paloalto TECHDOCS

GlobalProtect App User Guide

Version 6.2

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

Last Revised

May 19, 2023

Table of Contents

GlobalProtect App for Windows

GlobalProtect™ is an application that runs on your endpoint (desktop computer, laptop, tablet, or smart phone) to protect you by using the same security policies that protect the sensitive resources in your corporate network. GlobalProtect™ secures your data center, private cloud, public cloud, and internet traffic and allows you to access your company's resources from anywhere in the world.

The following topics describe how to install and use the GlobalProtect app for Windows:

Download and Install the GlobalProtect App for Windows

Before connecting to the GlobalProtect network, you must download and install the GlobalProtect app on your Windows endpoint. To ensure that you get the right app for your organization's GlobalProtect or Prisma Access deployment, you must download the app directly from a GlobalProtect portal within your organization. For this reason, there is no direct GP app download link available on the Palo Alto Networks site.

Before you can download and install the GP app, you must obtain the IP address or fully qualified domain name (FQDN) of the GlobalProtect portal from your GP administrator. In addition, your administrator should verify which username and password information you can use to connect to the portal and gateways. In most instances, the username and password is the same username and password that you use to connect to your corporate network. After you gather the required information, use the following steps to download and install the app:

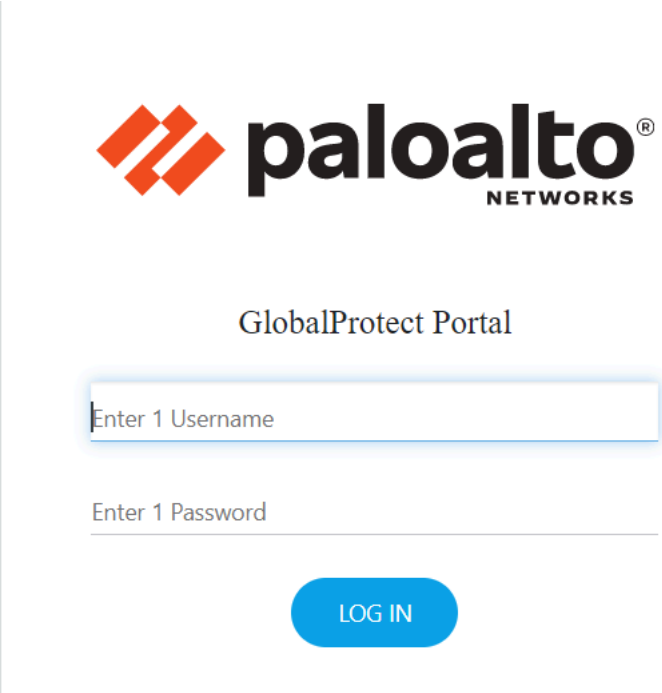
To run GlobalProtect app 5.0 and later, Windows endpoints require Visual C++ Redistributables 12.0.3 for Visual Studio 2013. If you have not already installed any redistributable packages on your endpoint, the GlobalProtect app installs Visual C ++ Redistributables 12.0.3 automatically. If you have already installed Visual C++ Redistributables 12.0.2 or an earlier release, you must either uninstall the existing redistributable packages from your endpoint or upgrade to Visual C++ Redistributables 12.0.3 prior to installing the GlobalProtect app.

STEP 1 | Log in to the GlobalProtect portal.

1. Launch a web browser and go to the following URL:

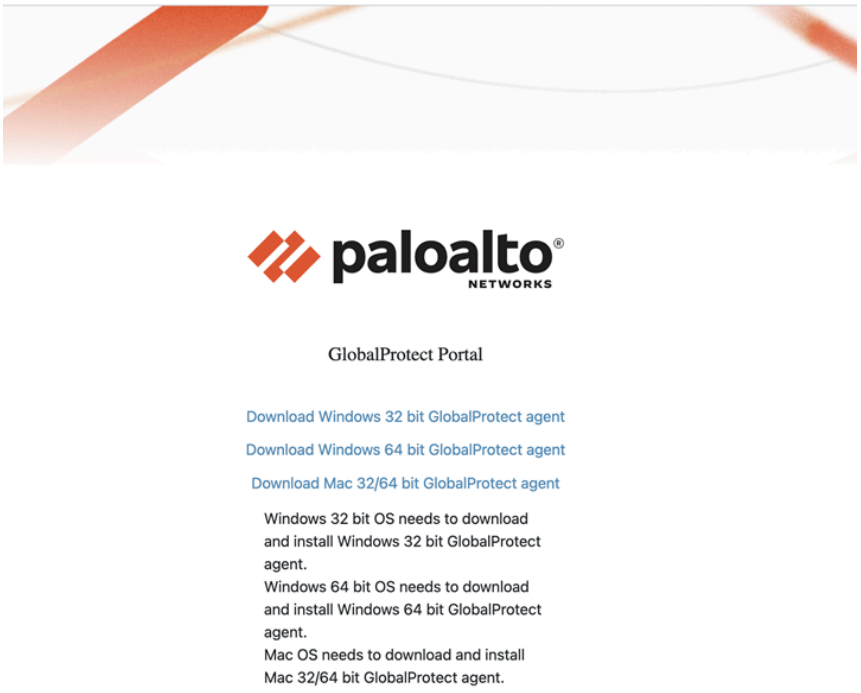
   `https://<portal IP address or FQDN>`

   Example: **`http://gp.acme.com`**
2. On the portal login page, enter your **Name** (username) and **Password**, and then click **LOG IN**. In most instances, you can use the same username and password that you use to connect to your corporate network.

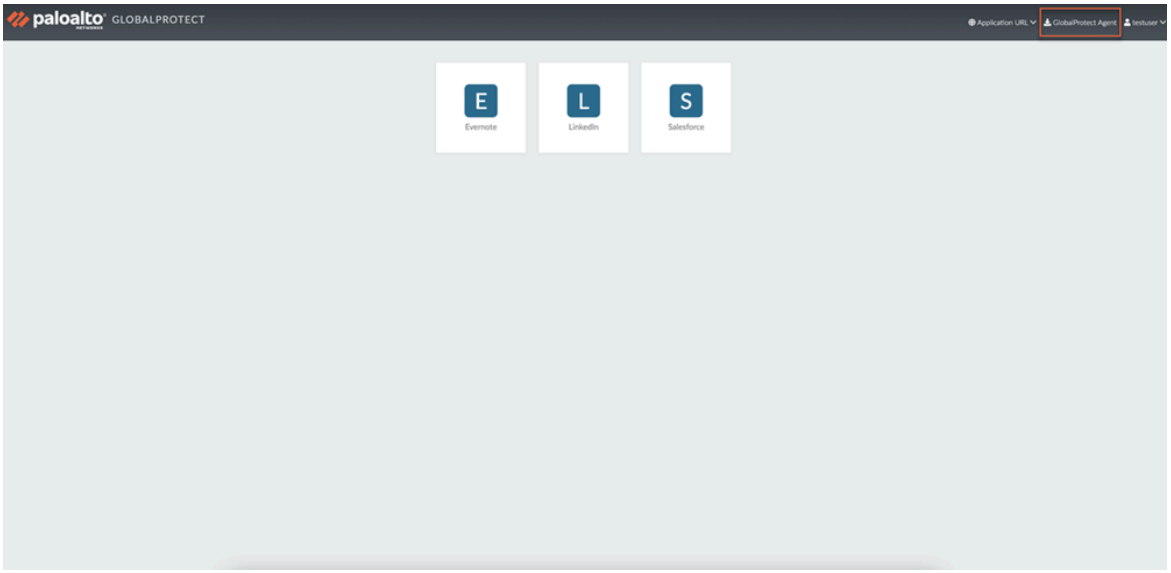


STEP 2 | Navigate to the app download page.

In most instances, the app download page appears immediately after you log in to the portal. Use this page to download the latest app software package.

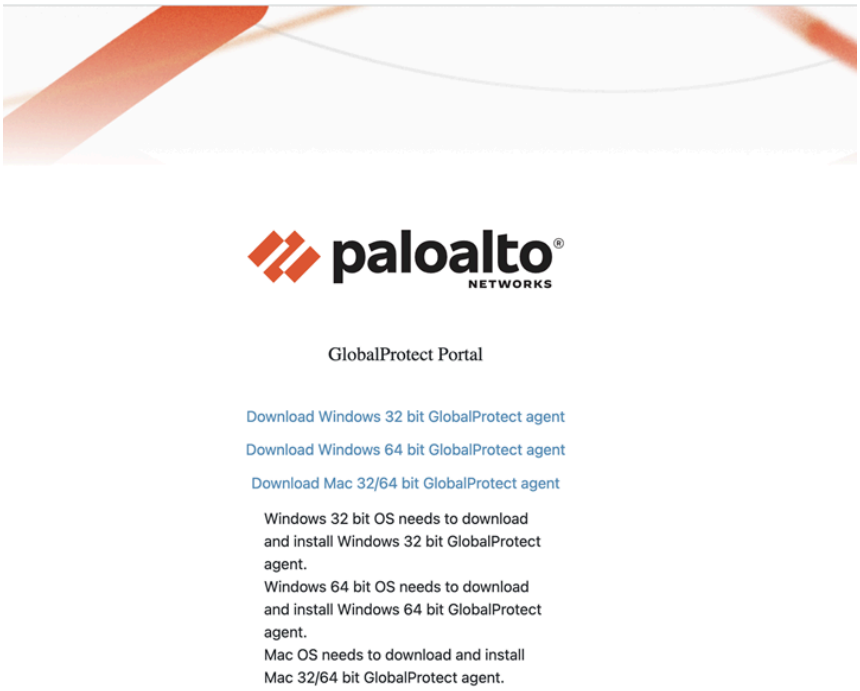


If your system administrator has enabled GlobalProtect Clientless VPN access, the applications page opens after you log in to the portal (instead of the app download page). Select **GlobalProtect Agent** to open the download page.



STEP 3 | Download the app.

1. To begin the download, click the software link that corresponds to the operating system running on your computer. If you are not sure whether the operating system is 32-bit or 64-bit, ask your system administrator before you proceed.



2. Open the software installation file.
3. When prompted, **Run** the software.
4. When prompted again, **Run** the GlobalProtect Setup Wizard.

STEP 4 | Complete the GlobalProtect app setup.

1. In the GlobalProtect Setup Wizard, click **Next**.
2. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks \GlobalProtect) and then click **Next** twice.

   *Although you can **Browse** to select a different location in which to install the GlobalProtect app, the best practice is to install it in the default location. The default installation location is read-only for non-privileged users and therefore installing to this location protects against malicious access to the app.*

3. After installation is complete, **Close** the wizard.

Use Connect Before Logon

The Pre-logon and Pre-logon then On-demand connection methods are not supported simultaneously with Connect Before Logon.

Connect Before Logon is not supported for internal gateway configurations.

To simplify the login process and improve your experience, GlobalProtect offers Connect Before Logon to allow you to establish the VPN connection to the corporate network before logging in to the Windows 10 endpoint using a Smart card, authentication service such as LDAP, RADIUS, or Security Assertion Markup Language (SAML), username/password-based authentication, or one-time password (OTP) authentication. Administrators can benefit from enabling Connect Before Logon when they onboard new GlobalProtect users on the endpoint that is not set up with a local profile or account for the user. Connect Before Logon is disabled by default. When the administrator enables Connect Before Logon, you can launch the GlobalProtect app credential provider and connect to the corporate network before logging in to Windows endpoint. After Connect Before Logon establishes a VPN connection, you can use the Windows logon screen to log in to the Windows endpoint. GlobalProtect can act as a Pre-Login Access Provider (PLAP) credential provider to provide access to your organization before logging in to Windows.

Because Connect Before Logon prompts you to authenticate twice on the portal and gateway when logging in to the Windows endpoint for the first time, the Authentication Override cookie is not working as expected.

To use Connect Before Logon, the administrator must deploy the settings in the Windows registry and you choose the authentication method:

- Connect Before Logon Using Smart Card Authentication
- Connect Before Logon Using SAML Authentication
- Connect Before Logon Using Username/Password-Based Authentication

Connect Before Logon Using Smart Card Authentication

Connect Before Logon supports smart card authentication. The administrator must import the Root CA certificate that issued the certificates contained on the smart card onto the portal and gateway. The administrator can apply the certificate profile and that Root CA to your portal or gateway configuration to enable use of the smart card in the authentication process. You can authenticate to GlobalProtect prior to logging into the Windows endpoint using a smart card. When prompted, insert your smart card to verify that smart card authentication is successful. If smart card authentication is successful, GlobalProtect will connect to the portal or gateway specified in the configuration.

STEP 1 | Before you can use Connect Before Logon, the administrator must have completed the following tasks:

1. Deploy Connect Before Logon Settings in the Windows Registry.
2. Set up the smart card for two-factor authentication.
3. Assign the certificate profile to the GlobalProtect portal.
4. Configure the gateway to authenticate end users based on a smart card.

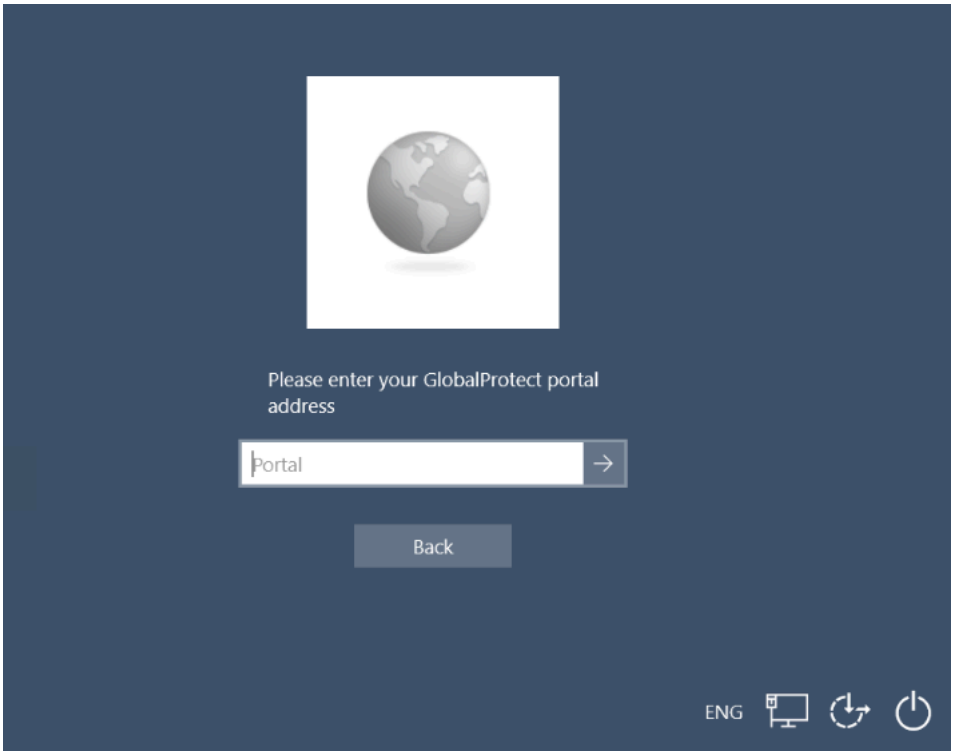
STEP 2 | Log in to the Windows endpoint using Connect Before Logon.

1. Click the **Network Sign-In** ( ) button at the lower right corner of the Windows logon screen.

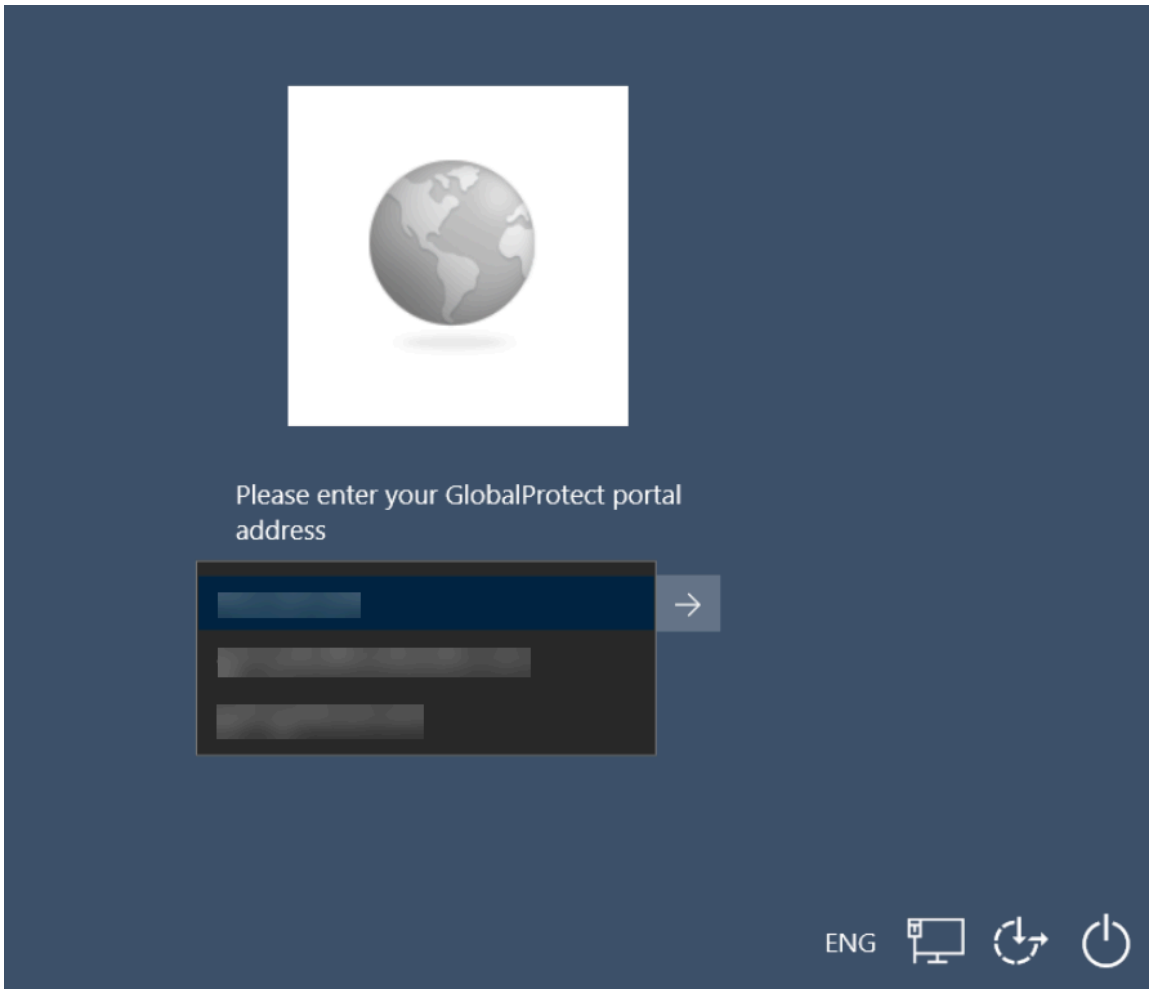
   If the VPN connection is successful, the **Disconnect** ( ) button appears next to the **Network Sign-In** button of the Windows logon screen. You are logged out of the VPN

if you have not yet logged in to your endpoint within the configured time period. This causes the VPN tunnel to disconnect.

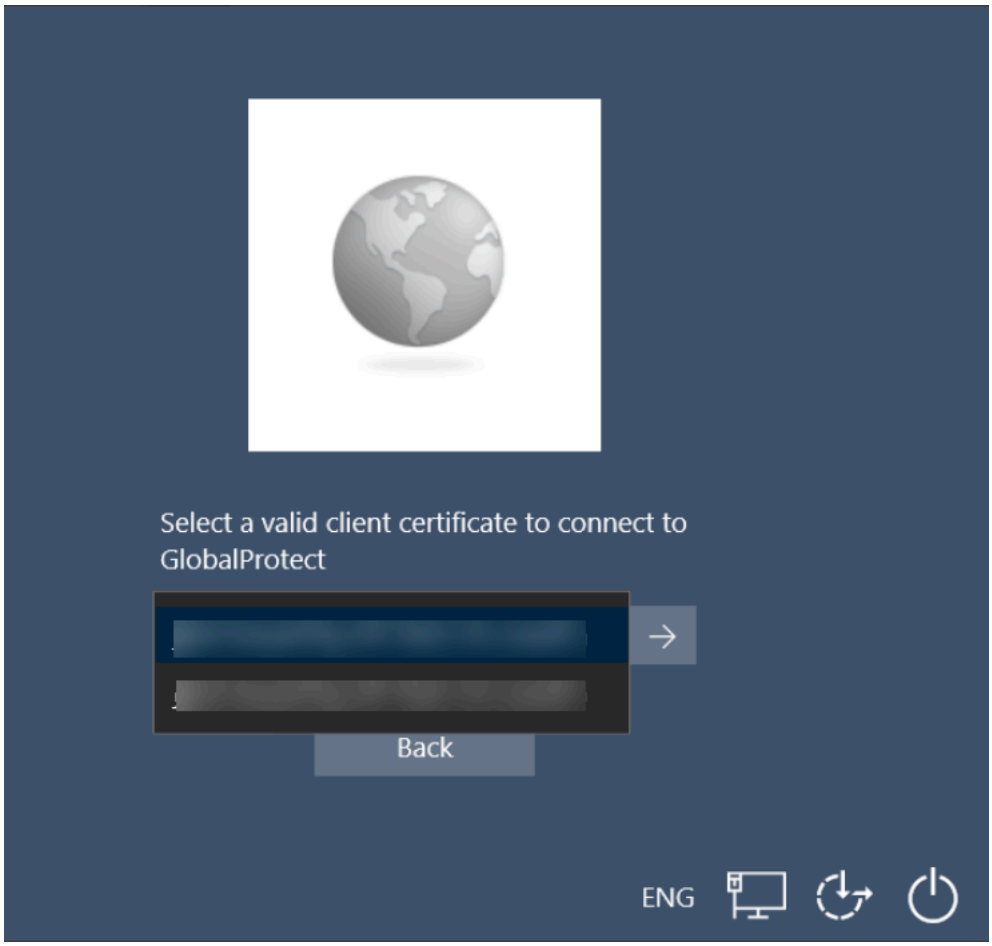
2. (Optional) If you are logging in to the endpoint for the first time and the portals have not been predefined by the administrator, enter the FQDN or IP address of the GlobalProtect portal, and **Submit**.



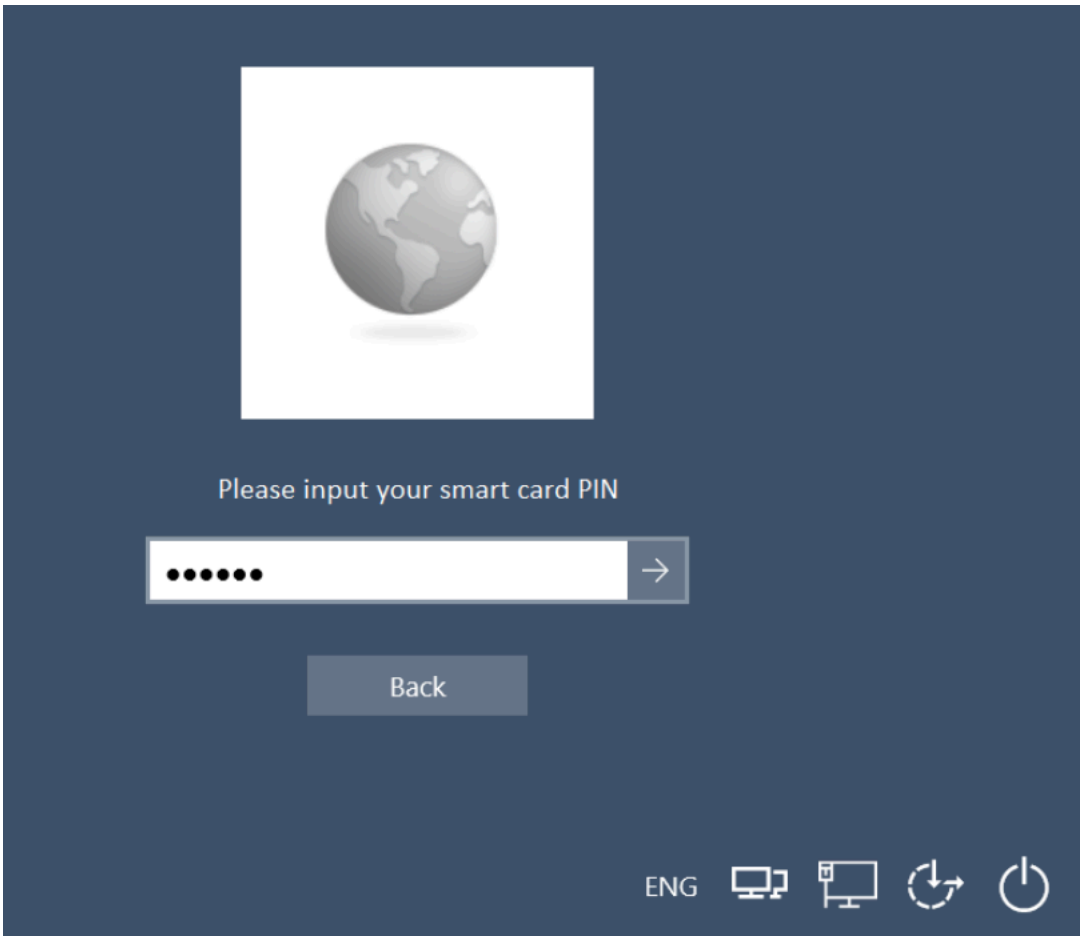
3. (Optional) If you are logging in to the endpoint for the first time and the portals have been predefined by the administrator, select a portal from the **Portal** drop-down, and click the arrow to submit.



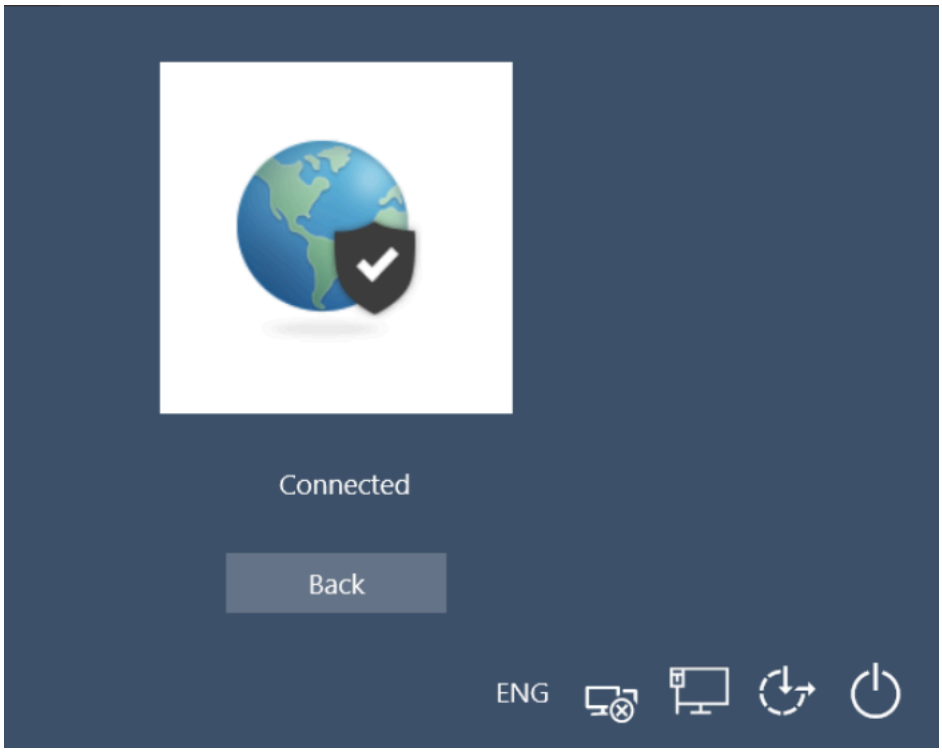
4. Select the client certificate from a list of valid certificates on the endpoint to authenticate with the portal or gateway, and click the arrow to submit.



5. Enter the Personal Identification Number (PIN) of the smart card, and click the arrow to submit.



6. If authentication is successful, the connection status displays **Connected** upon successful VPN connection. Click **Back** to display the Windows logon screen.



STEP 3 | Verify that you are connected to the GlobalProtect gateway.

1. Log in to the Windows endpoint again. Click the **Network Sign-In** ( ) button at the lower right corner of the Windows logon screen.
2. The status panel opens. By default, you are automatically connected to the **Best Available** gateway.

Connect Before Logon Using SAML Authentication

Connect Before Logon supports SAML authentication for user login. You can authenticate to GlobalProtect prior to logging into the Windows endpoint using the configured SAML identity providers (IdPs) such as Onelogin or Okta. If SAML authentication is successful, GlobalProtect will connect to the portal or gateway specified in the configuration.

Connect Before Logon with SAML authentication method is supported on all GlobalProtect versions when using the older embedded webview (oew). However, blank screen and JavaScript errors may be intermittently displayed when loading certain external IdP URLs in the Connect Before Logon mode. This issue arises from the fact that the older embedded webview uses the legacy IE browser, which has been deprecated in Windows 11. The alternative Edge browser-based WebView2 does not support Connect Before Logon method. GlobalProtect will continue to use the legacy IE-based older embedded webview (oew) with the above limitation.

STEP 1 | Before you can use Connect Before Logon, the administrator must have completed the following tasks:

1. Deploy Connect Before Logon Settings in the Windows registry.
2. Set up SAML authentication to authenticate end users.
   - Create a server profile with settings to the SAML authentication service.
   - Create an authentication profile that refers to the SAML server profile.
3. Specify SAML authentication for the GlobalProtect gateway.
4. Specify a SAML authentication for the client (see Define the GlobalProtect Client Authentication Configurations).

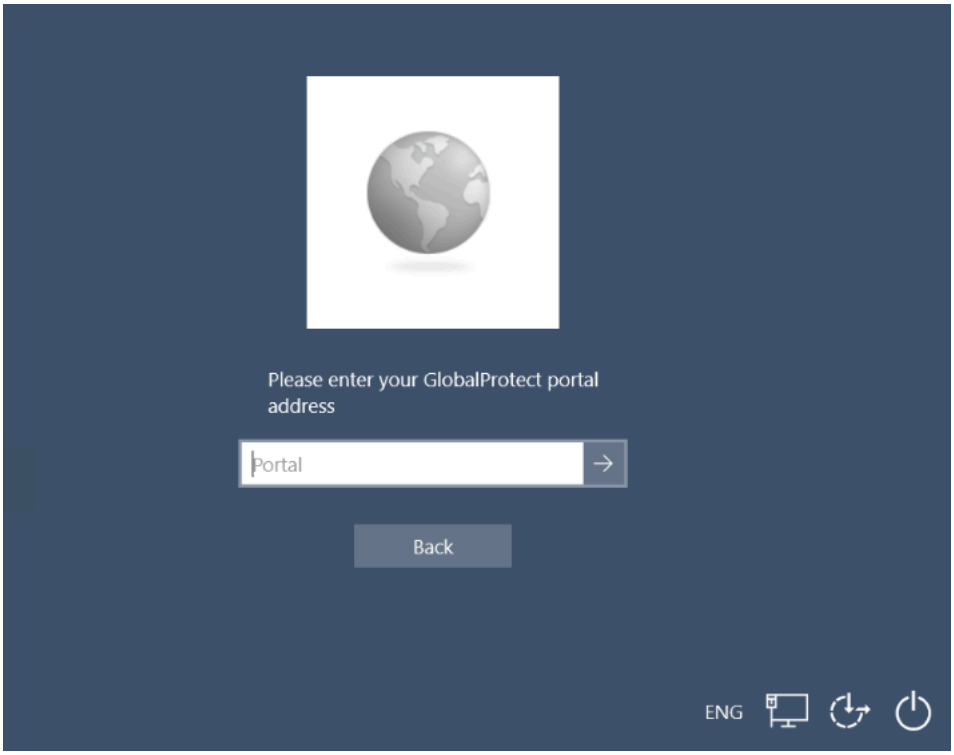
STEP 2 | Log in to the Windows endpoint using Connect Before Logon.

