paloalto TECHDOCS

GlobalProtect App User Guide

5.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2019-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

August 19, 2022

Table of Contents

GlobalProtect App for Windows 5
- Download and Install the GlobalProtect App for Windows 6
- Use the GlobalProtect App for Windows 12
- Disable the GlobalProtect App for Windows 18
- Uninstall the GlobalProtect App for Windows 20
- Fix a Microsoft Installer Conflict 21

GlobalProtect App for macOS 23
- Download and Install the GlobalProtect App for macOS 24
- Use the GlobalProtect App for macOS 32
- Disable the GlobalProtect App for macOS 39
- Uninstall the GlobalProtect App for macOS 41
- Remove the GlobalProtect Enforcer Kernel Extension 47
- Enable the GlobalProtect App for macOS to Use Client Certificates for Authentication 48

GlobalProtect App for iOS 49
- Download and Install the GlobalProtect App for iOS 50
- Use the GlobalProtect App for iOS 51
- Uninstall the GlobalProtect App for iOS 63

GlobalProtect App for Android 65
- Download and Install the GlobalProtect App for Android 66
- Download and Install the GlobalProtect App for Android on Chromebooks 67
- Use the GlobalProtect App for Android 68
- Disable the GlobalProtect App for Android 76
- Uninstall the GlobalProtect App for Android 78
- Uninstall the GlobalProtect App for Android from Chromebooks 79

GlobalProtect App for Linux 81
- Download and Install the GlobalProtect App for Linux 82
  - Download and Install the GUI Version of GlobalProtect for Linux 82
  - Download and Install the CLI Version of GlobalProtect for Linux 84
- Use the GlobalProtect App for Linux 88
  - Use the GUI Version of the GlobalProtect App for Linux 88
  - Use the CLI Version of the GlobalProtect App for Linux 95
- Disable the GlobalProtect App for Linux 101
- Uninstall the GlobalProtect App for Linux 102

GlobalProtect for IoT Devices 103

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

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 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 Windows:

- Download and Install the GlobalProtect App for Windows
- Use the GlobalProtect App for Windows
- Disable the GlobalProtect App for Windows
- Uninstall the GlobalProtect App for Windows
- Fix a Microsoft Installer Conflict

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.

To download and install the app, you must obtain the IP address or fully qualified domain name (FQDN) of the GlobalProtect portal from the 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 above, 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.

 ©2023 Palo Alto Networks, Inc.

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.

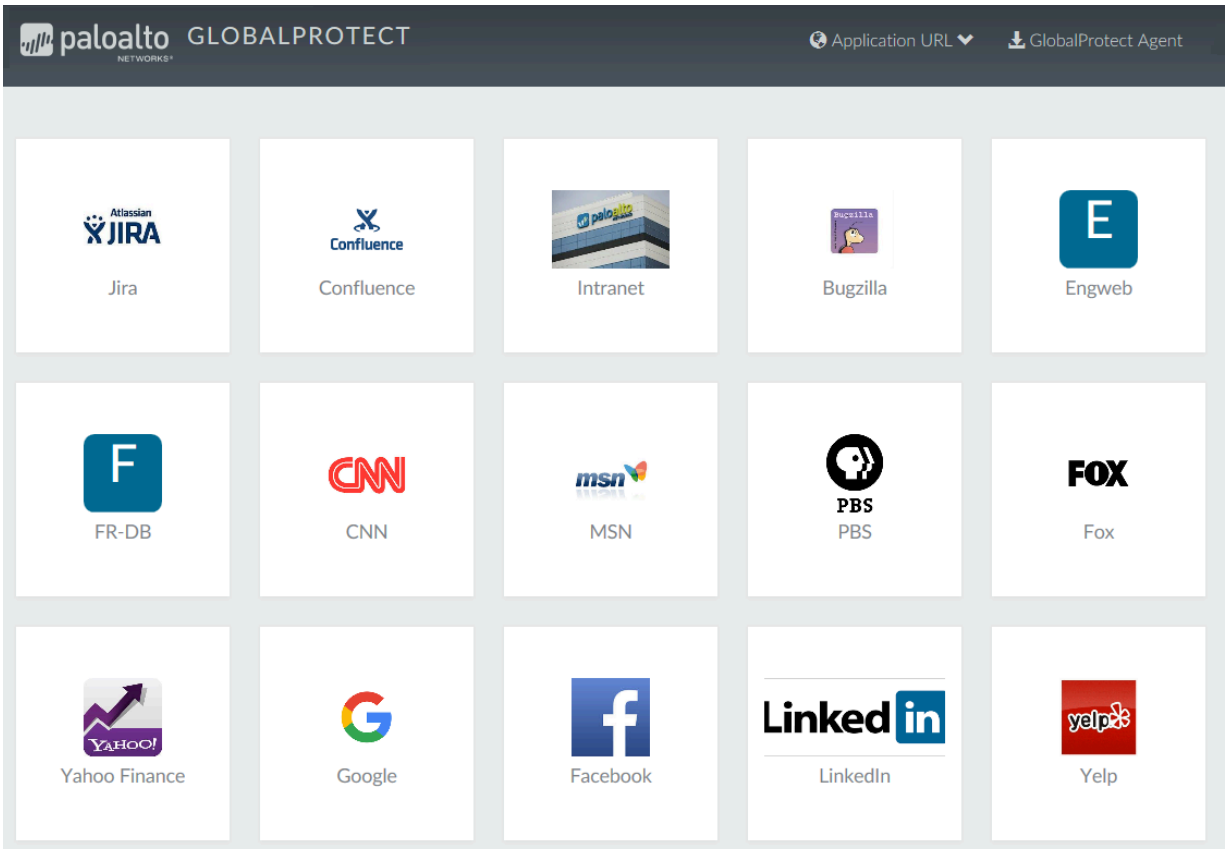
 ©2023 Palo Alto Networks, Inc.

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.

 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

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.

