이 자동으로 시작됩니다. 관리자가 사용자 자격 증명을 저장하도록 GlobalProtect 앱을 구성했는지 여부에 따라 앱을 실행하지 않고도 GlobalProtect 연결을 설정할 수 있습니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하면 사용자 상호 작용 없이 연결이 자동으로 설정됩니다. 관리자가 GlobalProtect에서 사용자 자격 증명 저장을 활성화하지 않은 경우 앱을 통해 로그인하여 연결을 설정해야 합니다.



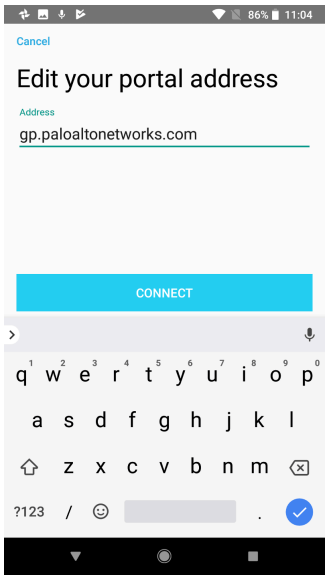
 ©2023 Palo Alto Networks, Inc.

STEP 2 | GlobalProtect 연결에 대한 정보를 봅니다.

GlobalProtect 연결을 설정한 후 GlobalProtect 앱을 실행합니다. 설정 아이콘을 탭하여 설정 메뉴를 엽니다. 설정 메뉴에서 설정을 탭하여 포털 주소 및 연결 상태를 포함하여 연결에 대한 정보를 봅니다.

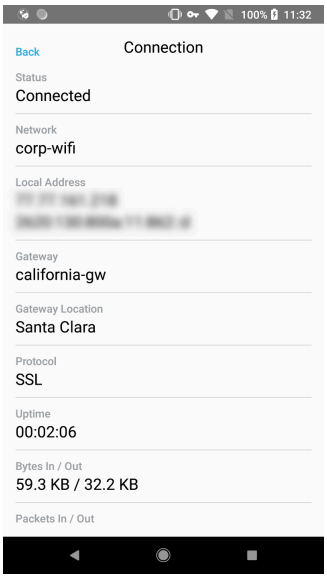


- 다른 GlobalProtect 포털에 연결하려면 포털 주소를 누릅니다. 메시지가 표시되면 새 포털 주소를 입력한 다음 연결을 탭합니다.



- 외부 게이트웨이에 연결된 경우 연결 상태를 탭하여 연결에 대한 추가 세부 정보 (네트워크 SSID 및 게이트웨이 IP 주소/FQDN 포함) 를 볼 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



STEP 3 | (선택 사항) 저장된 암호를 변경합니다.

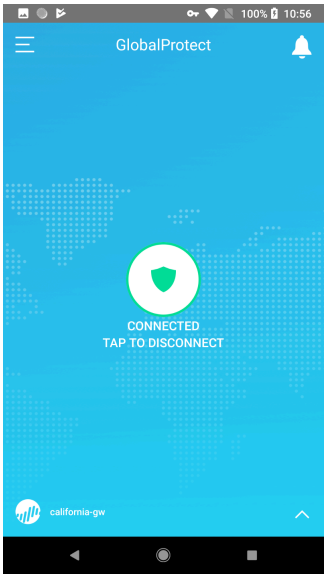
GlobalProtect 관리자가 GlobalProtect 포털 에이전트가 사용자 자격 증명을 저장하도록 구성하면 자격 증명이 GlobalProtect 앱에 자동으로 저장됩니다. 암호가 만료되거나 RADIUS 또는 AD 관리자가 다음 로그인 시 암호 변경을 요구하는 경우 앱에서 암호를 업데이트할 수 있습니다. 이 기능은 보호된 확장 프로그램 가능 인증 프로토콜 Microsoft 챌린지 핸드셰이크 인증 프로토콜 버전 2(PEAP-MSCHAPv2)를 사용하여 RADIUS 서버에서 인증된 경우에만 활성화됩니다.

1. GlobalProtect 앱을 사용합니다.
2. 홈 화면에서 탭하여 연결합니다.
3. (선택 사항) 메시지가 표시되면 이전 사용자 이름과 암호를 입력한 다음 로그인합니다.
4. GlobalProtect 앱에서 **암호를 업데이트**하라는 메시지가 표시되면 현재 암호와 새 암호를 차례로 입력합니다.
5. 암호를 다시 입력하여 새 암호를 확인합니다.
6. 로그인하여 새 암호로 GlobalProtect에 다시 연결합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (선택 사항) GlobalProtect와의 연결을 끊습니다.

관리자가 온디맨드 연결 방식으로 GlobalProtect를 구성한 경우 홈 화면에서 탭하여 연결을 끊을 수 있습니다.



 ©2023 Palo Alto Networks, Inc.

Android용 GlobalProtect 앱에서 문제 보고하기

네트워크 성능이 저하되거나 포털 및 게이트웨이와의 연결이 설정되지 않는 등의 비정상적인 동작이 발생하는 경우 관리자가 액세스할 수 있는 Cortex Data Lake에 직접 문제를 보고할 수 있습니다. 더 이상 이메일을 통해 GlobalProtect 앱 로그를 수동으로 수집 및 전송하거나 클라우드 드라이브에 저장할 필요가 없습니다.

GlobalProtect 앱에 문제 보고 옵션을 표시하려면 관리자가 ***GlobalProtect*** 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화해야 합니다.

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

1. GlobalProtect 앱을 사용합니다.
2. GlobalProtect 포털 주소를 입력합니다.
3. (선택 사항) 연결 모드에 따라 연결을 탭하여 연결을 시작합니다.
4. (선택 사항) 메시지가 표시되면 사용자 이름과 암호를 입력한 다음 로그인합니다.
5. 연결 요청 메시지가 나타나면 확인을 탭하여 GlobalProtect가 엔드포인트에서 VPN 연결을 설정하도록 허용합니다.
6. 홈 화면이 나타나면 연결이 설정되었는지 확인합니다. 연결에 성공하면 홈 화면에 연결됨 상태가 표시됩니다 .
7. (선택 사항) 기본적으로 엔드포인트는 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 홈 화면 하단의 게이트웨이 드롭다운을 탭한 다음 목록에서 게이트웨이를 선택합니다(외부 게이트웨이만 해당).

STEP 2 | GlobalProtect 연결에 대한 정보를 봅니다.

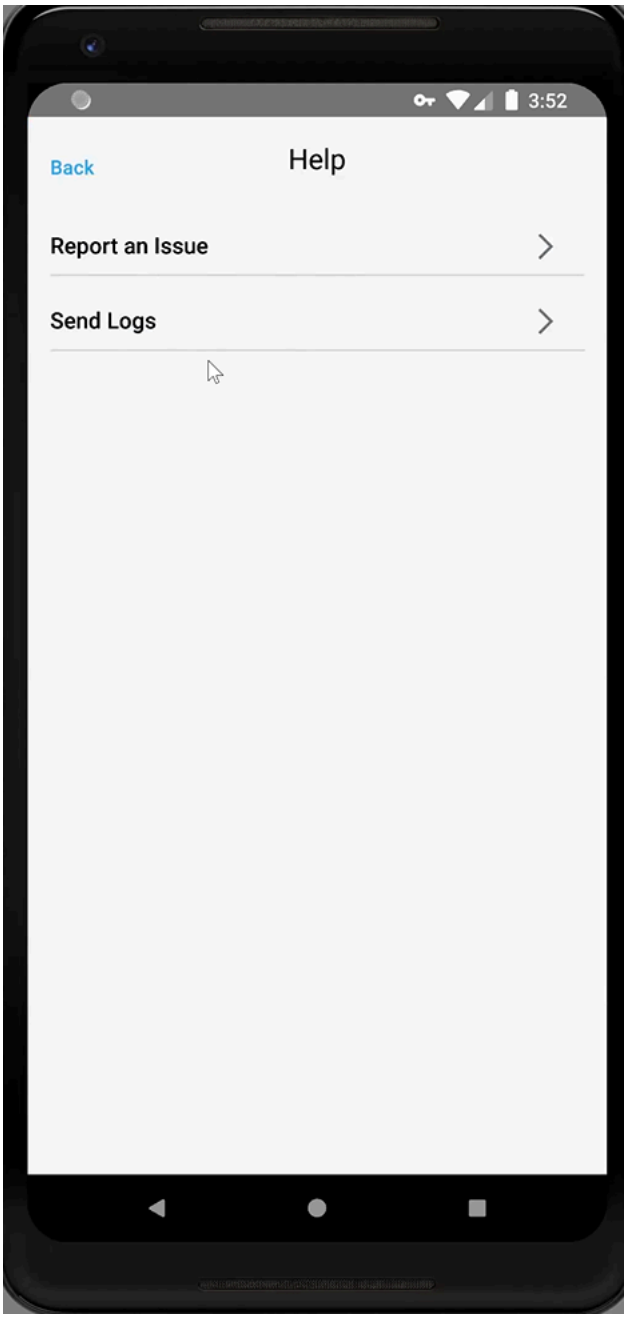
GlobalProtect 연결을 설정한 후 GlobalProtect 앱을 실행합니다. 설정 아이콘을 탭하여 설정 메뉴를 엽니다. 설정 메뉴에서 설정을 탭하여 포털 주소 및 연결 상태를 포함하여 연결에 대한 정보를 봅니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 최종 사용자의 엔드포인트에서 GlobalProtect 앱의 문제를 보고합니다.

앱을 시작한 후 도움말을 탭하여 엔드포인트에서 문제를 보고합니다.

1. 문제 신고를 탭합니다.



2. 진단 테스트를 실행하고 진단 로그를 포함하도록 GlobalProtect 앱을 활성화합니다. 진단 및 문제 해결 로그가 모두 수집되어 간결한 문제 해결 보고서로 Cortex Data Lake에 전송됩니다.

   진단 테스트가 완료되면 GlobalProtect 디버그 로그 파일이 엔드포인트에서 Cortex Data Lake로 업로드됩니다.

 ©2023 Palo Alto Networks, Inc.

> 앱에서 진단 테스트를 실행하고 진단 로그를 포함하도록 설정하지 않으면 문제 해결 로그만 수집되어 압축 문제 해결 보고서로 ***Cortex Data Lake***에 전송됩니다. ***GlobalProtect*** 앱은 ***`.json`*** 형식으로 자동 생성되는 보고서 파일(***pan_gp.trb.log*** 또는 ***pan_gp_trbl.log***)을 확인합니다. 문제 해결 로그에서 문제가 발견되지 않은 경우 알림 메시지가 표시됩니다. 다시 시도를 클릭하여 ***pan_gp.trb*.log*** 파일이 있는지 확인합니다.

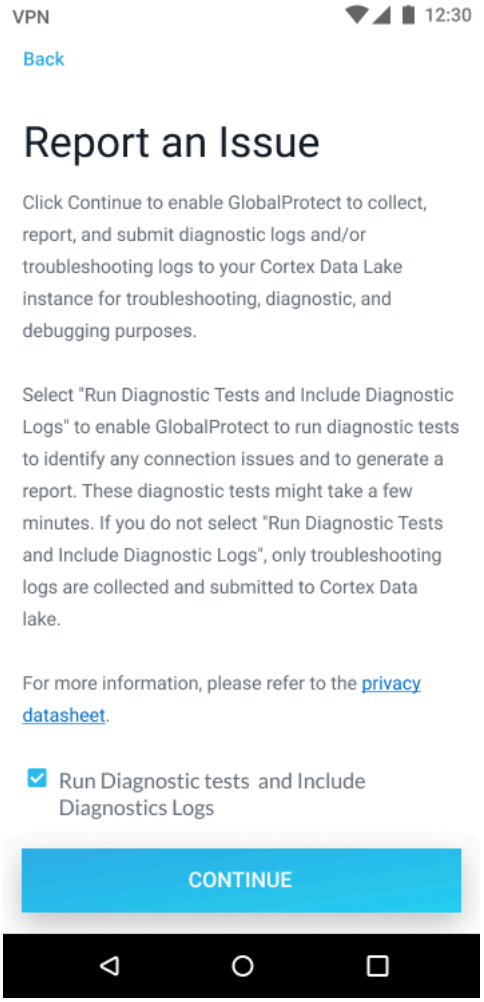
3. 진단 테스트 실행 및 진단 로그 포함 확인란을 선택합니다.
4. 앱이 문제 해결 로그를 만들고 관리자의 Cortex Data Lake 인스턴스로 보고서를 보낼 수 있도록 허용하려면 계속을 누릅니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다. GlobalProtect 앱은 터널을 사용하거나 터널 없이 진단 테스트를 실행할 수 있습니다. 예를 들어

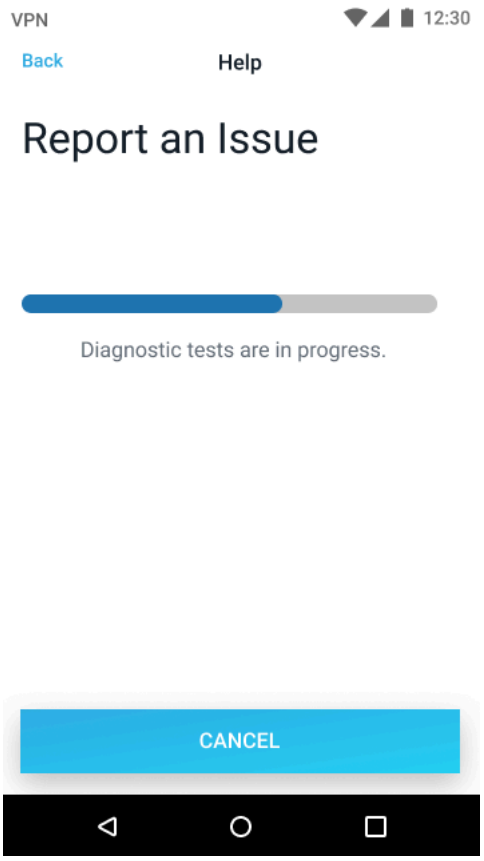
 ©2023 Palo Alto Networks, Inc.