1. Click the **Network Sign-In** ( ) button at the lower right corner of the Windows logon screen.

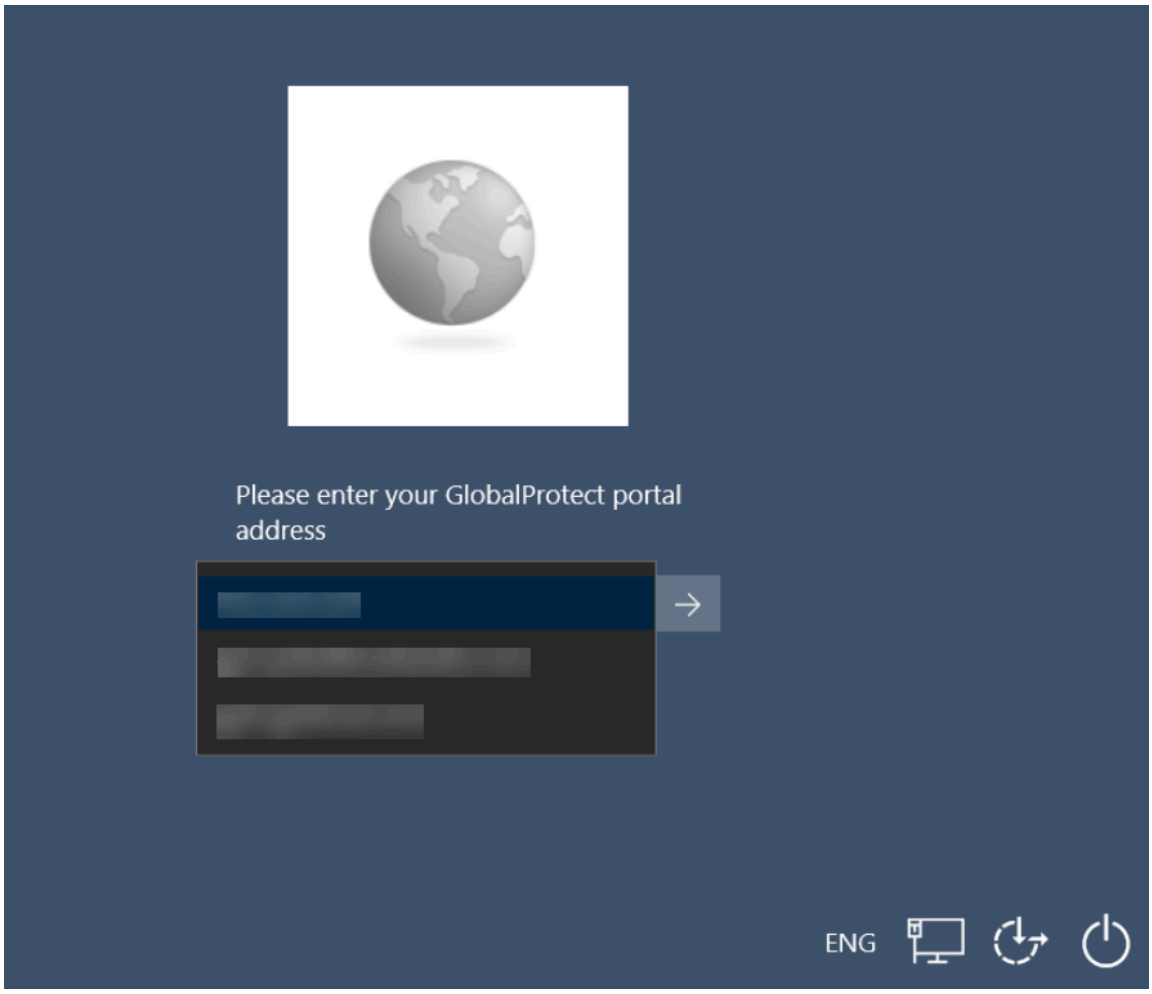
   If the VPN connection is successful, the **Disconnect** ( ) button appears next to the **Network Sign-In** button of the Windows logon screen. You are logged out of the VPN

if you have not yet logged in to your endpoint within the configured time period. This causes the VPN tunnel to disconnect.

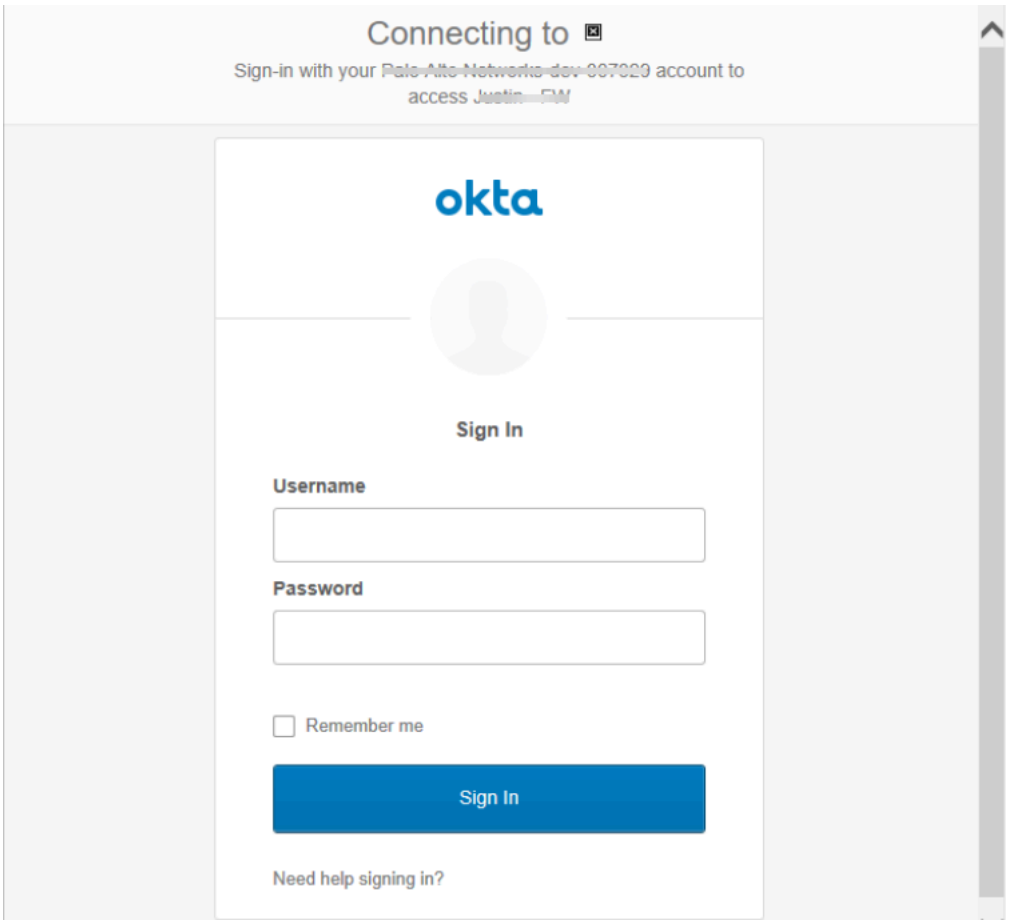
2. (Optional) If you are logging in to the endpoint for the first time and the portals have not been predefined by the administrator, enter the FQDN or IP address of the GlobalProtect portal, and click the arrow to submit.



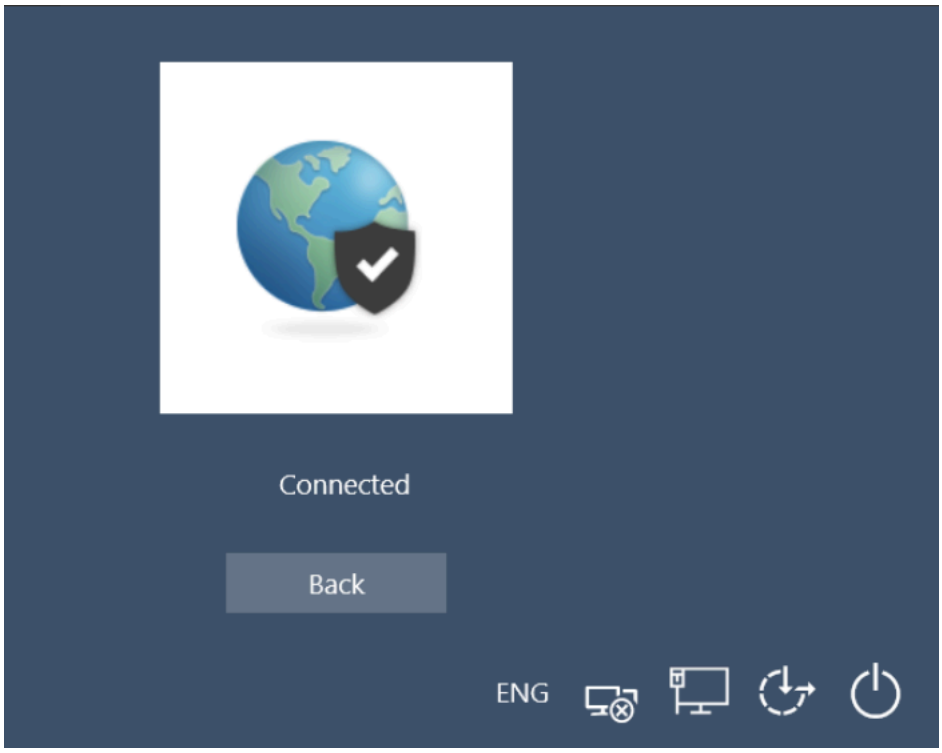
3. (Optional) If you are logging in to the endpoint for the first time and the portals have been predefined by the administrator, select a portal from the **Portal** drop-down, and click the arrow to submit.



4. Enter the username and password to authenticate to the IdP, and then click **Sign In**.



5. If authentication is successful, the connection status displays **Connected** upon successful VPN connection. Click **Back** to display the Windows logon screen.



STEP 3 | Verify that you are connected to the GlobalProtect gateway.

1. Log in to the Windows endpoint again. Click the **Network Sign-In** ( ) button at the lower right corner of the Windows logon screen.
2. The status panel opens. By default, you are automatically connected to the **Best Available** gateway.

Connect Before Logon Using Username/Password-Based Authentication

Connect Before Logon supports username/password-based authentication for user login using an authentication service such as LDAP, RADIUS, or OTP. You can authenticate to GlobalProtect prior to logging into the Windows endpoint using the username and password credentials. If username/password-based authentication is successful, GlobalProtect will connect to the portal or gateway specified in the configuration.

STEP 1 | Before you can use Connect Before Logon, the administrator must have completed the following tasks:

1. Deploy Connect Before Logon Settings in the Windows registry.
2. Set up access to the GlobalProtect portal to authenticate end users to the portal using their credentials.
3. Configure a GlobalProtect gateway to authenticate end users to the gateway using their credentials.

Connect Before Logon does not support a custom authentication message.

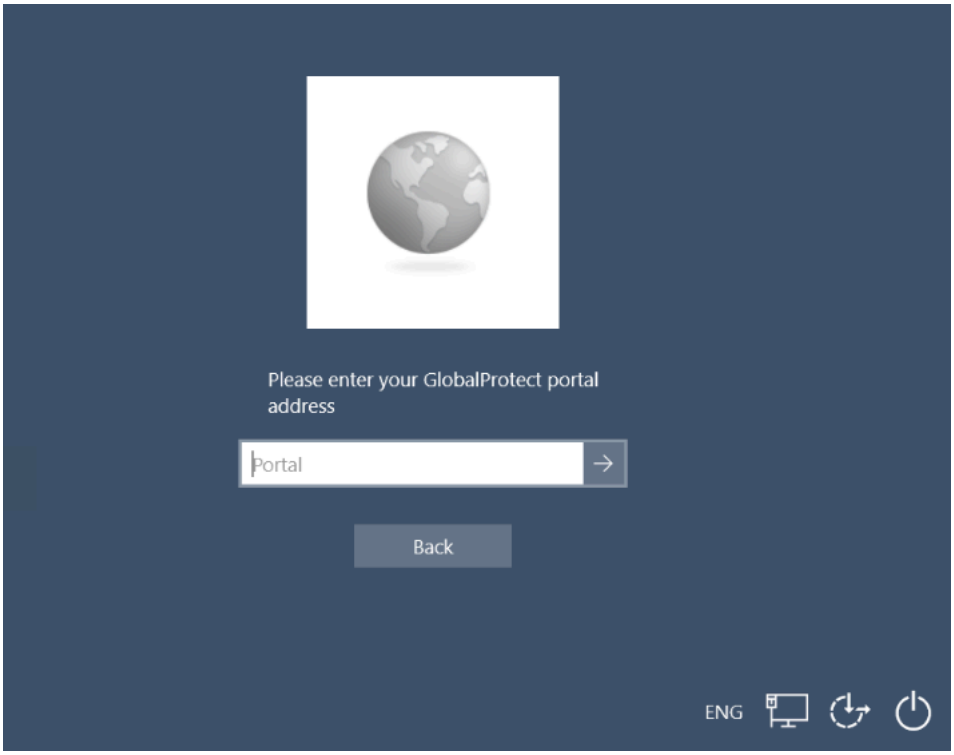
STEP 2 | Log in to the Windows endpoint using Connect Before Logon.

1. Click the **Network Sign-In** ( ) button at the lower right corner of the Windows logon screen.

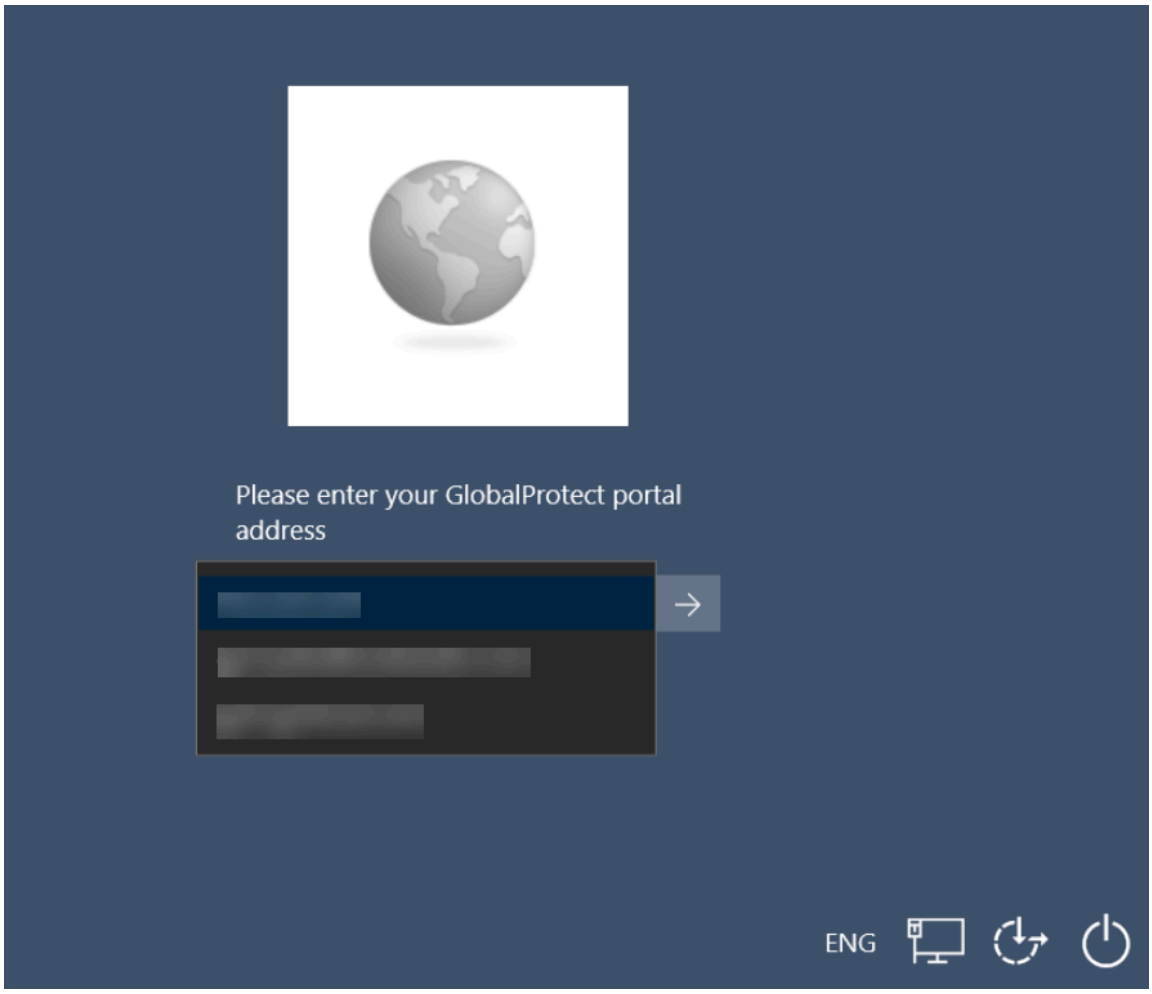
   If the VPN connection is successful, the **Disconnect** ( ) button appears next to the **Network Sign-In** button of the Windows logon screen. You are logged out of the VPN

if you have not yet logged in to your endpoint within the configured time period. This causes the VPN tunnel to disconnect.

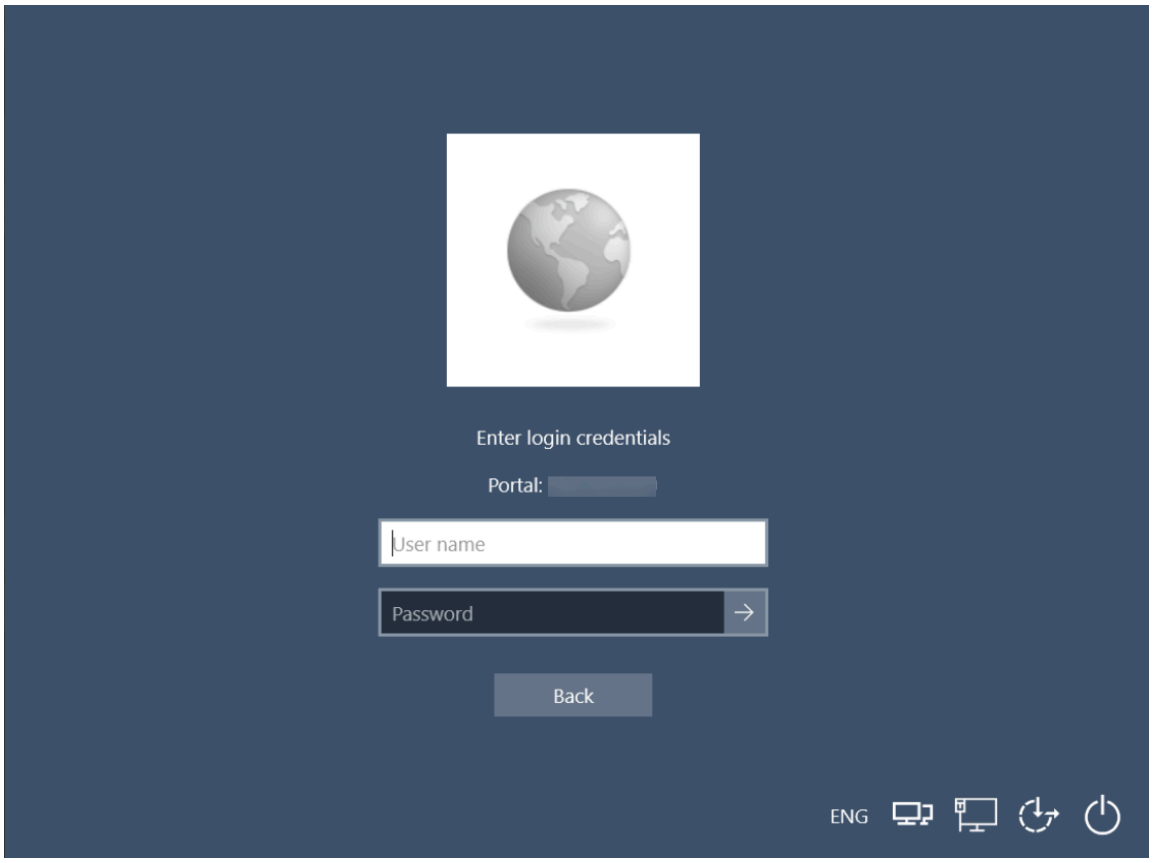
2. (Optional) If you are logging in to the endpoint for the first time and the portals have not been predefined by the administrator, enter the FQDN or IP address of the GlobalProtect portal, and click the arrow to submit.



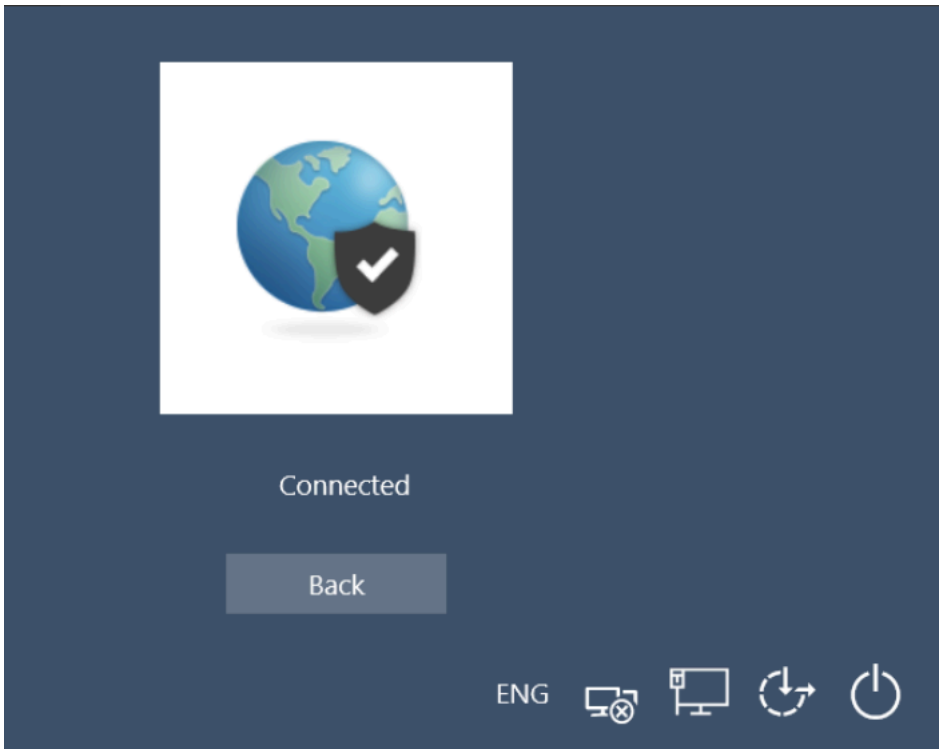
3. (Optional) If you are logging in to the endpoint for the first time and the portals have been predefined by the administrator, select a portal from the **Portal** drop-down, and click the arrow to submit.



4. Enter the username and password, and click the arrow to submit.



5. If authentication is successful, the connection status displays **Connected** upon successful VPN connection. Click **Back** to display the Windows logon screen.



STEP 3 | Verify that you are connected to the GlobalProtect gateway.

1. Log in to the Windows endpoint again. Click the **Network Sign-In** () button at the lower right corner of the Windows logon screen.
2. The status panel opens. By default, you are automatically connected to the **Best Available** gateway.

Use Single Sign-On for Smart Card Authentication

If your administrator has configured the GlobalProtect portal to allow you to authenticate through single sign-on (SSO) using smart card authentication, you can connect without re-entering your smart card Personal Identification Number (PIN) in the GlobalProtect app for a seamless SSO experience. You can leverage the same smart card PIN for GlobalProtect with your Windows endpoint. You can benefit from using SSO for smart card authentication by reducing the number of times you must enter your smart card PIN when you log in. After you successfully log in to the Windows endpoint, the GlobalProtect app acquires and remembers your smart card PIN to authenticate with the GlobalProtect portal and gateway.

Your administrator can define the type of PIN caching policy for Windows that is associated with the PIN for the smart card provider. The PIN is cached only if allowed from the smart card provider. GlobalProtect clears the PIN from the cache if you manually sign out of the GlobalProtect app, sign out of Windows, or the PIN is changed.

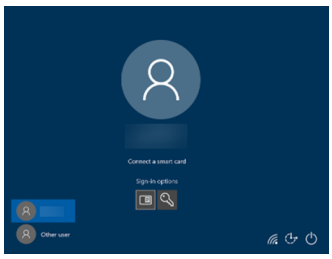
STEP 1 | Before you can use SSO for smart card authentication, the administrator must have completed the following tasks:

1. Set the pre-deployed setting on Windows endpoints to use SSO for smart card authentication.

   Your administrator must set the pre-deployed setting on your Windows endpoint prior to enabling SSO for smart card PIN. GlobalProtect retrieves this entry only once, when the GlobalProtect app initializes.
2. Set up the smart card for two-factor authentication.
3. Assign the certificate profile to the GlobalProtect portal.
4. Configure the gateway so that you can authenticate using a smart card.
5. Enable the GlobalProtect app to use SSO for smart card PIN on the GlobalProtect portal so that you can levearage the same smart card PIN for GlobalProtect with your Windows endpoint.

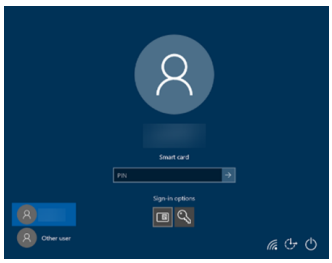
STEP 2 | Log in to the Windows endpoint using the smart card PIN.

1. Click **Sign-in options**, and then click the **smart card** ( ) button.
2. When prompted, insert the smart card to verify that smart card authentication is successful.



3. Enter the PIN for the smart card, and click the arrow to submit.

   If smart card authentication is successful, you can connect to the portal or gateway specified in the configuration without having to re-enter your smart card PIN.

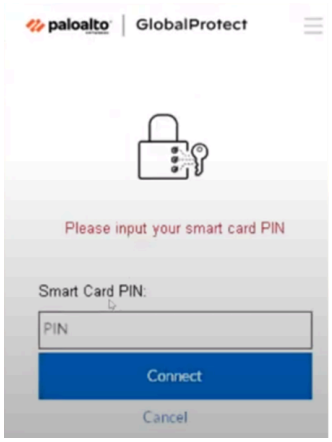


STEP 3 | (Optional) Log in to GlobalProtect using the same smart card PIN.

You can leverage the same smart card PIN that you used to log in to your Windows endpoint.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Click the hamburger menu to open the **Settings** panel.
3. On the **Settings** panel, **Sign Out** to clear your saved user credentials from the GlobalProtect app.
4. Reconnect to GlobalProtect with the same smart card PIN.

   The GlobalProtect app displays a smart card PIN error if the PIN is not valid.



Use the GlobalProtect App for Windows

This chapter applies to you only if your setup requires you to enter your GlobalProtect login credentials after you have logged in to your endpoint (single sign-on is disabled).

We typically recommend that organizations allow its GlobalProtect users to log in transparently following app installation. After you log in to an endpoint with transparent GlobalProtect login, the GlobalProtect app automatically initiates and connects to the corporate network without further user intervention.

If your setup requires you to enter your GlobalProtect credentials, follow the applicable steps below.

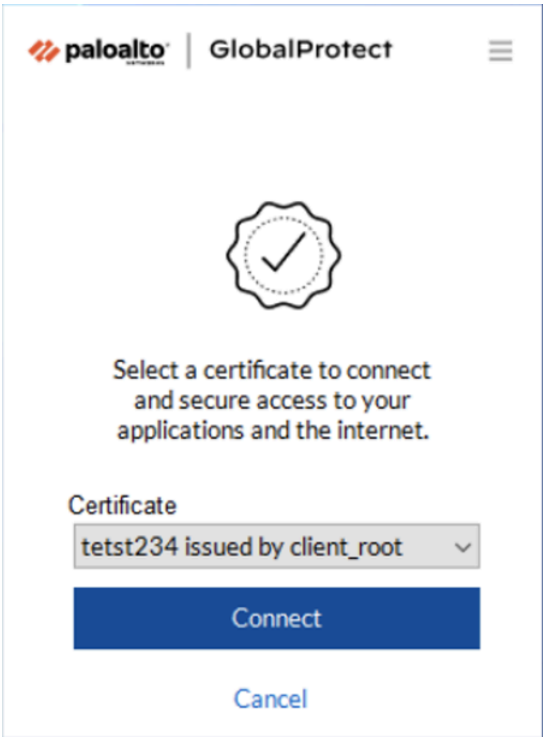
STEP 1 | Log in to GlobalProtect.

If you are logging in to the endpoint for the first time, the GlobalProtect app displays a friendly, welcome page upon successful login. Click **Get Started**.

1. (Optional) If your administrator configures GlobalProtect with the **On-Demand** connect method and you are logging in to GlobalProtect for the first time, select the client

certificate from a list of valid certificates from the **Certificate** drop-down to authenticate with the portal or gateway.

2. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.

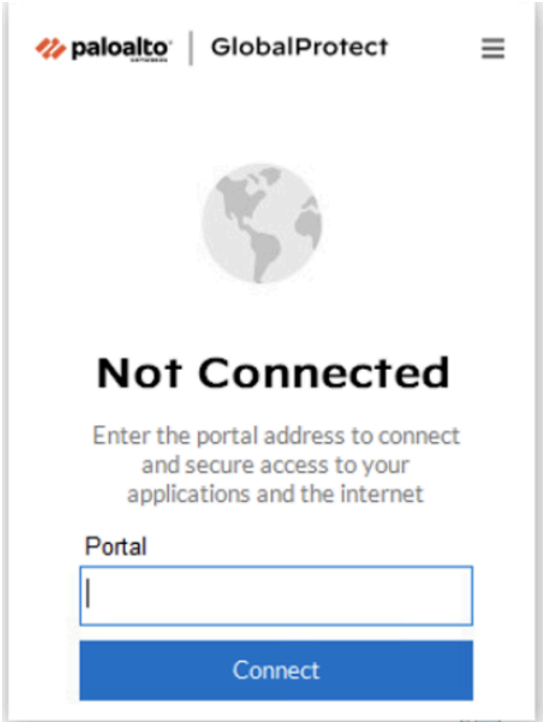


3. (Optional) Review your company's terms of service before connecting to GlobalProtect if your administrator requires you to see a page to access internal resources.

   If you do not accept terms of use, you will not be able to connect to GlobalProtect.

   Optionally, if you click **Cancel**, you must enter the IP address (or domain) of the GlobalProtect portal, and then click **Connect** to initiate the connection.

4. Enter the IP address or domain of the portal that your GlobalProtect administrator provided, and then click **Connect**.



5. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, select the gateway from the **Change Gateway** drop-down (for external gateways only).

   This option is only available if your administrator enables manual gateway selection.

6. (Optional) Depending on the connection mode, click **Connect** to initiate the connection.
7. (Optional) If prompted, enter your **Username** and **Password**, and then click **Sign In**.

   If your administrator has allowed you to use biometric (fingerprint) information to sign in, you need to first sign-in with a username and password twice (once to save it and again to authenticate); you can then use biometric information to sign in.

   If authentication is successful, you are connected to your corporate network, and the status panel displays the **Connected** or **Connected - Internal** status. If your administrator sets up a GlobalProtect welcome page, it displays after you log in successfully.

STEP 2 | Connect to the GlobalProtect portal or gateway.

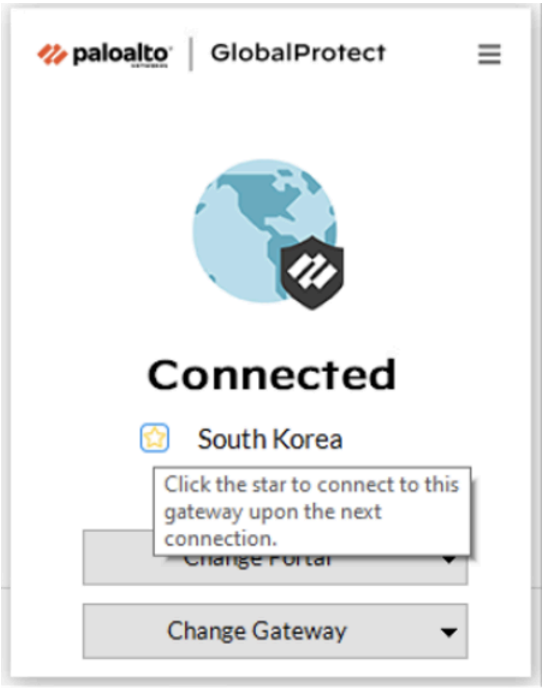
You can determine whether you are connected by checking the GlobalProtect system tray icon. If you are not connected, the icon is gray (), and ***Not Connected*** *appears when the you hover over the icon.*

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) If you are logging in to the GlobalProtect app for the first time, enter the IP address or domain of the GlobalProtect portal, and then click **Connect**.
3. (Optional) If multiple portals are saved on your app, select a portal from the **Change Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Change Portal** drop-down.
4. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the

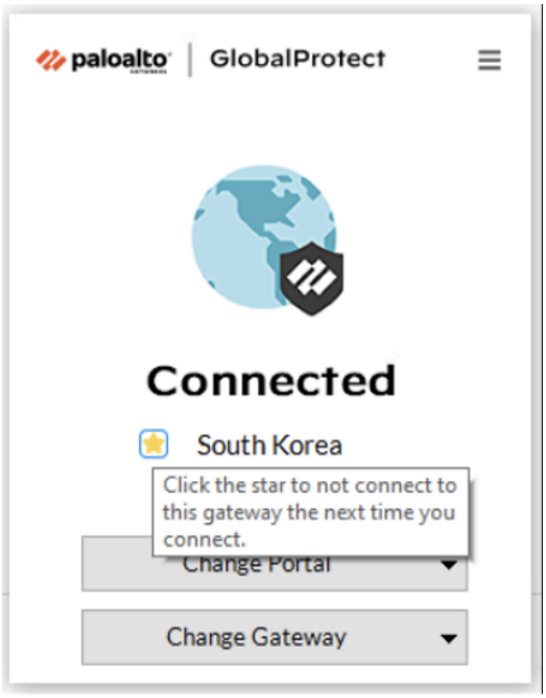
available gateways. To connect to a different gateway, click the **Change Gateway** drop-down and then use one of the following options:

- Select a gateway manually (external gateways only). This option is only available if your administrator enables manual gateway selection.
- Assign and automatically connect to a preferred gateway:

  1. To designate a preferred gateway, click the star icon (☆). The next time you connect, you will automatically connect to your designated preferred gateway.