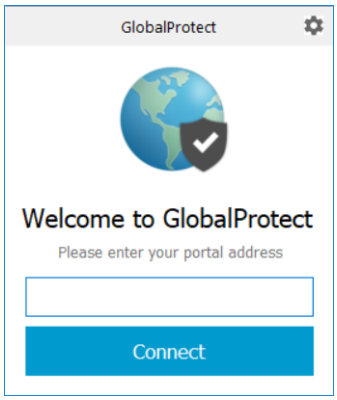
1. In the GlobalProtect Setup Wizard, click **Next**.
2. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks \GlobalProtect) and then click **Next** twice.

   *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.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Log in to GlobalProtect.



1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. Enter the FQDN or IP address of the portal that your GlobalProtect administrator provided, and then click **Connect**.
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, select the gateway from the **Gateway** drop-down (for external gateways only).

   This option is only available if your administrator enables manual gateway selection.
4. (Optional) Depending on the connection mode, click **Connect** to initiate the connection.
5. (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.

 ©2023 Palo Alto Networks, Inc.

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 | 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 **Disconnected** 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 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

 ©2023 Palo Alto Networks, Inc.

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 status panel, click the Settings (⚙) icon to open the settings menu.
  2. Select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.
  3. From the list of available gateways, select the gateway that you want to set as the preferred gateway and then **Set as Preferred**.
  4. **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 status panel, click the Settings (⚙) icon to open the settings menu.
  2. Select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.
  3. From the list of available gateways, select the preferred gateway and then **Remove Preferred**.
  4. **Close** the dialog.

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.

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 2 | Open the GlobalProtect app.

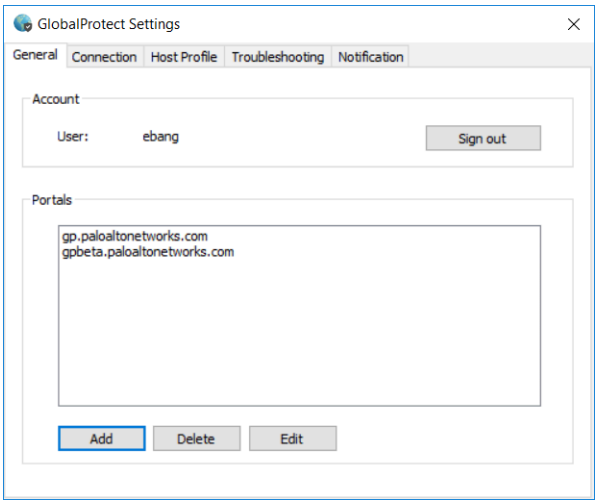
Click the GlobalProtect system tray icon to launch the app interface.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | View information about your network connection.

After you launch the app, click the settings icon (⚙) on the status panel to open the settings menu. 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 and uptime).*

 ©2023 Palo Alto Networks, Inc.

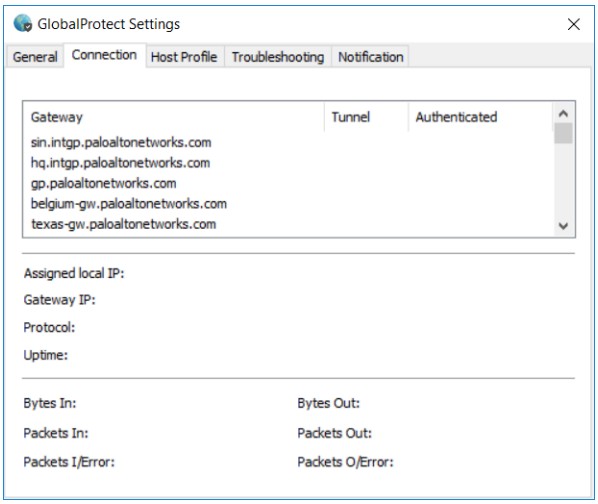


Figure 1: Connection Tab When In Internal Mode

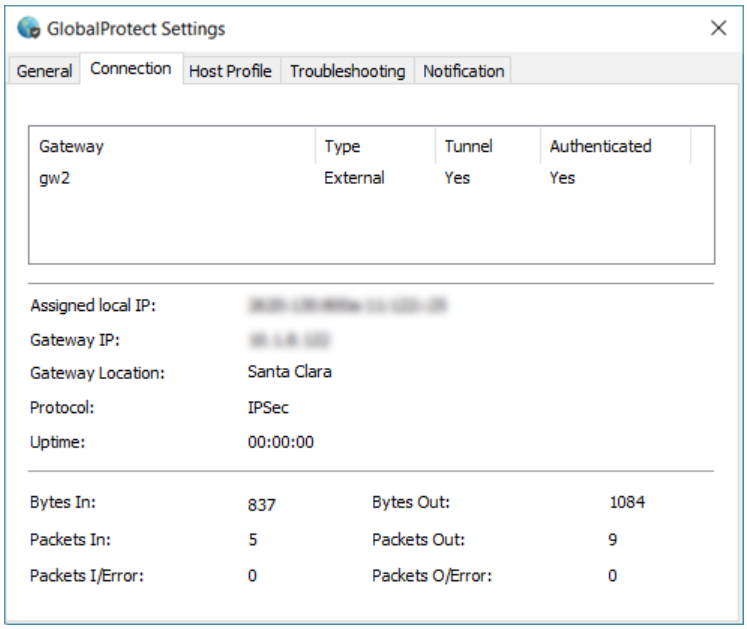


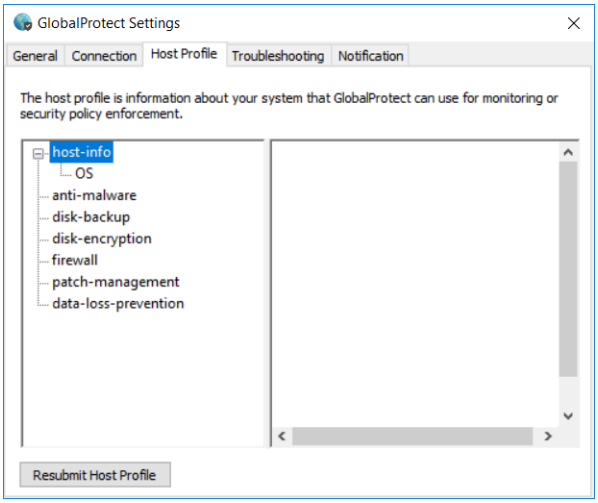
Figure 2: Connection Tab When In External Mode

- **Host Profile**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile (HIP). Click **Resubmit Host Profile** to manually resubmit HIP data to the gateway.