앱이 터널을 통해 진단 테스트를 연결하고 실행하기 전에 GlobalProtect 로그인 자격 증명을 입력할 수 있습니다.



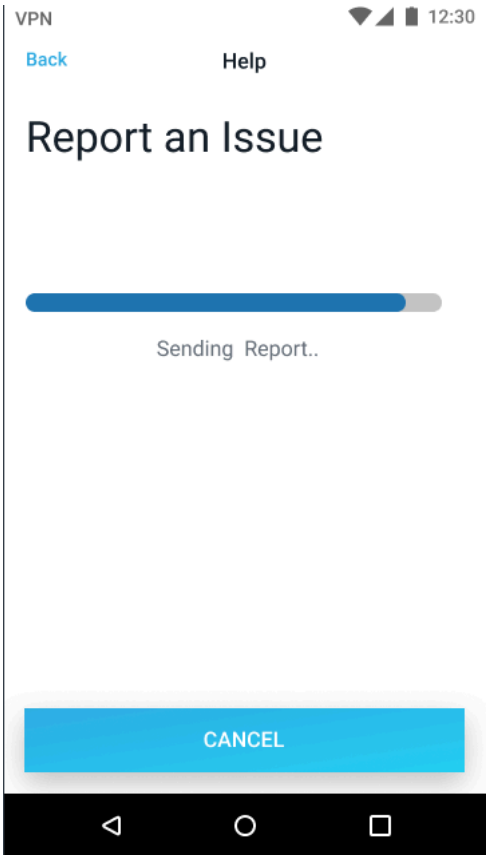
진단 테스트 실행 및 진단 로그 포함 확인란을 선택한 경우에만 앱이 진단 테스트를 실행하고 있음을 확인하는 메시지가 팝업됩니다.

 ©2023 Palo Alto Networks, Inc.



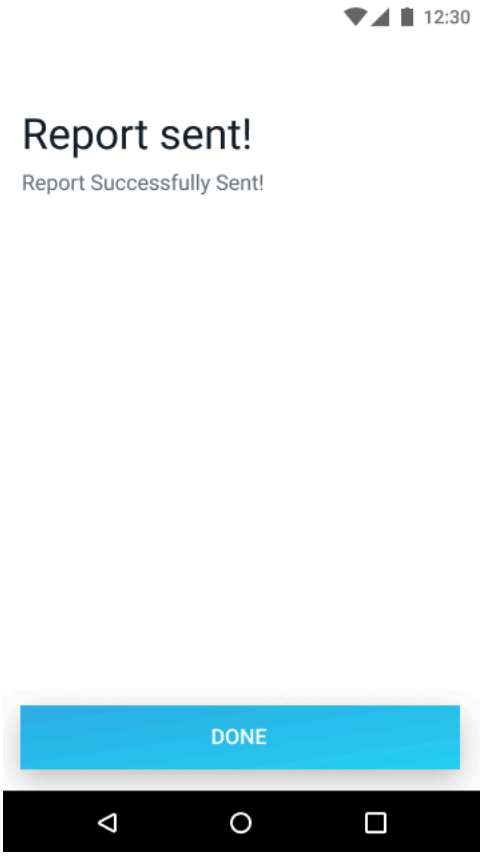
앱이 Cortex Data Lake로 보고서를 보내고 있음을 확인하는 메시지가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



5. 완료를 탭하여 앱이 보고서를 Cortex Data Lake로 전송했는지 확인합니다.

 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

Android용 GlobalProtect 앱 연결 해제

관리자가 GlobalProtect 연결 방법을 항상 켬으로 구성한 경우 GlobalProtect 앱의 연결을 끊을 수 있습니다. 예를 들어 호텔에서 GlobalProtect 가상 사설망(VPN)이 작동하지 않고 VPN 오류로 인해 인터넷에 연결할 수 없는 경우 앱 연결을 끊을 수 있습니다. GlobalProtect 앱의 연결을 끊은 후 보안되지 않은 통신(VPN 없이)을 사용하여 인터넷에 연결할 수 있습니다.

GlobalProtect 앱의 연결을 끊을 수 있는 방법, 시간 및 횟수는 관리자가 GlobalProtect 서비스(PanGPS)를 구성하는 방법에 따라 다릅니다. 이 구성을 사용하면 앱 연결을 완전히 끊지 못하거나 챌린지에 올바르게 응답한 후에만 앱 연결을 끊을 수 있습니다.

구성에 챌린지가 포함된 경우 GlobalProtect 앱은 다음 중 하나를 묻는 메시지를 표시합니다.

- 앱 연결을 해제하려는 이유
- 암호

챌린지에 암호와 관련된 경우 전화로 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 문의하는 것이 좋습니다. 관리자는 일반적으로 이메일(신규 GlobalProtect 사용자의 경우)을 통하거나 조직의 웹 사이트에 게시하여 암호를 미리 제공합니다. 중단 또는 시스템 문제에 대한 응답으로 관리자는 전화로 암호를 제공할 수도 있습니다.

다음 단계에서는 앱 연결을 끊고 챌린지를 통과하는 방법을 설명합니다.

STEP 1 | GlobalProtect 앱의 연결을 끊습니다.

1. GlobalProtect 앱을 사용합니다.
2. 설정 아이콘을 탭하여 설정 메뉴를 엽니다.
3. 설정 메뉴에서 연결 해제를 누릅니다.

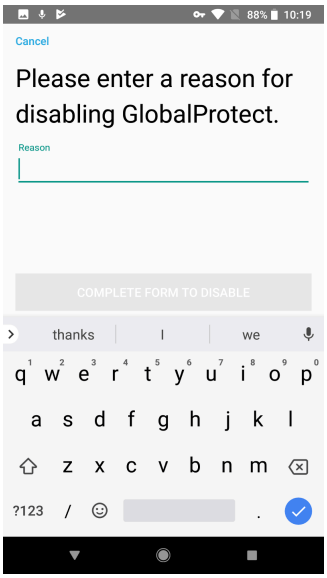
연결 해제 옵션은 ***GlobalProtect*** 에이전트 구성에서 앱 연결을 끊을 수 있는 경우에만 표시됩니다. 구성을 통해 챌린지에 응답할 필요 없이 ***GlobalProtect*** 앱의 연결을 끊을 수 있는 경우 추가 조치 없이 ***GlobalProtect*** 앱이 닫힙니다.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | 필요한 경우 하나 이상의 챌린지에 대응합니다.

메시지가 표시되면 다음 정보를 제공합니다.

- 이유—GlobalProtect 앱의 연결을 해제하는 이유입니다.



- 암호—앱 연결을 해제해야 하는 알려진 문제 또는 이벤트에 따라 관리자가 일반적으로 미리 제공하는 암호입니다.

 ©2023 Palo Alto Networks, Inc.

Android용 GlobalProtect 앱 제거

다음 단계를 사용하여 Android 엔드포인트에서 GlobalProtect 앱을 제거하십시오. 앱을 제거하면 더 이상 기업 네트워크에 VPN으로 액세스할 수 없으며 엔드포인트가 회사의 보안 정책에 의해 보호되지 않는다는 점에 유의하십시오.

STEP 1 | 설정 앱을 실행합니다.

STEP 2 | 앱 및 알림을 탭합니다.

STEP 3 | **GlobalProtect**를 탭합니다.

STEP 4 | 제거를 탭합니다.

 ©2023 Palo Alto Networks, Inc.

Chromebook에서 Android용 GlobalProtect 앱 제거

다음 단계에 따라 Chromebook에서 Android용 GlobalProtect 앱을 제거합니다. 앱을 제거하면 더 이상 기업 네트워크에 VPN으로 액세스할 수 없으며 엔드포인트가 회사의 보안 정책에 의해 보호되지 않는다는 점에 유의하십시오.

STEP 1 | Google Play 스토어 앱을 엽니다.

STEP 2 | 구글 플레이 검색창 옆에 있는 메뉴 버튼(☰)을 클릭합니다.

STEP 3 | 앱 및 게임 > 내 앱과 게임을 선택합니다.

STEP 4 | 설치됨을 선택합니다.

STEP 5 | 이 디바이스 영역에서 **GlobalProtect**를 선택합니다.

STEP 6 | 제거를 클릭합니다.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱

GlobalProtect™ 는 기업 네트워크의 중요한 리소스를 보호하는 동일한 보안 정책을 사용하여 사용자를 보호하기 위해 엔드포인트(데스크톱 컴퓨터, 노트북 또는 서버)에서 실행되는 프로그램입니다. GlobalProtect™는 인트라넷, 사설 클라우드, 공용 클라우드 및 인터넷 트래픽을 보호하고 전 세계 어디에서나 회사 리소스에 액세스할 수 있도록 합니다.

다음 섹션에서는 Linux용 GlobalProtect 앱을 설치하고 사용하기 위한 지침을 제공합니다.

> Linux용 GlobalProtect 앱 다운로드 및 설치하기
> Linux용 GlobalProtect 앱 사용하기
> Linux용 GlobalProtect 앱에서 문제 보고하기
> Linux용 GlobalProtect 앱 비활성화
> Linux용 GlobalProtect 앱 제거

Linux용 GlobalProtect 앱 다운로드 및 설치하기

GlobalProtect는 Linux 디바이스에 GlobalProtect 앱을 설치하는 두 가지 방법, 즉 GUI 기반 설치 버전과 CLI 버전을 제공합니다. 그래픽 인터페이스를 지원하는 지원되는 Linux 운영 체제를 사용하는 경우 GUI 버전의 GlobalProtect를 설치할 수 있습니다. 그렇지 않으면 CLI 버전의 GlobalProtect 앱을 다운로드하여 설치합니다.

- Linux용 GlobalProtect의 GUI 버전 다운로드 및 설치하기
- Linux용 GlobalProtect의 CLI 버전을 다운로드하고 설치합니다.

Linux용 GlobalProtect의 GUI 버전 다운로드 및 설치하기

Linux 디바이스가 그래픽 사용자 인터페이스를 지원하는 경우 다음 단계를 완료하여 Linux용 GlobalProtect GUI 버전을 설치하십시오.

STEP 1 | Linux용 GlobalProtect 앱을 다운로드합니다.

1. 고객 지원 포털에 로그인합니다. 사용자 이름 및 암호 자격 증명을 입력하면 인증되고 지원 사이트에 로그인됩니다.
2. 업데이트 > 소프트웨어 업데이트를 선택합니다.
3. Linux용 GlobalProtect 에이전트로 필터링하고 관련 TGZ 파일을 다운로드합니다.
4. 패키지에서 파일을 추출합니다.

```
user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
 ./ ./GlobalProtect_deb-6.0.0.0-62.deb ./
GlobalProtect_deb_arm-6.0.0.0-62.deb ./
GlobalProtect_rpm-6.0.0.0-62.rpm ./
GlobalProtect_rpm_arm-6.0.0.0-62.rpm ./
GlobalProtect_tar-6.0.0.0-62.tgz ./
GlobalProtect_tar_arm-6.0.0.0-62.tgz ./
GlobalProtect_UI_deb-6.0.0.0-62.deb ./
GlobalProtect_UI_rpm-6.0.0.0-62.rpm ./
GlobalProtect_UI_tar-6.0.0.0-62.tgz ./manifest ./relinfo
```

지원되는 운영 체제 버전에 대한 여러 설치 패키지(Debian 및 Ubuntu용 DEB, CentOS 및 Red Hat용 RPM)가 표시됩니다. GUI 버전의 패키지는 GlobalProtect_UI 접두어로 표시됩니다.

STEP 2 | (선택 사항) Linux 엔드포인트에서 수동 프록시 서버 구성을 사용해야 하는 경우 프록시 설정을 구성합니다.

> *Linux용 GlobalProtect* 앱은 기본 프록시 서버 구성만 지원하지만 프록시 자동 구성*(PAC)* 파일 및 프록시 인증 사용은 지원하지 않습니다.

Linux용 GlobalProtect 앱은 `/etc/environment` 파일의 `HTTP_PROXY`, `HTTPS_PROXY` 및 `NO_PROXY` 환경 변수에서 프록시 설정을 가져옵니다. 나중에 시스템 프록시 구성을 변경하는 경우

 ©2023 Palo Alto Networks, Inc.

GlobalProtect가 실행되는 터미널이 프록시 환경 변수를 사용하는지 확인합니다. 새 설정이 표시되지 않으면 로그아웃했다가 다시 로그인하여 새로운 설정을 적용합니다.

HTTP_PROXY 변수 또는 *HTTPS_PROXY* 변수를 구성한 경우 *GlobalProtect* 포털이 *NO_PROXY* 변수에 대해 구성된 설정과 일치하는지 확인합니다.