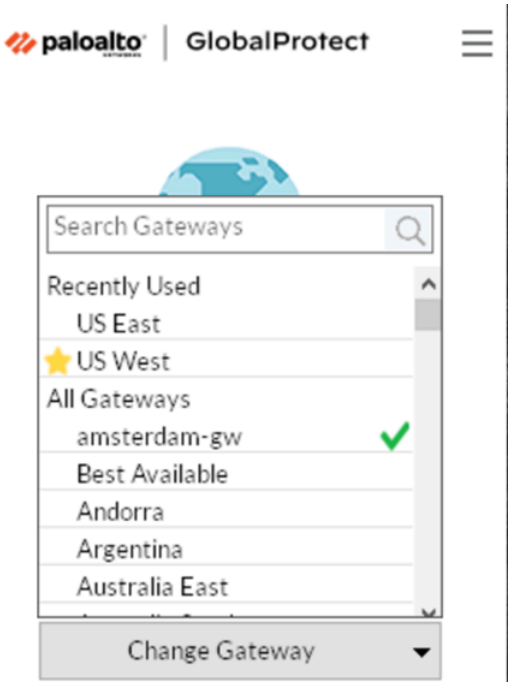
  If you later decide you no longer want this gateway as your preferred gateway, you can clear the star icon. The next time you connect you will automatically be connected to the best available gateway



2. By default, you automatically connect to the **Best Available** gateway that is identified by a check mark from the **Change Gateway** drop-down. If you set

the preferred gateway, a star displays by the starred gateway from the **Change Gateway** drop-down.

If your administrator configured manual external gateways in the portal agent configuration, you can choose a specific gateway using the gateway search field.



5. (Optional) Depending on the connection mode, click **Connect** to initiate the connection.
6. (Optional) If prompted, enter your **Username** and **Password** and then **Connect**.

   If your administrator has allowed you to use biometric (fingerprint) information to sign in, you need to first sign-in with a username and password twice (once to save it and again to authenticate); you can then use biometric information to sign in.

When the app connects in external mode, the GlobalProtect system tray icon displays a shield (), and **Connected** appears when you hover over the icon. When the app connects in internal mode, the GlobalProtect system tray icon displays a house (), and **Internal Network** appears when you hover over the icon.

STEP 3 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

A notification appears if your administrator configured the portal to install the Autonomous DEM (ADEM) endpoint agent during the GlobalProtect app installation and has either allowed you to enable the tests or not allowed you to enable the tests. If your administrator has already installed the ADEM endpoint agent and later configured the portal to uninstall the ADEM endpoint agent, a notification appears at the next login.

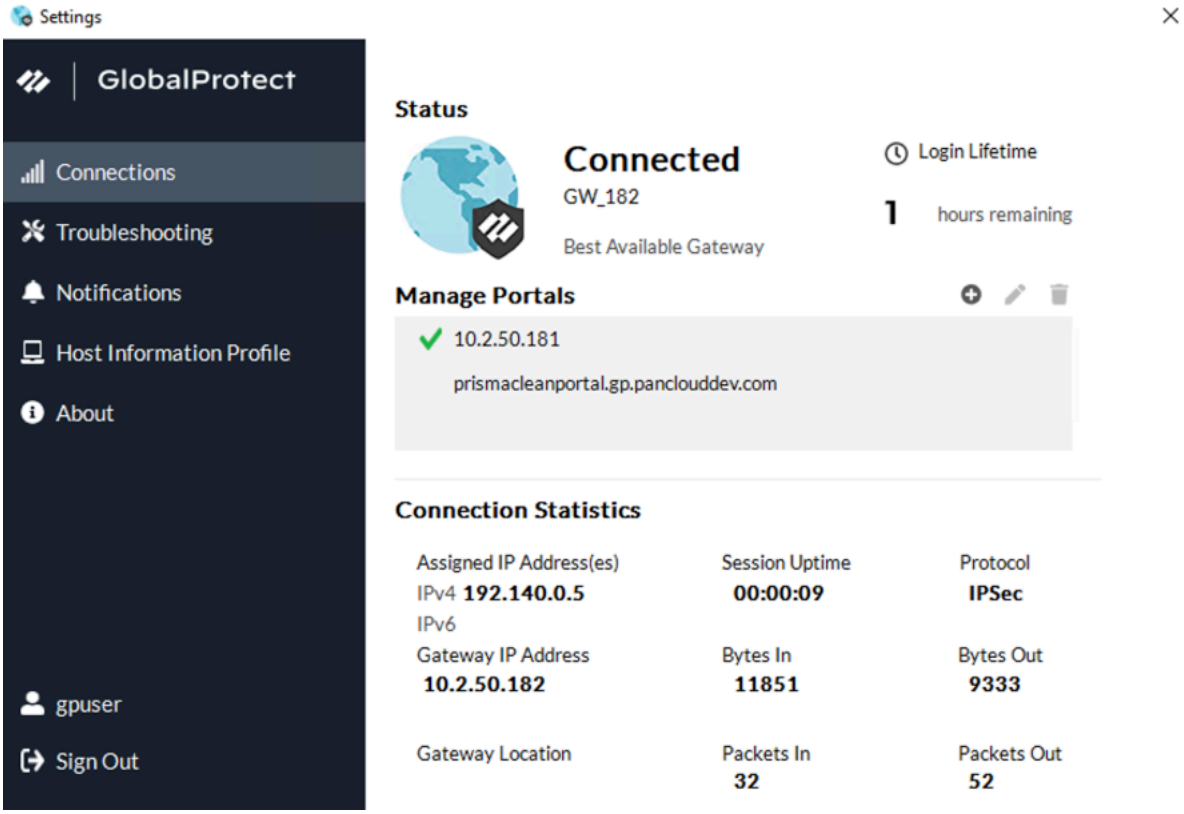
STEP 4 | View information about your network connection.

After you launch the app, click the hamburger menu on the status panel to open the settings menu. Select **Settings** to open the **GlobalProtect Settings** panel, and then select one of the following settings to view and modify the GlobalProtect app:

- **Connections**—The **Connections** tab displays the portal(s) associated with the GlobalProtect account. You can add, edit, or delete portals from this tab. This tab also displays the gateway to which you are connected. You can view connection statistics about the gateway (for example, gateway IP address, location, and VPN session uptime) when

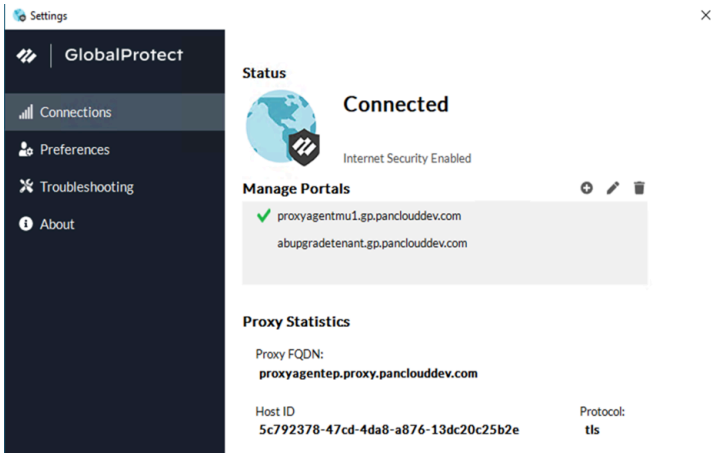
your administrator sets **Enable Advanced View** to **Yes** in the GlobalProtect portal agent configuration.

The **Connections** tab also displays the count down timer for the login lifetime.



The **Connections** tab displays the proxy details if the Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security functionality is enabled for the app through Prisma Access.

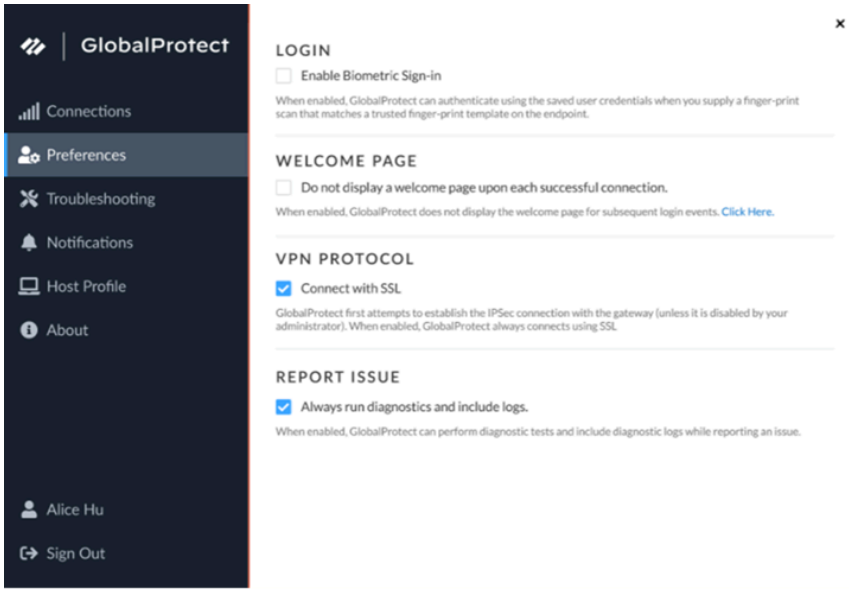
Proxy Mode:



- **Preferences**—The **Preferences** tab is now available only if your administrator configures at least one of the following options:

- **Enable Biometric Sign-in**—You can choose to use biometric (fingerprint) information to sign in. This option is available only if your administrator configures the **Save User Credentials** to **Only with User Fingerprint** in the GlobalProtect agent configuration. You must supply a fingerprint that matches a trusted fingerprint template on the endpoint to use a saved password for authentication to GlobalProtect portal and gateways.
- **Do not display a welcome page upon each successful connection**—You can choose to display a welcome page upon successful login. This option is available only if your administrator sets the **Welcome Page** to **factory-default** in the GlobalProtect portal agent configuration.
- **Connect with SSL**—You can choose to use SSL or stay with IPSec. This option is available only if your administrator sets **Connect with SSL Only** to **User can Change** in the GlobalProtect portal agent configuration .
- **Always run diagnostic tests and include logs**—You can choose to enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs. This option

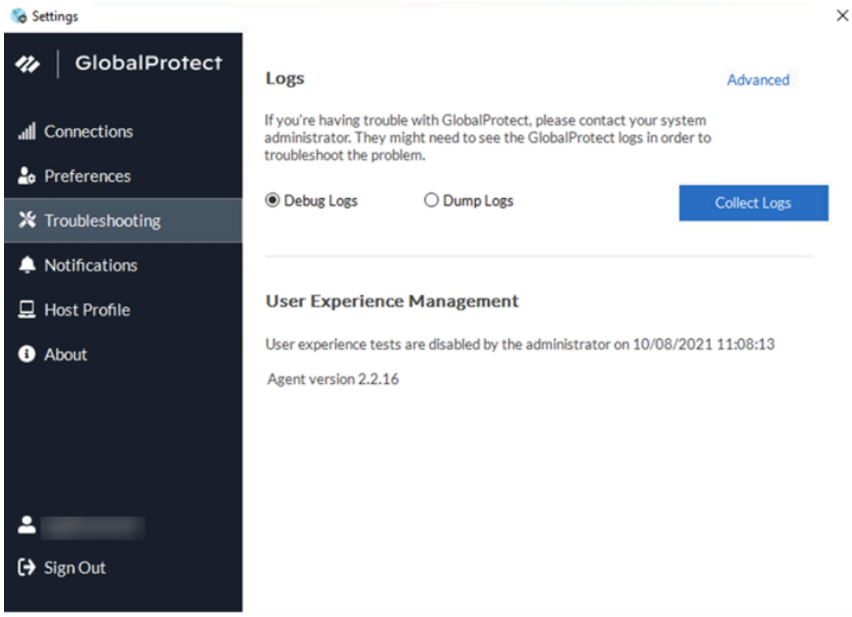
is available only if your administrator enables the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.



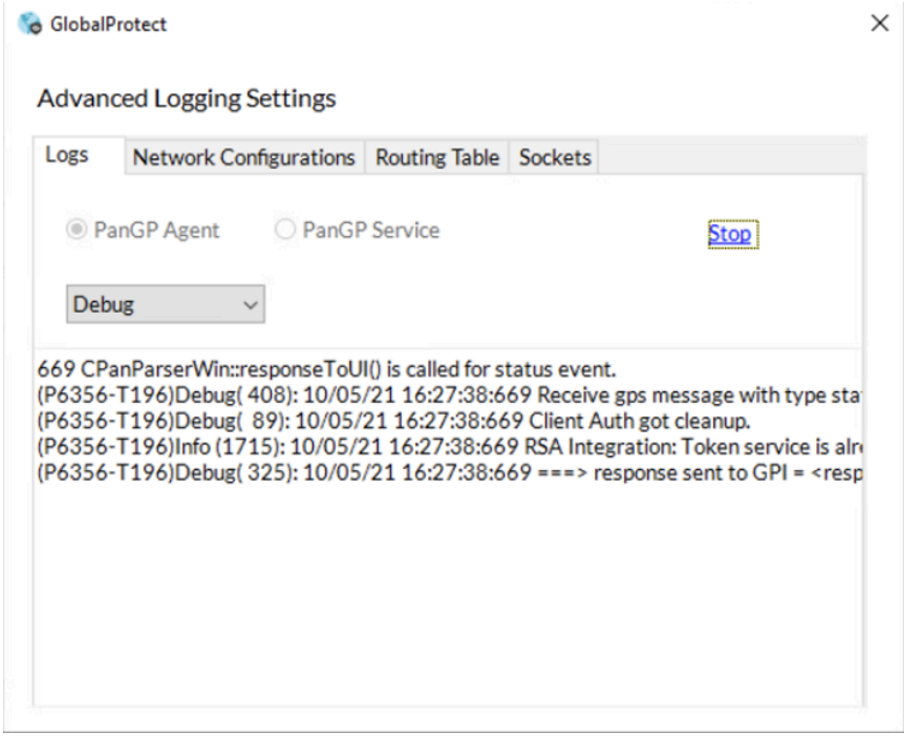
- **Troubleshooting**—The **Troubleshooting** tab allows you to **Collect Logs** and set the logging level to **Debug Logs** or **Dump Logs**, and optionally **Enable User Experience Tests**.

  In order for the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Strata Logging Service for further analysis, you must configure the GlobalProtect portal to enable the GlobalProtect app log collection for troubleshooting. Additionally, you can configure the HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names of the web servers/resources that you want to probe, and to determine issues such as latency or network performance on the end user's endpoint.

  You can click **Advanced** to view detailed information about their endpoint.



The **Advanced Logging Settings** window displays information about the network configuration, route settings, active connections, and logs.



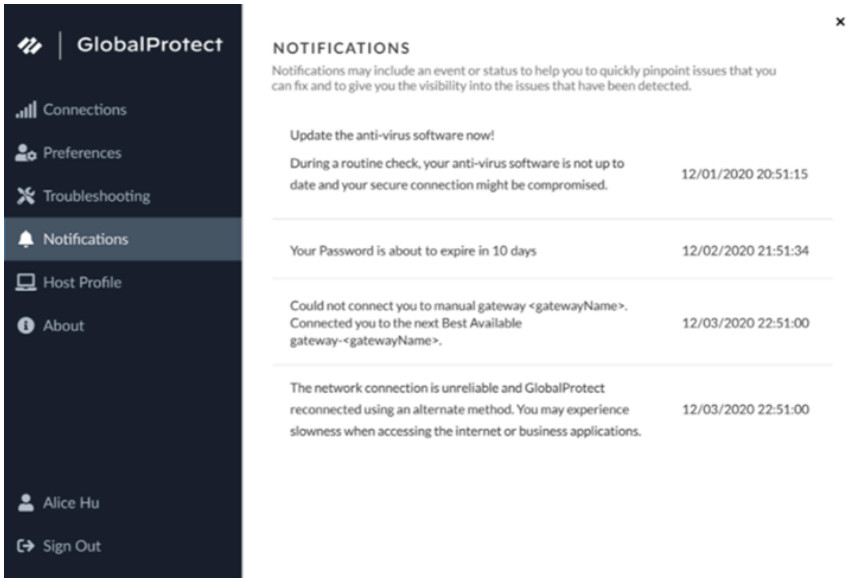
When GlobalProtect is connected, you can verify that the Autonomous DEM (ADEM) endpoint agent can perform user experience tests if the **Enable user experience tests** check box is displayed on the GlobalProtect app. Or you can verify that a message is displayed if your administrator installed the ADEM endpoint agent during the GlobalProtect app installation but does not allow you to enable or disable user experience tests from the GlobalProtect app. By default, heartbeat alerts are still forwarded to ADEM even when GlobalProtect is disabled or disconnected.

If your administrator configured the portal to install the Autonomous DEM endpoint agent during the GlobalProtect app installation and has allowed you to enable the tests, select the check box to **Enable user experience tests** on the GlobalProtect app. This check box does not appear if your administrator does not allow you to enable or disable user experience tests from the GlobalProtect app. Instead, a message is displayed, confirming that the app is enabled to run user experience tests.

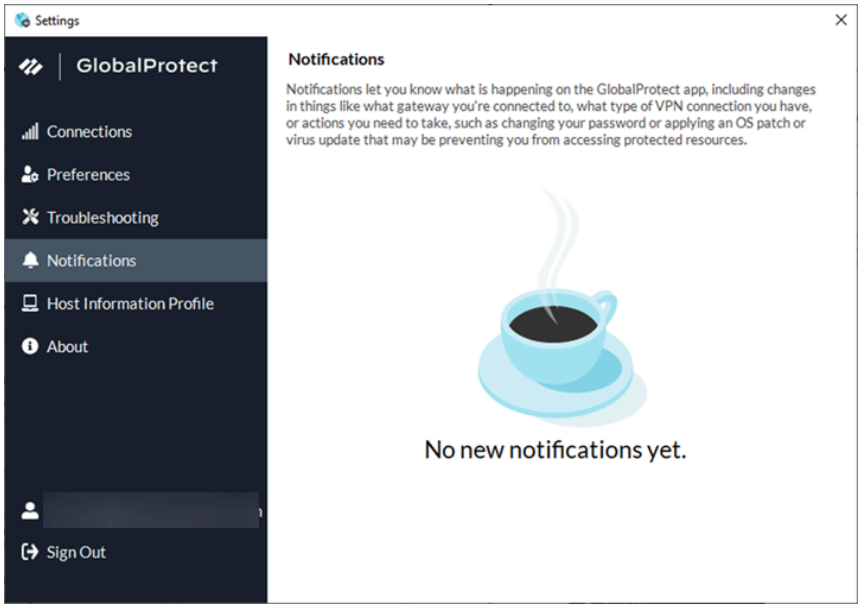
If you do not select the check box to **Enable user experience tests**, heartbeat alerts are still forwarded to ADEM.

- **Notifications**—The **Notifications** tab displays the detailed information about specific notifications triggered on the GlobalProtect app. You can configure end-user notifications

about expiry of GlobalProtect app sessions on the gateway and schedule the display of these custom notifications on the app.



You are also notified if there are no new notifications triggered on the GlobalProtect app.

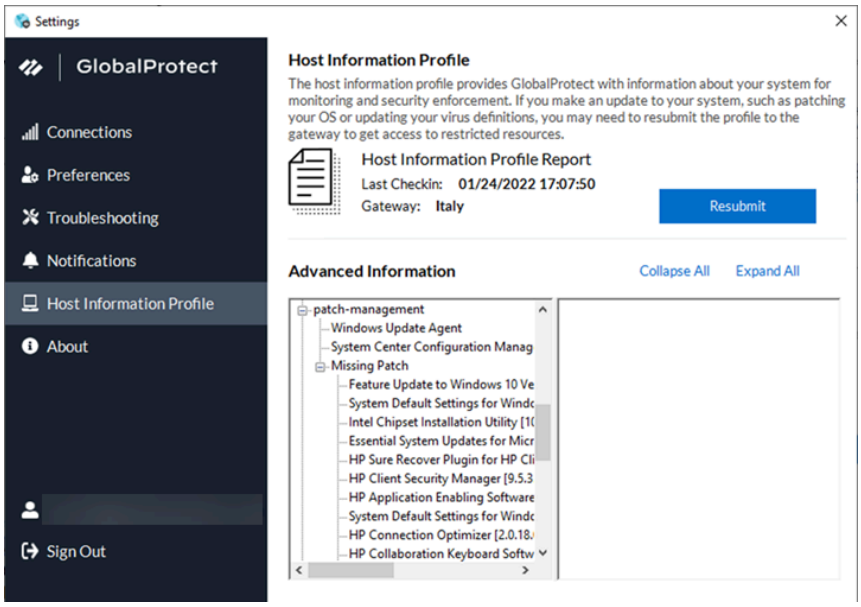


Starting from GlobalProtect app version 6.2.3, session and idle timeout messages are suppressed for the always-on connect method.

Starting from GlobalProtect app version 6.2, you can extend the login lifetime session of the GlobalProtect app before it expires to avoid abrupt app session logout. The login lifetime expiry notification informs you in advance when the app sessions are about to expire and provides the option to extend the duration of the user session so that you are not logged out of your session abruptly. The app will display the expiry notification with extend user

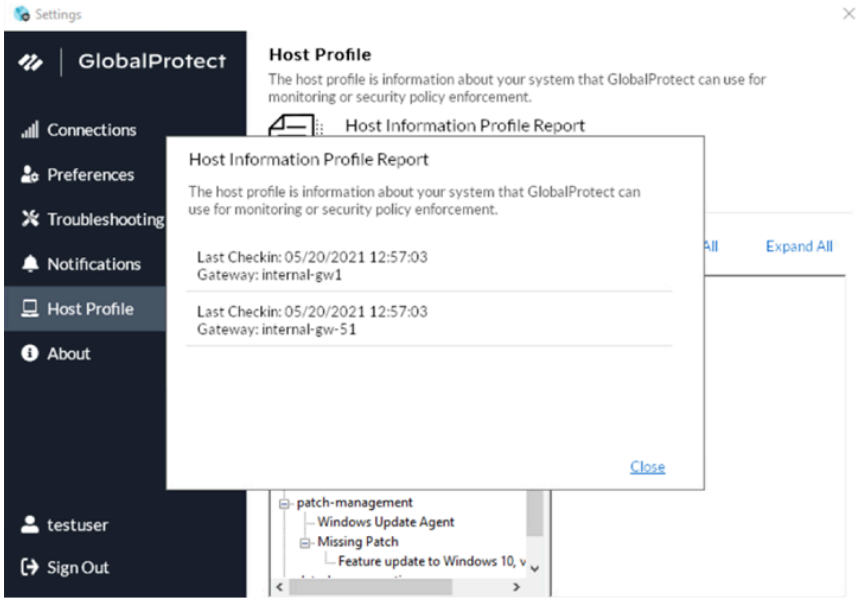
session option if your administrator has configured the notification settings for extending the session.

- **Host Information Profile**—The **Host Information Profile** tab displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile. You can **Resubmit** to manually resubmit HIP data to the gateway.

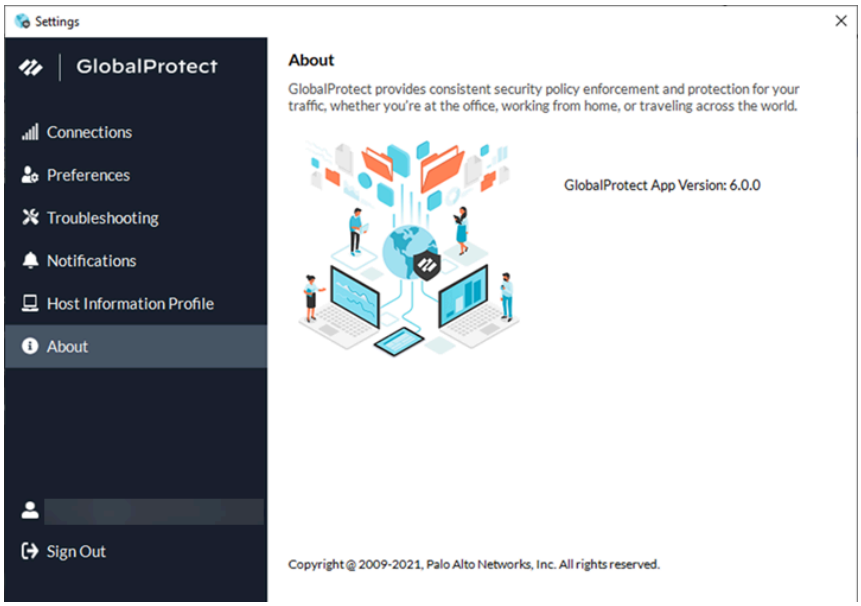


If your administrator configured multiple internal gateways in non-tunnel mode and internal host detection, you can click **More Details** to monitor the Host Information Profile

(HIP) report submission for each gateway from a central location to help you to quickly troubleshoot HIP related issues.



- **About**—The **About** tab displays the version of GlobalProtect currently installed on the endpoint and allows you to **Check for Updates**.



STEP 5 | (Optional) Log in using a new password.

*If your GlobalProtect administrator configures the GlobalProtect portal agent to **Save User Credentials**, your credentials are automatically saved to the GlobalProtect app. If your password for accessing the corporate network changes, you must log in to GlobalProtect using your new password.*

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Click the hamburger menu to open the settings menu.
3. Select **Settings** to open the **GlobalProtect Settings** panel.
4. On the **GlobalProtect Settings** panel, **Sign Out** to clear your saved user credentials from the GlobalProtect app.
5. After you clear your user credentials, you can reconnect to GlobalProtect with your new username and password.

STEP 6 | (Optional) Disconnect from GlobalProtect.

If your administrator configures GlobalProtect with the **On-Demand** connect method, you can disconnect from GlobalProtect by clicking **Disconnect** on the status panel.

Report an Issue From the GlobalProtect App for Windows

When you experience unusual behavior such as poor network performance or a connection is not established with the portal and gateway, you can report an issue directly to Strata Logging Service to which your administrator can access. You no longer need to manually collect and send the GlobalProtect app logs through email or to store them on a cloud drive.

*To display the **Report an Issue** option on the GlobalProtect app, your administrator must enable the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.*

STEP 1 | Connect to the GlobalProtect portal or gateway.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) If you are logging in to the GlobalProtect app for the first time, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.
3. (Optional) If multiple portals are saved on your app, select a portal from the **Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Portal** drop-down.
4. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, click the gateway drop-down.

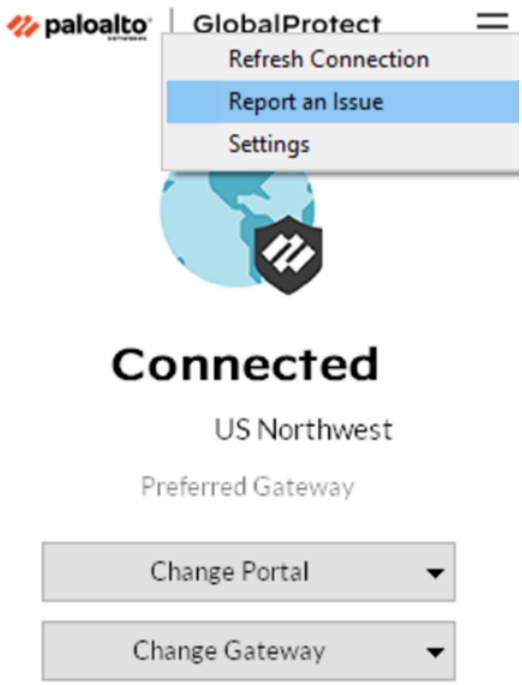
STEP 2 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

STEP 3 | Report an issue from the GlobalProtect app from your endpoint.

After you launch the app, click the hamburger menu on the status panel to report an issue to your administrator.

1. Select **Report an Issue**.



2. Enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs. Both diagnostic and troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report.

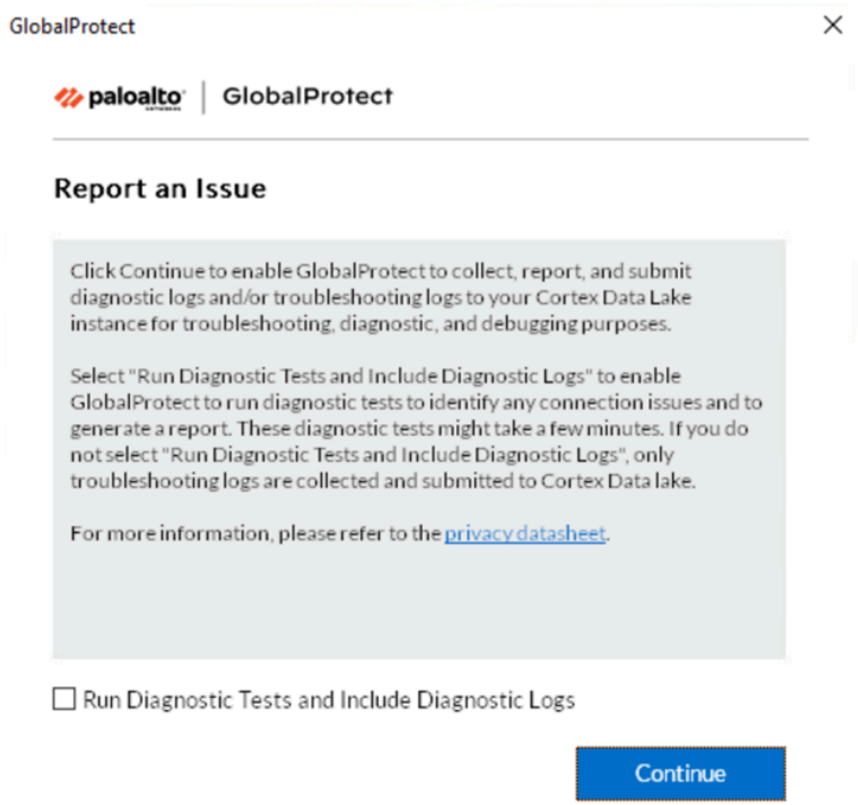
   After the diagnostic tests are successfully completed, the GlobalProtect debug log files are uploaded to Strata Logging Service from your endpoint.

   *If you do not enable the app to run diagnostic tests and to include diagnostic logs, only troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report. The GlobalProtect app checks for the report files (pan_gp.trb.log or pan_gp_trbl.log) that are automatically generated in `.json` format. A notification message appears if no issues were found in the troubleshooting logs. Click **Retry** to check if the pan_gp.trb*.log files exist.*

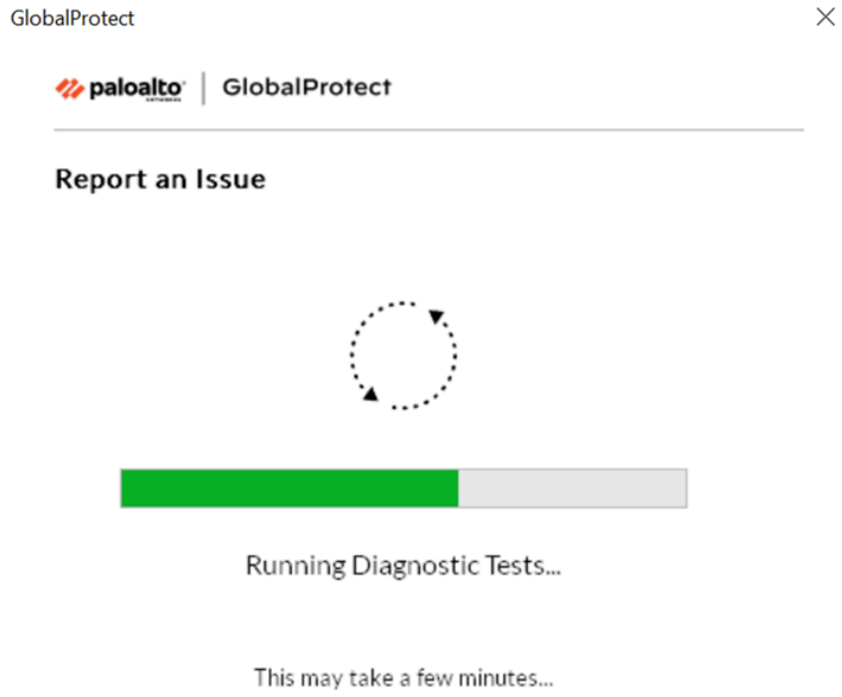
3. Select the **Run Diagnostic Tests and Include Diagnostic Logs** check box.
4. Click **Continue** to allow the app to create a troubleshooting log and to send the report to your administrator's Strata Logging Service instance.