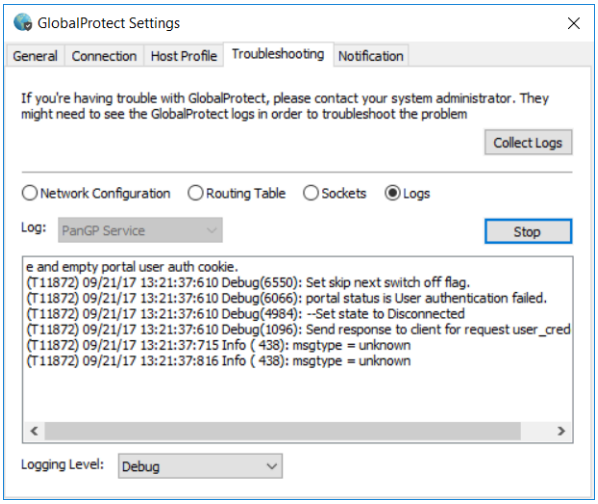
 ©2023 Palo Alto Networks, Inc.

*If your administrator configures the **Severity** value for missing patches as a HIP match condition, use the following mappings between the GlobalProtect severity values and the OPSWAT severity ratings to understand what each value means:*

Severity Value Displayed on the GlobalProtect App	*OPSWAT Severity Rating*
0	*Low*
1	*Moderate*
2	*Important*
3	*Critical*



- **Troubleshooting**—Enables you to **Collect Logs**, set the **Logging Level**, and view information about the network configuration, route settings, active connections, and logs.



 ©2023 Palo Alto Networks, Inc.

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. Click the settings icon (⚙) to open the settings menu.
3. Select **Settings** to open the **GlobalProtect Settings** panel.
4. On the **General** tab of 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 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.

 ©2023 Palo Alto Networks, Inc.

Disable the GlobalProtect App for Windows

If your administrator configures the GlobalProtect connect method as **Always On**, you can disable the GlobalProtect app. For example, you might want to disable 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 disabling 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 disable the GlobalProtect app depends on how the administrator configures your GlobalProtect service (PanGPS). This configuration can prevent you from disabling the app entirely or allow you to disable 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 disable the app
- 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 disable request is approved, you will receive a valid ticket number that you can use to disable GlobalProtect.

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

STEP 1 | Disable the GlobalProtect app.

1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the settings icon (

) to open the settings menu.
3. Select **Disable**.

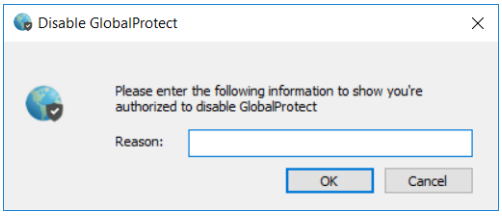
*The **Disable** option is visible only if your GlobalProtect agent configuration allows you to disable the app. If the configuration allows you disable the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*

 ©2023 Palo Alto Networks, Inc.

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

If prompted, provide the following information:

- **Reason**—Your reason for disabling 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 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 **Disable**. To disable 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**.

 ©2023 Palo Alto Networks, Inc.

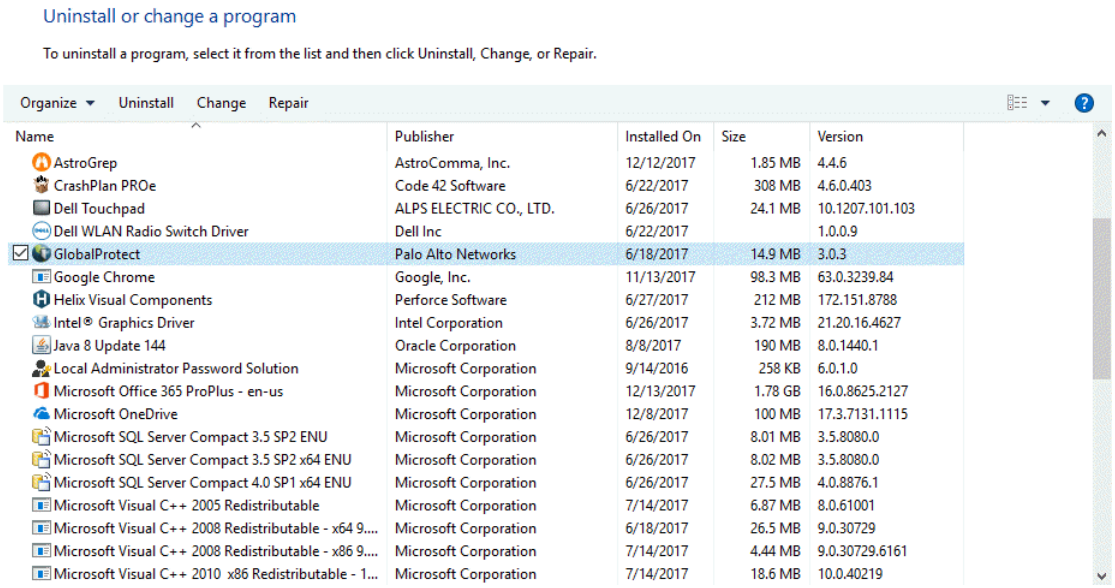
Uninstall the GlobalProtect App for Windows

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**.

 ©2023 Palo Alto Networks, Inc.

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.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

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
- Use the GlobalProtect App for macOS
- Disable the GlobalProtect App for macOS
- Uninstall the GlobalProtect App for macOS
- Remove the GlobalProtect Enforcer Kernel Extension
- Enable the GlobalProtect App for macOS to Use Client Certificates for Authentication

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.

To 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 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:

 ©2023 Palo Alto Networks, Inc.

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.