1. Linux 엔드포인트에서 프록시를 설정하려면 `HTTP_PROXY` 환경 변수 또는 `HTTPS_PROXY` 환경 변수(예: `HTTPS_PROXY="https://yourproxy.local:8080"`)를 편집합니다.
2. 프록시에서 제외할 IP 주소 또는 도메인 이름을 구성하려면 `NO_PROXY` 환경 변수(예: `NO_PROXY="www.gpqa.com"`)를 편집합니다.

   쉼표를 사용하여 여러 IP 주소 또는 도메인 이름을 구분합니다. GlobalProtect 앱 5.1.6부터 IP 주소 또는 도메인 이름에 와일드카드 문자(*)를 사용할 수 있습니다(예: `NO_PROXY="*.domain.com"`).

STEP 3 | (선택 사항) 인증서를 가져오려면 다음 단계를 완료하십시오.

인증서 기반 인증을 위해 엔드포인트에 클라이언트 인증서를 사전 배포하려는 경우 인증서를 엔드포인트에 복사하고 GlobalProtect 앱에서 사용할 수 있도록 가져올 수 있습니다. **`globalprotect import-certificate --location<`*`location`*`>`** 명령을 사용하여 엔드포인트에서 인증서를 가져옵니다. 메시지가 표시되면 인증서 암호를 제공해야 합니다.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 암호를 입력하십시오. 인증서
를 가져왔습니다.
```

STEP 4 | Linux용 GlobalProtect 앱의 GUI 버전을 설치합니다.

루트 권한을 사용하여 앱을 설치하고 GlobalProtect 앱에 필요한 누락된 패키지를 자동으로 추가하는 설치 방법을 사용합니다.

Debian과 Ubuntu의 경우, **`sudo apt-get install <`*`gp-app-pkg`*`>`** 명령을 사용합니다.

여기서 ***`<gp-app-pkg>`*** 은(는) Linux 버전에 대한 UI 배포 패키지의 경로입니다.

다음 예에서는 패키지 관리자에게 GlobalProtect_UI_deb-6.0.0.0-12.deb UI 배포 패키지를 설치하도록 지시합니다.

```
user@linuxhost:~$ sudo apt-get install
 GlobalProtect_UI_deb-6.0.0.0-12.deb gpqa의 [sudo] 암호: 패키지 목
록을 읽는 중... 완료 의존성 트리 구축 상태 정보 읽기 중... 완료 참고:
 '/home/gpqa/Downloads/GlobalProtect_UI_deb-6.0.0.0-12.deb' 대
신 'globalprotect'를 선택합니다. 다음 새 패키지가 설치됩니다.
 globalprotect 업그레이드 0건, 새로 설치됨 1건, 삭제할 0건 및 업
그레이드되지 않은 90건이 있습니다. 이 작업 후에는 0B의 추가 디
스크 공간이 사용됩니다. 가져오기 : 1 /home/gpqa/Downloads/
GlobalProtect_UI_deb-6.0.0.0-12.deb globalprotect all 5.2.6-12
 [7,416 kB] E: 읽기, 여전히 읽을 59개가 있지만 남은 것이 없습니다. E: 아
카이브 멤버 헤더를 읽는 중 오류가 발생했습니다. E: /home/gpqa/Downloads/
GlobalProtect_UI_deb-6.0.0.0-12.deb에 이전 오류가 적용됨 debconf:
```

 ©2023 Palo Alto Networks, Inc.

```
 apt-extracttemplates 실패: 해당 파일 또는 디렉토리가 없습니다. 이전
에 선택하지 않은 패키지 globalprotect를 선택합니다. (데이터베이스 읽
는 중 ... 318427개의 파일 및 디렉토리가 현재 설치되어 있습니다.) 언패
킹 준비 중 .../GlobalProtect_UI_deb-6.0.0.0-12.deb ... gp 설치 시
작... globalprotect(6.0.0-12) 언패킹... globalprotect(6.0.0-12) 설
정 중... gp 서비스 활성화... gp 서비스 시작 중... 기본 브라우저 설
정, gp.desktop 이외의 오류는 무시할 수 있습니다... ping 활성화
 net.ipv4.ping_group_range = 0 0 gpa를 시작하는 중... sudo 사용자
 gpqa용 GPA 시작 sudo gpqa용 PanGPU 시작 man-db(2.8.3-2ubuntu0.1)의 리
거 처리 중...
```

CentOS 및 Red Hat의 경우 **sudo yum install -y *<gp-app-pkg>*** 명령을 사용하십시오.

여기서 ***<gp-app-pkg>*** 은(는) Linux 버전에 대한 UI 배포 패키지의 경로입니다.

다음 예에서는 GlobalProtect_UI_rpm-6.0.0.0-9.rpm UI 배포 패키지를 저장소에서 시스템으로 설치합니다.

```
user@linuxhost:~$ sudo yum install -y ./
GlobalProtect_UI_rpm-6.0.0.0-9.rpm [gpqa의 [sudo] 암호: 로
드된 플러그인: langpacks, product-id, search-disabled-repos,
 subscription-manager 검사 중 ./GlobalProtect_UI_rpm-6.0.0.0-9.rpm:
 globalprotect_UI-6.0.0-9.x86_64 표시 중 ./
GlobalProtect_UI_rpm-6.0.0.0-9.rpm 설치 예정 의존성 해결 중 --> 트
랜잭션 검사 실행 ---> 패키지 globalprotect_UI.x86_64 0:6.0.0-9가 설
치됩니다. --> 의존성 해결 완료 https://cdn.redhat.com/content/dist/
rhel/server/7/7Server/x86_64/optional/os/repodata/repomd.xml: [오
류 번호 14] HTTPS 오류 403 - 금지됨 다른 미러를 시도합니다. 이 문제를 해
결하려면 아래 기술 자료 문서를 참조하십시오 https://access.redhat.com/
solutions/69319 위의 문서가 이 문제를 해결하는 데 도움이 되지 않으면
 Red Hat 지원에서 티켓을 여십시오. https://cdn.redhat.com/content/
dist/rhel/server/7/7Server/x86_64/os/repodata/repomd.xml: [오
류 번호 14] HTTPS 오류 403 - 금지됨다른 미러를 시도합니다. 의존성 해결
 ================================================================================
키지 아치 버전 저장소 크기
 ================================================================================
치 중: globalprotect_UI x86_64 6.0.0-9 /
GlobalProtect_UI_rpm-6.0.0.0-9 31 M Transaction 요
약================================================================================
키지 1개 설치 총 크기: 31M 설치 크기: 31M 패키지 다운로드: 트랜잭
션 확인 실행 중 트랜잭션 테스트 실행 중 트랜잭션 테스트 성공 트랜잭션 실
행 중 gp 설치 시작... 설치 중: globalprotect_UI-6.0.0-9.x86_64
 1/1 gp 서비스 활성화... 기본 브라우저 설정, gp.desktop 이외의 오
류는 무시할 수 있습니다... ping 활성화 /var/tmp/rpm-tmp.VLWi5h:
 line 23: $LOG: 모호한 리디렉션 gp 서비스를 시작하는 중... gpa를 시
작하는 중... 확인 중 : globalprotect_UI-6.0.0-9.x86_64 1/1
 https://cdn.redhat.com/content/dist/rhel/server/7/7Server/
x86_64/os/repodata/c76c2299-12f3-4f9c-b7bd-03bacee2c363 : [오
류 번호 14] HTTPS 오류 403 - 금지됨다른 미러를 시도합니다. 설치됨:
 globalprotect_UI.x86_64 0:6.0.0-9 완료!
```

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Linux용 GlobalProtect 앱의 GUI 버전을 사용합니다.

설치가 완료되면 GlobalProtect 앱이 자동으로 실행됩니다. 포털 주소를 지정하고 연결 프로세스를 시작하라는 메시지가 표시되면 자격 증명을 입력합니다.

> ***GlobalProtect*** 서비스는 ***GlobalProtect*** 에이전트 및 ***GUI*** 버전의 ***GlobalProtect*** 앱에 대한 하나의 소켓 연결만 지원하므로 앱을 설치한 후 루트 사용자로 사용되는 설치 방법에 따라 ***Linux*** 운영 체제 또는 ***SSH*** 세션에서 로그아웃해야 합니다. 권한이 없는 사용자 권한이 있는 다른 사용자로 ***Linux*** 엔드포인트에 다시 로그인해야 앱이 시작됩니다.

Linux용 GlobalProtect의 CLI 버전을 다운로드하고 설치합니다.

Linux 디바이스가 GUI를 지원하지 않는 경우 다음 단계를 완료하여 Linux용 GlobalProtect 앱을 설치합니다. Linux용 GlobalProtect 앱은 DEB, RPM 및 TAR 설치 패키지를 지원합니다.

STEP 1 | Linux용 GlobalProtect 앱을 다운로드합니다.

1. IT 관리자로부터 앱 패키지를 가져온 다음, TGZ 파일을 Linux 엔드포인트에 복사합니다.

   예를 들어 패키지를 macOS 엔드포인트에 다운로드한 경우 터미널을 열고 파일을 복사할 수 있습니다.

   ```
   macUser@mac:~$ scp ~/Downloads/PanGPLinux-6.0.0.tgz
    linuxUser@linuxHost: <DestinationFolder>
   ```

   여기서 ***<DestinationFolder>*** 은(는) TGZ 파일을 저장할 `~/pkgs/`와 같은 위치입니다.

2. Linux 엔드포인트에서 패키지의 압축을 풉니다.

   ```
   user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
   ```

   패키지의 압축을 풀면 설치 패키지(Ubuntu용 DEB, CentOS 및 Red Hat용 RPM)와 패키지를 설치 및 제거하는 스크립트가 표시됩니다.

STEP 2 | (선택 사항) Linux 엔드포인트에서 수동 프록시 서버 구성을 사용해야 하는 경우 프록시 설정을 구성합니다.

> ***Linux*용 *GlobalProtect*** 앱은 기본 프록시 서버 구성만 지원하지만 프록시 자동 구성***(PAC)*** 파일 및 프록시 인증 사용은 지원하지 않습니다.

Linux용 GlobalProtect 앱은 `/etc/environment` 파일의 `HTTP_PROXY`, `HTTPS_PROXY` 및 `NO_PROXY` 환경 변수에서 프록시 설정을 가져옵니다. 나중에 시스템 프록시 구성을 변경하는 경우

 ©2023 Palo Alto Networks, Inc.

GlobalProtect가 실행되는 터미널이 프록시 환경 변수를 사용하는지 확인합니다. 새 설정이 표시되지 않으면 로그아웃했다가 다시 로그인하여 새로운 설정을 적용합니다.

HTTP_PROXY 변수 또는 *HTTPS_PROXY* 변수를 구성한 경우 *GlobalProtect* 포털이 *NO_PROXY* 변수에 대해 구성된 설정과 일치하는지 확인합니다.

1. Linux 엔드포인트에서 프록시를 설정하려면 `HTTP_PROXY` 환경 변수 또는 `HTTPS_PROXY` 환경 변수(예: `HTTPS_PROXY="https://yourproxy.local:8080"`)를 편집합니다.
2. 프록시에서 제외할 IP 주소 또는 도메인 이름을 구성하려면 `NO_PROXY` 환경 변수(예: `NO_PROXY="www.gpqa.com"`)를 편집합니다.

   쉼표를 사용하여 여러 IP 주소 또는 도메인 이름을 구분합니다. GlobalProtect 앱 5.1.6부터 IP 주소 또는 도메인 이름에 와일드카드 문자(*)를 사용할 수 있습니다(예: `NO_PROXY="*.domain.com"`).

STEP 3 | 앱 패키지를 설치합니다.

GlobalProtect에 사용할 수 있는 두 개의 앱 패키지가 있습니다.

- CLI 버전(예: GlobalProtect_deb-6.0.0.0-12.deb)—**sudo dpkg -i *<gp-app-pkg>*** 또는 **sudo apt-get install *<gp-app-pkg>*** 명령을 사용합니다.
- UI 버전(예: GlobalProtect_UI_deb-6.0.0.0-12.deb)—**sudo apt-get install *<gp-app-pkg>*** 명령을 사용하여 설치합니다.

여기서 ***<gp-app-pkg>*** 은(는) Linux 버전에 대한 CLI 또는 UI 배포 패키지의 경로입니다. **apt-get** 명령의 경우 패키지 이름 앞에 **./**를 추가해야 합니다.

*Linux Ubuntu 20.04 LTS*에 *CLI* 버전을 설치하는 경우 기본 운영 체제 문제로 인해 ***sudo apt-get install <gp-app-pkg>*** 명령을 사용할 수 없습니다. 대신 ***sudo dpkg -i <gp-app-pkg>*** 명령을 사용하여 *CLI* 버전의 *GlobalProtect* 앱을 설치합니다. 자세한 내용은 GlobalProtect 5.2.x 이상이 Ubuntu 20.04에서 apt-get 유틸리티를 사용할 때 패키지를 설치하지 못함을 참조하십시오.

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-6.0.0.0-12.deb 이
전에 선택하지 않은 GlobalProtect 패키지를 선택합니다. (데이터베이
스 읽는 중 ... 67776개의 파일 및 디렉토리가 현재 설치되어 있습니다.)
 GlobalProtect_deb-6.0.0.0-12.deb 언패킹 준비 중 ... gp 설치 시작...
 GlobalProtect(6.0.0-12) 언패킹 중... GlobalProtect(6.0.0-12) 설
정 중... gp 서비스 활성화... gp 서비스 시작 중... gp cli에 대한 심볼릭 링
크 만들기...
```

```
user@linuxhost:~$ sudo apt-get install ./
GlobalProtect_deb-6.0.0.0-12.deb gpqa의 [sudo] 암호: 패키지 목
록을 읽는 중... 완료 의존성 트리 구축 상태 정보 읽기 중... 완료 '/
home/gpqa/Downloads/GlobalProtect_deb-6.0.0.0-12.deb' 대신
 'globalprotect'를 선택합니다. 다음 패키지가 자동으로 설치되었으며 더 이
상 필요하지 않습니다. linux-headers-5.10.0-28 linux-headers-5.10.0-28-
```