   The results of the end-to-end diagnostic tests are stored in the pan_gp_diag.log file in `.json` format and sent to your administrator's Strata Logging Service instance along with the pan_gp.trb*.log files. The GlobalProtect app can run diagnostic tests with a tunnel or without a tunnel. For example, you might want to enter your GlobalProtect

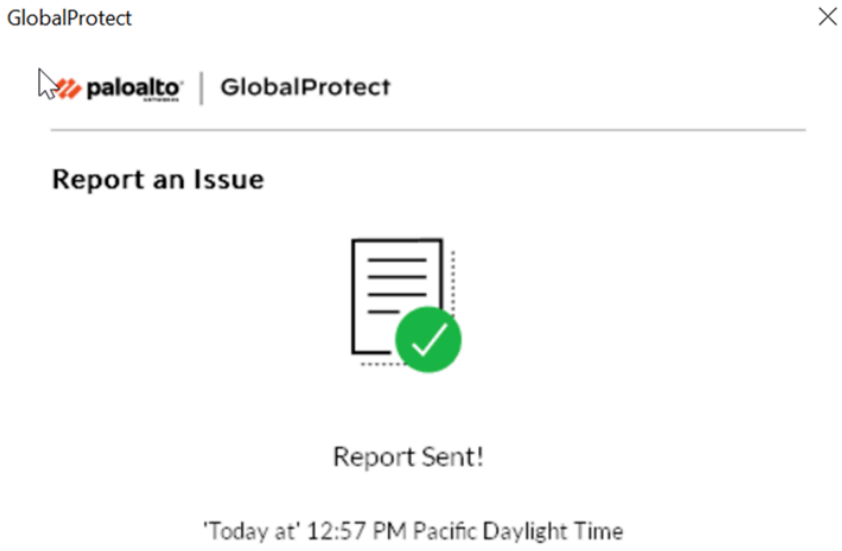
login credentials prior to the app connecting and running diagnostic tests through the tunnel.



A message pops-up, confirming that the app is running diagnostic tests only if you selected the **Run Diagnostic Tests and Include Diagnostic Logs** check box.



5. Click **Close** to confirm that the app successfully sent the report to Strata Logging Service. This confirmation message displays the date and time when the report was processed and sent.



Disconnect the GlobalProtect App for Windows

If your administrator configures the GlobalProtect connect method as **Always On**, you can disconnect the GlobalProtect app if you have a good reason. For example, you might want to disconnect the app if the GlobalProtect virtual private network (VPN) is not working in a hotel, and the VPN failure prevents you from connecting to the internet. After disconnecting the GlobalProtect app, you can connect to the internet using unsecured communication (without a VPN).

The method, amount of time, and number of times for which you can disconnect e the GlobalProtect app depends on how the administrator configures your GlobalProtect service (PanGPS). This configuration can prevent you from disconnecting the app entirely or allow you to disconnect the app only after responding to a challenge correctly.

If your configuration includes a challenge, the GlobalProtect app prompts you for one of the following:

- Reason you want to disconnect the app
- Respond to one or more reasons such as **Internet speed slow** or **App not working** (if required)
- Passcode
- Ticket number

If the challenge requires a passcode or ticket number, we recommend that you contact a GlobalProtect administrator or Help Desk person by phone.

Administrators typically provide passcodes in advance, either through email (for new GlobalProtect users) or posted on your organization's website. In response to an outage or system issue, administrators may also provide passcodes by phone.

Before you can obtain a valid ticket number, your endpoint displays a ticket request number that you must communicate to your GlobalProtect administrator or Help Desk person. If your disconnect request is approved, you will receive a valid ticket number that you can use to disconnect GlobalProtect.

The following steps describe how to disconnect the app and pass a challenge:

STEP 1 | Disconnect the GlobalProtect app.

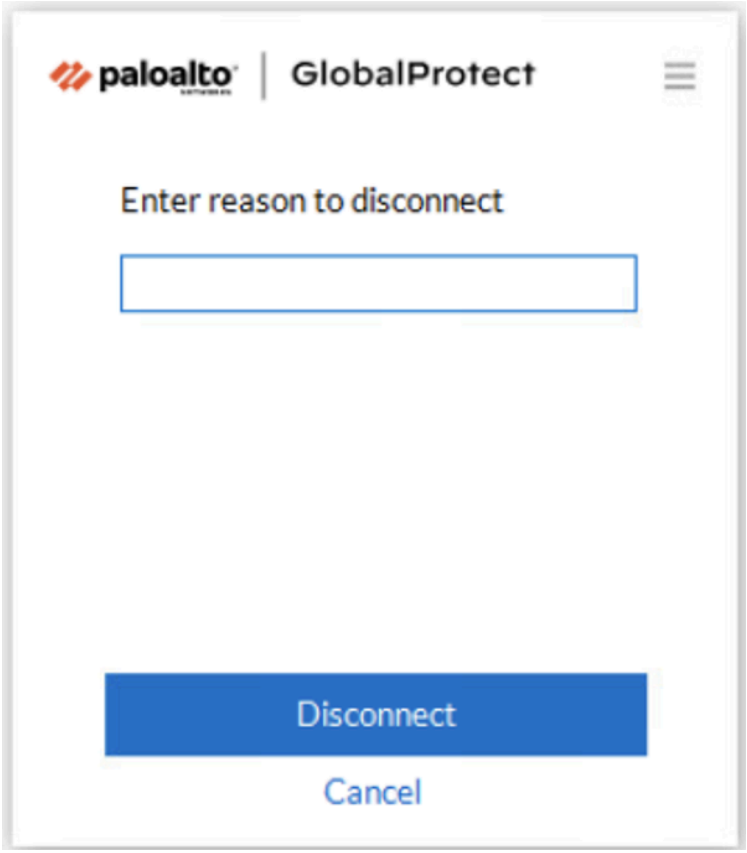
1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the hamburger menu to open the settings menu.
3. Select **Disconnect**.

*The **Disconnect** option is visible only if your GlobalProtect agent configuration allows you to disconnect the app. If the configuration allows you to disconnect the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*

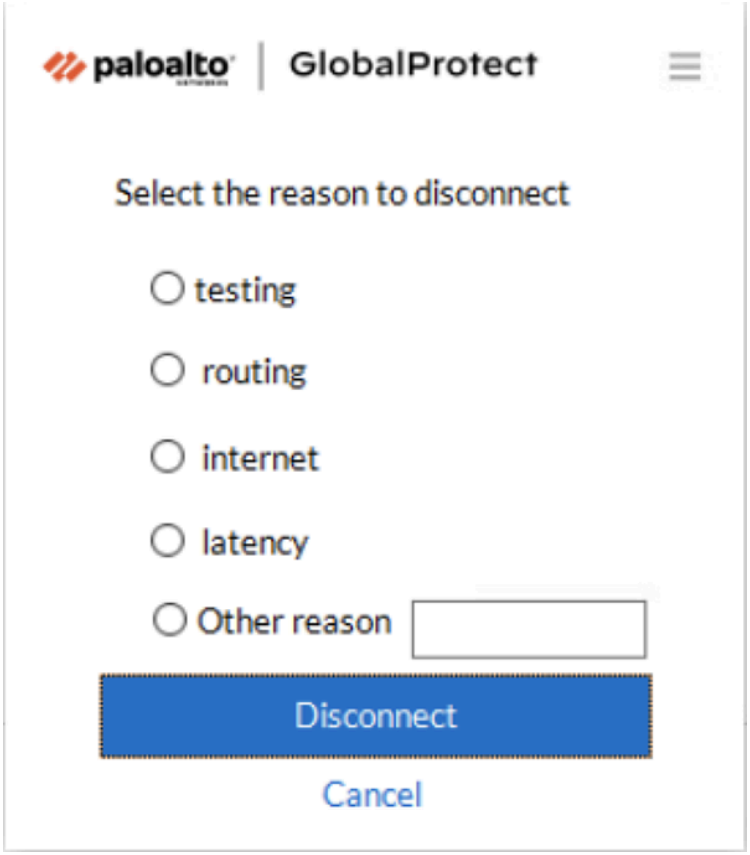
STEP 2 | Respond to one or more challenges, if required.

If prompted, provide the following information:

- **Tell us the issue to disconnect**—Your reason for disconnecting the GlobalProtect app.



- **Select the reason to disconnect**—If your configuration requires you to respond to one or more reasons or enter another reason, the GlobalProtect app displays the reasons as soon as you select **Disconnect**.



- **Passcode**—A passcode that is typically provided by your administrator in advance, based on a known issue or event that requires you to disable the app.
- **Ticket**—If your configuration requires you to provide a ticket number, the GlobalProtect app displays an eight-character hexadecimal ticket request number as soon as you select **Disconnect**. To disconnect the app with a ticket number, contact your administrator or Help Desk person (by phone) and provide the ticket request number. After approving your request, your administrator or Help Desk person provides you with an eight-character hexadecimal ticket number. Enter the ticket number in the **Ticket** field, and then click **OK**.

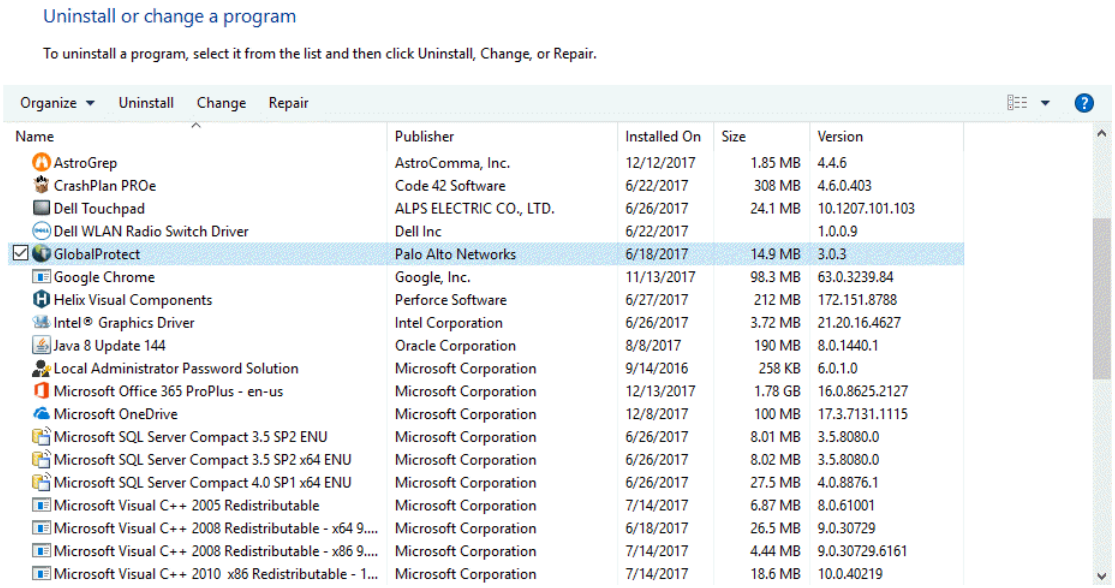
Uninstall the GlobalProtect App for Windows

Use the following steps to uninstall the GlobalProtect app from your Windows endpoint . Keep in mind that by uninstalling the app, you no longer have VPN access to your corporate network and your endpoint will not be protected by your company's security policies.

Only users with administrator privileges can uninstall the GlobalProtect app from Windows endpoints.

STEP 1 | Select **Start** > **Control Panel** > **Programs** > **Programs and Features**.

STEP 2 | Select **GlobalProtect** from the list, and then click **Uninstall**.



STEP 3 | When prompted to continue with the uninstall, click **Yes**.

Fix a Microsoft Installer Conflict

If you **Enforce GlobalProtect for Network Access** in a GlobalProtect portal agent configuration, and then you upgrade a Windows endpoint to a newer version of the GlobalProtect app, installation can fail and the enforcement configuration can block all traffic.

This issue is caused by an OS limitation that occurs when multiple Microsoft installer (`msiexec.exe`) instances run simultaneously on a Windows endpoint. You must use the following procedure to resolve the Microsoft installer conflict:

STEP 1 | Restart the endpoint.

STEP 2 | Stop all third-party installers that are running in the background.

1. Press **Ctrl+Alt+Delete**, and then click **Task Manager.**
2. In the **Task Manager**, locate all third-party `msiexec` programs that are currently running (for example, **`msiexec command line - Google Search`**).
3. Select the third party installer, and then click **End Task** to stop the installer.

STEP 3 | Restore the existing version of GlobalProtect, and then upgrade to the newer version of the app.

1. (Optional) If necessary, re-install the existing (older) version of GlobalProtect to repair it. This step is required if the upgrade continues to fail.
2. Allow the upgrade to proceed as expected.

GlobalProtect App for macOS

GlobalProtect™ is an application that runs on your endpoint (desktop computer, laptop, tablet, or smart phone) to protect you by using the same security policies that protect the sensitive resources in your corporate network. GlobalProtect™ secures your intranet, private cloud, public cloud, and internet traffic and allows you to access your company's resources from anywhere in the world.

The following topics describe how to install and use the GlobalProtect app for macOS:

Download and Install the GlobalProtect App for macOS

Before connecting to the GlobalProtect network, you must download and install the GlobalProtect app on your macOS endpoint. To ensure that you get the right app for your organization's GlobalProtect or Prisma Access deployment, you must download the app directly from a GlobalProtect portal within your organization. For this reason, there is no direct GP app download link available on the Palo Alto Networks site.

Before you can download and install the GlobalProtect app, you must obtain the IP address or FQDN of the GlobalProtect portal from your administrator. In addition, your administrator should verify which username and password you can use to connect to the portal and gateways. This is typically the same username and password that you use to connect to your corporate network.

When you install the GlobalProtect app for the first time on a macOS device running macOS Catalina 10.15.4, macOS Big Sur 11, or later or upgrade to GlobalProtect app 5.1.4, you must enable the system extensions that are used for specific GlobalProtect features. If your administrator has configured split tunnel on the GlobalProtect gateway based on the destination domain name and application process name or enforced GlobalProtect connections for network access on the GlobalProtect portal (see GlobalProtect App Customization), the **System Extension Blocked** notification message displays on the GlobalProtect app during the installation. The message prompts users to enable and allow the system extensions in macOS that are blocked from loading to use the split tunnel and Enforce GlobalProtect for Network Access features.

Follow these guidelines when you use system extensions:

- *Only users with administrator privileges can enable the system extensions on the GlobalProtect app for macOS endpoints.*
- *Due to the security enhancement on macOS Catalina 10.15 and macOS Big Sur 11 to ensure that your data is protected while using third-party applications, GlobalProtect must request your permission before attempting access to files and folders stored in your Documents, Desktop, and Downloads folders and network drives. If your administrator has enabled HIP checks, new permission pop-ups appear on your macOS endpoint when GlobalProtect requests access to certain files and folder stored in your file system.*
- *The GlobalProtect app 5.1.4 running on macOS Catalina 10.15.4, macOS Big Sur 11, or later does not use kernel extensions and will use system extensions.*
- *The GlobalProtect app 5.1.4 running on macOS Catalina 10.15.4, macOS Big Sur 11, or later will not use the kernel extensions (**com.paloaltonetworks.kext.pangpd**) and instead will use any of the available utun interfaces provided by macOS as the virtual adapter.*
- *If you are upgrading from an earlier release to the GlobalProtect app 5.1.4 running on macOS Catalina 10.15.4, macOS Big Sur 11, or later, kernel extensions are no longer needed. After the upgrade, the **System Extension Blocked** notification message displays on the GlobalProtect app, prompting users to enable and allow the system extensions in macOS that was blocked from loading. By default, the app will not install system extensions and the same default settings are applied.*

After you gather the required information, use the following steps to download and install the app:

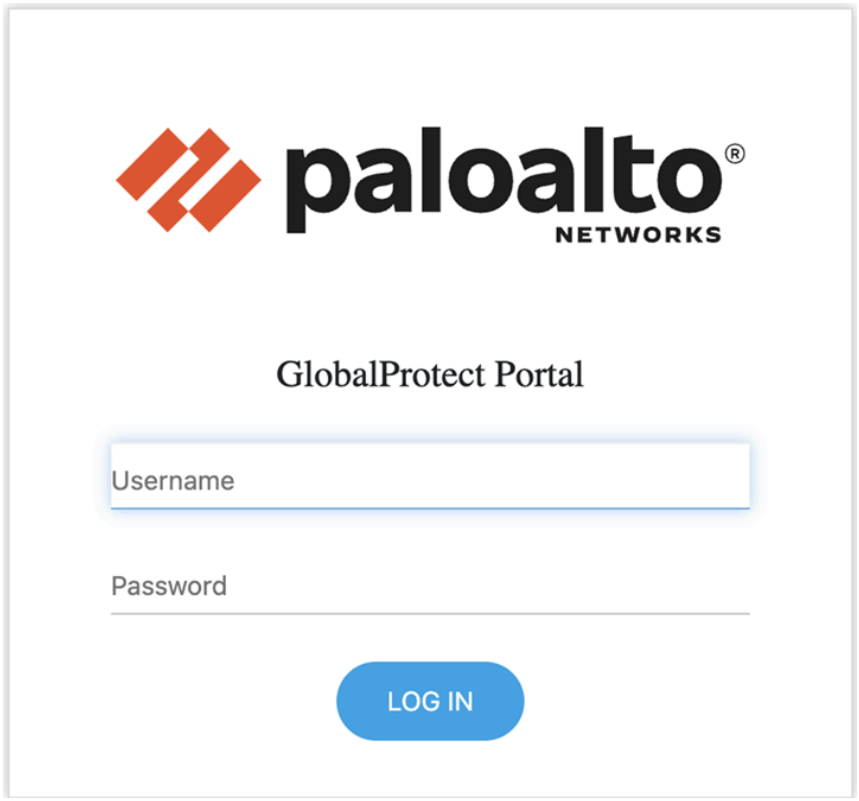
STEP 1 | Log in to the GlobalProtect portal.

1. Launch a web browser and go to the following URL:

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

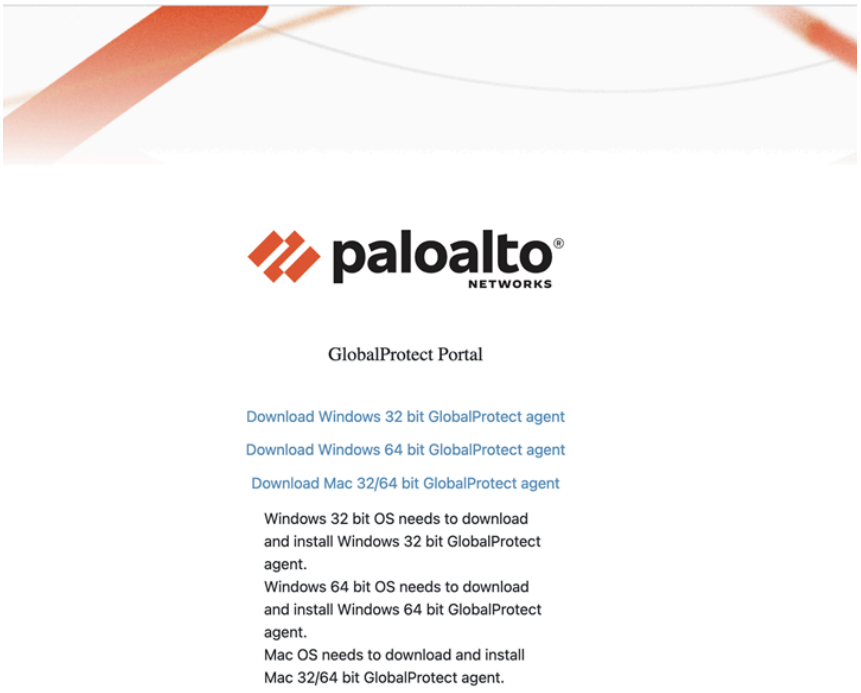
   Example: **`http://gp.acme.com`**

2. On the portal login page, enter your **Name** (username) and **Password** and then click **LOG IN**. In most instances, you can use the same username and password that you use to connect to your corporate network.

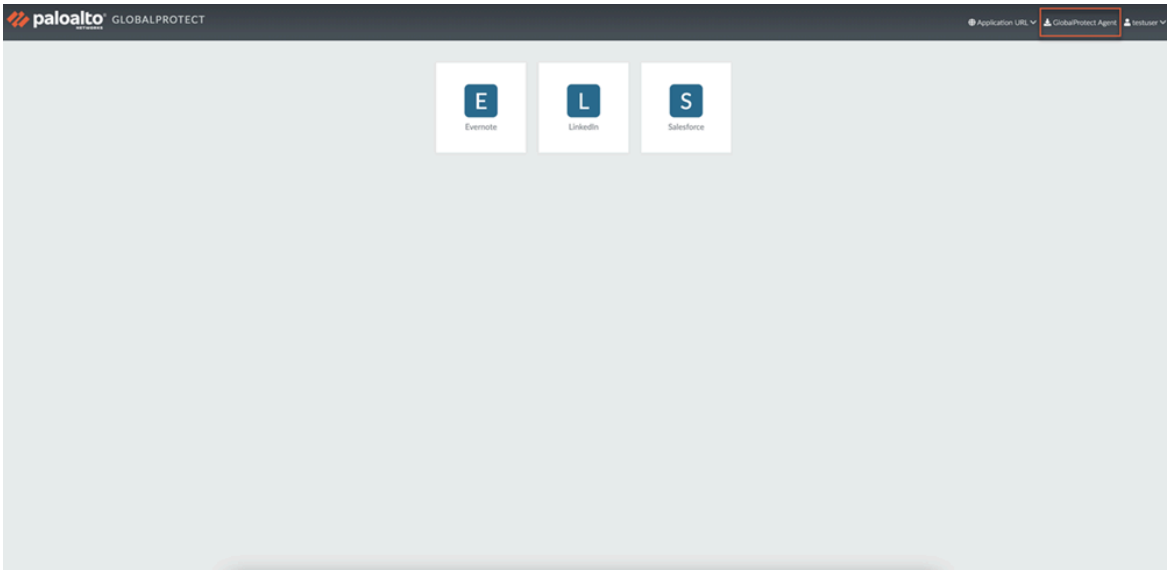


STEP 2 | Navigate to the app download page.

In most instances, the app download pages appears immediately after you log in to the portal. Use this page to download the latest app software package.

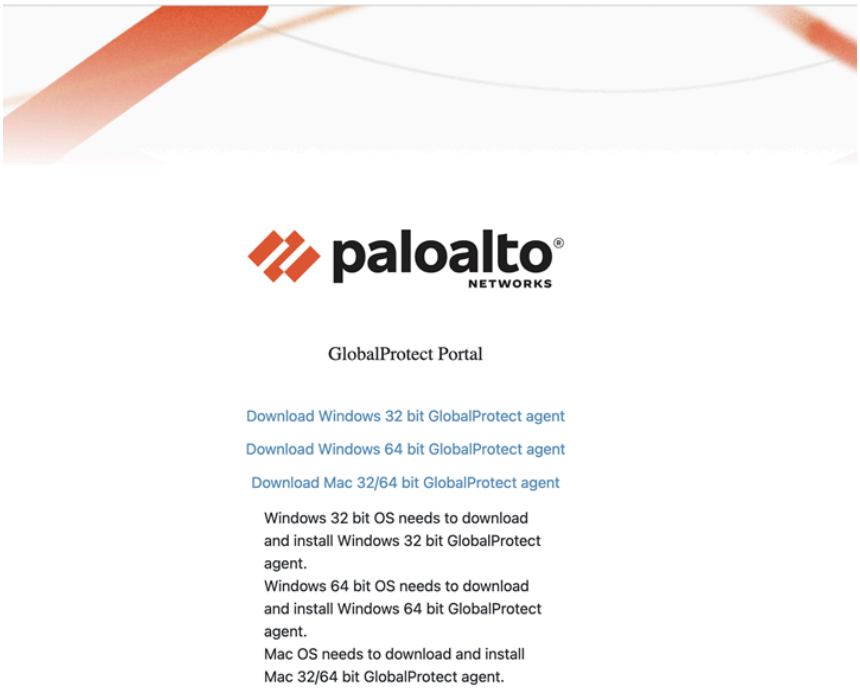


If your system administrator has enabled GlobalProtect Clientless VPN access, the applications page opens after you log in to the portal (instead of the app download page). Select **GlobalProtect Agent** to open the download page.



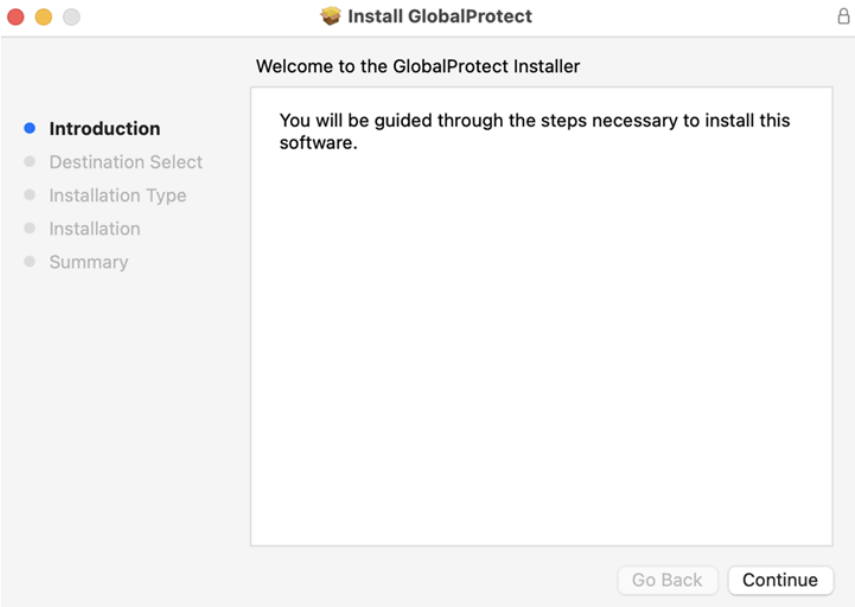
STEP 3 | Download the app.

1. Click **Download Mac 32/64 bit GlobalProtect agent**.

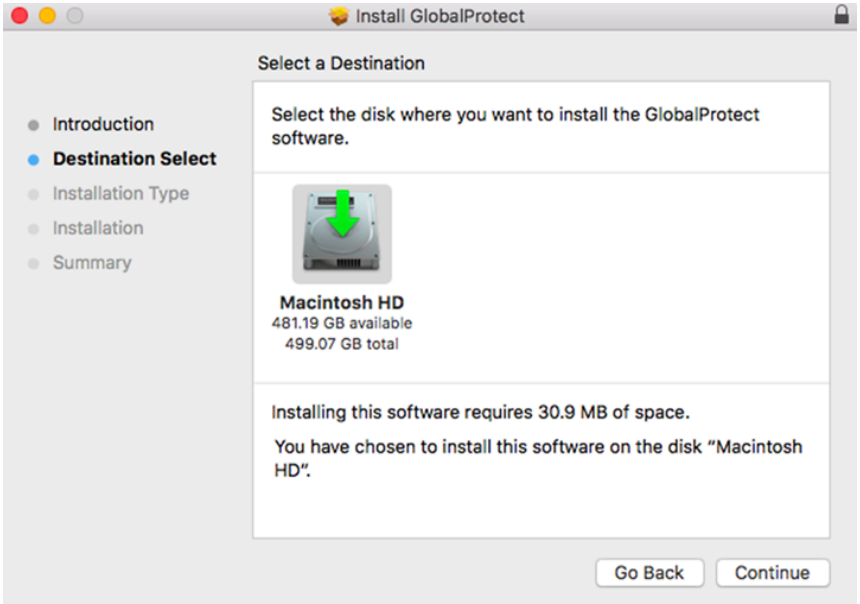


2. When prompted, **Run** the software.
3. When prompted again, **Run** the GlobalProtect Installer.

STEP 4 | Complete the GlobalProtect app setup using the GlobalProtect Installer.



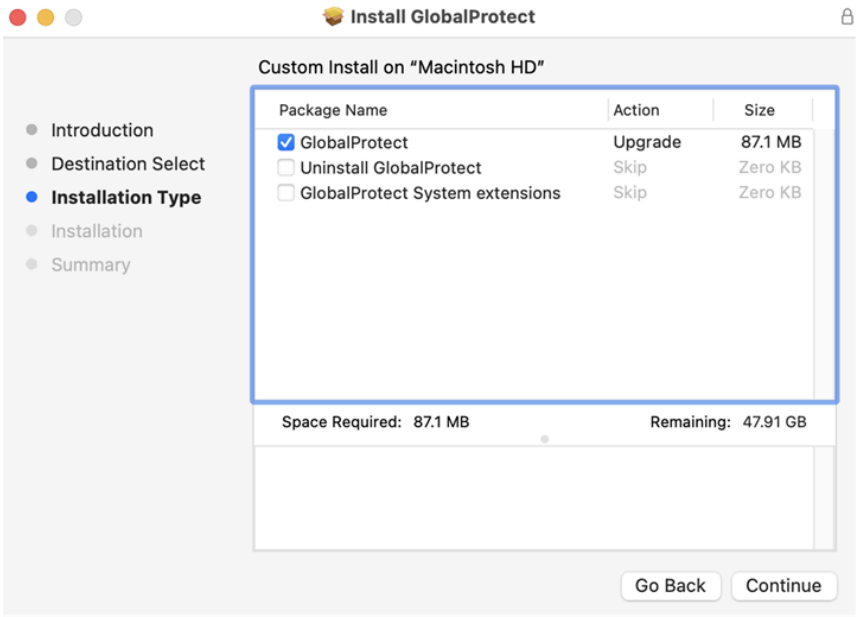
1. From the GlobalProtect Installer, click **Continue**.
2. On the **Destination Select** screen, select the installation folder for the GlobalProtect app, and then click **Continue**.



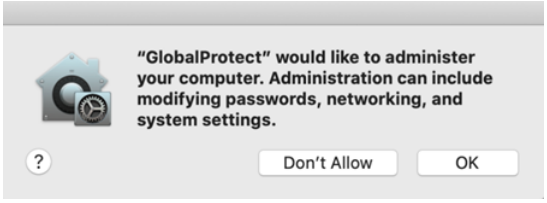
3. On the **Installation Type** screen, select the **GlobalProtect** installation package check box.

   If your system administrator has configured the split tunnel on the gateway or enforced GlobalProtect connections for network access on the portal, select the **GlobalProtect System extensions** check box (disabled by default).

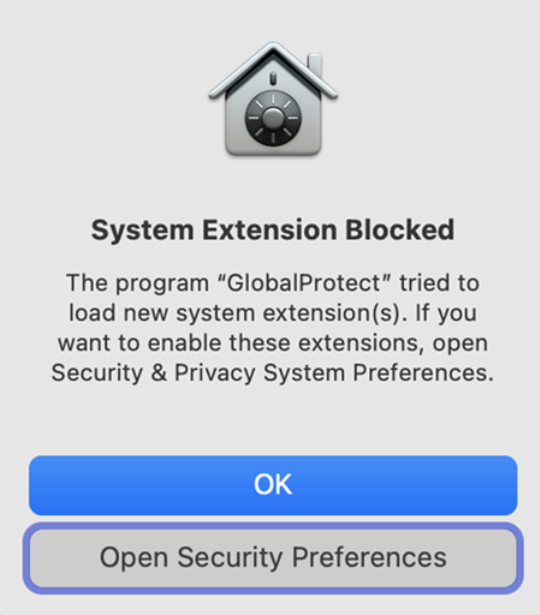
   Click **Continue**.



4. Click **Install** to confirm that you want to install GlobalProtect.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to begin the installation.
6. After installation is complete, **Close** the installer.
7. If your administrator has configured the portal to install the Autonomous DEM (ADEM) endpoint agent during the GlobalProtect app installation for the first time, select **OK** in the following pop-up pop-up prompt so that it will not appear again:

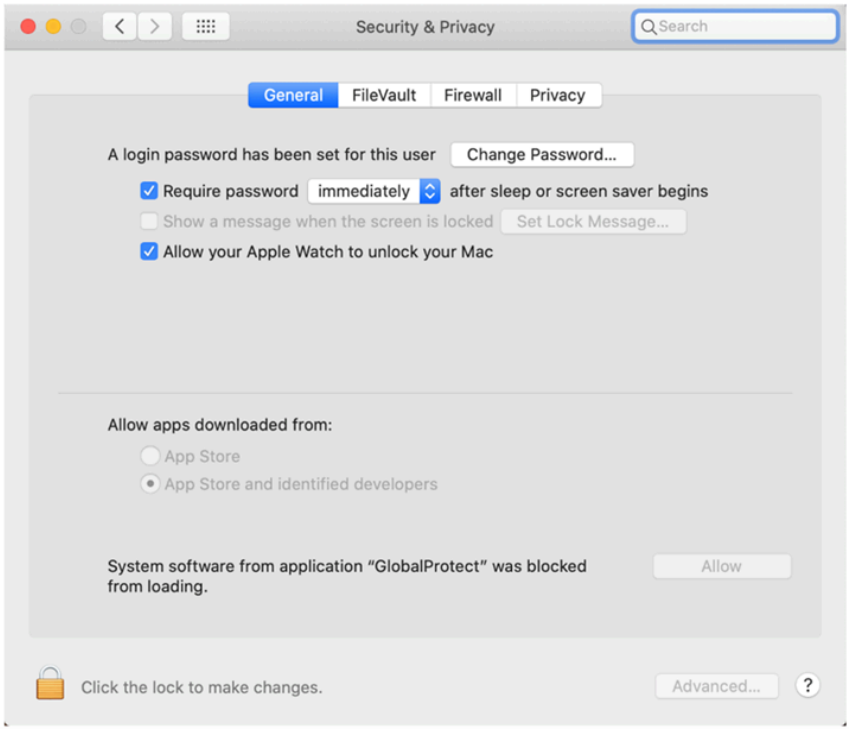


8. If you enabled the **GlobalProtect System Extensions**, select **Open Security Preferences** to enable the system extensions in macOS that was blocked from loading from the following **System Extension Blocked** notification:



If your administrator has suppressed this notification by using the supported mobile device management system (MDM), Jamf Pro, you can automatically load the system extensions without receiving this notification.