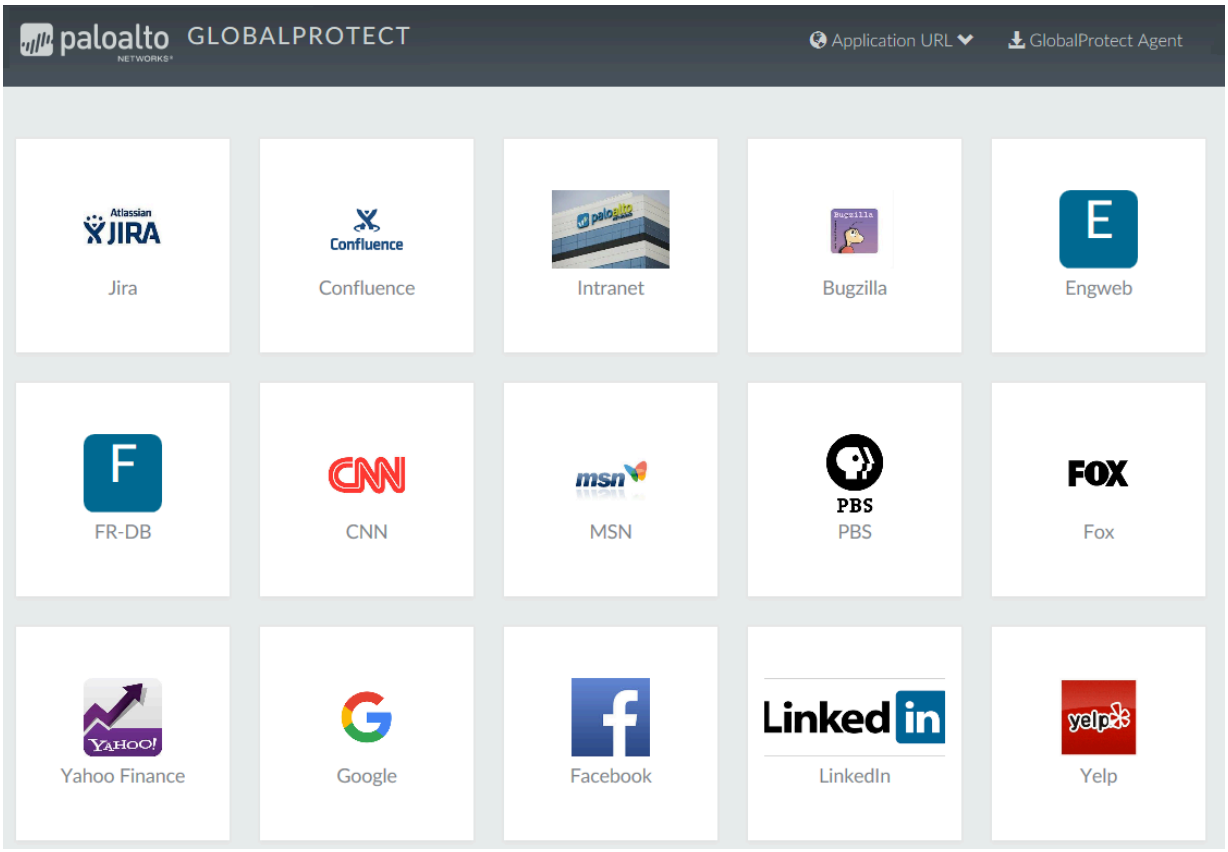
 ©2023 Palo Alto Networks, Inc.

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.

 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

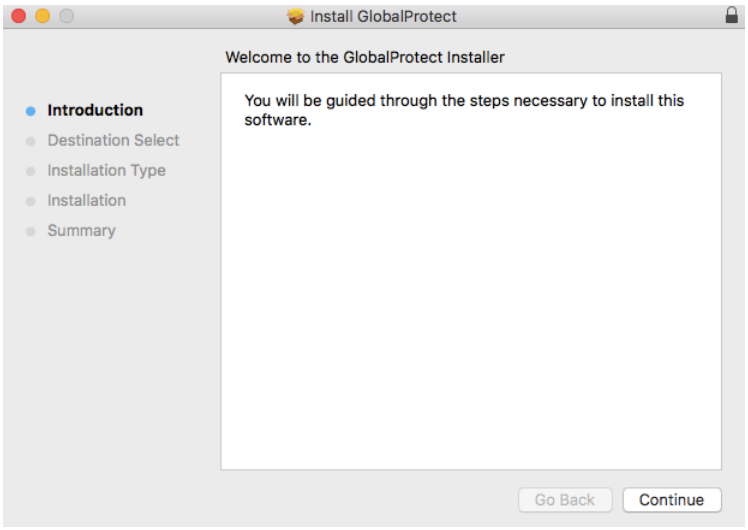
STEP 3 | Download the app.

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

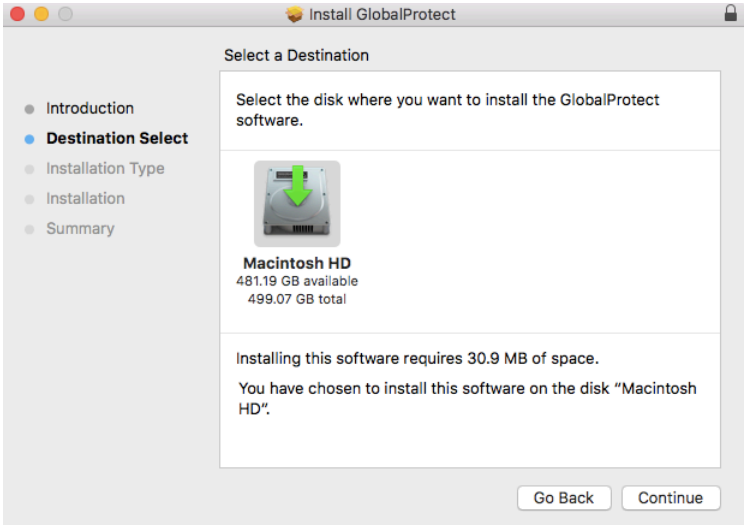
2. When prompted, **Run** the software.
3. When prompted again, **Run** the GlobalProtect Installer.