 ©2023 Palo Alto Networks, Inc.

```
generic linux-image-5.10.0-28-generic linux-image-extra-5.10.0-28-
generic 'sudo apt autoremove'를 사용하여 삭제하십시오. 다음 새 패키
지가 설치됩니다. globalprotect 업그레이드 0건, 새로 설치됨 1건, 삭제
할 0건 및 업그레이드되지 않은 73건이 있습니다. 이 작업 후에는 0B의 추
가 디스크 공간이 사용됩니다. 가져오기: 1 /home/gpqa/Downloads/
GlobalProtect_deb-6.0.0.0-12.deb globalprotect all 6.0.0-12 [1,334
 kB] E: 읽기, 여전히 읽을 59개가 있지만 남은 것이 없습니다. E : 아카이
브 멤버 헤더를 읽는 중에 오류가 발생했습니다. E: 이전 오류는 /home/gpqa/
Downloads/GlobalProtect_deb-6.0.0.0-24.deb에 적용됩니다 debconf:
 apt-extracttemplates 실패: 해당 파일 또는 디렉토리가 없습니다. 이전
에 선택하지 않은 패키지 globalprotect를 선택합니다. (데이터베이스 읽
는 중 ... 247210개의 파일 및 디렉터리가 현재 설치되어 있습니다.) 언패
킹 준비 중 .../GlobalProtect_deb-6.0.0.0-12.deb... gp 설치 시작...
 globalprotect(6.0.0-12) 언패킹... globalprotect(6.0.0-12) 설정 중...
 gp 서비스 활성화... gp 서비스 시작 중... gp cli에 대한 심볼릭 링크 만들
기...
```

Linux용 GlobalProtect 앱은 **/opt/paloaltonetworks/globalprotect** 디렉토리에 설치됩니다. GlobalProtect가 처음 실행된 후 앱은 사용자 레지스트리 구성 및 기타 CLI 관련 설정을 저장하기 위해 GlobalProtect 사용자 폴더 **$HOME/.globalprotect**도 만듭니다.

STEP 4 | (선택 사항) CLI 모드를 변경합니다.

명령줄 또는 프롬프트 모드에서 명령을 실행할 수 있습니다. 명령줄 모드에서는 전체 GlobalProtect 명령을 지정해야 합니다. 프롬프트 모드에서는 명령(앱 이름 제외)만 지정하면 되며 명령줄 모드보다 더 자세한 출력을 표시합니다.

1. 프롬프트 모드로 전환하려면 인수 없이 **globalprotect**를 입력합니다.

```
user@linuxhost:~$ globalprotect >>
```

2. 프롬프트 모드를 종료하려면 **quit**를 입력합니다.

```
>> quit user@linuxhost:~$
```

STEP 5 | Linux용 GlobalProtect 앱에 대한 도움말을 참조하십시오.

프롬프트 모드:

```
>> help 사용법: 다음 명령만 지원됩니다. collect-log -- collect log
 information connect -- connect to server disconnect -- disconnect
 disable -- disable connection import-certificate -- import client
 certificate file quit -- quit from prompt mode rediscover-network
 -- network rediscovery remove-user -- clear credential resubmit-
hip -- resubmit hip information set-log -- set debug level show --
 show information
```

 ©2023 Palo Alto Networks, Inc.

명령줄 모드:

```
user@linuxhost:~$ globalprotect help 사용법: 다음 명령만 지원됩니다.
 collect-log -- collect log information connect -- connect to
 server disconnect -- disconnect disable -- disable connection
 import-certificate -- import client certificate file quit -- quit
 from prompt mode rediscover-network -- network rediscovery remove-
user -- clear credential resubmit-hip -- resubmit hip information
 set-log -- set debug level show -- show information
```

STEP 6 | Linux용 GlobalProtect 앱의 CLI 버전을 사용합니다.

 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱 사용하기

GlobalProtect는 Linux용 GlobalProtect 앱의 두 가지 버전을 지원합니다. Linux 디바이스가 GUI를 지원하는 경우 One 버전, Linux 디바이스가 GUI를 지원하지 않는 경우 CLI 버전을 지원합니다.

- Linux용 GlobalProtect 앱의 GUI 버전 사용하기
- Linux용 GlobalProtect 앱의 CLI 버전 사용하기

Linux용 GlobalProtect 앱의 GUI 버전 사용하기

Linux용 GlobalProtect 앱의 GUI 버전을 사용하려면 다음 단계를 완료하십시오.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | (RHEL/CentOS 7.7 이상에만 해당) GlobalProtect 아이콘이 기본적으로 시스템 트레이에 표시되지 않으면 확장 프로그램을 추가하여 활성화하십시오.

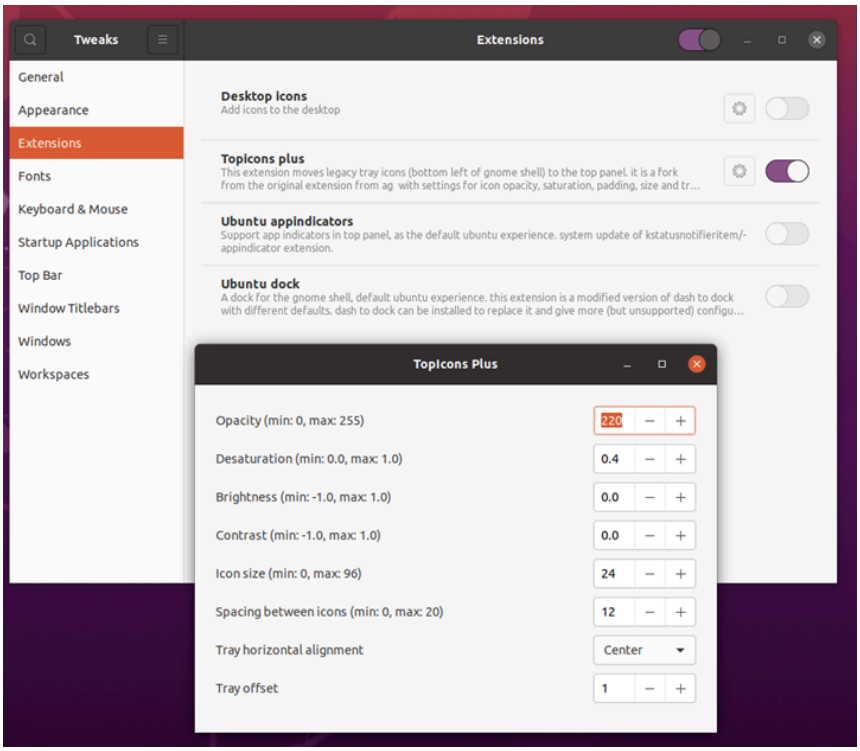
1. 다음 명령을 실행하여 Topicons Gnome Tweak Tool 확장 프로그램을 설치합니다.

   ```
   sudo apt-get install gnome-shell-extension-top-icons-plus
   sudo apt-get install gnome-tweak-tool
   ```

2. 시스템을 재부팅합니다.
3. 애플리케이션 메뉴에서 **Tweaks** > 확장 프로그램을 선택합니다.
4. GlobalProtect 아이콘이 시스템 트레이에 표시되도록 **Topicons Plus** 확장 프로그램을 토글합니다.

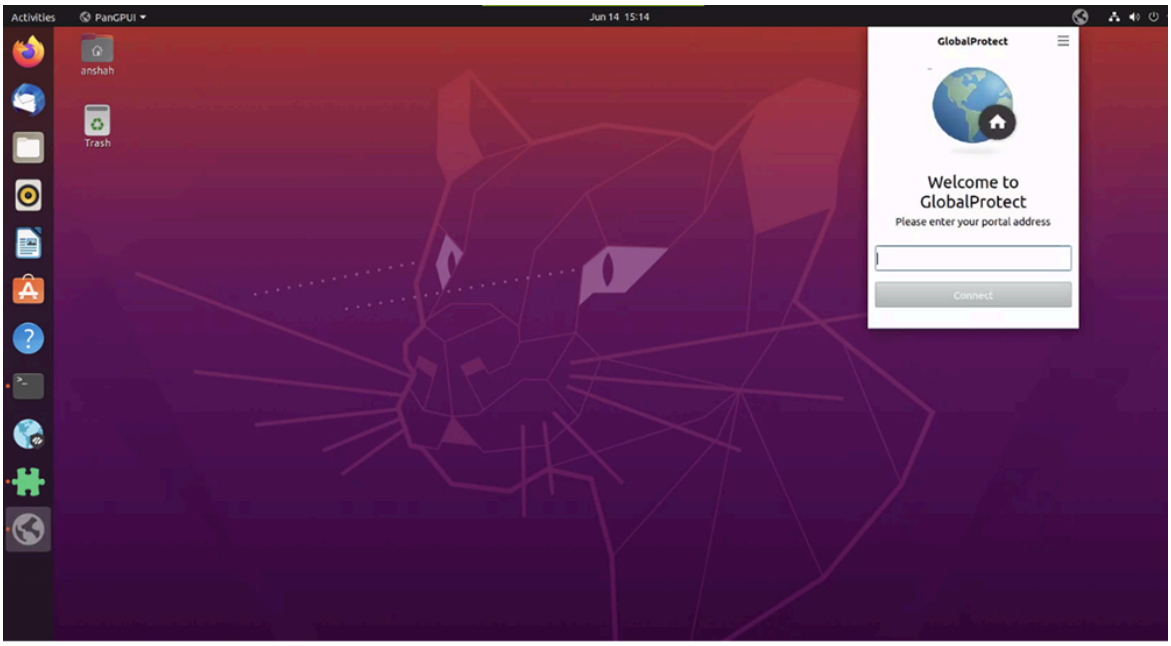
   Topicons Plus 확장 프로그램이 표시되지 않으면 확장 프로그램을 설치한 후 재부팅하지 않았을 수 있습니다.

   아이콘 크기, 정렬 및 불투명도와 같은 아이콘 설정을 사용자 지정할 수도 있습니다.



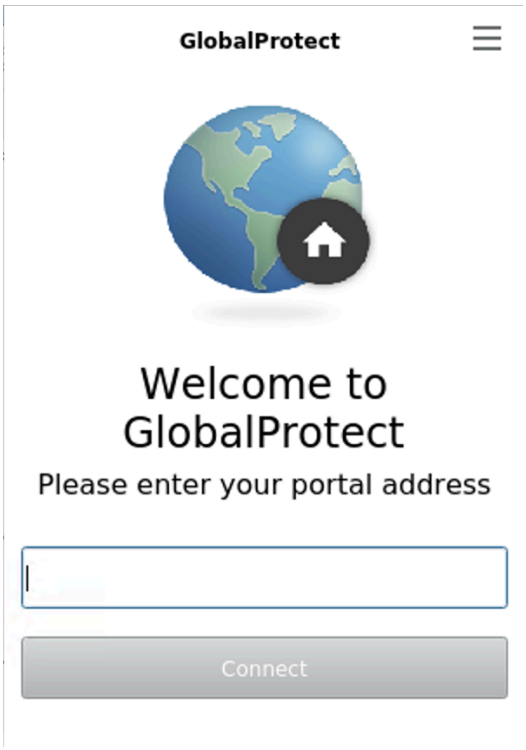
5. 이제 시스템 트레이에서 GlobalProtect 앱을 실행할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.



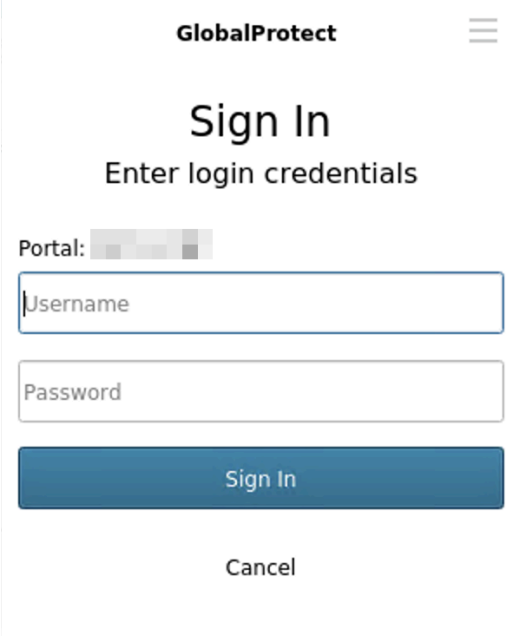
 ©2023 Palo Alto Networks, Inc.

STEP 2 | GlobalProtect 창에서 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력한 다음 연결을 클릭합니다.



Linux용 GlobalProtect 앱의 GUI 버전을 다운로드하고 설치한 다음 GlobalProtect 앱이 자동으로 실행됩니다.