9. On the **Security & Privacy** dialog, click the **padlock** icon to make changes, and then select **App Store and identified developers** in the **Allow apps downloaded from** area. Click **Allow**.



Use the GlobalProtect App for macOS

This topic applies to you only if your setup requires you to enter your GlobalProtect login credentials after you have logged into your endpoint (single sign-on is disabled).

We typically recommend that organizations allow its GlobalProtect users to log in transparently following app installation. After you log in to an endpoint with transparent GlobalProtect login, the GlobalProtect app automatically initiates and connects to the corporate network without further user intervention.

After the installation is complete, the **System Extension Blocked** notification message appears, prompting users to enable the system extensions in macOS that was blocked from loading. If the **GlobalProtect System Extensions** option is not selected during the installation, this notification message appears once users connect to the gateway. This notification appears if your administrator has configured either split tunnel on the GlobalProtect gateway, enforced GlobalProtect connections for network access on the GlobalProtect portal (see GlobalProtect App Customization), or both. Both features require users to enable the system extensions.

If your setup requires you to enter your GlobalProtect credentials, follow the applicable steps below.

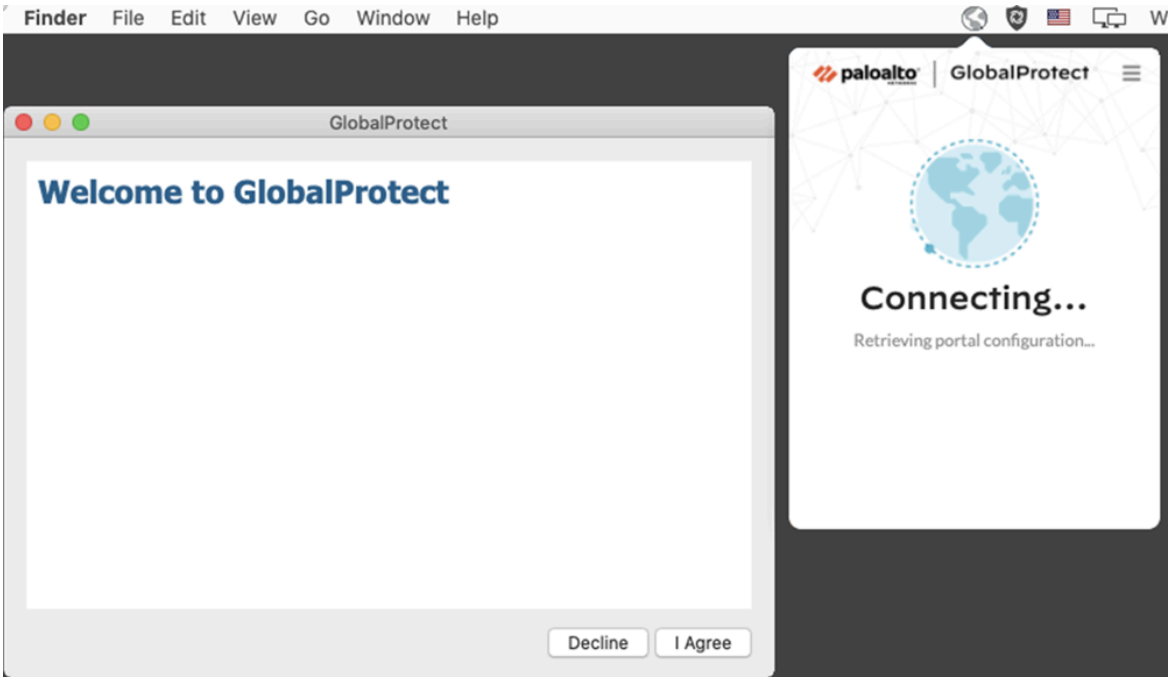
STEP 1 | Log in to GlobalProtect.

If you are logging in to the endpoint for the first time, the GlobalProtect app displays a friendly, welcome page upon successful login. Click **Get Started**.

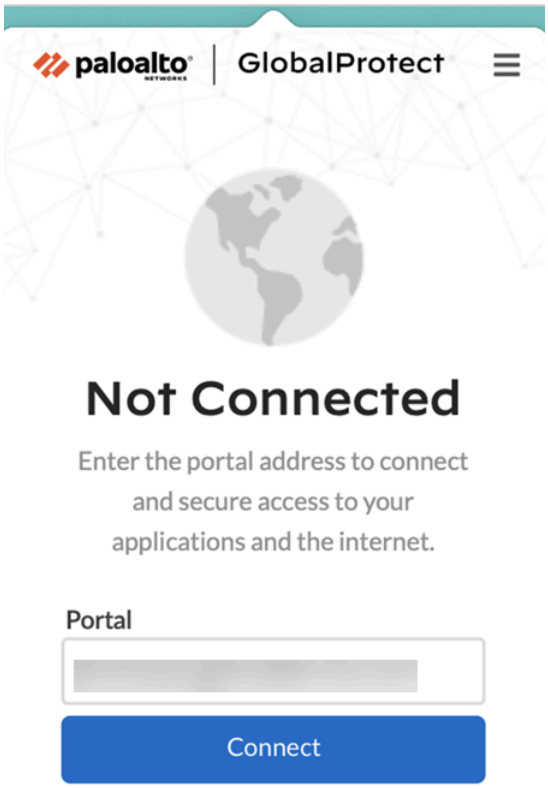
1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) Review your company's terms of service before connecting to GlobalProtect if your administrator requires you to see a page to access internal resources.

   If you do not accept terms of use, you will not be able to connect to GlobalProtect.

   Optionally, if you click **Cancel**, you must enter the IP address (or domain) of the GlobalProtect portal, and then click **Connect** to initiate the connection.



3. Enter the IP address or domain of the portal that your GlobalProtect administrator provided, and then click **Connect**.



STEP 2 | Connect to the GlobalProtect portal or gateway.

*You can determine if you are connected by checking the GlobalProtect system tray icon. If you are not connected, the icon is gray (), and **Not Connected** appears when you hover over the icon.*

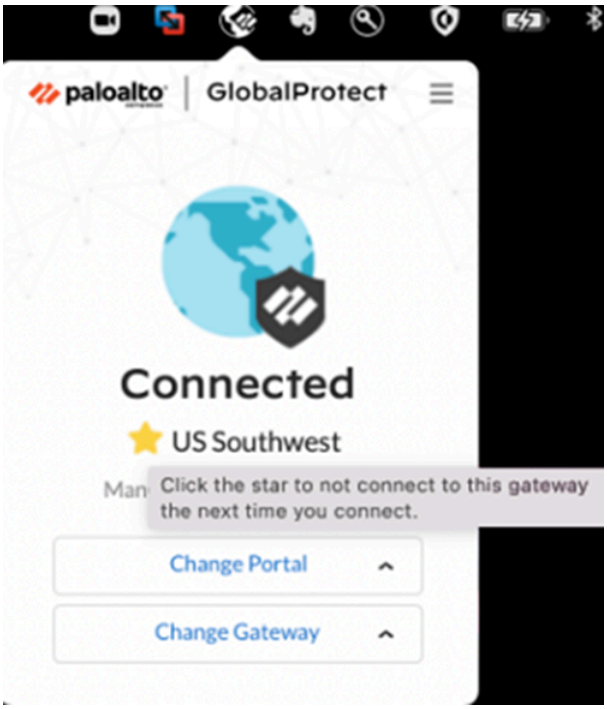
1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) If you are logging in to the GlobalProtect app for the first time, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.
3. (Optional) If multiple portals are saved on your app, select a portal from the **Change Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Change Portal** drop-down.
4. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the

available gateways. To connect to a different gateway, click the **Change Gateway** drop-down and then use one of the following options:

- Select a gateway manually (external gateways only). This option is only available if your administrator enables manual gateway selection.
- Assign and automatically connect to a preferred gateway:

  1. To designate a gateway as preferred, click the star icon (☆). The next time you connect, you will automatically connect to this preferred gateway.

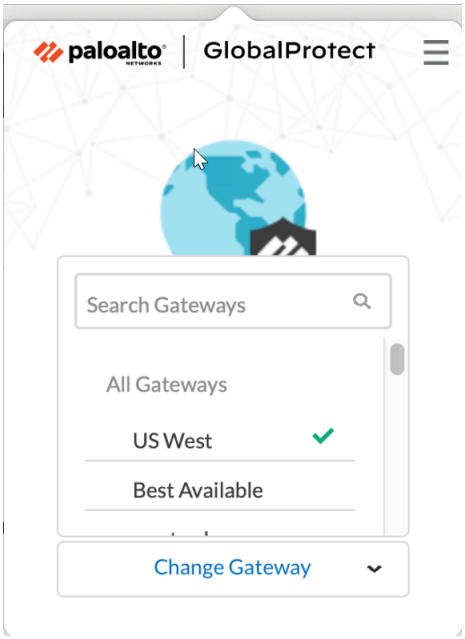
  If you later decide that you don't want the gateway as your preferred gateway anymore, you can simply clear the star icon to remove this gateway as a preferred connection.



2. By default, you automatically connect to the **Best Available** gateway that is identified by a check mark from the **Change Gateway** drop-down. If you set

the preferred gateway, a star displays by the starred gateway from the **Change Gateway** drop-down.

If your administrator configured manual external gateways in the portal agent configuration, you can choose a specific gateway using the gateway search field.



5. (Optional) Depending on the connection mode, click **Connect** to initiate the connection.
6. (Optional) If prompted, enter your **Username** and **Password** and then **Sign In**.

   If your administrator has allowed you to use biometric (fingerprint) information to sign in, you need to first sign-in with a username and password twice (once to save it and again to authenticate); you can then use biometric information to sign in.

   If your system administrator has enabled the **GlobalProtect System Extensions**, you must enable the system extensions in macOS that was blocked from loading to use the split tunnel and Enforce GlobalProtect for Network Access features.

   *Users do not need administrator privileges to allow both the **Network Extensions Configuration** pop-up prompts. Your administrator can suppress these message prompts by using the mobile device management system (MDM) such as Jamf Pro to automatically load the network extensions without receiving these prompts. Refer to the knowledge base article at https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 for information on how to enable system and network extensions using Jamf Pro.*

   1. (macOS Catalina 10.15.4 or later and macOS Big Sur 11 or later only) If your system administrator has configured split tunnel based on domains and applications on

the GlobalProtect gateway or enabled the Enforce GlobalProtect Connections for Network Access feature, select **Allow** in the following pop-up prompt:

If you select **Don't Allow**, the Split Tunnel feature cannot be used on the GlobalProtect app, the Enforce GlobalProtect Connections for Network Access feature will not work, and the GlobalProtect connections for network access cannot be enforced. This pop-up prompt will appear the next time you connect to the portal or gateway or until you select **Allow**.

When the app connects in external mode, the GlobalProtect system tray icon displays a shield ( ), and **Connected** appears when you hover over the icon. When the app connects in internal mode, the GlobalProtect system tray icon displays a house ( ), and **Internal Network** appears when you hover over the icon.

STEP 3 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

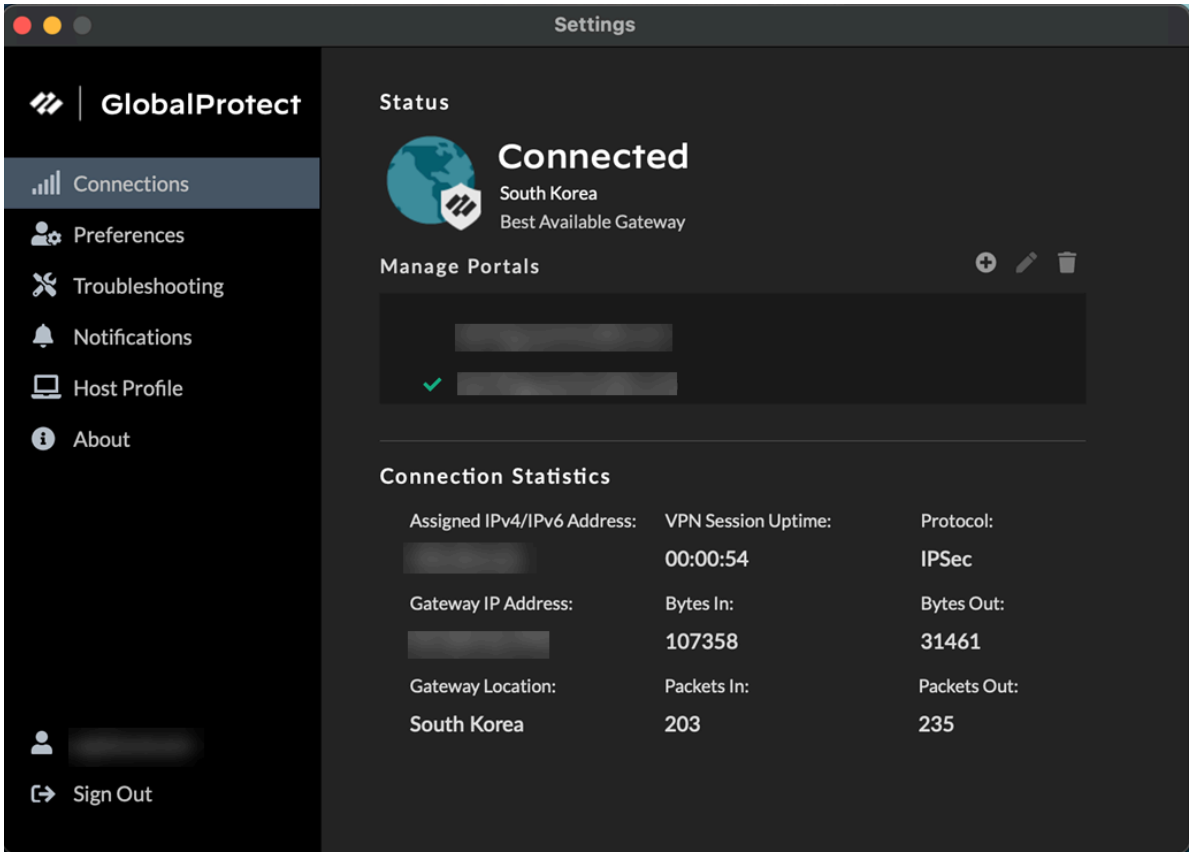
A notification appears if your administrator configured the portal to install the Autonomous DEM (ADEM) endpoint agent during the GlobalProtect app installation and has either allowed you to enable the tests or not allowed you to enable the tests. If your administrator has already installed the ADEM endpoint agent and later configured the portal to uninstall the ADEM endpoint agent, a notification appears at the next login.

STEP 4 | View information about your network connection.

After you launch the app, click the hamburger menu on the status panel to open the settings menu. Select **Settings** to open the **GlobalProtect Settings** panel, and then select one of the following settings to view and modify the GlobalProtect app:

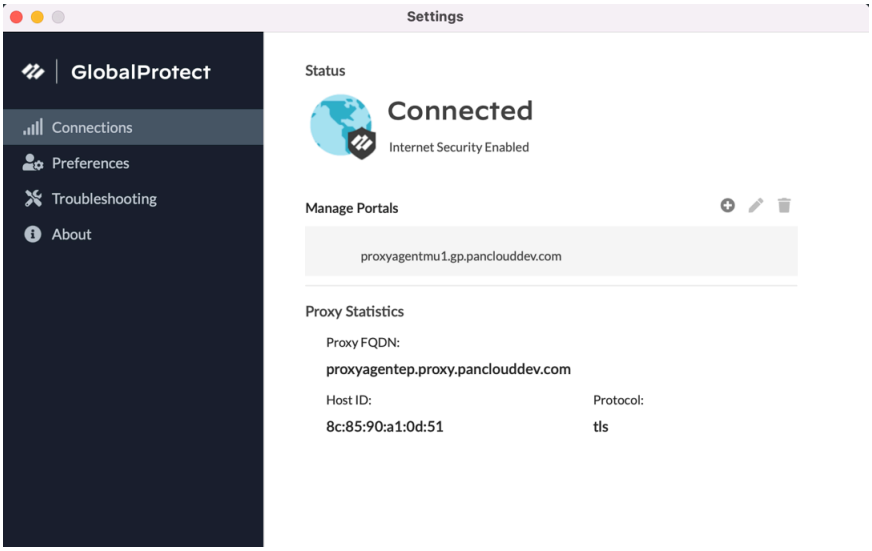
- **Connections**—The **Connections** tab displays the portal(s) associated with the GlobalProtect account. You can add, edit, or delete portals from this tab. This tab also displays the gateway to which you are connected. You can view connection statistics about the gateway (for example, gateway IP address, location, and VPN session uptime) when

your administrator sets **Enable Advanced View** to **Yes** in the GlobalProtect portal agent configuration. Select the **Connections** tab to see the countdown timer for the login lifetime.



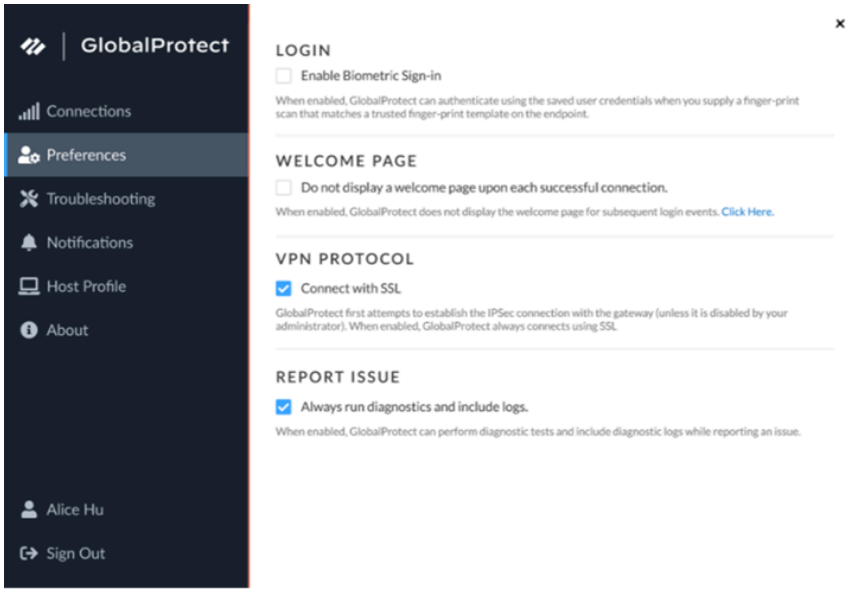
The **Connections** tab displays the proxy details if the Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security functionality is enabled for the app through Prisma Access.

Proxy Mode:



- **Preferences**—The **Preferences** tab is now available only if your administrator configures at least one of the following options:
  - **Enable Biometric Sign-in**—You can choose to use biometric (fingerprint) information to sign in. This option is available only if your administrator configures the **Save User Credentials** to **Only with User Fingerprint** in the GlobalProtect agent configuration. You must supply a fingerprint that matches a trusted fingerprint template on the endpoint to use a saved password for authentication to GlobalProtect portal and gateways.
  - **Do not display a welcome page upon each successful connection**—You can choose to display a welcome page upon successful login. This option is available only if your administrator sets the **Welcome Page** to **factory-default** in the GlobalProtect portal agent configuration.
  - **Connect with SSL**—You can choose to use SSL or stay with IPSec. This option is available only if your administrator sets **Connect with SSL Only** to **User can Change** in the GlobalProtect portal agent configuration .
  - **Always run diagnostic tests and include logs**—You can choose to enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs. This option

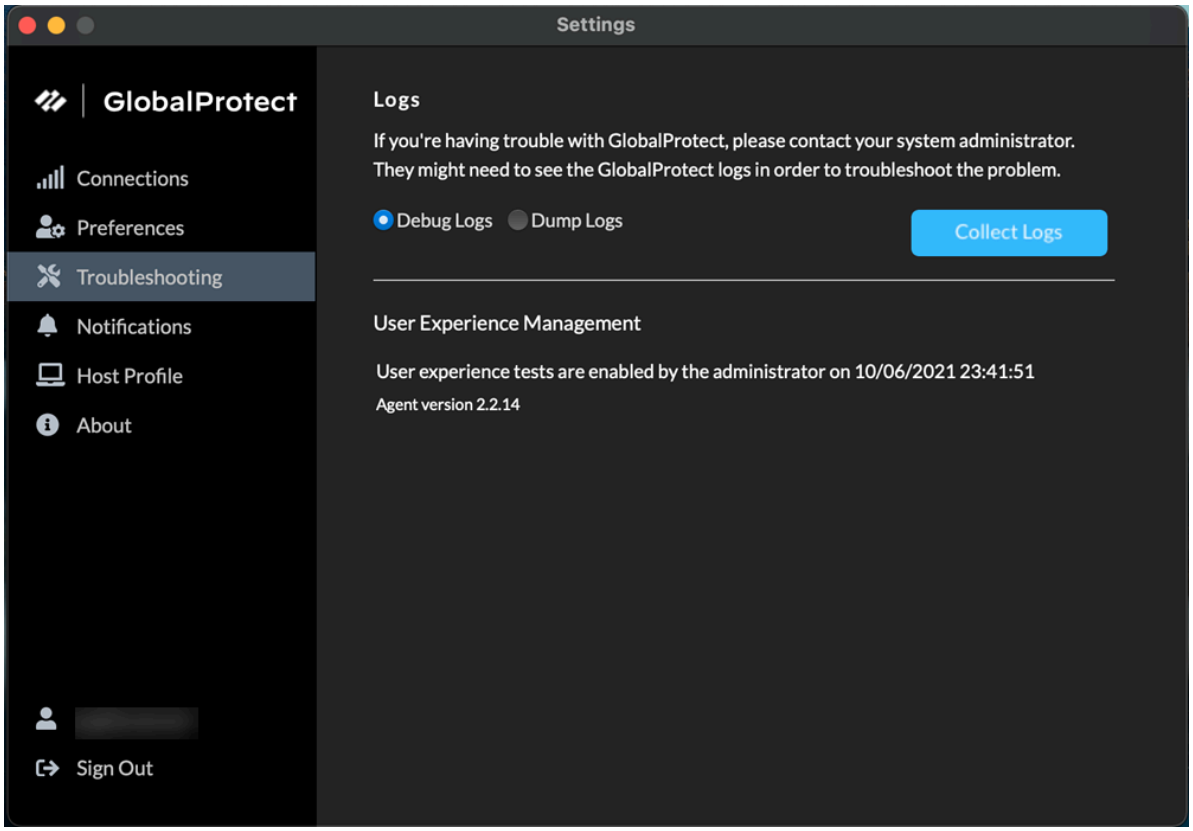
is available only if your administrator enables the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.



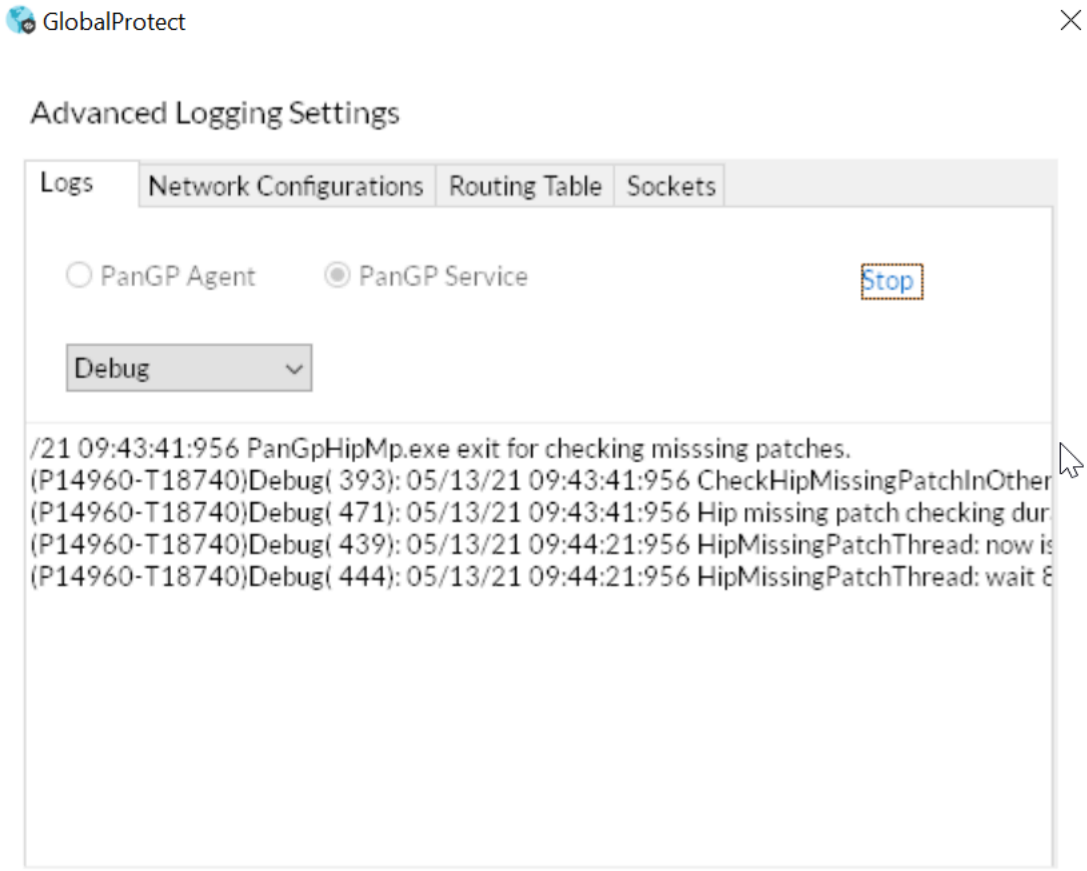
- **Troubleshooting**—The **Troubleshooting** tab allows you to **Collect Logs** and set the logging level to **Debug Logs** or **Dump Logs**, and optionally **Enable User Experience Tests**.

  In order for the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Strata Logging Service for further analysis, you must configure the GlobalProtect portal to enable the GlobalProtect app log collection for troubleshooting. Additionally, you can configure the HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names of the web servers/resources that you want to probe, and to determine issues such as latency or network performance on the end user's endpoint.

  You can click **Advanced** to view detailed information about their endpoint.



The **Advanced Logging Settings** window displays information about the network configuration, route settings, active connections, and logs.



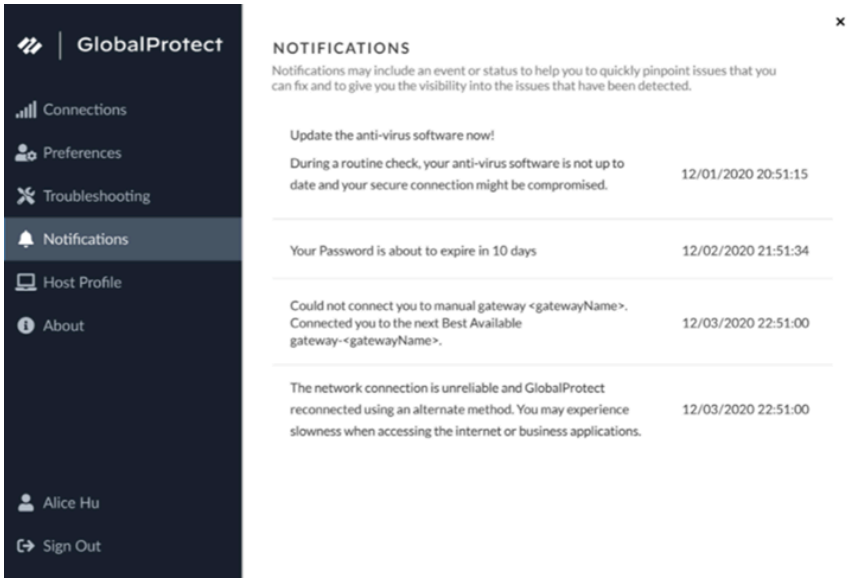
When GlobalProtect is connected, verify that the ADEM endpoint agent can perform user experience tests if the **Enable user experience tests** check box is displayed on the GlobalProtect app. Or you can verify that a message is displayed if your administrator installed the ADEM endpoint agent during the GlobalProtect app installation but does not allow you to enable or disable user experience tests from the GlobalProtect app. By default, heartbeat alerts are still forwarded to ADEM even when GlobalProtect is disabled or disconnected.

If your administrator configured the portal to install the Autonomous DEM endpoint agent during the GlobalProtect app installation and has allowed you to enable the tests, select the check box to **Enable user experience tests** on the GlobalProtect app. This check box does not appear if your administrator does not allow you to enable or disable user experience tests from the GlobalProtect app. Instead, a message is displayed, confirming that the app is enabled to run user experience tests.

If you do not select the check box to **Enable user experience tests**, heartbeat alerts are still forwarded to ADEM.

- **Notifications**—The **Notifications** tab displays the detailed information about specific notifications triggered on the GlobalProtect app. You can configure end-user notifications

about expiry of GlobalProtect app sessions on the gateway and schedule the display of these custom notifications on the app.

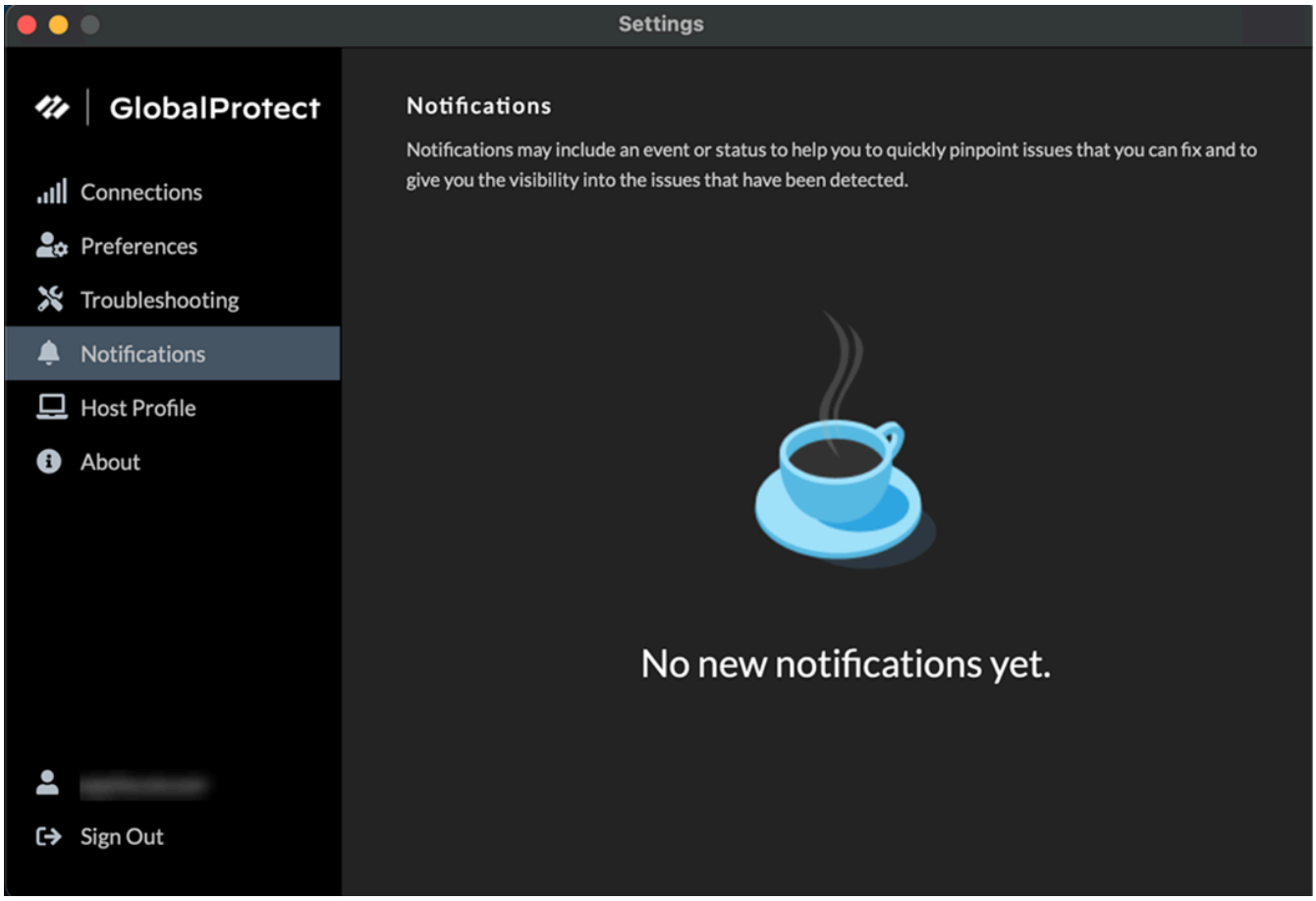


Starting from GlobalProtect app version 6.2.3, session and idle timeout messages are suppressed for the always-on connect method.