 ©2023 Palo Alto Networks, Inc.

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**.

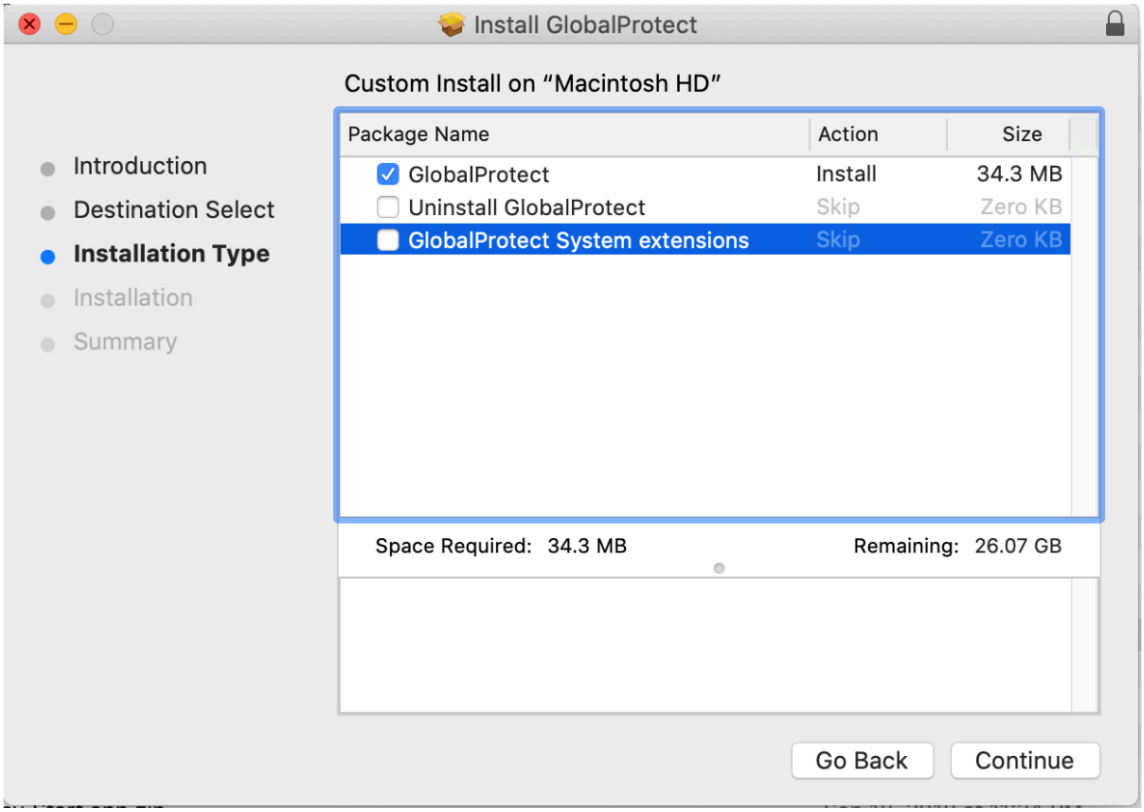


3. On the **Installation Type** screen, select the **GlobalProtect** installation package check box.

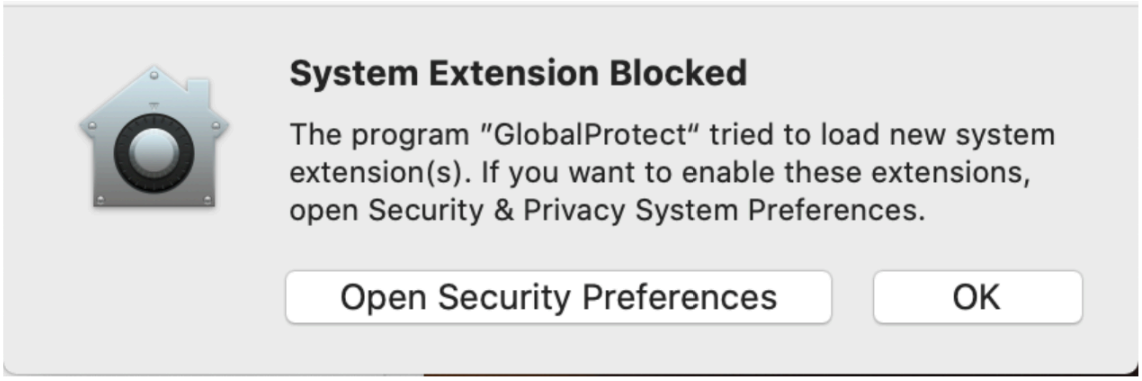
   If your system administrator has configured the split tunnel on the gateway or enforced GlobalProtect connections for network access on the portal, select the **GlobalProtect System Extensions** check box (disabled by default).

   Click **Continue**.

 ©2023 Palo Alto Networks, Inc.