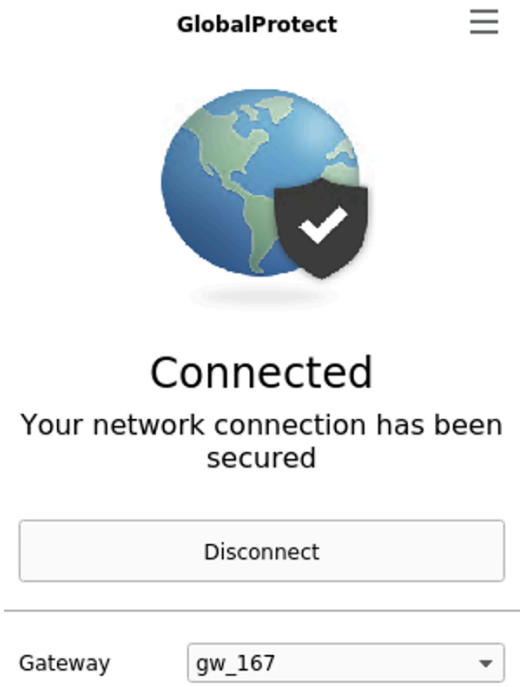
1. (선택 사항) 앱에 여러 포털이 저장되어 있는 경우 포털 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 드롭다운에서 미리 선택됩니다.



2. 포털의 사용자 이름 및 암호를 입력한 다음 로그인합니다.

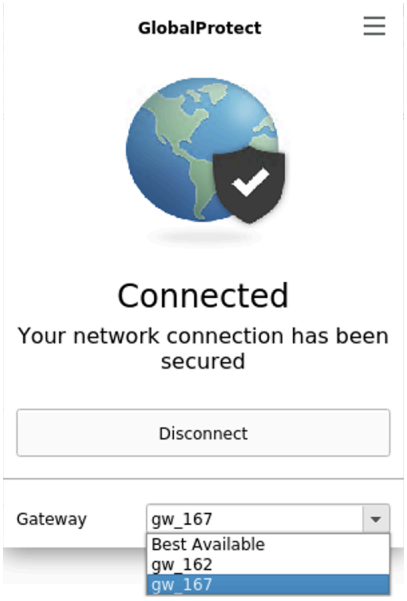
 ©2023 Palo Alto Networks, Inc.

대부분의 경우 회사 네트워크에 연결할 때 사용하는 것과 동일한 사용자 이름과 암호를 사용할 수 있습니다. 로그인하면 GlobalProtect 포털에 연결됨 상태가 표시됩니다.



3. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 드롭다운을 클릭하고 다음 옵션 중 하나를 사용합니다.
   - 게이트웨이를 수동으로 선택합니다(외부 게이트웨이만 해당).

     이 옵션은 관리자가 수동 게이트웨이 선택을 활성화한 경우에만 사용할 수 있습니다.



 ©2023 Palo Alto Networks, Inc.

- 기본 게이트웨이 할당 및 자동 연결:

  1. 앱 상태 패널의 오른쪽 상단에 있는 메뉴에서 기본 게이트웨이를 선택하여 GlobalProtect를 엽니다. 기본 게이트웨이 대화 상자입니다.

  2. 사용 가능한 게이트웨이 목록에서 기본 게이트웨이로 설정할 게이트웨이를 선택한 다음기본 설정으로 설정하십시오.
  3. 대화 상자를 닫습니다.

  더 이상 게이트웨이에 자동으로 연결하지 않으려면 기본 게이트웨이 할당을 삭제할 수도 있습니다.

  1. 앱 상태 패널의 오른쪽 상단에 있는 메뉴에서 기본 게이트웨이를 선택하여 GlobalProtect를 엽니다. 기본 게이트웨이 대화 상자입니다.
  2. 사용 가능한 게이트웨이 목록에서 기본 게이트웨이를 선택한 다음 기본 설정 삭제를 선택합니다.
  3. 대화 상자를 닫습니다.

STEP 3 | GlobalProtect 앱을 엽니다.

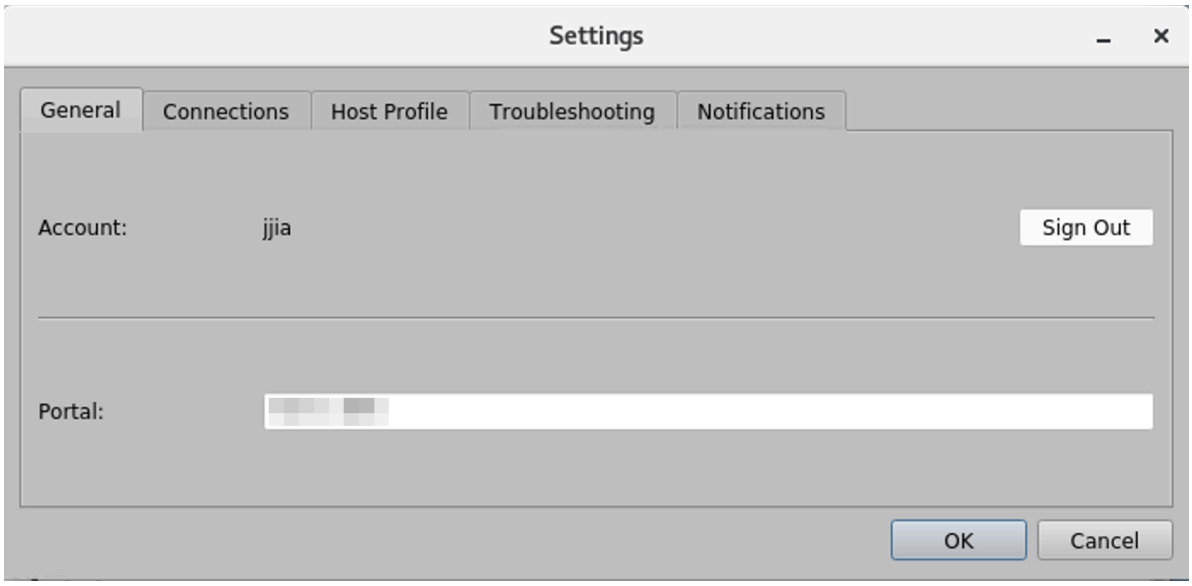
GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | 네트워크 연결에 대한 정보를 봅니다.

앱을 실행한 후 메뉴(≡) 앱 패널의 오른쪽 상단에서 설정을 선택하여 **GlobalProtect** 설정 패널을 연 후 다음 탭 중 하나를 선택하여 네트워크 연결에 대한 정보를 확인합니다.

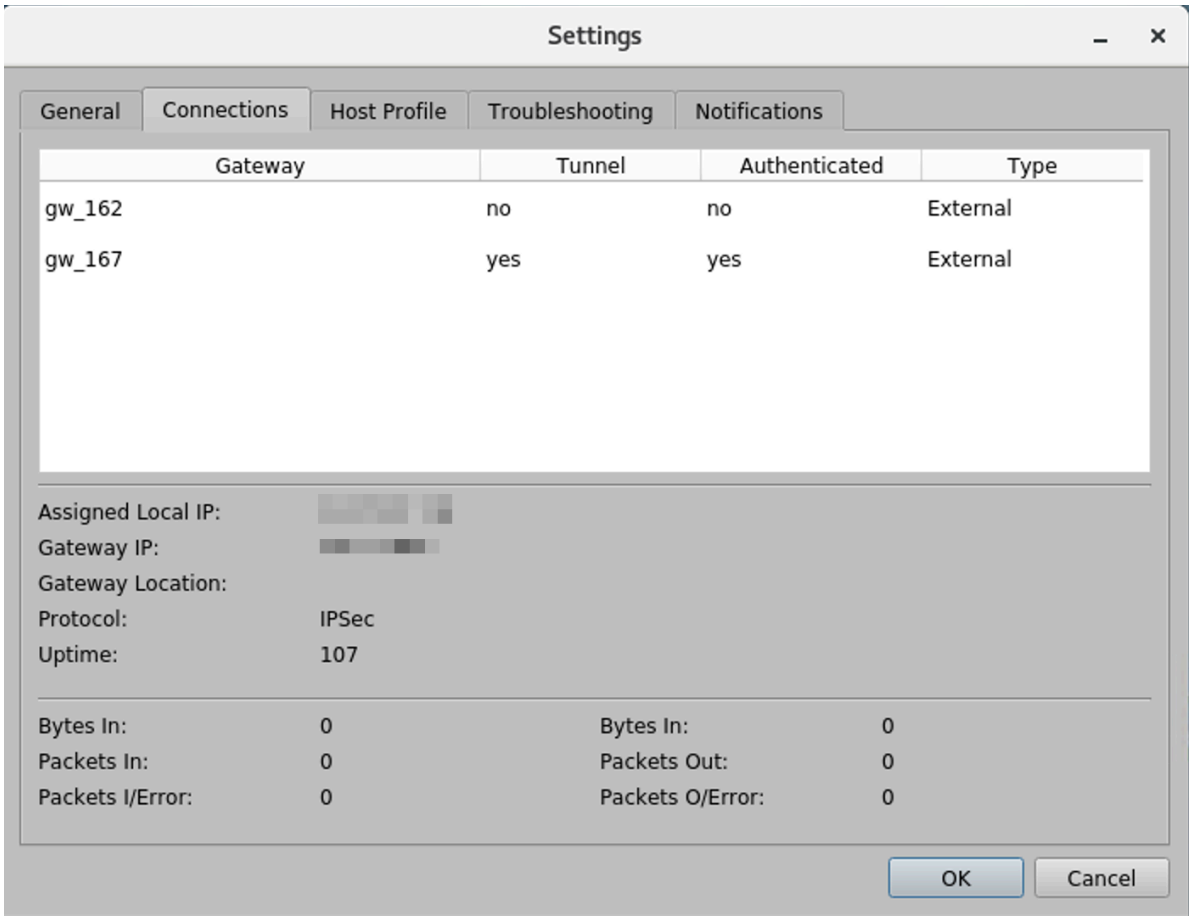
- 일반 탭—GlobalProtect 계정과 연결된 사용자명 및 포털을 표시합니다. 이 탭에서 포털을 추가, 삭제 또는 수정할 수도 있습니다.



- 연결 탭—GlobalProtect 앱에 대해 구성된 게이트웨이를 표시하고 각 게이트웨이에 대한 다음 정보를 제공합니다.
  - 게이트웨이 이름
  - 터널 상태
  - 인증 상태
  - 연결 타입
  - 게이트웨이 IP 주소 또는 FQDN(외부 모드에서만 사용 가능)

> 내부 모드의 경우 연결 탭에 사용 가능한 게이트웨이의 전체 목록이 표시됩니다. 외부 모드의 경우 연결 탭에는 연결된 게이트웨이와 게이트웨이에 대한 추가 세부 정보(예: 게이트웨이 *IP* 주소, 위치 및 가동 시간)가 표시됩니다.

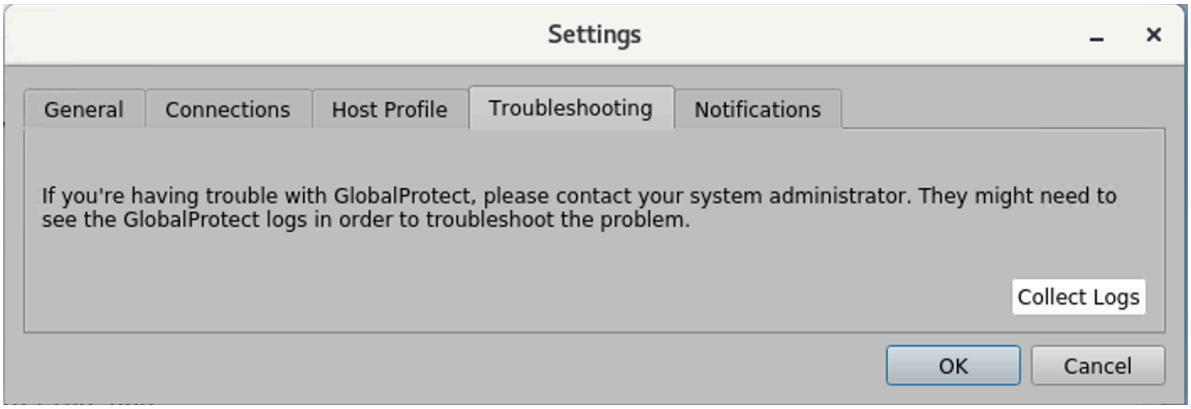
 ©2023 Palo Alto Networks, Inc.



- 문제 해결—로그를 수집하고 로깅 수준을 설정할 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

GlobalProtect 앱이 추가 분석을 위해 문제 해결 로그, 진단 로그 또는 둘 모두를 Cortex Data Lake로 보내려면 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화하도록 *GlobalProtect* 포털을 구성해야 합니다. 또한 프로브하려는 웹 서버/리소스의 *IP* 주소 또는 정규화된 도메인 이름을 포함할 수 있는 HTTPS 기반 대상 URL을 구성하고 최종 사용자 엔드포인트에서 대기 시간 또는 네트워크 성능과 같은 문제를 확인할 수 있습니다.



STEP 5 | (선택 사항) 새 암호를 사용하여 로그인합니다.

GlobalProtect 관리자가 *GlobalProtect* 포털 에이전트가 사용자 자격 증명을 저장하도록 구성하면 자격 증명이 *GlobalProtect* 앱에 자동으로 저장됩니다. 회사 네트워크에 액세스하기 위한 암호가 변경되면 새 암호를 사용하여 *GlobalProtect*에 로그인해야 합니다.

1. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 메뉴(≡)를 선택한 다음 설정을 선택하여 **GlobalProtect** 설정 패널을 엽니다.
3. **GlobalProtect** 설정 패널의 일반 탭에서 로그아웃하여 GlobalProtect 앱에서 저장된 사용자 자격 증명을 지웁니다.
4. 사용자 자격 증명을 지운 후 새 사용자 이름과 암호를 사용하여 GlobalProtect에 다시 연결할 수 있습니다.

STEP 6 | (선택 사항) GlobalProtect와의 연결을 끊습니다.

관리자가 주문형 연결 방법으로 GlobalProtect를 구성한 경우 상태 패널에서 연결 해제를 클릭하여 GlobalProtect에서 연결을 끊을 수 있습니다.

 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱의 CLI 버전 사용하기

Linux용 GlobalProtect™ 앱의 명령줄 인터페이스(CLI)를 사용하여 GlobalProtect 앱에 공통적인 작업을 수행할 수 있습니다. 다음 예제는 명령줄 모드에서 출력을 표시합니다. 프롬프트 모드에서 동일한 명령을 실행하려면 **globalprotect** 접두어 없이 입력하십시오(자세한 내용은 Linux용 GlobalProtect 앱 다운로드 및 설치 참조).

- GlobalProtect 포털에 연결:

  <gp-portal>이(가) GlobalProtect 포털의 IP 주소 또는 FQDN인 위치에서 **globalprotect connect --portal*<gp-portal>*** 명령을 사용합니다.

  예:

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com 구성 검색 중... 연결 해제됨 myportal.example.com
 - portal:local:로그인 자격 증명 입력 사용자 이름:사용자1 암호: 구성 검
색 중... 네트워크 검색 중... 연결 중... 연결됨
```

  인증서 기반 인증을 사용하는 경우, 루트 CA 인증서 없이 처음 연결하면 GlobalProtect 앱과 GlobalProtect 포털이 인증서를 교환합니다. GlobalProtect 앱은 인증하기 전에 확인해야 하는 인증서 오류를 표시합니다. 다음에 연결할 때 인증서 오류 메시지가 표시되지 않습니다.

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com 구성 검
색 중...                                                  연결 해
제됨 보안 인증서에 문제가 있어 10.3.188.61의 ID를 확인할 수 없
습니다. 문제를 해결하려면 조직의 지원 센터에 문의하십시오. 경고:
 10.3.188.61과의 통신이 손상되었을 수 있습니다. 이 연결을 계속하
지 않는 것이 좋습니다. 오류 세부 정보:계속하시겠습니까(y/n)?y 구성 검
색 중...                                                  연결 해제됨
 10.3.188.61 - portal:local:로그인 자격 증명 입력 사용자 이름:user1 암
호: 구성 검색 중...                                                네트워
크 검색 중... 연결 중... 연결됨
```

  --username <username> 옵션을 사용하여 명령에 사용자 이름을 지정할 수도 있습니다. *GlobalProtect* 앱은 인증하라는 메시지를 표시하고 사용자 이름 옵션을 지정한 경우 사용자 이름을 확인합니다.

- 인증서를 가져옵니다.

  인증서 기반 인증을 위해 엔드포인트에 클라이언트 인증서를 사전 배포하려는 경우 인증서를 엔드포인트에 복사하고 GlobalProtect 앱에서 사용할 수 있도록 가져올 수 있습니다. **globalprotect**

 ©2023 Palo Alto Networks, Inc.

import-certificate --location<*location*> 명령을 사용하여 엔드포인트에서 인증서를 가져옵니다. 메시지가 표시되면 인증서 암호를 제공해야 합니다.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 암호를 입력하십시오. 인증서
를 가져왔습니다.
```

- 게이트웨이에 연결:
  1. (선택 사항) **globalprotect show --manual-gateway** 명령을 사용하여 연결할 수 있는 수동 게이트웨이를 표시합니다.
  2. ***<gp-gateway>***이(가) GlobalProtect 게이트웨이의 IP 주소 또는 FQDN인 위치에서 **globalprotect connect --gateway<*gp-gateway*>** 명령을 사용하여 게이트웨이에 연결합니다.
  3. **globalprotect show --details** 명령을 사용하여 연결에 대한 세부 정보를 봅니다.

```
user@linuxhost:~$ globalprotect show --manual-gateway 이
름 주소 --------------- gw1 192.168.1.180 gw2 192.168.1.181
 user@linuxhost:~$globalprotect connect --gateway 192.168.1.180 구
성 검색 중... 네트워크 검색 중... 연결 중... 연결됨
```

- GlobalProtect 연결 상태를 확인하고 세부 정보 보기:

  globalprotect show --status 명령을 사용하여 연결 상태를 확인하십시오.

  연결 세부 정보를 보려면 **globalprotect show --details** 명령을 사용하십시오.

```
user@linuxhost:~$ globalprotect show --status GlobalProtect 상태: 연
결됨 user@linuxhost:~$ globalprotect show --details 할당된 IP 주소:
 192.168.1.132 게이트웨이 IP 주소: 192.168.1.180 프로토콜: IPSec 가동 시
간(초): 231
```

- 네트워크 재발견하기:

  globalprotect rediscover-network 명령을 사용하여 GlobalProtect에서 연결을 끊었다가 다시 연결합니다.

```
user@linuxhost:~$ globalprotect rediscover-network 연결 해제 중... 구
성 검색 중... 구성 검색 중... 네트워크 검색 중... 연결 중... 연결 중... 연
결된 GlobalProtect 상태: 연결됨
```

 ©2023 Palo Alto Networks, Inc.

- 현재 사용자의 자격 증명 지우기:

  globalprotect remove-user 명령을 사용하여 포털 및 게이트웨이 인증에 사용되는 자격 증명을 지웁니다. GlobalProtect 앱이 자격 증명을 지워야 한다고 확인한 후 GlobalProtect 앱은 터널 연결을 끊고 다음에 연결할 때 자격 증명을 입력하도록 요구합니다.

```
user@linuxhost:~$ globalprotect remove-user 자격 증명이 지워지고 현
재 터널이 종료됩니다. 계속하시겠습니까(y/n)?y 지우기가 완료되었습니다.
 user@linuxhost:~$ globalprotect connect --portal 192.168.1.179 구
성 검색 중... 연결 끊김 192.168.1.179 - portal:local:로그인 자격 증
명 입력 사용자 이름:user1 암호: 구성 검색 중... 네트워크 검색 중... 연
결 중... 연결됨
```

- 게이트웨이에 호스트 정보를 다시 제출하십시오.

  globalprotect show --host-state 명령을 사용하여 엔드포인트의 현재 호스트 정보를 봅니다. **globalprotect resubmit-hip** 명령을 사용하여 엔드포인트 정보를 게이트웨이에 다시 제출하십시오. 이는 사용자가 엔드포인트에서 규정 준수 문제를 수정한 다음 HIP를 다시 제출할 수 있도록 허용하기 때문에 HIP 기반 보안 정책이 사용자가 리소스에 액세스하지 못하게 하는 경우에 유용합니다.

```
user@linuxhost:~$ globalprotect show --host-state 생성 시간: 2017년
 9월 28일 11:24:07 카테고리 호스트 정보 클라이언트 버전: 4.1.0 OS:
 Linux Ubuntu 16.04.3 LTS OS 공급업체: Linux 도메인: 호스트 이름:
 linuxhost 호스트 ID: 4C4C4544-0034-4D10-804C-************ 네트워
크 인터페이스 enp0s31f6 설명: enp0s31f6 mac 주소: D4:81:D7:D4:5A:A5
 wlp2s0 설명: wlp2s0 mac 주소: 14:AB:C5:DE:D1:0E user@linuxhost:~
$ globalprotect resubmit-hip 다시 제출했습니다.
```

- GlobalProtect 알림을 봅니다.

  알림을 보려면 **globalprotect show --notification** 명령을 사용합니다.

- GlobalProtect 시스템 트레이 아이콘을 봅니다.

  globalprotect launch-ui 명령을 사용하여 바탕 화면에 시스템 트레이 아이콘을 표시합니다. 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행할 수 있습니다.

- 환영 페이지를 봅니다.

  globalprotect show --welcome-page 명령을 사용합니다. GlobalProtect 앱은 환영 페이지가 있으면 브라우저에 환영 페이지를 표시하고 환영 페이지가 없으면 알림을 표시합니다.

 ©2023 Palo Alto Networks, Inc.

- 오류를 봅니다.

  앱에서 보고된 오류를 보려면 **globalprotect show --error** 명령을 사용합니다.

```
user@linuxhost:~$ globalprotect show --error 오류: GlobalProtect 포
털에 연결할 수 없습니다.
```

- 로그를 수집합니다.

  앱은 PanGPA 및 PanGPI 로그 파일을 `/home/<user>/.Globalprotect` 디렉토리에 저장합니다 **globalprotect collect-logs** 명령을 사용하여 Linux용 GlobalProtect 앱이 이러한 로그 및 기타 유용한 정보를 패키징할 수 있도록 합니다. 그 다음 로그를 사용하여 문제를 해결하거나 전문가 분석을 위해 지원 엔지니어에게 전달할 수 있습니다.

```
user@linuxhost:~$ globalprotect collect-log 수집 시작... 네트워크 정
보 수집... 머신 정보 수집... 파일 복사... 최종 결과 파일 생성... 지원 파일은
 /home/user/.GlobalProtect/Collect.tgz에 저장됩니다.
```

- Linux용 GlobalProtect 앱의 버전을 표시합니다.