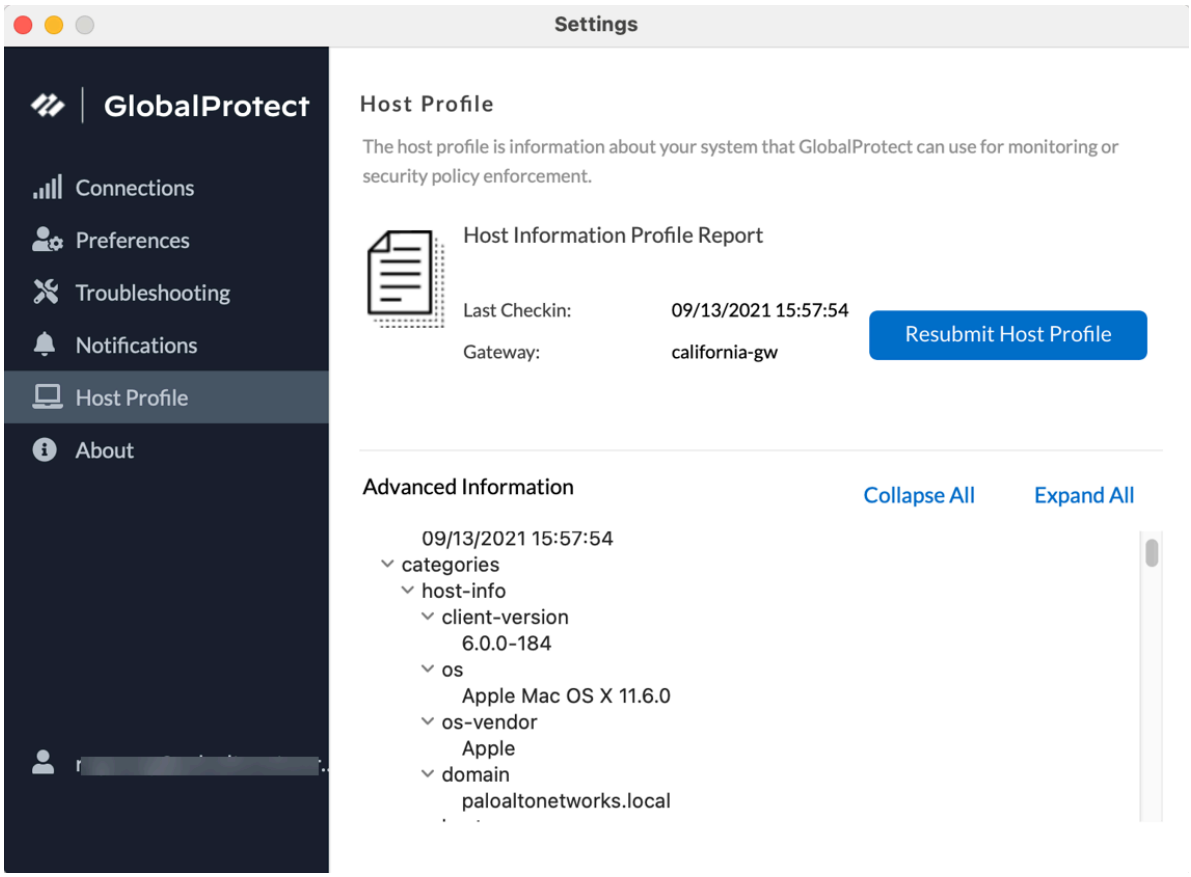
Starting from GlobalProtect app version 6.2, you can extend the login lifetime session of the GlobalProtect app before it expires to avoid abrupt app session logout. The login lifetime expiry notification informs you in advance when the app sessions are about to expire and provides the option to extend the duration of the user session so that you are not logged out of your session abruptly. The app will display the expiry notification with extend user

session option if your administrator has configured the notification settings for extending the session.

You are also notified if there are no new notifications triggered on the GlobalProtect app.

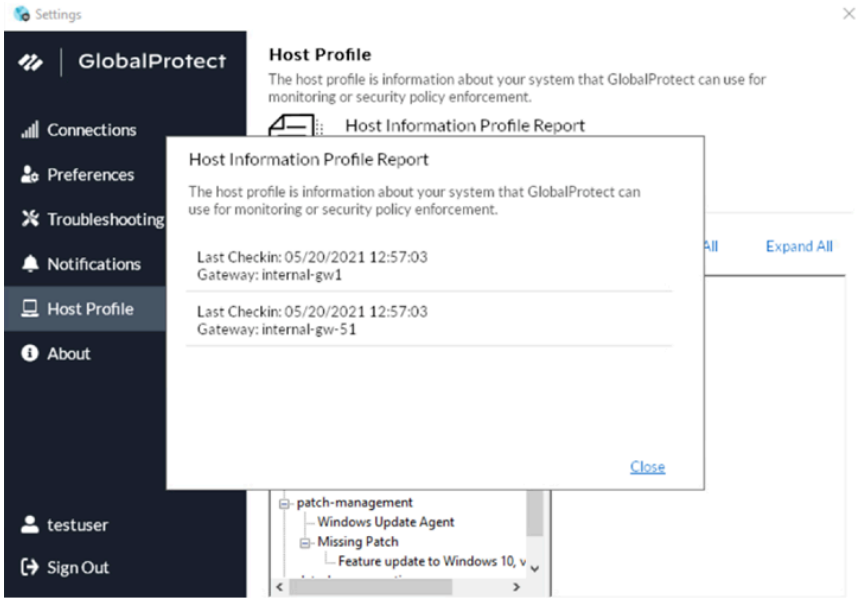


- **Host Profile**—The **Host Profile** tab displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile. You can **Resubmit Host Profile** to manually resubmit HIP data to the gateway.

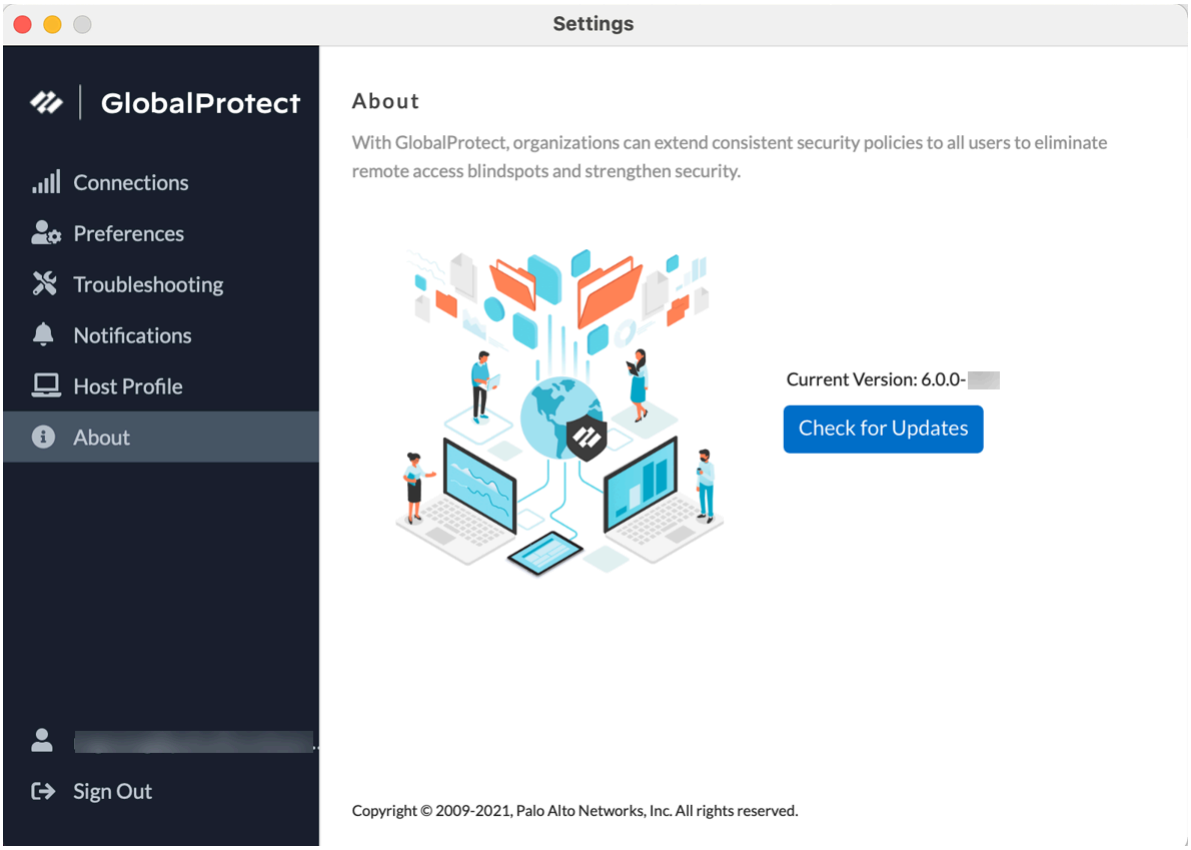


If your administrator configured multiple internal gateways in non-tunnel mode and internal host detection, you can click **More Details** to monitor the Host Information Profile

(HIP) report submission for each gateway from a central location to help you to quickly troubleshoot HIP related issues.



- **About**—The **About** tab displays the version of GlobalProtect currently installed on the endpoint and allows end users to **Check for Updates**.



STEP 5 | (Optional) Log in using a new password.

*If your GlobalProtect administrator configures the GlobalProtect portal agent to **Save User Credentials**, your credentials are automatically saved to the GlobalProtect app. If your password for accessing the corporate network changes, you must log in to GlobalProtect using your new password.*

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Click the hamburger menu to open the settings menu.
3. Select **Settings** to open the **GlobalProtect Settings** panel.
4. On the **GlobalProtect Settings** panel, **Sign Out** to clear your saved user credentials from the GlobalProtect app.
5. After you clear your user credentials, you can reconnect to GlobalProtect with your new username and password.

STEP 6 | (Optional) Disconnect from GlobalProtect.

If your administrator configures GlobalProtect with the **On-Demand** connect method, you can disconnect from GlobalProtect by clicking **Disconnect** on the status panel.

Report an Issue From the GlobalProtect App for macOS

When you experience unusual behavior such as poor network performance or a connection is not established with the portal and gateway, you can report an issue directly to Strata Logging Service to which your administrator can access. You no longer need to manually collect and send the GlobalProtect app logs through email or to store them on a cloud drive.

*To display the **Report an Issue** option on the GlobalProtect app, your administrator must enable the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.*

STEP 1 | Connect to the GlobalProtect portal or gateway.

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) If you are logging in to the GlobalProtect app for the first time, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.
3. (Optional) If multiple portals are saved on your app, select a portal from the **Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Portal** drop-down.
4. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, click the gateway drop-down.

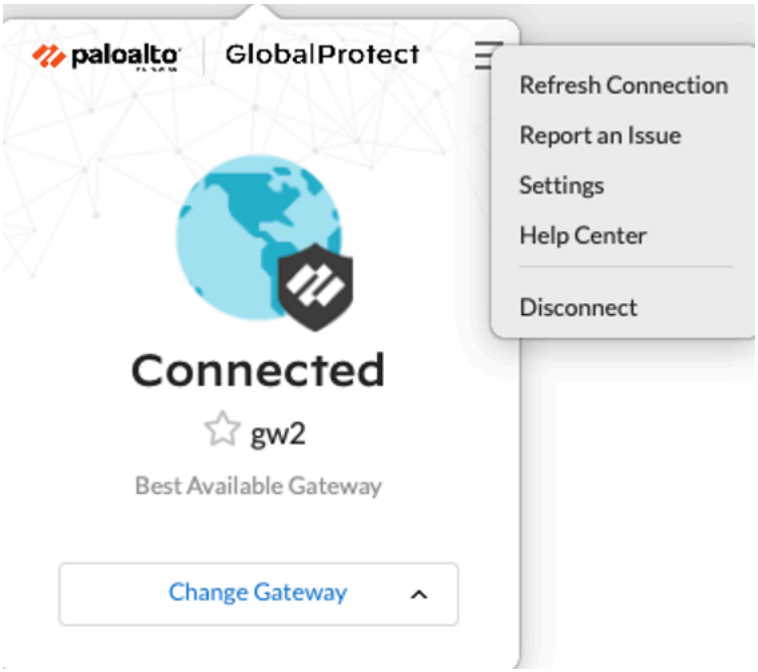
STEP 2 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

STEP 3 | Report an issue from the GlobalProtect app from your endpoint.

After you launch the app, click the hamburger menu on the status panel to report an issue to your administrator.

1. Select **Report an Issue**.



2. Enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs. Both diagnostic and troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report.

   After the diagnostic tests are successfully completed, the GlobalProtect debug log files are uploaded to Strata Logging Service from your endpoint.

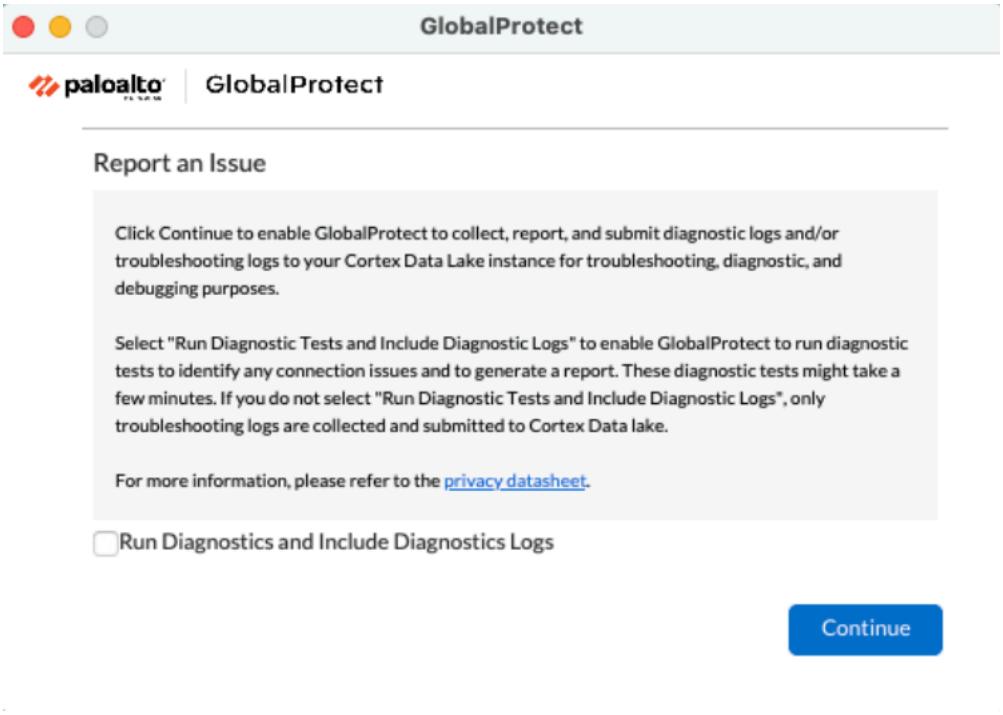
   *If you do not enable the app to run diagnostic tests and to include diagnostic logs, only troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report. The GlobalProtect app checks for the report files (pan_gp.trb.log or pan_gp_trbl.log) that are automatically generated in `.json` format. A notification message appears if no issues were found in the troubleshooting logs. Click **Retry** to check if the pan_gp.trb*.log files exist.*

3. Select the **Run Diagnostic Tests and Include Diagnostic Logs** check box.
4. Click **Continue** to allow the app to create a troubleshooting log and to send the report to your administrator's Strata Logging Service instance.

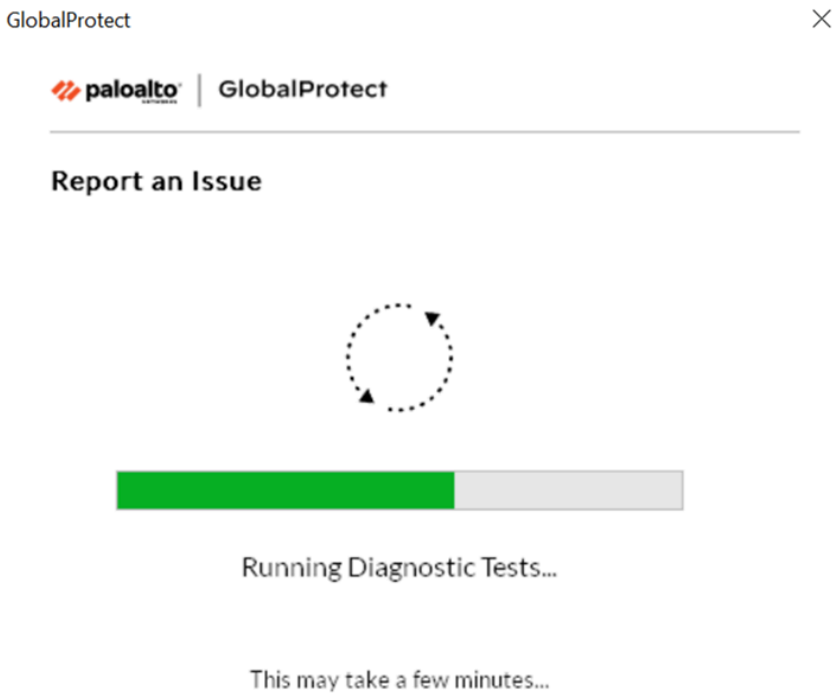
   The results of the end-to-end diagnostic tests are stored in the pan_gp_diag.log file in `.json` format and sent to your administrator's Strata Logging Service instance along with the pan_gp.trb*.log files.

   The results of the end-to-end diagnostic tests are stored in the pan_gp_diag.log file in `.json` format and sent to your administrator's Strata Logging Service instance along with the pan_gp.trb*.log files. The GlobalProtect app can run diagnostic tests with a tunnel or without a tunnel. For example, you might want to enter your GlobalProtect

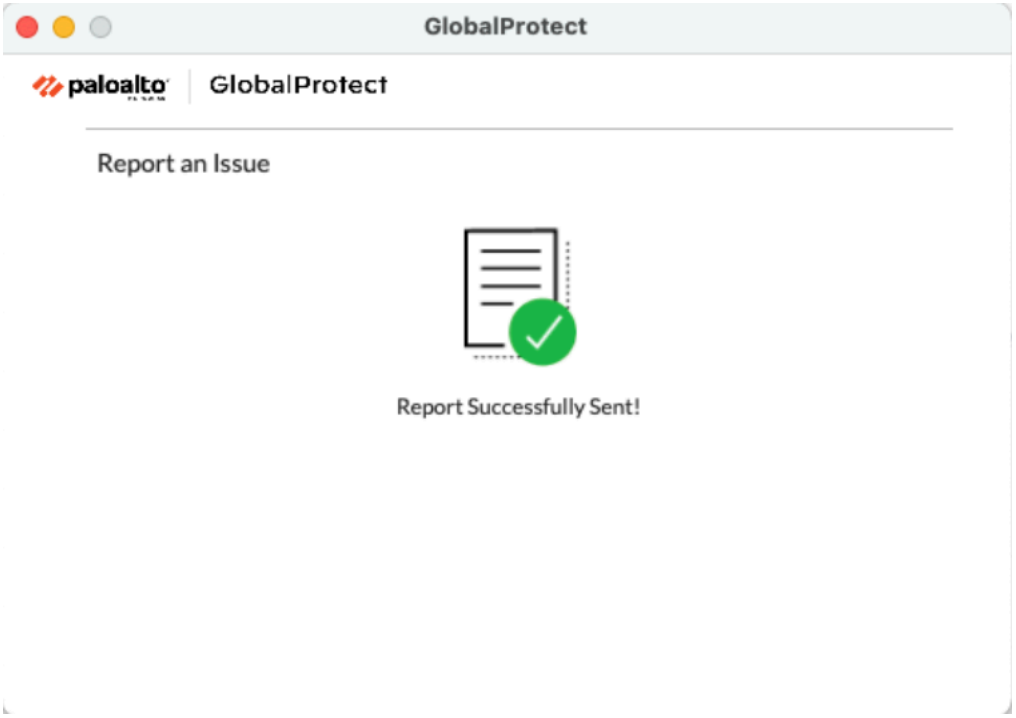
login credentials prior to the app connecting and running diagnostic tests through the tunnel.



A message pops-up, confirming that the app is running diagnostic tests only if you selected the **Run Diagnostic Tests and Include Diagnostic Logs** check box.



5. Click **Close** to confirm that the app successfully sent the report to Strata Logging Service. This confirmation message displays the date and time when the report was processed and sent.



Disconnect the GlobalProtect App for macOS

If your administrator configures the GlobalProtect connect method as **Always On**, you can disconnect the GlobalProtect app. For example, you might want to disconnect the app if the GlobalProtect virtual private network (VPN) is not working in a hotel, and the VPN failure prevents you from connecting to the internet. After disconnecting the GlobalProtect app, you can connect to the internet using unsecured communication (without a VPN).

The method, amount of time, and number of times for which you can disconnect the GlobalProtect app depends on how the administrator configures your GlobalProtect service (PanGPS). This configuration can prevent you from disconnecting the app entirely or allow you to disconnect the app only after responding to a challenge correctly.

If your configuration includes a challenge, the GlobalProtect app prompts for one of the following:

- Reason you want to disconnect the app
- Respond to one or more reasons such as **Internet speed slow** or **App not working** (if required)
- Passcode
- Ticket number

If the challenge involves a passcode or ticket number, we recommend that you contact a GlobalProtect administrator or Help Desk person by phone.

Administrators typically provide passcodes in advance, either through email (for new GlobalProtect users) or posted on your organization's website. In response to an outage or system issue, administrators may also provide passcodes by phone.

Before you can obtain a valid ticket number, your endpoint displays a ticket request number that you must communicate to your GlobalProtect administrator or a Help Desk person. If your disconnect request is approved, you will receive a valid ticket number that you can use to disconnect GlobalProtect.

The following steps describe how to disconnect the app and pass a challenge:

STEP 1 | Disconnect the GlobalProtect app.

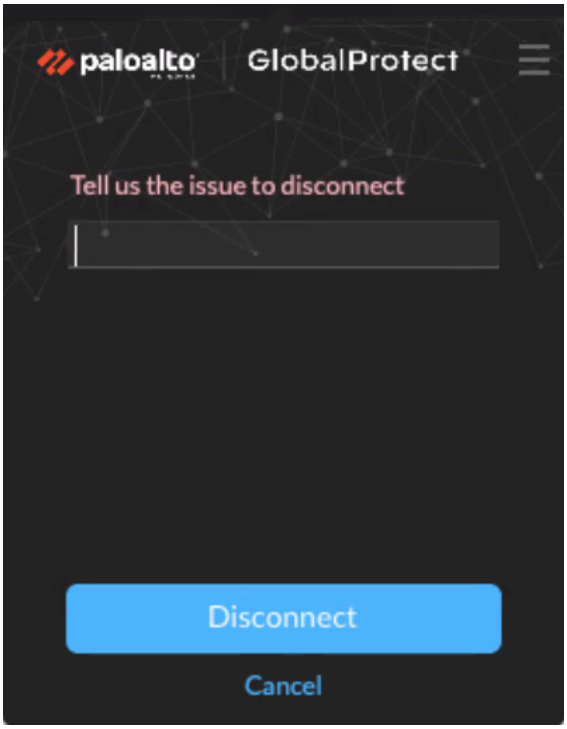
1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the hamburger menu to open the settings menu.
3. Select **Disconnect**.

*The **Disconnect** option is visible only if your GlobalProtect agent configuration allows you to disconnect the app. If the configuration allows you to disconnect the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*

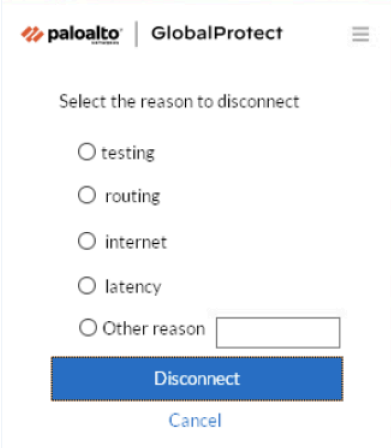
STEP 2 | Respond to one or more challenges, if required.

If prompted, provide the following information:

- **Tell us the issue to disconnect**—Your reason for disconnecting the GlobalProtect app.



- **Select the reason to disconnect**—If your configuration requires you to respond to one or more reasons or enter another reason, the GlobalProtect app displays the reasons as soon as you select **Disconnect**.



- **Passcode**—A passcode that is typically provided by your administrator in advance, based on a known issue or event that requires you to disconnect the app.
- **Ticket**—If your configuration requires you to provide a ticket number, the GlobalProtect app displays an eight-character hexadecimal ticket request number as soon as you select **Disconnect**. To disconnect the app with a ticket number, contact your administrator or Help Desk person (by phone) and provide the ticket request number. After approving your

request, your administrator or Help Desk person provides you with an eight-character hexadecimal ticket number. Enter the ticket number in the **Ticket** field, and then click **OK**.

Uninstall the GlobalProtect App for macOS

Use the following steps to uninstall the GlobalProtect app from your macOS endpoint . Keep in mind that by uninstalling the app, you no longer have VPN access to your corporate network and your endpoint will not be protected your company's security policies.

Only users with administrator privileges can uninstall the GlobalProtect app from macOS endpoints.

On macOS endpoints, you can use the macOS installation program (in this case, the GlobalProtect Installer) to uninstall a program. To uninstall the GlobalProtect app from your endpoint, install the GlobalProtect software package, and then launch the GlobalProtect Installer. The GlobalProtect Installer prompts you to select the **Uninstall GlobalProtect** package. If your administrator enabled the system extensions in the GlobalProtect app for your macOS endpoint during the GlobalProtect app installation, the GlobalProtect app will also prompt you to remove the system extensions during the GlobalProtect uninstallation. After the **Uninstall GlobalProtect** package was successfully installed, the GlobalProtect app is removed from the endpoint.

If you no longer have the GlobalProtect Installer on your macOS endpoint, you can uninstall GlobalProtect by running the following command from the command line:

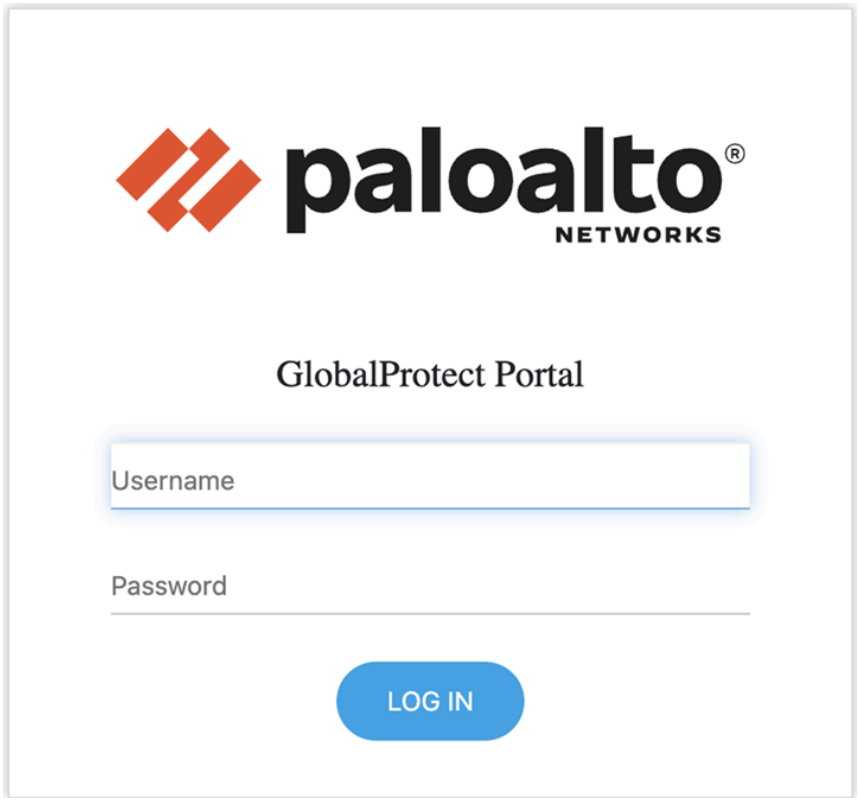
```
sudo /Applications/GlobalProtect.app/Contents/Resources/
uninstall_gp.sh
```


STEP 1 | Log in to the GlobalProtect portal.

1. Launch your web browser and go to the following URL:

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

   Example: **`http://gp.acme.com`**
2. On the portal login page, enter your **Name** (username) and **Password**, and then click **LOG IN**. In most instances, you can use the same username and password that you use to connect to your corporate network.



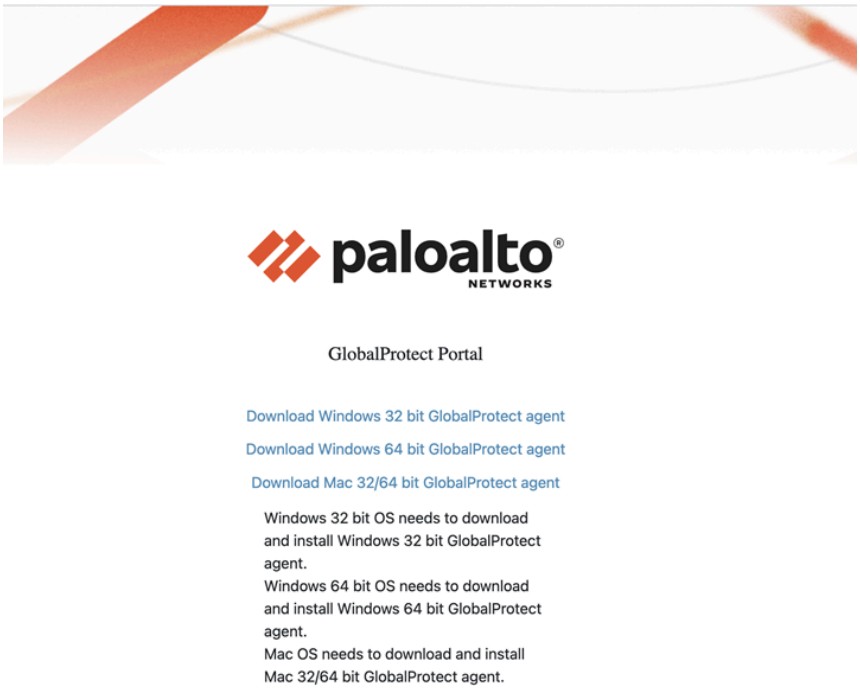
STEP 2 | Navigate to the app download page.

In most instances, the app download page appears immediately after you log in to the portal.

*If your system administrator has enabled GlobalProtect Clientless VPN access, the application page opens after you log in to the portal (instead of the app download page). Select **GlobalProtect Agent** to open the download page.*

STEP 3 | Download the app.

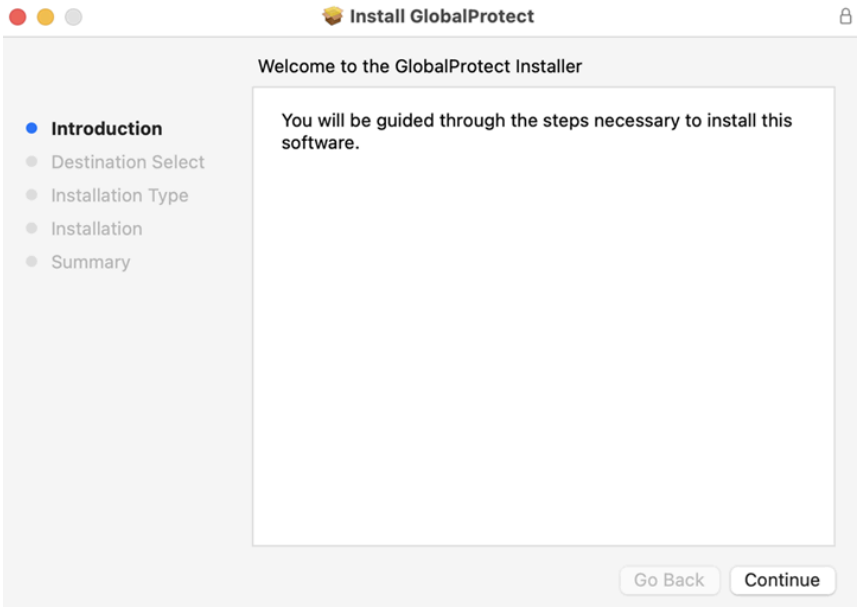
1. Click **Download Mac 32/64 bit GlobalProtect agent**.