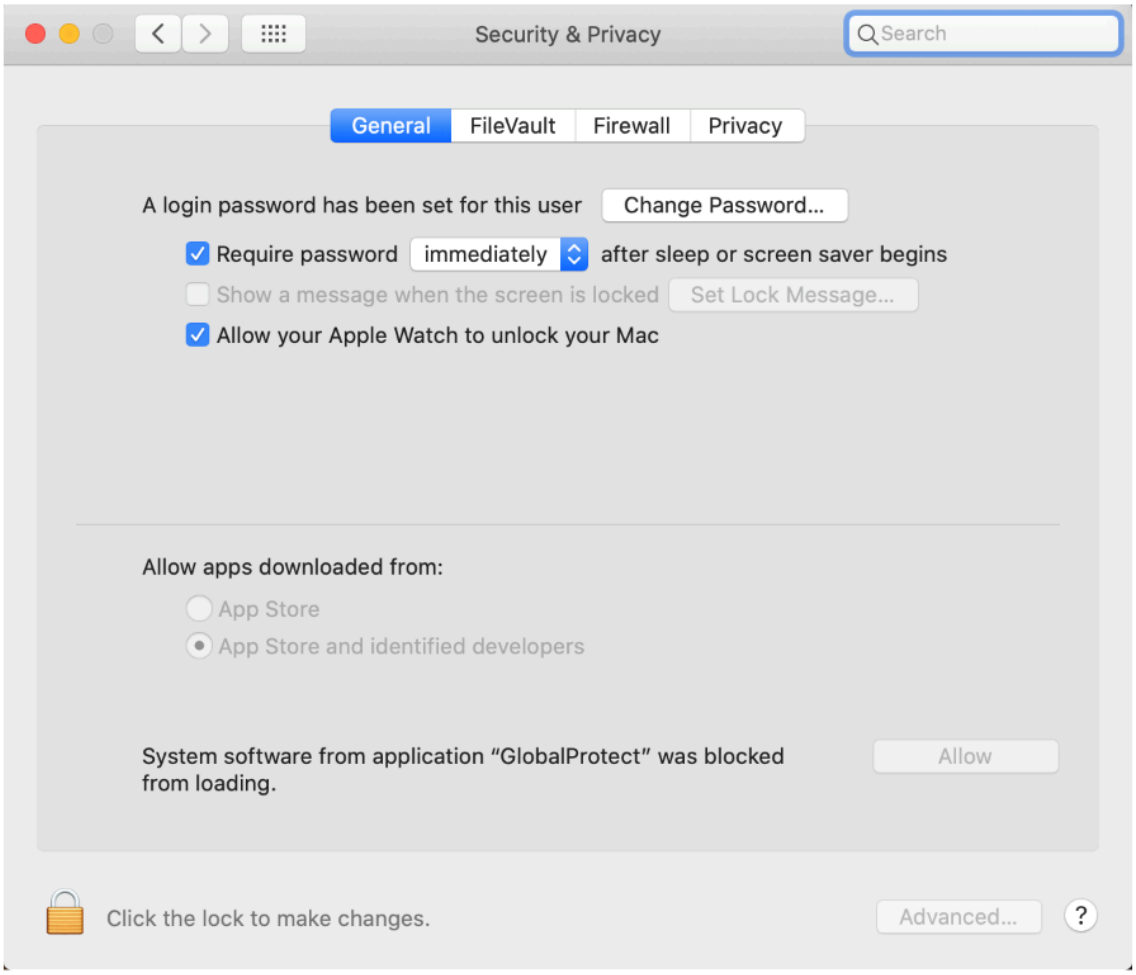


4. Click **Install** to confirm that you want to install GlobalProtect.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to begin the installation.
6. After installation is complete, **Close** the installer.
7. If you enabled the **GlobalProtect System 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) such as Workspace ONE, you can automatically load the system extensionswithout receiving this notification.
8. 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**.

 ©2023 Palo Alto Networks, Inc.



 ©2023 Palo Alto Networks, Inc.

Use the GlobalProtect App for macOS

This chapter 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 | 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 **Disconnected** appears when you hover over the icon.*

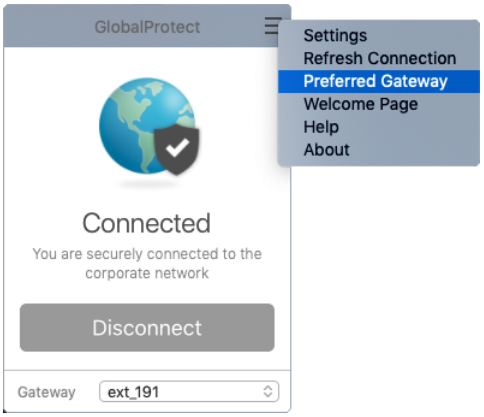
1. Launch the GlobalProtect app by clicking the system tray icon. The status panel opens.
2. (Optional) If you are logging in to the GlobalProtect app for the first time, enter the FQDN or IP address of the GlobalProtect portal, and then click **Connect**.
3. (Optional) If multiple portals are saved on your app, select a portal from the **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

 ©2023 Palo Alto Networks, Inc.

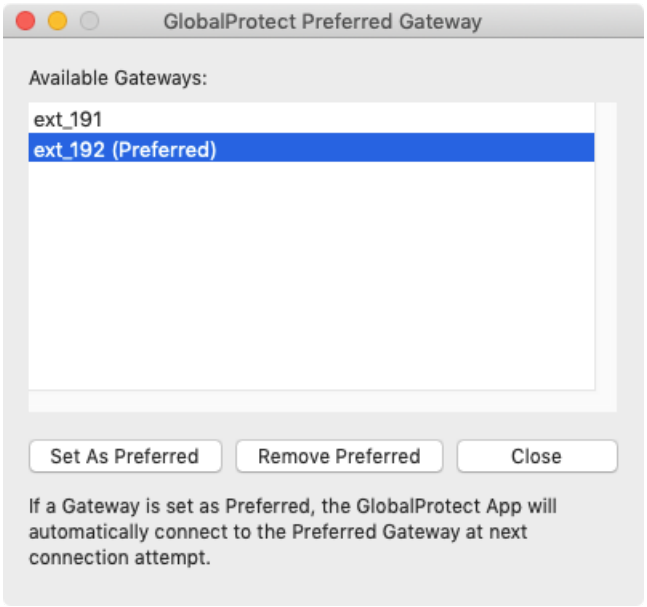
available gateways. To connect to a different gateway, click the gateway drop-down and then use one of the following options:

- 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 status panel, click the Settings (⚙) icon to open the settings menu.
  2. Select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.



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



  4. **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 status panel, click the Settings (⚙) icon to open the settings menu.
  2. Select **Preferred Gateway** to open the GlobalProtect: Preferred Gateway dialog.
  3. From the list of available gateways, select the preferred gateway and then **Remove Preferred**.

 ©2023 Palo Alto Networks, Inc.

4. **Close** the dialog.