```
user@linuxhost:~$ globalprotect show --version GlobalProtect:
 6.0.0-23 Copyright(c) 2009-2021 Palo Alto Networks, Inc.
```

 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱에서 문제 보고하기

네트워크 성능이 저하되거나 포털 및 게이트웨이와의 연결이 설정되지 않는 등의 비정상적인 동작이 발생하는 경우 관리자가 액세스할 수 있는 Cortex Data Lake에 직접 문제를 보고할 수 있습니다. 더 이상 이메일을 통해 GlobalProtect 앱 로그를 수동으로 수집 및 전송하거나 클라우드 드라이브에 저장할 필요가 없습니다.

***Linux*용 *GlobalProtect* 앱의 *GUI* 버전을 사용하여 관리자에게만 문제를 보고할 수 있습니다.**

***GlobalProtect* 앱에 문제 보고 옵션을 표시하려면 관리자가 *GlobalProtect* 포털에서 문제 해결을 위해 GlobalProtect 앱 로그 수집을 활성화해야 합니다.**

STEP 1 | GlobalProtect 포털 또는 게이트웨이에 연결합니다.

1. GlobalProtect 창에서 GlobalProtect 포털의 FQDN 또는 IP 주소를 입력한 다음 연결을 클릭합니다.

   Linux용 GlobalProtect 앱의 GUI 버전을 다운로드하여 설치하면 GlobalProtect 앱이 자동으로 실행됩니다.
2. (선택 사항) 앱에 여러 포털이 저장되어 있는 경우 포털 드롭다운에서 포털을 선택합니다. 기본적으로 가장 최근에 연결된 포털은 포털 드롭다운에서 미리 선택됩니다.
3. 포털의 사용자 이름 및 암호를 입력한 다음 로그인합니다.

   대부분의 경우 회사 네트워크에 연결할 때 사용하는 것과 동일한 사용자 이름과 암호를 사용할 수 있습니다. 로그인하면 GlobalProtect 포털에 연결됨 상태가 표시됩니다.
4. (선택 사항) 기본적으로 관리자가 정의한 구성과 사용 가능한 게이트웨이의 응답 시간에 따라 사용 가능한 최상의 게이트웨이에 자동으로 연결됩니다. 다른 게이트웨이에 연결하려면 게이트웨이 드롭다운을 클릭합니다.

STEP 2 | GlobalProtect 앱을 엽니다.

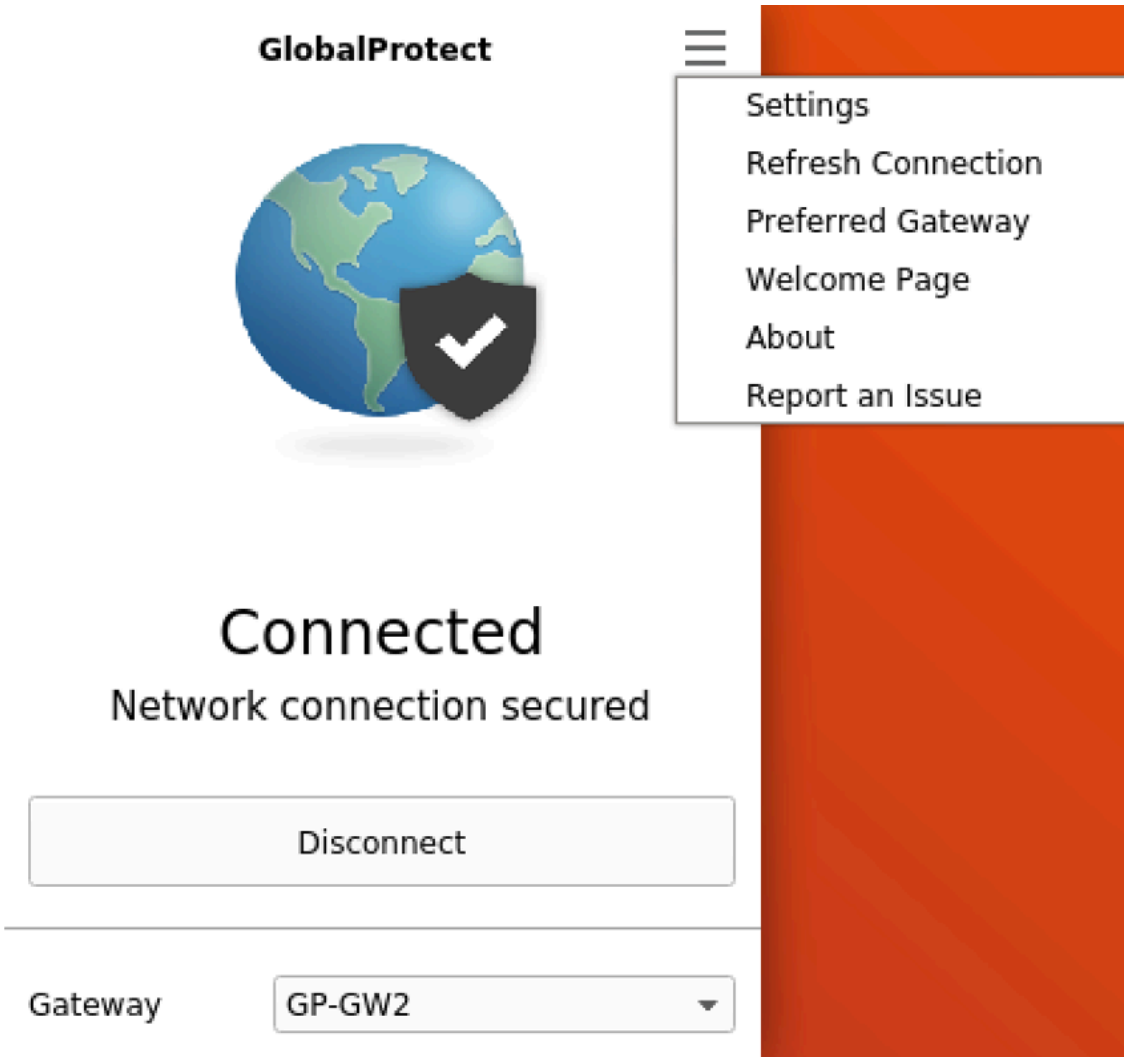
GlobalProtect 시스템 트레이 아이콘을 클릭하여 앱 인터페이스를 시작합니다.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | 엔드포인트에서 GlobalProtect 앱의 문제를 보고합니다.

앱을 실행한 후 앱 패널의 오른쪽 상단에 있는 메뉴(≡)를 선택하여 관리자에게 문제를 보고합니다.

1. 문제 신고를 선택합니다.



2. 진단 테스트를 실행하고 진단 로그를 포함하도록 GlobalProtect 앱을 활성화합니다. 진단 및 문제 해결 로그가 모두 수집되어 간결한 문제 해결 보고서로 Cortex Data Lake에 전송됩니다.

   진단 테스트가 완료되면 GlobalProtect 디버그 로그 파일이 엔드포인트에서 Cortex Data Lake로 업로드됩니다.

   앱에서 진단 테스트를 실행하고 진단 로그를 포함하도록 설정하지 않으면 문제 해결 로그만 수집되어 압축 문제 해결 보고서로 *Cortex Data Lake*에 전송됩니다. *GlobalProtect* 앱은 `.json` 형식으로 자동 생성되는 보고서 파일(*pan_gp.trb.log* 또는 *pan_gp_trbl.log*)을 확인합니다. 문제 해결 로그에서 문제가 발견되지 않은 경우 알림 메시지가 표시됩니다. 다시 시도를 클릭하여 *pan_gp.trb*.log* 파일이 있는지 확인합니다.

3. 진단 테스트 실행 및 진단 로그 포함 확인란을 선택합니다.

 ©2023 Palo Alto Networks, Inc.

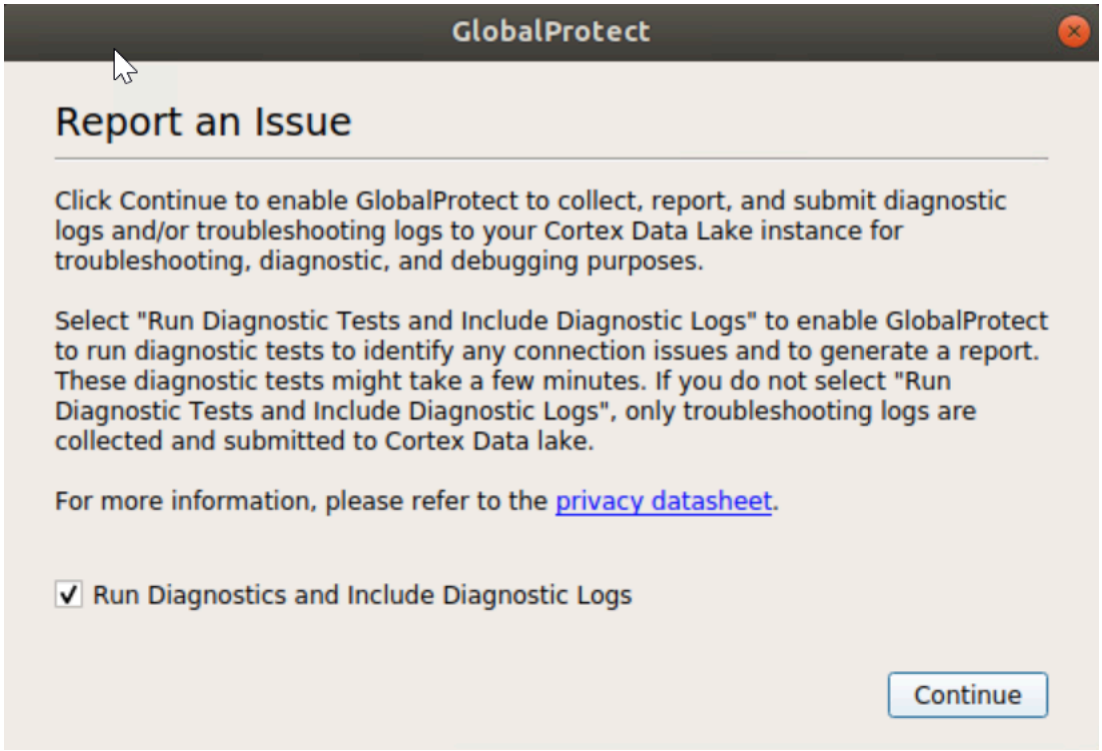
4. 계속을 클릭하면 앱이 문제 해결 로그를 생성하고 관리자의 Cortex Data Lake 인스턴스로 보고서를 전송할 수 있습니다.

   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다.

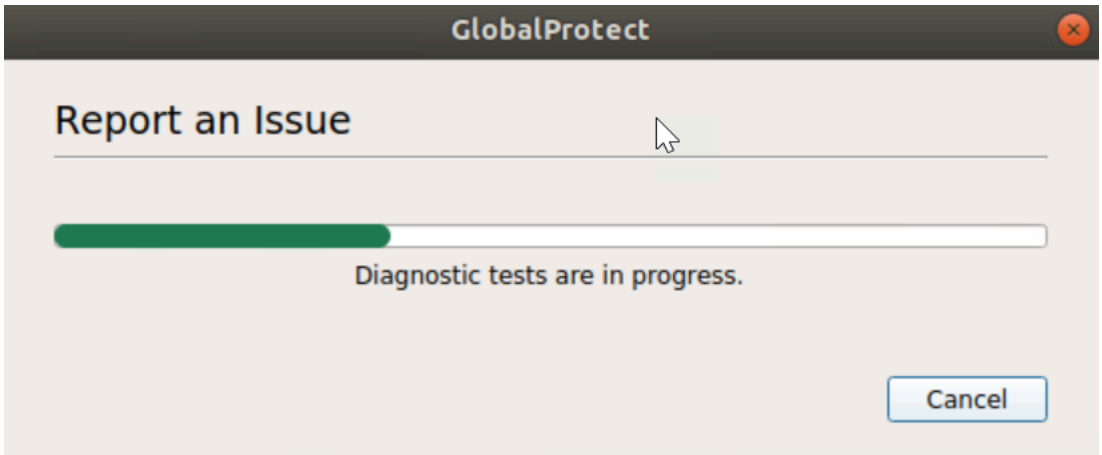
   종단 간 진단 테스트의 결과는 pan_gp_diag.log 파일에 `.json` 형식으로 저장되고 pan_gp.trb*.log 파일과 함께 관리자의 Cortex Data Lake 인스턴스로 전송됩니다. GlobalProtect 앱은 터널을 사용하거나 터널 없이 진단 테스트를 실행할 수 있습니다. 예를 들어

 ©2023 Palo Alto Networks, Inc.

앱이 터널을 통해 진단 테스트를 연결하고 실행하기 전에 GlobalProtect 로그인 자격 증명을 입력할 수 있습니다.

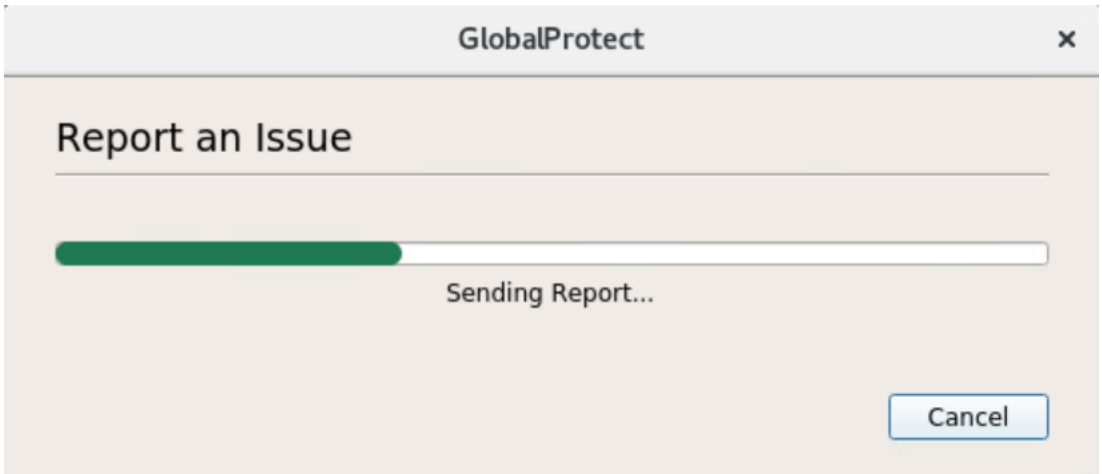


진단 테스트 실행 및 진단 로그 포함 확인란을 선택한 경우에만 앱이 진단 테스트를 실행하고 있음을 확인하는 메시지가 팝업됩니다.

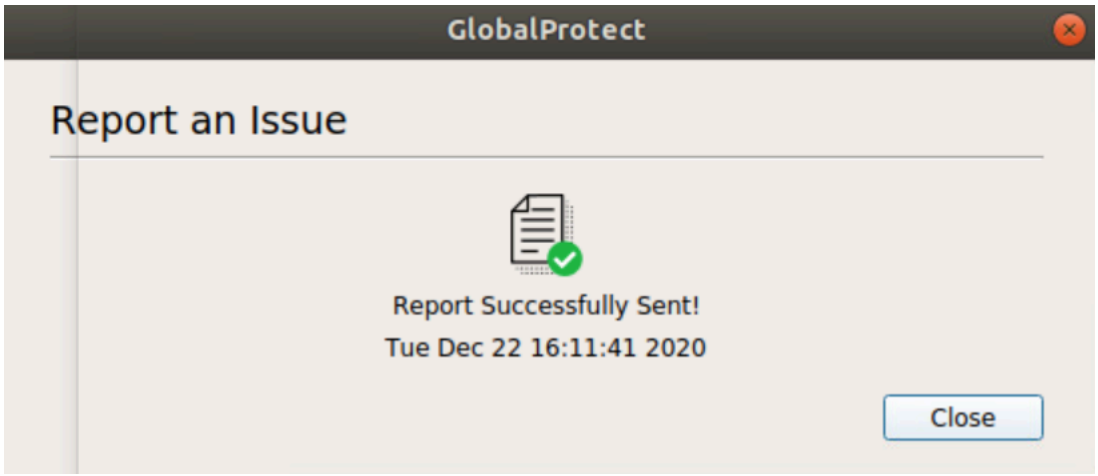


앱이 Cortex Data Lake로 보고서를 보내고 있음을 확인하는 메시지가 표시됩니다.

 ©2023 Palo Alto Networks, Inc.



5. 닫기를 클릭하여 앱이 Cortex Data Lake로 보고서를 전송했는지 확인합니다. 이 확인 메시지에는 보고서가 처리되고 전송된 날짜 및 시간이 표시됩니다.



 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱 연결 해제

관리자가 GlobalProtect 연결 방법을 항상 켬으로 구성한 경우 GlobalProtect 앱의 연결을 끊을 수 있습니다. 예를 들어 호텔에서 GlobalProtect 가상 사설망(VPN)이 작동하지 않고 VPN 오류로 인해 인터넷에 연결할 수 없는 경우 앱 연결을 끊을 수 있습니다. GlobalProtect 앱의 연결을 끊은 후 보안되지 않은 통신(VPN 없이)을 사용하여 인터넷에 연결할 수 있습니다.

GlobalProtect 앱의 연결을 끊을 수 있는 방법, 시간 및 횟수는 관리자가 GlobalProtect 서비스를 구성하는 방법에 따라 다릅니다. 이 구성을 사용하면 앱 연결을 완전히 끊지 못하거나 챌린지에 올바르게 응답한 후에만 앱 연결을 끊을 수 있습니다.

구성에 챌린지가 포함된 경우 GlobalProtect 앱은 다음 중 하나를 묻는 메시지를 표시합니다.

- 앱 연결을 해제하려는 이유
- 암호

챌린지에 암호와 관련된 경우 전화로 GlobalProtect 관리자 또는 헬프 데스크 담당자에게 문의하는 것이 좋습니다. 관리자는 일반적으로 이메일(신규 GlobalProtect 사용자의 경우)을 통하거나 조직의 웹 사이트에 게시하여 암호를 미리 제공합니다. 중단 또는 시스템 문제에 대한 응답으로 관리자는 전화로 암호를 제공할 수도 있습니다.

GlobalProtect는 Linux용 GlobalProtect 앱의 두 가지 버전을 지원합니다. Linux 디바이스가 GUI를 지원하는 경우 One 버전, Linux 디바이스가 GUI를 지원하지 않는 경우 CLI 버전을 지원합니다.

- GUI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 끊기
- CLI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 해제

GUI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 끊기

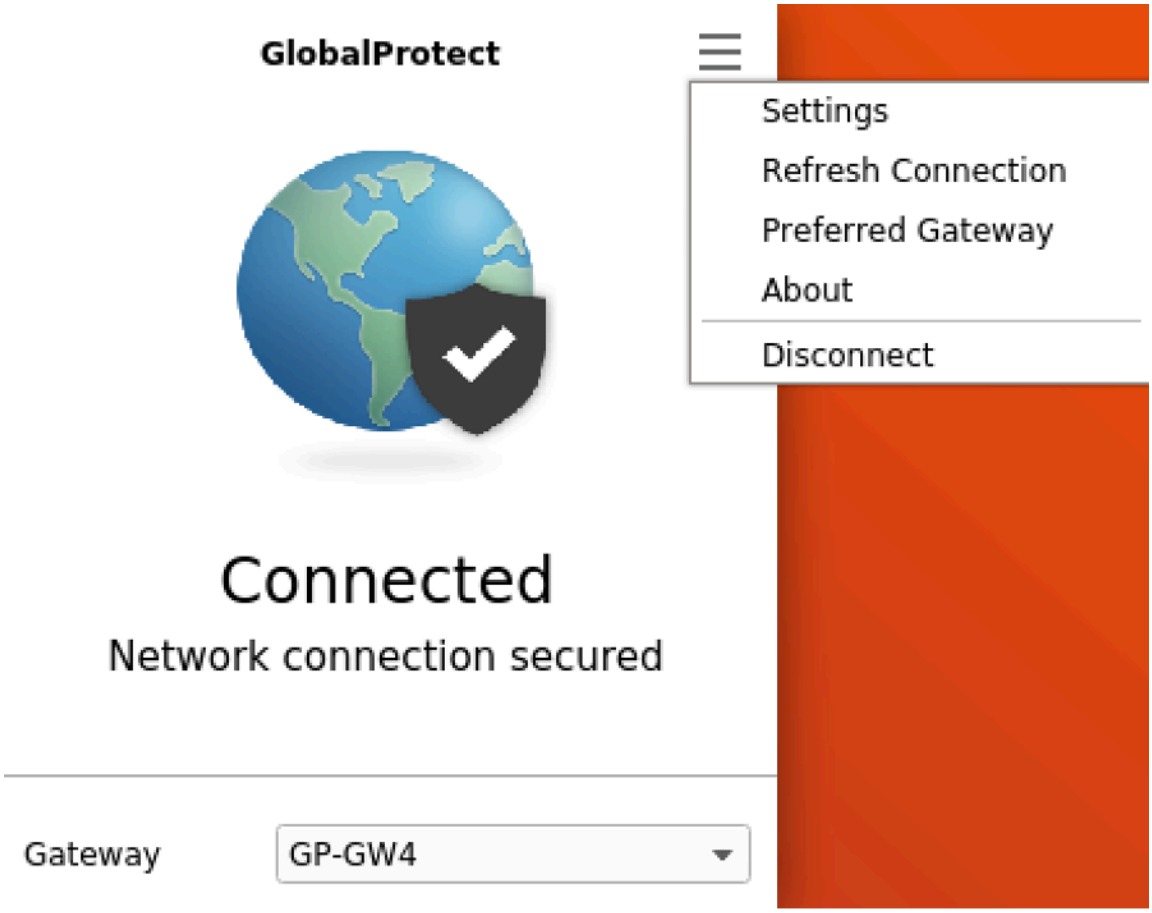
(항상 켬 모드에서만 사용 가능) GUI 버전을 사용하여 Linux용 GlobalProtect 앱의 연결을 해제하려면 다음 단계를 완료하십시오.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | GlobalProtect 앱의 연결을 끊습니다.

1. GlobalProtect 시스템 트레이 아이콘을 클릭하여 GlobalProtect 앱을 실행합니다. 상태 패널이 열립니다.
2. 앱 패널의 오른쪽 상단에 있는 메뉴(≡)를 선택하여 설정 메뉴를 엽니다.
3. 연결 해제를 선택합니다.

> 연결 해제 옵션은 *GlobalProtect* 에이전트 구성에서 앱 연결을 끊을 수 있는 경우에만 표시됩니다. 구성을 통해 챌린지에 응답할 필요 없이 *GlobalProtect* 앱의 연결을 끊을 수 있는 경우 추가 조치 없이 *GlobalProtect* 앱이 닫힙니다.

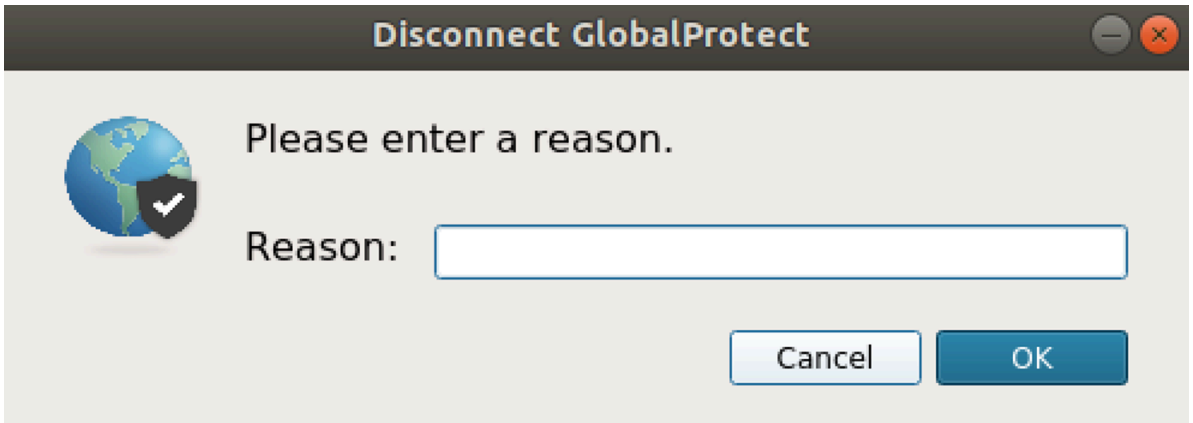


 ©2023 Palo Alto Networks, Inc.

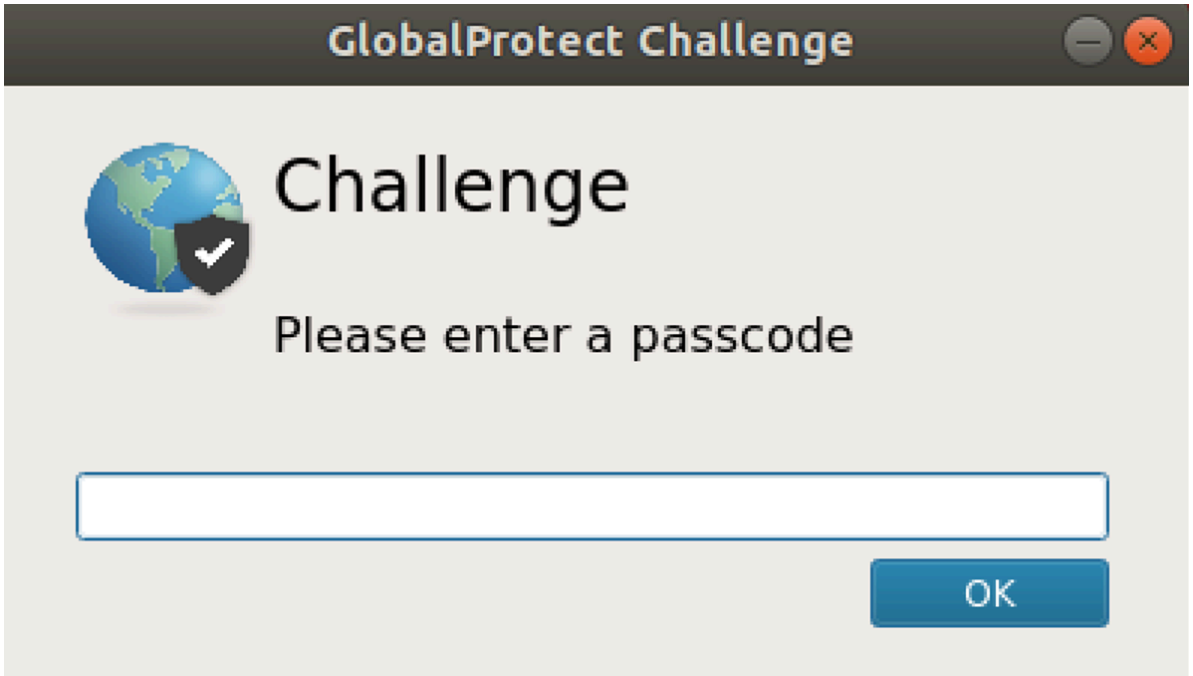
STEP 2 | 필요한 경우 하나 이상의 챌린지에 대응합니다.

메시지가 표시되면 다음 정보를 제공합니다.

- 이유—GlobalProtect 앱의 연결을 해제하는 이유입니다.



- 암호—앱 연결을 해제해야 하는 알려진 문제 또는 이벤트에 따라 관리자가 일반적으로 미리 제공하는 암호입니다.



CLI 버전을 사용하여 Linux용 GlobalProtect 앱 연결 해제

CLI 버전을 사용하여 Linux용 GlobalProtect 앱의 연결을 끊으려면 다음 단계를 완료하십시오.

 ©2023 Palo Alto Networks, Inc.

- (주문형 모드에서만 사용 가능) GlobalProtect에서 연결 해제:

  globalprotect disconnect 명령을 사용하여 GlobalProtect의 연결을 끊습니다.