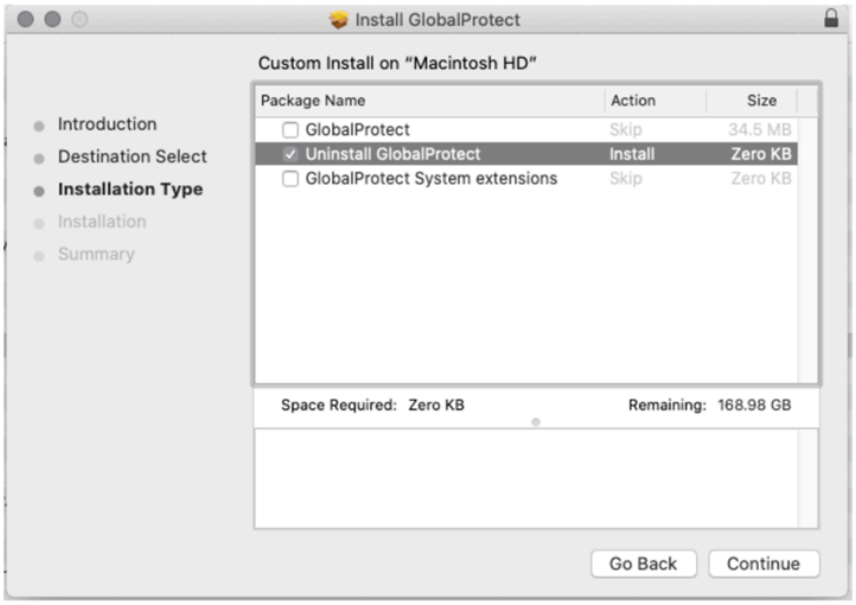
2. When prompted, **Run** the software.
3. When prompted again, **Run** the GlobalProtect Installer.

STEP 4 | Uninstall GlobalProtect.

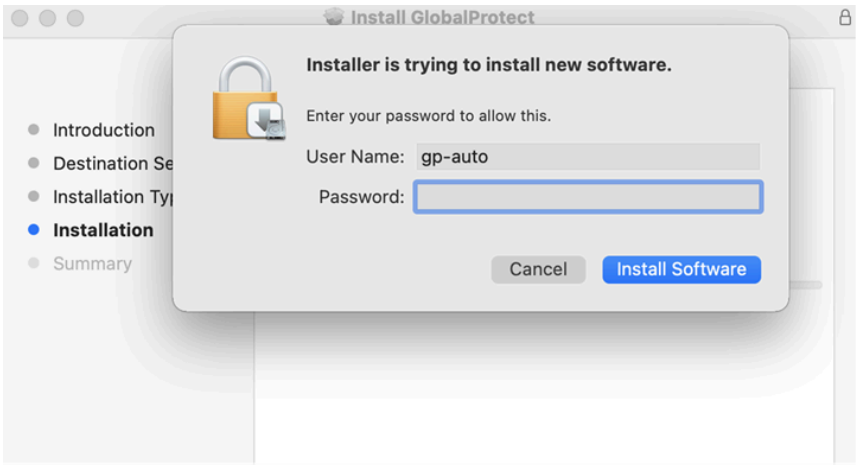
1. From the GlobalProtect Installer, click **Continue**.



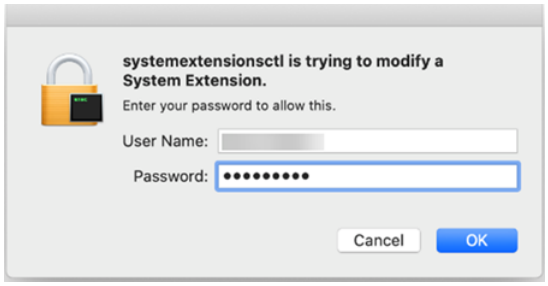
2. On the **Destination Select** screen, click **Continue**.
3. On the **Installation Type** screen, select the **Uninstall GlobalProtect** check box, and then click **Continue**.



4. Click **Install** to confirm that you want to remove the GlobalProtect app.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to uninstall GlobalProtect.

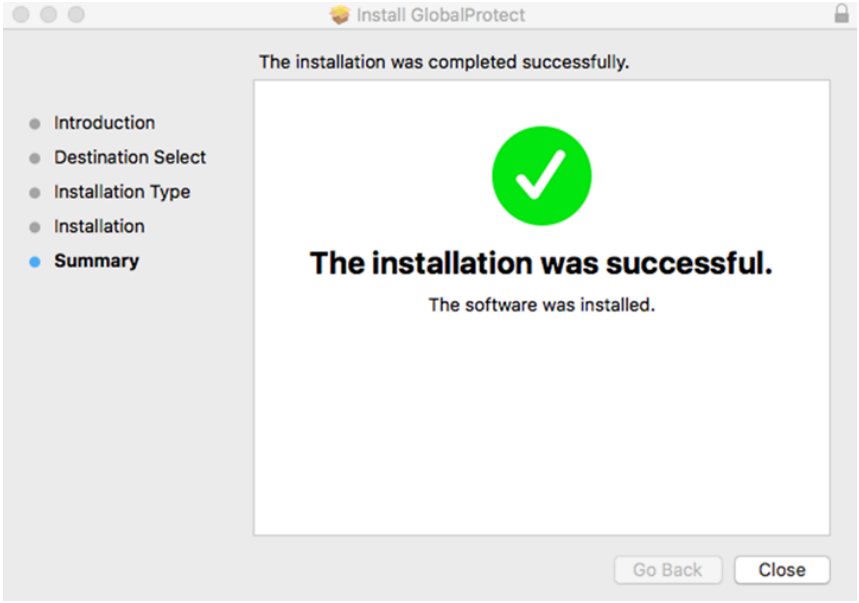


6. If your system administrator has enabled the macOS system extensions during the GlobalProtect app 5.1.4 installation running macOS Catalina 10.15.4 or later, the pop-up prompt appears for you to uninstall the system extensions. When prompted, enter your **User Name** and **Password**, and then click **OK** to remove the system extensions.



STEP 5 | Confirm that the GlobalProtect app is no longer installed.

A message pops up, confirming that the **Uninstall GlobalProtect** package was successfully installed. This confirmation indicates that the GlobalProtect app has been removed from your endpoint.



Remove the GlobalProtect Enforcer Kernel Extension

When you uninstall the GlobalProtect app for macOS, and then install a new instance of the app, you may encounter connection issues if the GlobalProtect enforcer kernel extension is not updated correctly. A kernel extension (`kext`) is a plugin for the macOS operating system that manages applications. If you cannot connect to GlobalProtect after installing a new instance of the app, use the following procedures to locate and remove the GlobalProtect enforcer kernel extension.

STEP 1 | Uninstall the GlobalProtect App for Mac.

STEP 2 | Determine if the GlobalProtect enforcer kernel extension exists on the endpoint.

On the macOS endpoint, open the **Terminal** application under the **Applications** > **Utilities** folder, and then enter the following command:

```
kextstat | grep gplock
```

STEP 3 | If the extension exists, unload the enforcer.

Enter the following command on the **Terminal** application to unload the enforcer:

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

STEP 4 | Prevent the enforcer from reloading after a reboot.

Enter the following command on the **Terminal** application to remove the enforcer from the macOS hard disk:

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

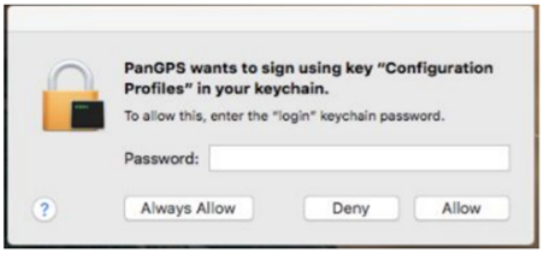
STEP 5 | Download and Install the GlobalProtect App for Mac.

Enable the GlobalProtect App for macOS to Use Client Certificates for Authentication

When the GlobalProtect app is installed on macOS endpoints for the first time and client certificate authentication is enabled on the portal or gateway, the Keychain Pop-Up prompt appears, prompting users to enter their password so that GlobalProtect can access and use client certificates from the login keychain. The Keychain Pop-Up prompt can also appear when a new certificate is installed because the previous certificate expired.

You must use the following procedure to enable the GlobalProtect app for macOS to use client certificates for authentication:

STEP 1 | Enter your password to allow login keychain access with the macOS endpoint in the following Keychain Pop-Up prompt:



STEP 2 | Select **Always Allow** to let GlobalProtect to establish the VPN tunnel. The Keychain Pop-Up prompt does not appear until the client certificate has expired. This pop-up prompt can appear again when the client certificate is renewed.

*If you select **Allow**, the Keychain Pop-Up prompt will appear every time users connect to GlobalProtect. If you select **Deny**, GlobalProtect cannot establish a VPN tunnel and the Keychain Pop-Up prompt will appear. GlobalProtect can establish a VPN tunnel only after you allow access to the login keychain.*

GlobalProtect App for Linux

GlobalProtect™ is a program that runs on your endpoint (desktop computer, laptop, or server) to protect you by using the same security policies that protect the sensitive resources in your corporate network. GlobalProtect™ secures your intranet, private cloud, public cloud, and internet traffic and allows you to access your company's resources from anywhere in the world.

The following sections provide instructions for installing and using the GlobalProtect app for Linux:

- Download and Install the GlobalProtect App for Linux
- Use the GlobalProtect App for Linux
- Report an Issue From the GlobalProtect App for Linux
- Disable the GlobalProtect App for Linux
- Uninstall the GlobalProtect App for Linux

Download and Install the GlobalProtect App for Linux

GlobalProtect offers you two different methods to install the GlobalProtect app on your Linux device: a GUI-based installation version and a CLI version. If you use a supported Linux operating system that supports a graphical interface, you can install the GUI version of the GlobalProtect; otherwise, download and install the CLI version of the GlobalProtect app.

- Download and Install the GUI Version of GlobalProtect for Linux
- Download and Install the CLI Version of GlobalProtect for Linux

Download and Install the GUI Version of GlobalProtect for Linux

If your Linux device supports a graphical user interface, complete these steps to install the GUI version of GlobalProtect for Linux.

The GUI version of GlobalProtect for Linux works with the default display manager, GNOME, on supported Linux platforms.

STEP 1 | Download the GlobalProtect app for Linux.

1. Log in to the Customer Support Portal. After you enter your username and password credentials, you are authenticated and you are logged in to the support site.
2. Select **Updates** > **Software Updates**.
3. Filter by GlobalProtect Agent for Linux, and download the associated TGZ file.
4. Extract the files from the package.

```
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
                                                 ./
gp_install.sh

 ./gp_uninstall.sh
```

You will see multiple installation packages for supported operating system versions—DEB for Debian and Ubuntu and RPM for CentOS and Red Hat. The package for the GUI version is denoted by a GlobalProtect_UI prefix.

STEP 2 | (Optional) If your Linux endpoint must use a manual proxy server configuration, configure the proxy settings.

The GlobalProtect app for Linux supports only a basic proxy server configuration but does not support the use of Proxy Auto-Configuration (PAC) files and proxy authentication.

The GlobalProtect app for Linux obtains the proxy settings from the HTTP_PROXY, HTTPS_PROXY and NO_PROXY environment variables in the `/etc/environment` file. If you later change the system proxy configuration, verify that the terminal from which GlobalProtect runs uses the proxy environment variables. If you do not see the new settings, log out and back in for the new settings to take effect.

If you have configured the HTTP_PROXY variable or the HTTPS_PROXY variable, make sure that the GlobalProtect portal matches the settings configured for the NO_PROXY variable.

1. To set your proxy on your Linux endpoint, edit the HTTP_PROXY environment variable or HTTPS_PROXY environment variable (for example, HTTPS_PROXY=”`https://yourproxy.local:8080`”).
2. To configure the IP addresses or domain names that you want to exclude from the proxy, edit the NO_PROXY environment variable (for example, NO_PROXY=”`www.gpqa.com`”).

   Use commas to separate multiple IP addresses or domain names. Starting with GlobalProtect app 5.1.6, you can use the wildcard character (*) for IP addresses or domain names (for example, NO_PROXY=”`*.domain.com`”).

STEP 3 | Install the GUI version of the GlobalProtect app for Linux.

To Install the GlobalProtect app UI distribution package, use the **`$ ./gp_install.sh`** command:

```
$ ./gp_install.sh --help
Usage: $ sudo ./gp_install [--cli-only | --arm | --help]
  --cli-only: CLI Only
  --arm:      ARM
```



```
no options: UI
```

Starting from GlobalProtect Linux version 6.2.1, you must use the following commands to install the CLI or GUI versions of the app:

- *To install the GlobalProtect UI package-* ***$ ./gp_install.sh***
- *To install the GlobalProtect CLI package-* ***$ ./gp_install.sh --cli-only***

You don't need to run the ***./gp_install.sh*** *with* ***sudo*** *for GlobalProtect app Linux 6.2.1 and later versions. As the script executes, users will be prompted to enter the* ***sudo*** *password.*

The script checks the Linux distribution and version in your environment to identify and install the packages required. After installation completes, the GlobalProtect app automatically launches.

STEP 4 | Log out of the Linux operating system or the SSH session depending on the installation method you used and log back in.

When you log out, package updates are applied and you are able to see the GlobalProtect icon (as well as any other relevant updates) when you log back in. This step is required to ensure that any new package updates during install are applied to the GlobalProtect app.

If you do not see the GlobalProtect icon in the tray after logging in, follow one of the steps below:

- *Type the* `globalprotect launch-ui` *CLI command in a terminal window.*
- *Search for globalprotect in the application list and pin it to your dashboard.*

STEP 5 | Specify your portal address and enter your credentials when prompted to begin the connection process.

STEP 6 | (Optional) To import a certificate, complete the following steps.

When you want to pre-deploy a client certificate to an endpoint for certificate-based authentication, you can copy the certificate to the endpoint and import it for use by the GlobalProtect app. Use the **globalprotect import-certificate --location <*location*>** command to import the certificate on the endpoint. When prompted you must supply the certificate password.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12
Please input passcode:
Import certificate is successful.
```

Download and Install the CLI Version of GlobalProtect for Linux

If your Linux device does not support a GUI, install the GlobalProtect app for Linux by completing these steps. The GlobalProtect app for Linux supports the DEB, RPM, and TAR installation packages.

STEP 1 | Download the GlobalProtect app for Linux.

1. Obtain the app package from your IT administrator and then copy the TGZ file to the Linux endpoint.

   For example, if you downloaded the package to a macOS endpoint, you can open a terminal and then copy the file:

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

   where ***<DestinationFolder>*** is a location such as `~/pkgs/` where you want to store the TGZ file.

2. From the Linux endpoint, unzip the package.

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

   After you unzip the package, you will see installation packages—DEB for Ubuntu and RPM for CentOS and Red Hat—and the scripts to install and uninstall the packages.

STEP 2 | (Optional) If your Linux endpoint must use a manual proxy server configuration, configure the proxy settings.

The GlobalProtect app for Linux supports only a basic proxy server configuration but does not support the use of Proxy Auto-Configuration (PAC) files and proxy authentication.

The GlobalProtect app for Linux obtains the proxy settings from the HTTP_PROXY, HTTPS_PROXY and NO_PROXY environment variables in the `/etc/environment` file. If you later change the system proxy configuration, verify that the terminal from which GlobalProtect

runs uses the proxy environment variables. If you do not see the new settings, log out and back in for the new settings to take effect.

If you have configured the HTTP_PROXY variable or the HTTPS_PROXY variable, make sure that the GlobalProtect portal matches the settings configured for the NO_PROXY variable.

1. To set your proxy on your Linux endpoint, edit the HTTP_PROXY environment variable or HTTPS_PROXY environment variable (for example, HTTPS_PROXY="https://yourproxy.local:8080").
2. To configure the IP addresses or domain names that you want to exclude from the proxy, edit the NO_PROXY environment variable (for example, NO_PROXY="www.gpqa.com").

   Use commas to separate multiple IP addresses or domain names. Starting with GlobalProtect app 5.1.6, you can use the wildcard character (*) for IP addresses or domain names (for example, NO_PROXY="*.domain.com").

STEP 3 | Install the app package using **CLI Only** command:

```
$ ./gp_install.sh --help
Usage: $ sudo ./gp_install [--cli-only | --arm | --help]
  --cli-only: CLI Only
  --arm:      ARM
  no options: UI
```

Starting from GlobalProtect Linux version 6.2.1, you must use the following commands to install the CLI or GUI versions of the app:

- *To install the GlobalProtect UI package- **$ ./gp_install.sh***
- *To install the GlobalProtect CLI package- **$ ./gp_install.sh --cli-only***

*You don't need to run the **./gp_install.sh** with **sudo** for GlobalProtect app Linux 6.2.1 and later versions. As the script executes, users will be prompted to enter the **sudo** password.*

STEP 4 | (Optional) Change CLI modes.

You can run commands in either command-line or prompt mode. Command-line mode requires you to specify the full GlobalProtect command. Prompt mode requires you to specify only the command (without the app name) and displays more detailed output than command-line mode.

1. To switch to prompt mode, enter **globalprotect** without any arguments.

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


2. To exit prompt mode, enter **quit**.

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

STEP 5 | View the help for GlobalProtect app for Linux.

Prompt mode:

```
>>
      help
      Usage: only the following commands are supported:
      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
```

Command-line mode:

```
user@linuxhost:~$
      globalprotect help
      Usage: only the following commands are supported:
      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 | Use the CLI version of the GlobalProtect app for Linux.

Use the GlobalProtect App for Linux

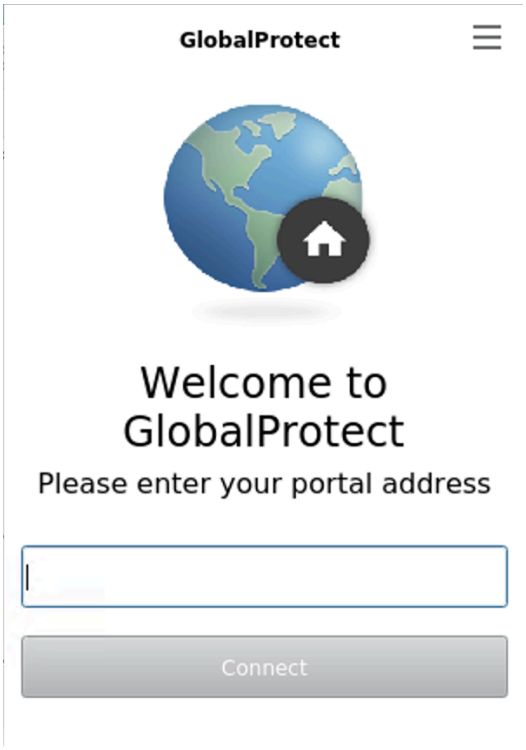
GlobalProtect supports two versions of the GlobalProtect app for Linux: One version if your Linux device supports a GUI, and CLI version if your Linux device does not support a GUI.

- Use the GUI Version of the GlobalProtect App for Linux
- Use the CLI Version of the GlobalProtect App for Linux

Use the GUI Version of the GlobalProtect App for Linux

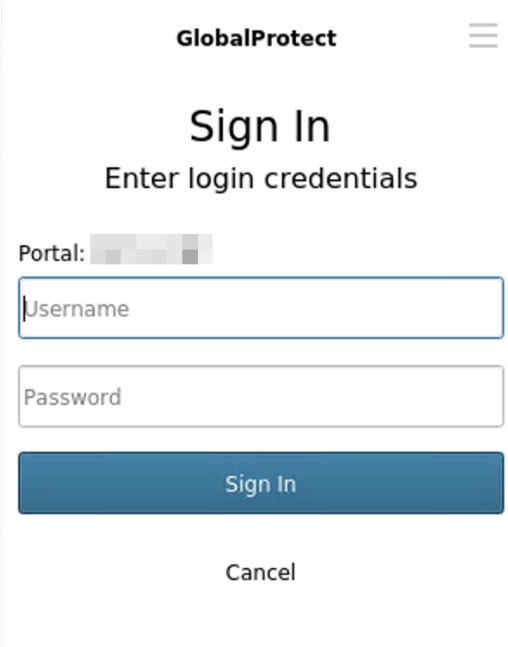
To use the GUI version of the GlobalProtect app for Linux, complete these steps.

STEP 1 | In the GlobalProtect window, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.



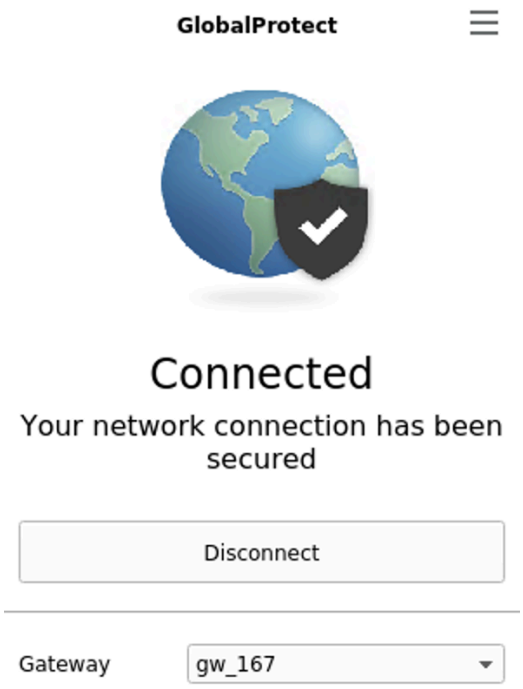
After you download and install the GUI version of the GlobalProtect app for Linux, the GlobalProtect app automatically launches.

1. (Optional) If multiple portals are saved on your app, select a portal from the **Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Portal** drop-down.



2. Enter the **Username** and **Password** for the portal and then **Sign In**.

In most instances, you can use the same username and password that you use to connect to your corporate network. After you sign in, the GlobalProtect portal shows a status of **Connected**.

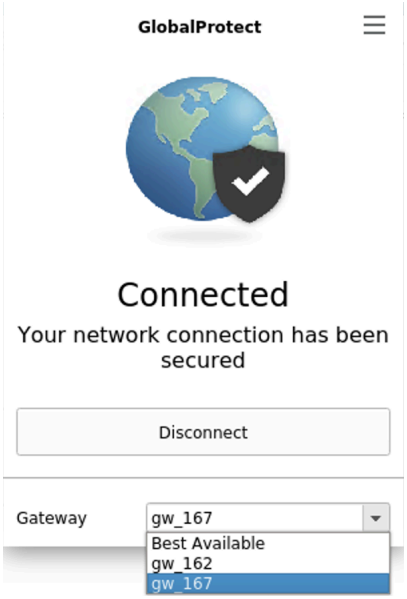


3. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the

available gateways. To connect to a different gateway, click the gateway drop-down and then use one of the following options:

- Select a gateway manually (external gateways only).

  This option is only available if your administrator enables manual gateway selection.



- Assign and automatically connect to a preferred gateway:

  1. From the menu on the top right of the app's status panel, select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.

2. From the list of available gateways, select the gateway that you want to set as the preferred gateway and then **Set as Preferred**.
3. **Close** the dialog.

If you no longer want to connect to the gateway automatically, you can also remove the preferred gateway assignment:

1. From the menu on the top right of the app's status panel, select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.
2. From the list of available gateways, select the preferred gateway and then **Remove Preferred**.
3. **Close** the dialog.

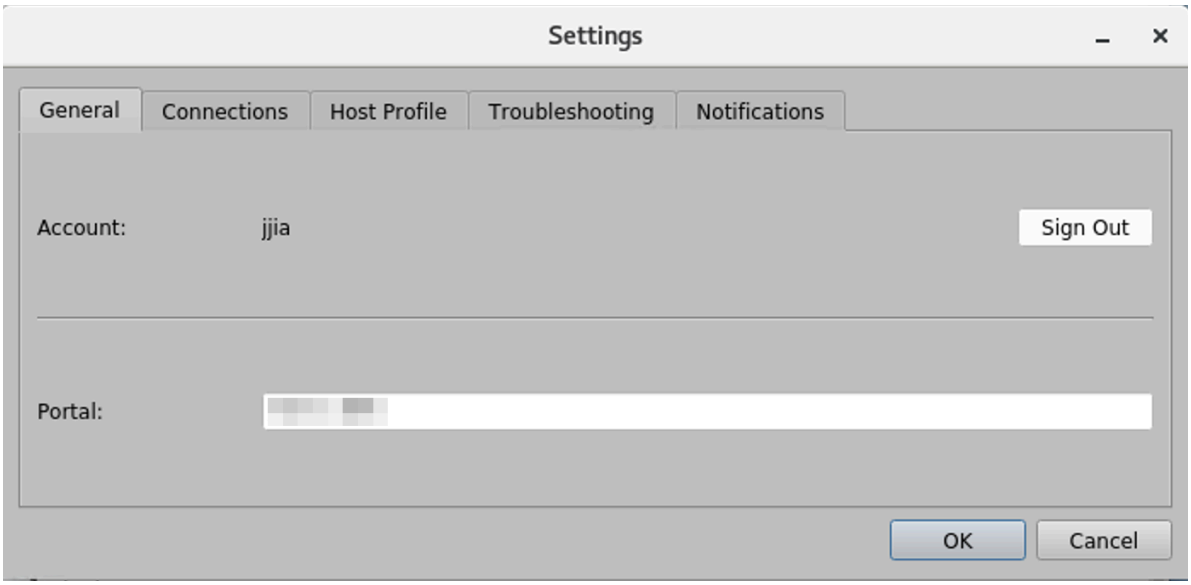
STEP 2 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

STEP 3 | View information about your network connection.

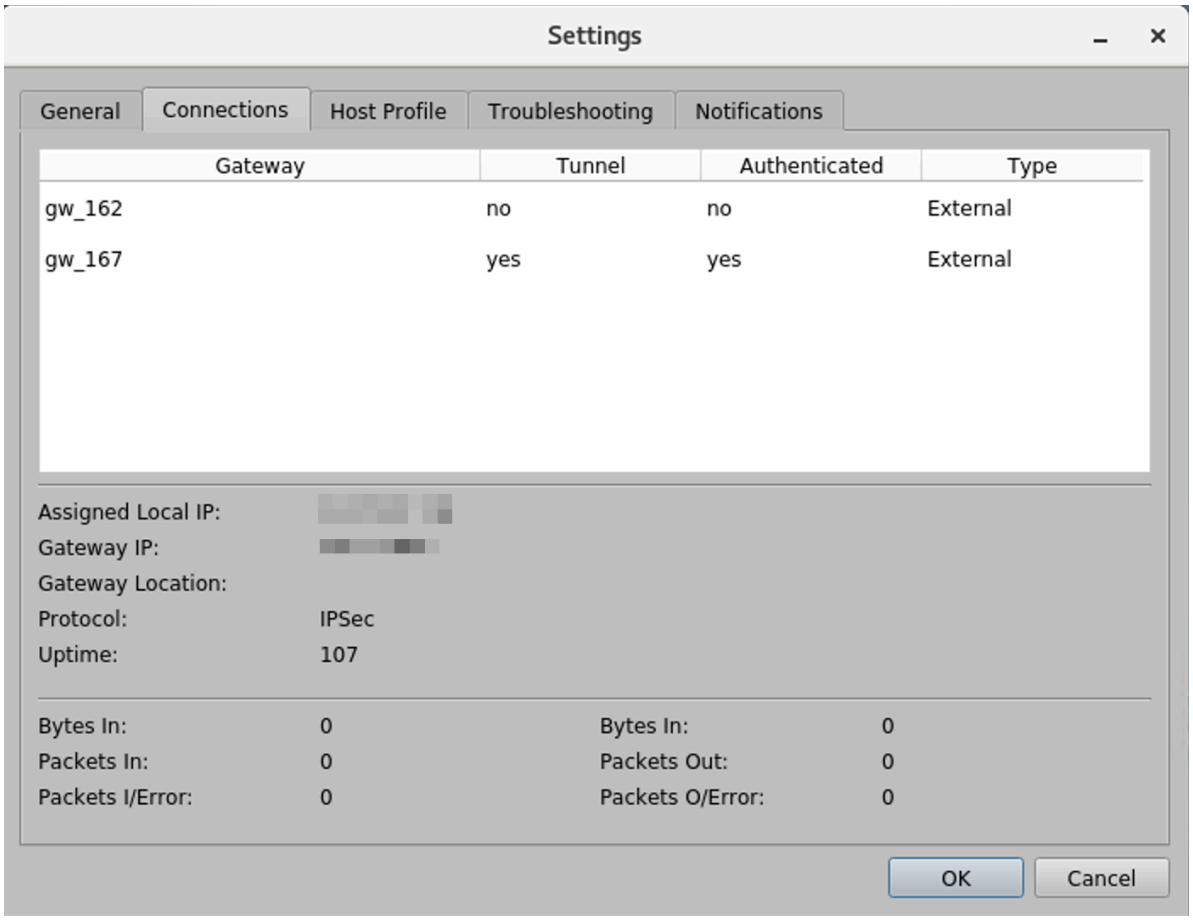
After you launch the app, select the menu (☰) on the top right of the app's panel, select **Settings** to open the **GlobalProtect Settings** panel, and then select one of the following tabs to view information about your network connection:

- **General**—Displays the username and portal(s) associated with the GlobalProtect account. You can also add, delete, or modify portals from this tab.



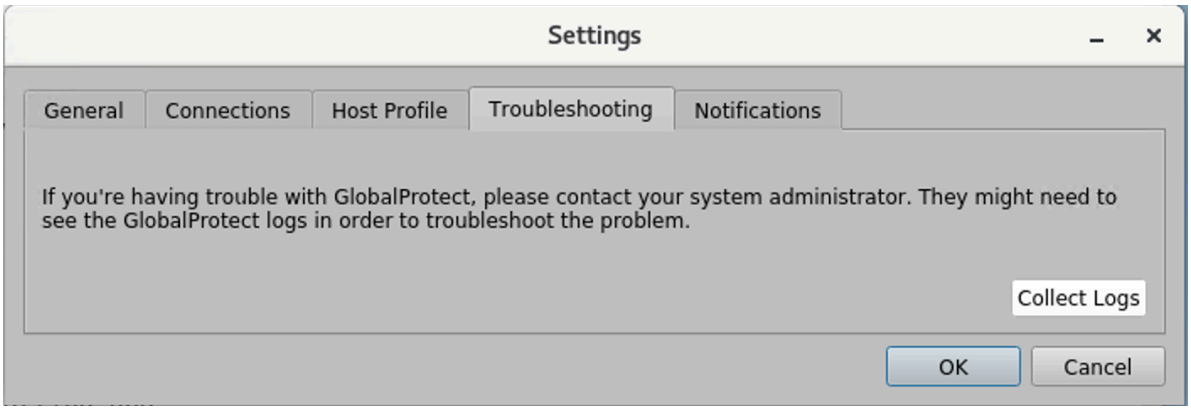
- **Connection**—Lists the gateways configured for the GlobalProtect app and provides the following information about each gateway:
  - Gateway name
  - Tunnel status
  - Authentication status
  - Connection type
  - Gateway IP address or FQDN (only available in external mode)

  *For internal mode, the **Connection** tab displays the entire list of available gateways. For external mode, the **Connection** tab displays only the gateway to which you are connected and additional details about the gateway (such as the gateway IP address, location, and uptime).*



- **Troubleshooting**—Enables you to **Collect Logs** and set the **Logging Level**.

In order for the GlobalProtect app to send troubleshooting logs, diagnostic logs, or both to Strata Logging Service for further analysis, you must configure the GlobalProtect portal to enable the GlobalProtect app log collection for troubleshooting. Additionally, you can configure the HTTPS-based destination URLs that can contain IP addresses or fully qualified domain names of the web servers/resources that you want to probe, and to determine issues such as latency or network performance on the end user's endpoint.



STEP 4 | (Optional) Log in using a new password.

*If your GlobalProtect administrator configures the GlobalProtect portal agent to **Save User Credentials**, your credentials are automatically saved to the GlobalProtect app. If your password for accessing the corporate network changes, you must log in to GlobalProtect using your new password.*

1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Select the menu (≡) on the top right of the app's panel, then select **Settings** to open the **GlobalProtect Settings** panel.
3. On the **General** tab of the **GlobalProtect Settings** panel, **Sign Out** to clear your saved user credentials from the GlobalProtect app.
4. After you clear your user credentials, you can reconnect to GlobalProtect with your new username and password.

STEP 5 | (Optional) Disconnect from GlobalProtect.

If your administrator configures GlobalProtect with the **On-Demand** connect method, you can disconnect from GlobalProtect by clicking **Disconnect** on the status panel.

Use the CLI Version of the GlobalProtect App for Linux

Using the command-line interface (CLI) of the GlobalProtect™ app for Linux, you can perform tasks that are common to the GlobalProtect app. The following examples display the output in command-line mode. To run the same command in prompt-mode, enter it without the **globalprotect** prefix (for more information, see Download and Install the GlobalProtect App for Linux).

- Connect to a GlobalProtect portal:

  Use the **globalprotect connect --portal *<gp-portal>*** command where ***<gp-portal>*** is the IP address or FQDN of your GlobalProtect portal.