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.*

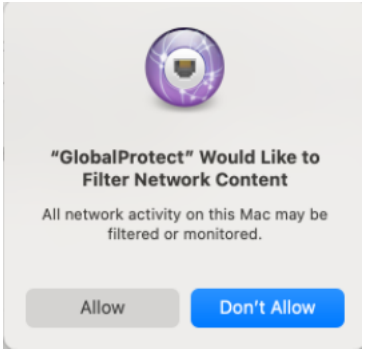
   1. (macOS Catalina 10.15.4 or later only) If your system administrator has configured split tunnel based on domains and applications on the GlobalProtect gateway, select **Allow** in the following pop-up prompt:

      If you select **Don't Allow**, the Split Tunnel feature cannot be used on the GlobalProtect app. This pop-up prompt will appear the next time you connect to the portal or gateway.
   2. (macOS Catalina 10.15.4 or later only) If your system administrator has enabled the Enforce GlobalProtect Connections for Network Access feature, select **Allow** in the following pop-up prompt:

 ©2023 Palo Alto Networks, Inc.

If you select **Don't Allow**, 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 until you select **Allow**.

3. (macOS Big Sur 11 or later only) If your system administrator has configured split tunnel based on domains and applications on the GlobalProtect gateway and 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 2 | Open the GlobalProtect app.

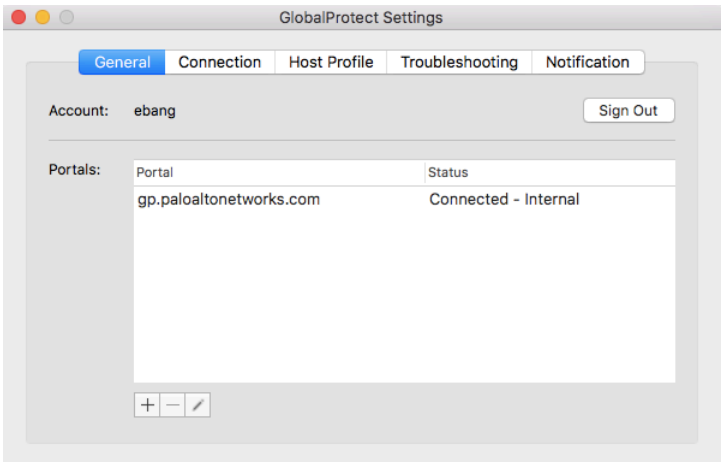
Click the GlobalProtect system tray icon to launch the app interface.

 ©2023 Palo Alto Networks, Inc.

STEP 3 | View information about your network connection.

After you launch the app, click the settings icon (⚙) on the status panel to open the settings menu. 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).*

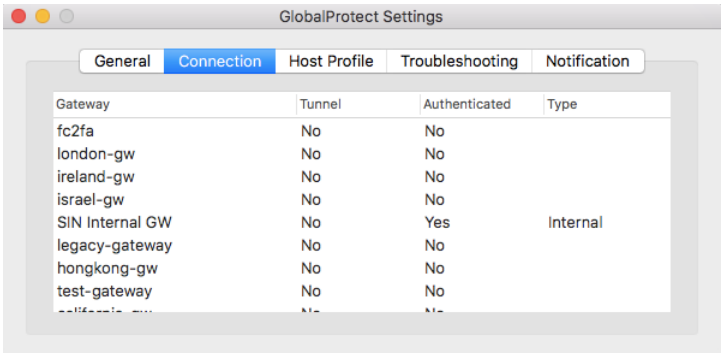


Figure 3: Connection Tab When In Internal Mode

 ©2023 Palo Alto Networks, Inc.

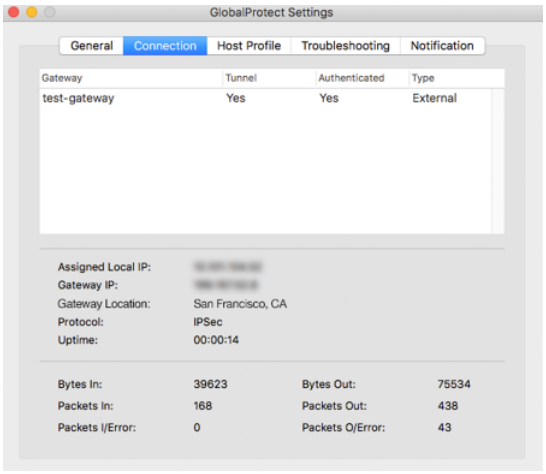


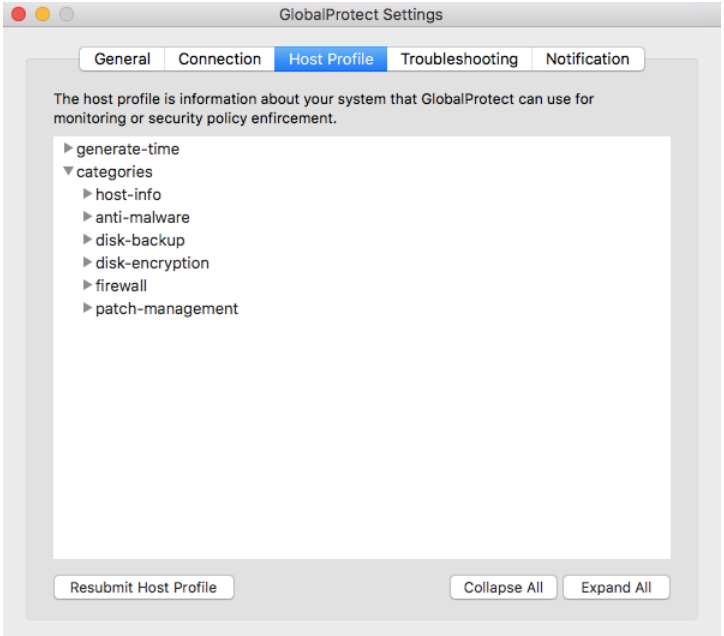
Figure 4: Connection Tab When In External Mode

- **Host Profile**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile (HIP). Click **Resubmit Host Profile** to manually resubmit HIP data to the gateway.

*If your administrator configures the **Severity** value for missing patches as a HIP match condition, use the following mappings between the GlobalProtect severity values and the OPSWAT severity ratings to understand what each value means:*

Severity Value Displayed on the GlobalProtect App	*OPSWAT Severity Rating*
0	*Low*
1	*Moderate*
2	*Important*
3	*Critical*

 ©2023 Palo Alto Networks, Inc.