```
user@linuxhost:~$ globalprotect disconnect GlobalProtect 상태: 연
결 해제됨
```

- (항상 켬 모드에서만 사용 가능) GlobalProtect 연결 해제:

  globalprotect disconnect 명령을 사용하여 GlobalProtect 앱의 연결을 끊고 비활성화합니다. 구성에 필요한 경우 메시지가 표시되면 이유 또는 암호도 지정해야 합니다.

```
user@linuxhost:~$ globalprotect disconnect
```

```
user@linuxhost:~$ globalprotect disconnect 연결을 끊는 이유를 입력하십
시오. 이것이 연결을 끊는 이유입니다.
```

```
user@linuxhost:~$ globalprotect disconnect 연결 해제 암호를 입력하십시
오 ITp@ssw0rd
```

 ©2023 Palo Alto Networks, Inc.

Linux용 GlobalProtect 앱 제거

Linux용 GlobalProtect 앱은 dpkg와 apt-get 유틸리티를 사용하여 제거할 수 있습니다. GlobalProtect 앱을 제거하려면 루트 권한으로 명령을 실행해야 합니다.

- **sudo dpkg -P globalprotect** 명령을 입력하여 설치 제거 프로세스를 시작합니다.

```
user@linuxhost:~$ sudo dpkg -P globalprotect(데이터베이스 읽
기 ... 209181개의 파일 및 디렉토리가 현재 설치되어 있습니다.)
 globalprotect(4.1.0-12) 제거 중... GP 서비스가 실행 중이며 중지해야 합니
다... 서비스 비활성화... GP 서비스를 제거하는 중... GP 서비스가 삭제되었습니
다. 구성 제거 중...
```

- **sudo apt-get remove globalprotect** 명령을 입력하여 Linux용 GlobalProtect 앱을 삭제합니다.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

IoT 디바이스용 GlobalProtect

GlobalProtect™는 엔드포인트(데스크톱 컴퓨터, 노트북, 서버 또는 IoT 디바이스)에서 실행되는 애플리케이션으로, 회사 네트워크의 중요한 리소스를 보호하는 것과 동일한 보안 정책을 사용하여 사용자를 보호합니다. IoT 디바이스의 경우 GlobalProtect™는 인터넷 또는 회사 네트워크 내의 모든 소스 또는 대상에 대한 디바이스 간 트래픽을 보호합니다.

다음 운영 체제에 내장된 IoT 디바이스에 GlobalProtect를 설치할 수 있습니다.

> Android의 IoT

> Raspbian의 IoT

> Ubuntu의 IoT

> Windows의 IoT

 ©2023 Palo Alto Networks, Inc.