  For example:

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com
Retrieving configuration...

Disconnected
myportal.example.com - portal:local:Enter login credentials
username:user1
Password:
Retrieving configuration...

Discovering network...
Connecting...
Connected
```

  Starting from GlobalProtect Linux version 6.2.1, you have the option to use the command-line interface (CLI) to connect to the GlobalProtect app when it is configured with SAML authentication and the default browser. Previously, the only way to connect to the GlobalProtect app configured with SAML authentication and the default browser was through the GUI version.

  To connect to the GlobalProtect app configured with SAML authentication using either the CLI or GUI version, it is mandatory to have the Firefox browser installed on the Linux endpoint. Use the latest Firefox ESR release version to ensure a seamless connection with SAML authentication on the default browser using either the CLI or GUI version

  Starting from GlobalProtect Linux version 6.2.1, you must use the following commands to install the CLI or GUI versions of the app:

  - To install the GlobalProtect UI package- **$ ./gp_install.sh**
  - To install the GlobalProtect CLI package- **$ ./gp_install.sh --cli-only**

  You don't need to run the **./gp_install.sh** with **sudo** for GlobalProtect app Linux 6.2.1 and later versions. As the script executes, users will be prompted to enter the **sudo** password.

  When you use certificate-based authentication, the first time you connect without a root CA certificate, the GlobalProtect app and GlobalProtect portal exchange certificates. The GlobalProtect app displays a certificate error, which you must acknowledge before you

authenticate. When you next connect, you will not be prompted with the certificate error message.

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com
Retrieving
 configuration...
Disconnected
There is a problem with the security certificate, so the identity
 of 10.3.188.61 cannot be verified. Please contact the Help Desk
 for your organization to have the issue rectified.
Warning: The communication with 10.3.188.61 may have been
 compromised. We recommend that you do not continue with this
 connection.
Error details:Do you want to continue(y/n)?y
Retrieving
 configuration...
Disconnected
10.3.188.61 - portal:local:Enter login credentials
username:user1
Password:
Retrieving
 configuration...
Discovering network...
Connecting...
Connected
```

*You can also specify a username in the command using the **--username <username>** option. The GlobalProtect app prompts you to authenticate and, if you specified the username option, confirm your username.*

- Import a certificate.

  When you want to pre-deploy a client certificate to an endpoint for certificate-based authentication, you can copy the certificate to the endpoint and import it for use by the GlobalProtect app. Use the **globalprotect import-certificate --location <location>** command to import the certificate on the endpoint. When prompted you must supply the certificate password.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12
Please input passcode:
Import certificate is successful.
```


- Connect to a gateway:
  1. (Optional) Display the manual gateways to which you can connect using the **globalprotect show --manual-gateway** command.
  2. Connect to a gateway using the **globalprotect connect --gateway *<gp-gateway>*** command where ***<gp-gateway>*** is the IP address or FQDN of the GlobalProtect gateway.
  3. View details about your connection using the **globalprotect show --details** command.

```
user@linuxhost:~$ globalprotect show --manual-gateway
Name                Address

-----------------------------
gw1                 192.168.1.180
gw2                 192.168.1.181
user@linuxhost:~$ globalprotect connect --gateway 192.168.1.180
Retrieving configuration...

Discovering network...
Connecting...
Connected
```

- Verify the status of and view details about your GlobalProtect connection:

  Use the **globalprotect show --status** command to verify the status of your connection.

  Use the **globalprotect show --details** command to view the details of your connection.

```
user@linuxhost:~$ globalprotect show --status
GlobalProtect status: Connected
user@linuxhost:~$ globalprotect show --details
Assigned IP address: 192.168.1.132

Gateway IP address: 192.168.1.180
Protocol: IPSec
Uptime(sec): 231
```

- Rediscover the network:

  Use the **globalprotect rediscover-network** command to disconnect and reconnect from GlobalProtect.

```
user@linuxhost:~$ globalprotect rediscover-network
Disconnecting...

Retrieving configuration...
Retrieving configuration...
```



```
Discovering network...
Connecting...
Connecting...
Connected

GlobalProtect status: Connected
```

- Clear the credentials for the current user:

  Use the **globalprotect remove-user** command to clear the credentials used to authenticate with the portal and gateways. After you confirm that the GlobalProtect app should clear your credentials, the GlobalProtect app disconnects the tunnel and then requires you to enter your credentials the next time you connect.

```
user@linuxhost:~$ globalprotect remove-user
Credential will be cleared and current tunnel will be terminated.
Do you want to continue(y/n)?y
Clear is done successfully.

user@linuxhost:~$ globalprotect connect --portal 192.168.1.179
Retrieving configuration...

Disconnected
192.168.1.179 - portal:local:Enter login credentials
username:user1
Password:
Retrieving configuration...

Discovering network...
Connecting...
Connected
```

- Resubmit host information to the gateway.

  Use the **globalprotect show --host-state** command to view the current host information about your endpoint. Use the **globalprotect resubmit-hip** command to resubmit information about the endpoint to the gateway. This is useful in cases where HIP-based security policy prevents users from accessing resources because it allows the user to fix the compliance issue on the endpoint and then resubmit the HIP.

```
user@linuxhost:~$ globalprotect show --host-state
generate-time: 09/28/2017 11:24:07

categories
    host-info
        client-version: 4.1.0
        os: Linux Ubuntu 16.04.3 LTS
        os-vendor: Linux
        domain:
        host-name: linuxhost
        host-id: 4C4C4544-0034-4D10-804C-************

        network-interface
```



```
            enp0s31f6
                description: enp0s31f6
                mac-address: D4:81:D7:D4:5A:A5
            wlp2s0
                description: wlp2s0
                mac-address: 14:AB:C5:DE:D1:0E
user@linuxhost:~$ globalprotect resubmit-hip
Resubmit is successful.
```

- View any GlobalProtect notifications.

  Use the **globalprotect show --notification** command to view notifications.

- View the GlobalProtect system tray icon.

  Use the **globalprotect launch-ui** command to display the system tray icon on your desktop. You can launch the GlobalProtect app by clicking the system tray icon.

- View the Welcome page.

  Use the **globalprotect show --welcome-page** command. The GlobalProtect app displays the Welcome page in a browser if a Welcome page exists or displays a notification if the Welcome page does not exist.

- View errors.

  Use the **globalprotect show --error** command to view errors reported by the app.

```
user@linuxhost:~$ globalprotect show --error
Error: Cannot connect to GlobalProtect Portal
```

- Collect logs.

  The app stores the PanGPA and PanGPI log files in the `/home/<user>/.Globalprotect` directory. Use the **globalprotect collect-logs** command to enable the GlobalProtect app for Linux to package these logs and other useful information. You can then use the logs to troubleshoot issues or forward them to a Support engineer for expert analysis.

```
user@linuxhost:~$ globalprotect collect-log
Start collecting...
collecting network info...
collecting machine info...
copying files...
generating final result file...
The support file is saved to /home/user/.GlobalProtect/Collect.tgz
```

- Display the version of the GlobalProtect app for Linux.

```
user@linuxhost:~$ globalprotect show --version
GlobalProtect: 6.0.0-23
```



```
Copyright(c) 2009-2021 Palo Alto Networks, Inc.
```


Report an Issue From the GlobalProtect App for Linux

When you experience unusual behavior such as poor network performance or a connection is not established with the portal and gateway, you can report an issue directly to Strata Logging Service to which your administrator can access. You no longer need to manually collect and send the GlobalProtect app logs through email or to store them on a cloud drive.

You can only report an issue to your administrator using the GUI version of the GlobalProtect app for Linux.

*To display the **Report an Issue** option on the GlobalProtect app, your administrator must enable the GlobalProtect app log collection for troubleshooting on the GlobalProtect portal.*

STEP 1 | Connect to the GlobalProtect portal or gateway.

1. In the GlobalProtect window, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.

   After you download and install the GUI version of GlobalProtect app for Linux, the GlobalProtect app automatically launches.
2. (Optional) If multiple portals are saved on your app, select a portal from the **Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Portal** drop-down.
3. Enter the **Username** and **Password** for the portal and then **Sign In**.

   In most instances, you can use the same username and password that you use to connect to your corporate network. After you sign in, the GlobalProtect portal shows a status of **Connected**.
4. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, click the gateway drop-down.

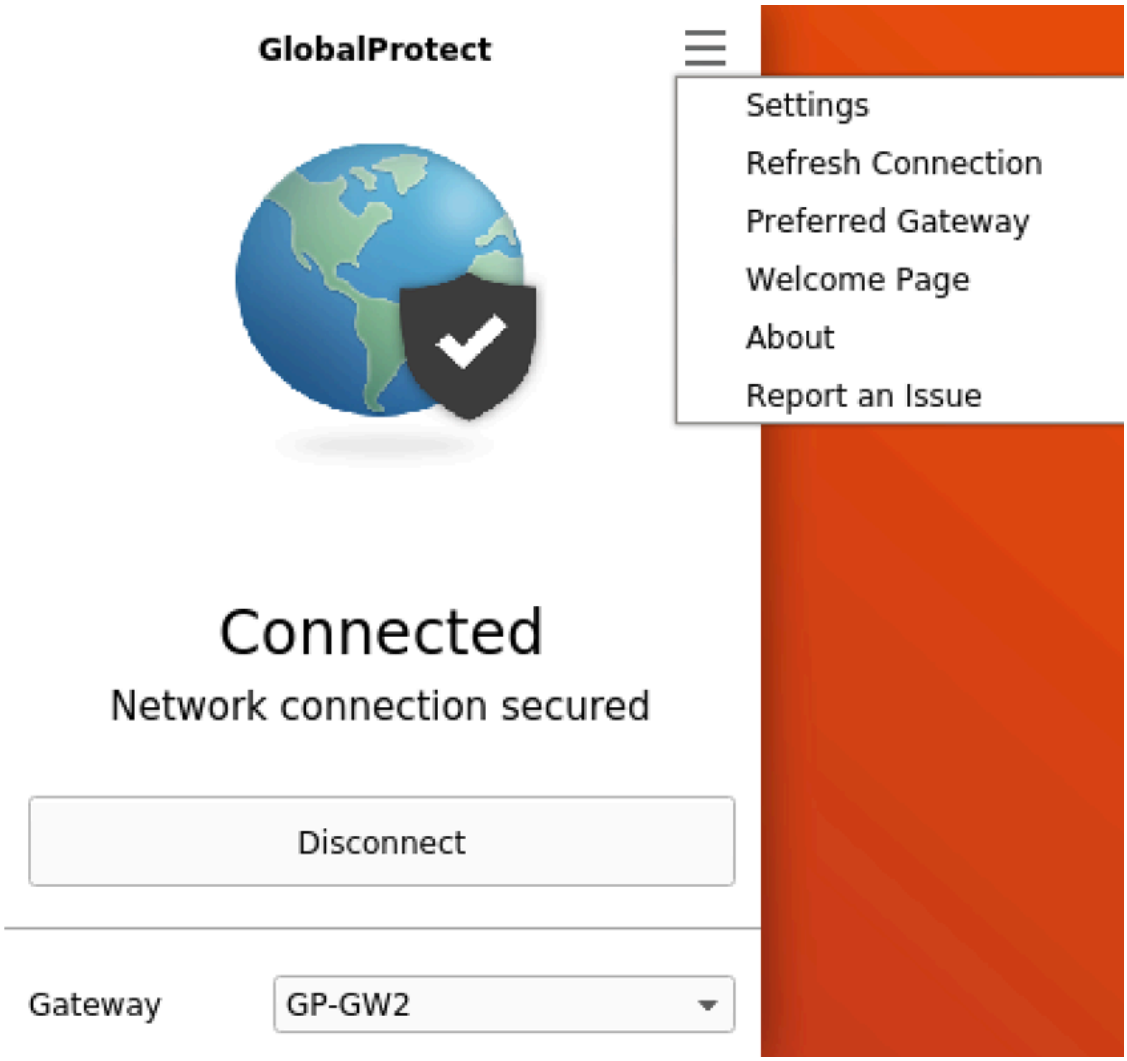
STEP 2 | Open the GlobalProtect app.

Click the GlobalProtect system tray icon to launch the app interface.

STEP 3 | Report an issue from the GlobalProtect app from your endpoint.

After you launch the app, select the menu (≡) on the top right of the app's panel to report an issue to your administrator.

1. Select **Report an Issue**.



2. Enable the GlobalProtect app to run diagnostic tests and to include diagnostic logs. Both diagnostic and troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report.

   After the diagnostic tests are successfully completed, the GlobalProtect debug log files are uploaded to Strata Logging Service from your endpoint.

   *If you do not enable the app to run diagnostic tests and to include diagnostic logs, only troubleshooting logs are collected and sent to Strata Logging Service as a compact troubleshooting report. The GlobalProtect app checks for the report files (pan_gp.trb.log or pan_gp_trbl.log) that are automatically generated in `.json` format. A notification message appears if no issues were found in the troubleshooting logs. Click **Retry** to check if the pan_gp.trb*.log files exist.*

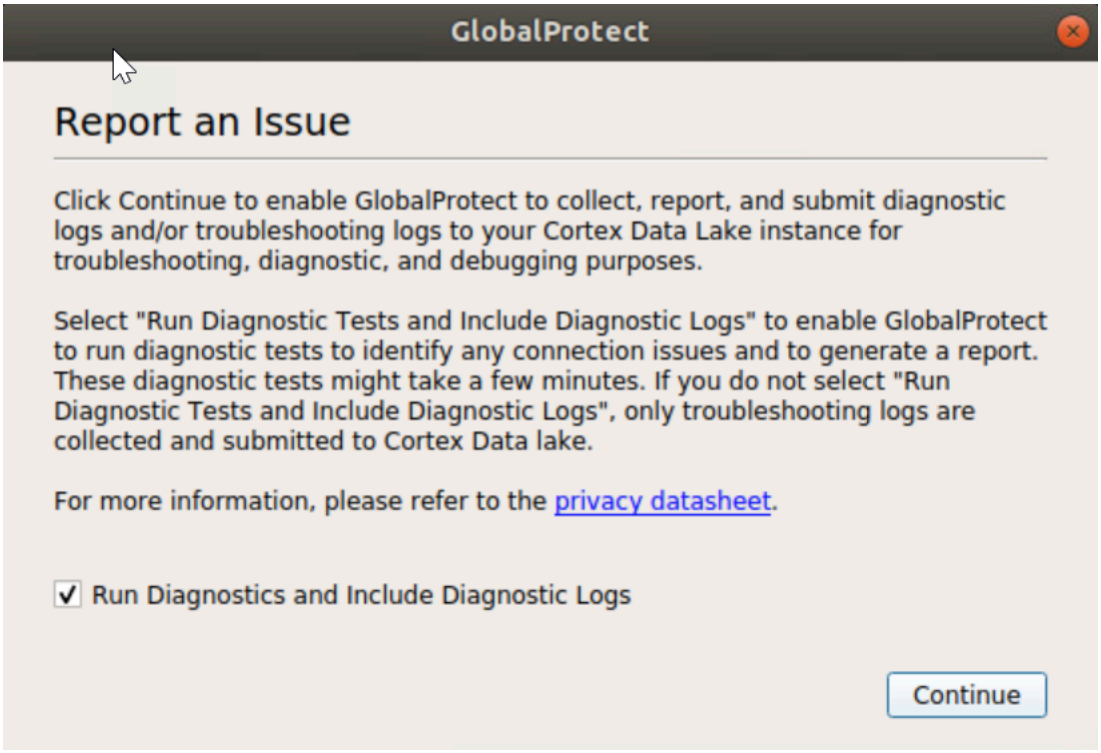
3. Select the **Run Diagnostic Tests and Include Diagnostic Logs** check box.

4. Click **Continue** to allow the app to create a troubleshooting log and to send the report to your administrator's Strata Logging Service instance.

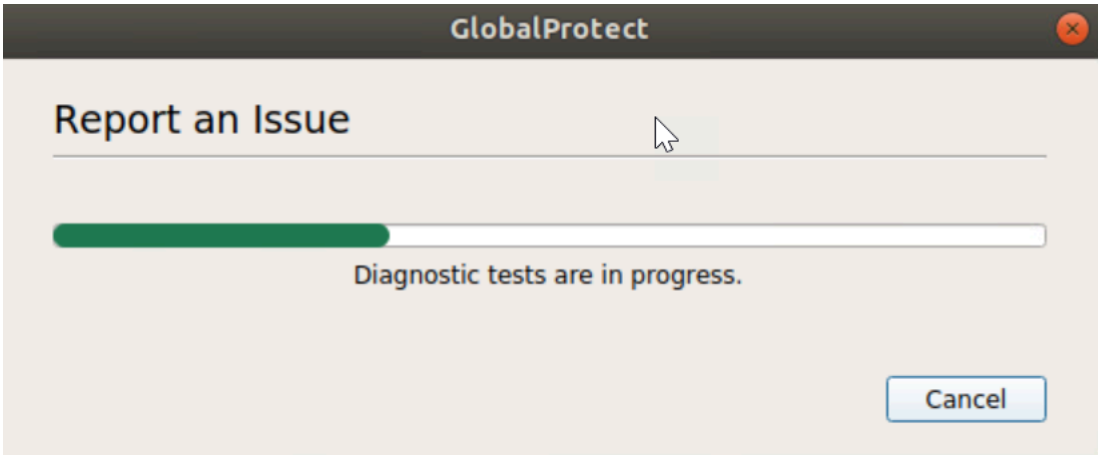
   The results of the end-to-end diagnostic tests are stored in the pan_gp_diag.log file in `.json` format and sent to your administrator's Strata Logging Service instance along with the pan_gp.trb*.log files.

   The results of the end-to-end diagnostic tests are stored in the pan_gp_diag.log file in `.json` format and sent to your administrator's Strata Logging Service instance along with the pan_gp.trb*.log files. The GlobalProtect app can run diagnostic tests with a tunnel or without a tunnel. For example, you might want to enter your GlobalProtect

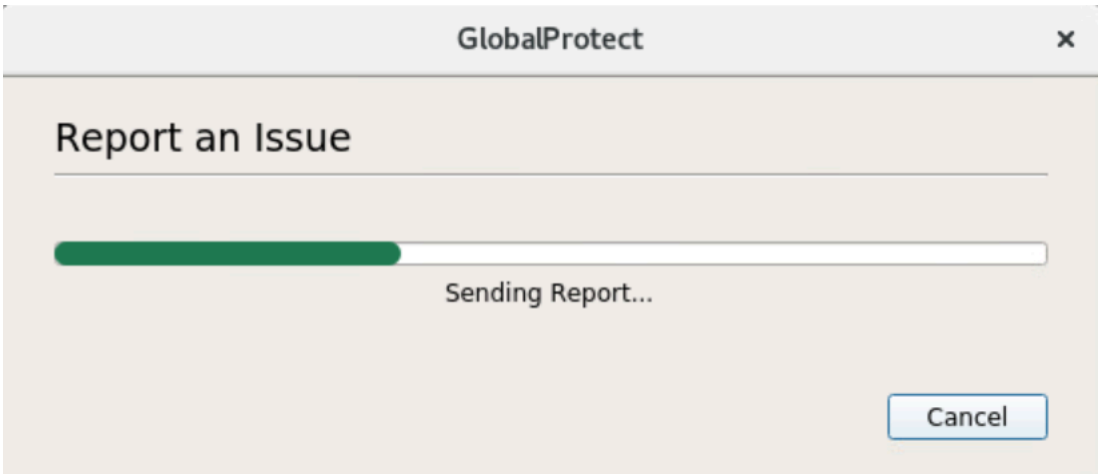
login credentials prior to the app connecting and running diagnostic tests through the tunnel.



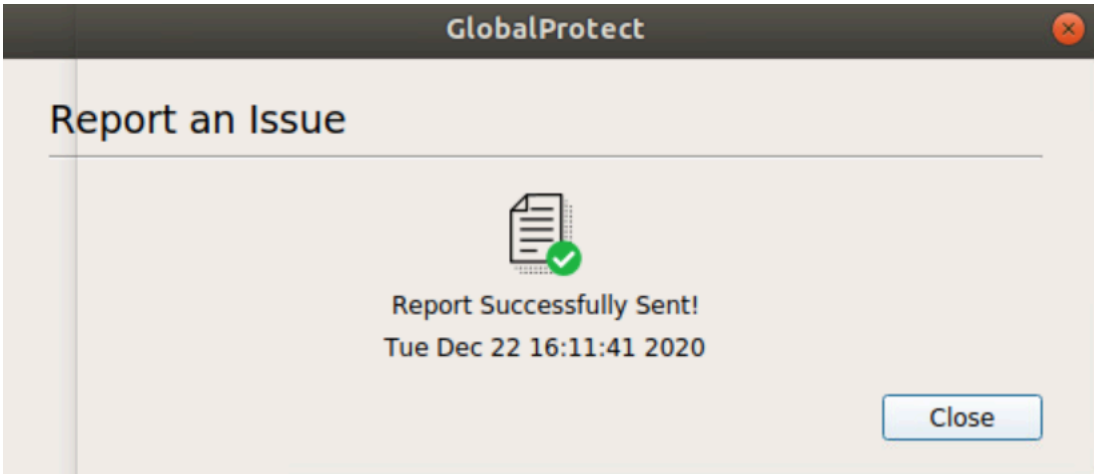
A message pops-up, confirming that the app is running diagnostic tests only if you selected the **Run Diagnostic Tests and Include Diagnostic Logs** check box.



A message pops-up, confirming that the app is sending the report to Strata Logging Service.



5. Click **Close** to confirm that the app successfully sent the report to Strata Logging Service. This confirmation message displays the date and time when the report was processed and sent.



Disconnect the GlobalProtect App for Linux

If your administrator configures the GlobalProtect connect method as **Always On**, you can disconnect the GlobalProtect app. For example, you might want to disconnect the app if the GlobalProtect virtual private network (VPN) is not working in a hotel, and the VPN failure prevents you from connecting to the internet. After disconnecting the GlobalProtect app, you can connect to the internet using unsecured communication (without a VPN).

The method, amount of time, and number of times for which you can disconnect the GlobalProtect app depends on how the administrator configures your GlobalProtect service. This configuration can prevent you from disconnecting the app entirely or allow you to disconnect the app only after responding to a challenge correctly.

If your configuration includes a challenge, the GlobalProtect app prompts for one of the following:

- Reason you want to disconnect the app
- Passcode

If the challenge involves a passcode, we recommend that you contact a GlobalProtect administrator or Help Desk person by phone. Administrators typically provide passcodes in advance, either through email (for new GlobalProtect users) or posted on your organization's website. In response to an outage or system issue, administrators may also provide passcodes by phone.

GlobalProtect supports two versions of the GlobalProtect app for Linux: One version if your Linux device supports a GUI, and CLI version if your Linux device does not support a GUI.

- Disconnect the GlobalProtect App for Linux Using the GUI Version
- Disconnect the GlobalProtect App for Linux Using the CLI Version

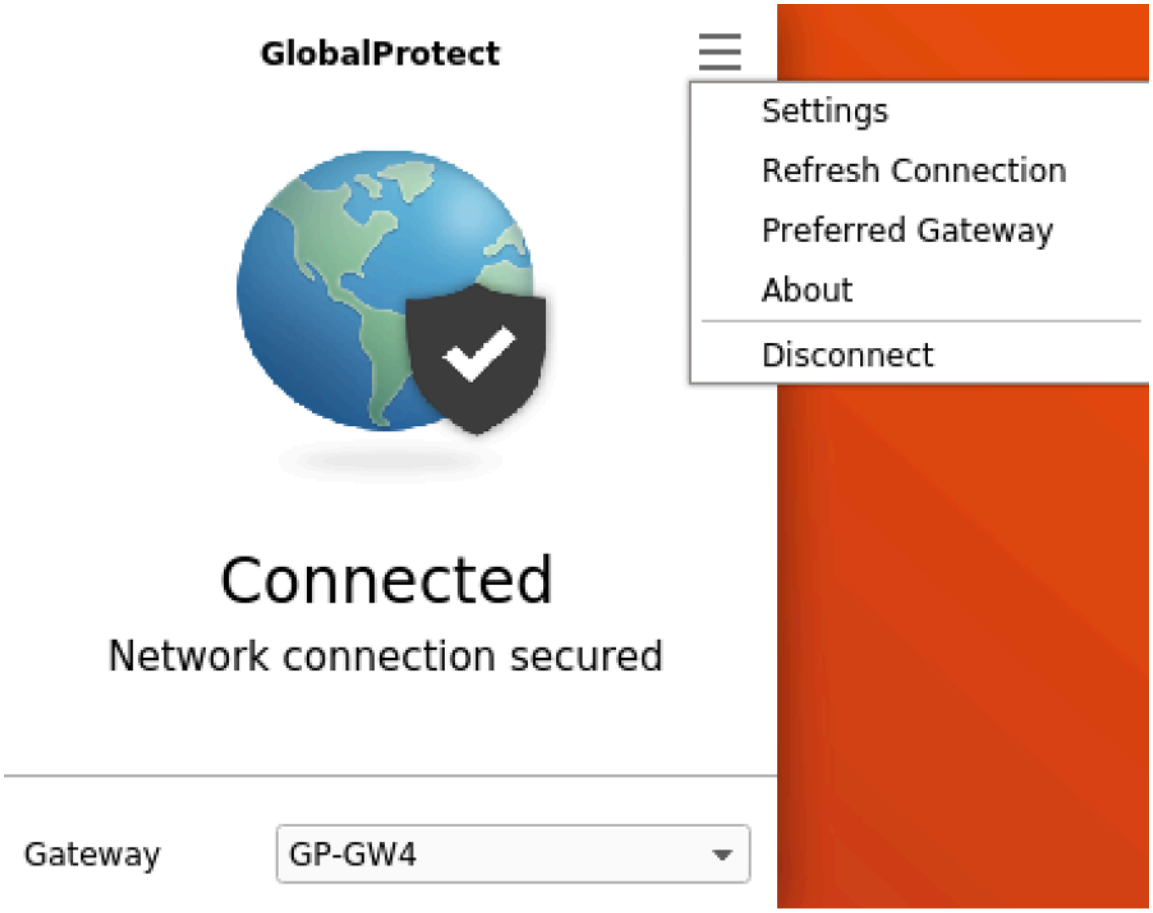
Disconnect the GlobalProtect App for Linux Using the GUI Version

(Available in always-on mode only) To disconnect the GlobalProtect app for Linux using the GUI version, complete these steps.

STEP 1 | Disconnect the GlobalProtect app.

1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Select the menu (≡) on the top right of the app's panel to open the settings menu.
3. Select **Disconnect**.

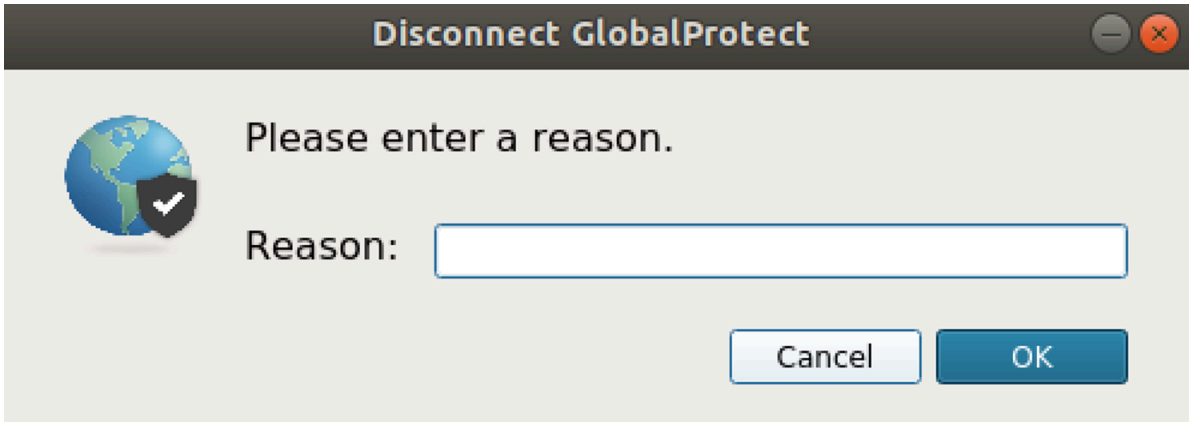
*The **Disconnect** option is visible only if your GlobalProtect agent configuration allows you to disconnect the app. If the configuration allows you to disconnect the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*



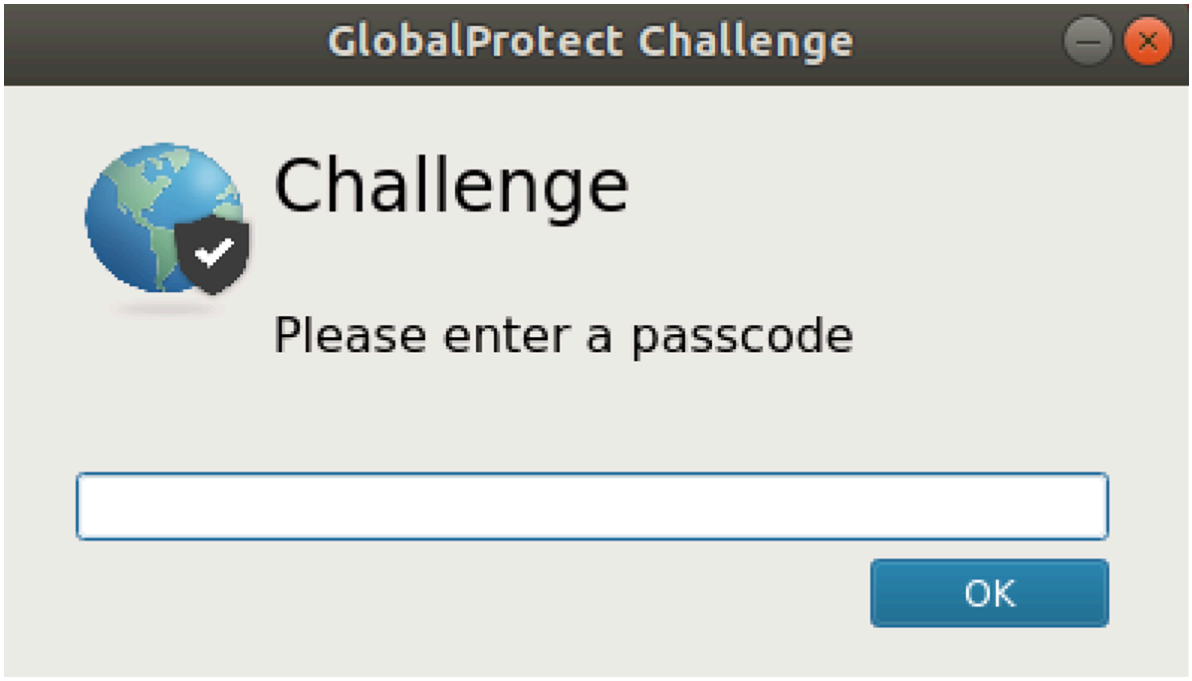
STEP 2 | Respond to one or more challenges, if required.

If prompted, provide the following information:

- **Reason**—Your reason for disconnecting the GlobalProtect app.



- **Passcode**—A passcode that is typically provided by your administrator in advance, based on a known issue or event that requires you to disconnect the app.



Disconnect the GlobalProtect App for Linux Using the CLI Version

To disconnect the GlobalProtect app for Linux using the CLI version, complete these steps.

- (Available in on-demand mode only) Disconnect from GlobalProtect:

  Use the **`globalprotect disconnect`** command to disconnect from GlobalProtect.

```
user@linuxhost:~$ globalprotect disconnect
GlobalProtect status: Disconnected
```


- (Available in always-on mode only) Disconnect GlobalProtect:

  Use the **globalprotect disconnect** command to disconnect and disable the GlobalProtect app. If your configuration requires it, you must also specify a reason or a passcode when prompted.

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

  ```
  user@linuxhost:~$ globalprotect disconnect Please enter reason for
   disconnecting: This is my reason for disconnecting
  ```

  ```
  user@linuxhost:~$ globalprotect disconnect Please enter passcode
   for disconnecting: ITp@ssw0rd
  ```


Uninstall the GlobalProtect App for Linux

You can uninstall the GlobalProtect app for Linux using the following command:

```
$ ./gp_uninstall.sh --help
Usage: $ sudo ./gp_uninstall [--cli-only | --arm | --help]
  --cli-only: CLI Only
  --arm:      ARM
  no options: UI
```

The following packages are not removed during the uninstall:

- Qt Packages
- resolvconf (Ubuntu only)
- Gnome Shell Extension Packages
  - Ubuntu 20
    - gnome-tweak-tool
    - gnome-shell-extension-top-icons-plus
  - Ubuntu 22
    - gnome-shell-extension-manager
    - gnome-shell-extension-appindicator
  - RHEL 8
    - gnome-tweaks
    - gnome-shell-extension-topicons-plus
  - RHEL 9
    - gnome-shell-extension-top-icons

You can delete the Ubuntu packages using the `$ sudo apt autoremove` command and RHEL packages with the `$ sudo yum autoremove` command. When you use either of these commands, the Qt Packages are deleted as well.