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

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. Click the settings icon (⚙) to open the settings menu.
3. Select **Settings** to open the **GlobalProtect Settings** panel.
4. On the **General** tab of 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 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.

 ©2023 Palo Alto Networks, Inc.

Disable the GlobalProtect App for macOS

If your administrator configures the GlobalProtect connect method as **Always On**, you can disable the GlobalProtect app. For example, you might want to disable 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 disabling 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 disable the GlobalProtect app depends on how the administrator configures your GlobalProtect service (PanGPS). This configuration can prevent you from disabling the app entirely or allow you to disable 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 disable the app
- 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 disable request is approved, you will receive a valid ticket number that you can use to disable GlobalProtect.

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

STEP 1 | Disable the GlobalProtect app.

1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the settings icon (

) to open the settings menu.
3. Select **Disable**.

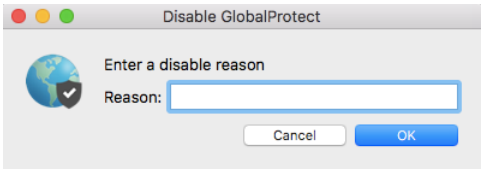
*The **Disable** option is visible only if your GlobalProtect agent configuration allows you to disable the app. If the configuration allows you to disable the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*

 ©2023 Palo Alto Networks, Inc.

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

If prompted, provide the following information:

- **Reason**—Your reason for disabling 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 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 **Disable**. To disable 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**.

 ©2023 Palo Alto Networks, Inc.

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
```

 ©2023 Palo Alto Networks, Inc.

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.*

 ©2023 Palo Alto Networks, Inc.

STEP 3 | Download the app.

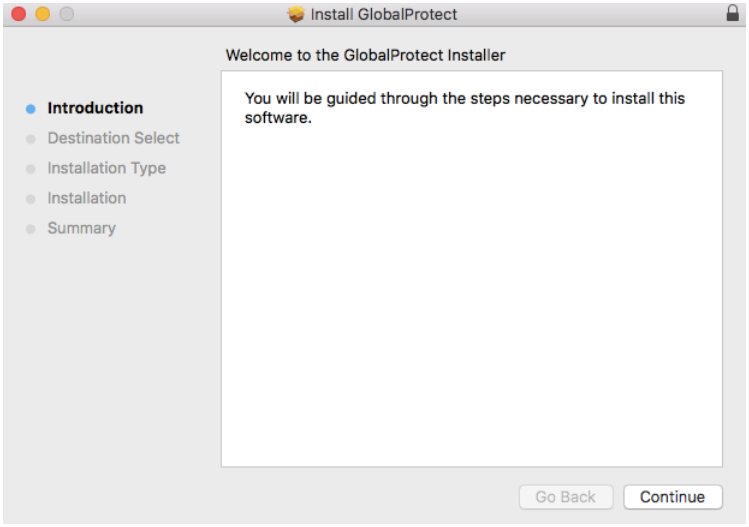
1. Click **Download Mac 32/64 bit GlobalProtect agent**.

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

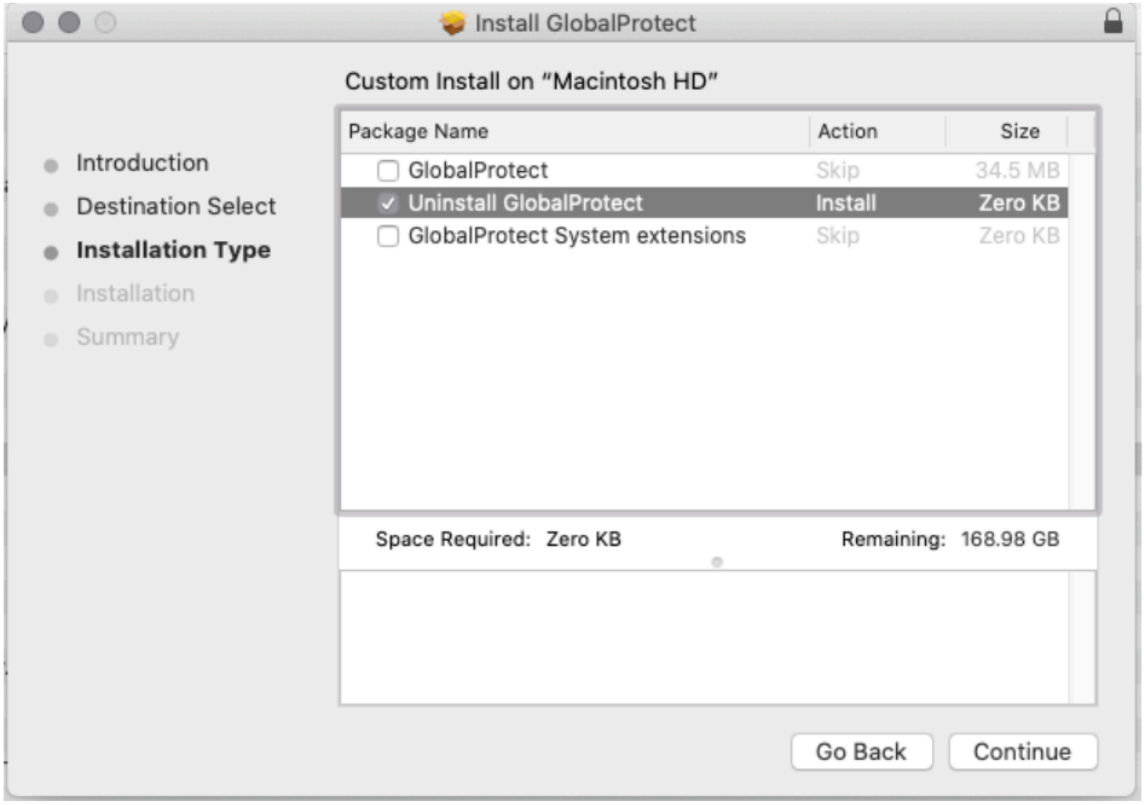
 ©2023 Palo Alto Networks, Inc.

STEP 4 | Uninstall GlobalProtect.

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

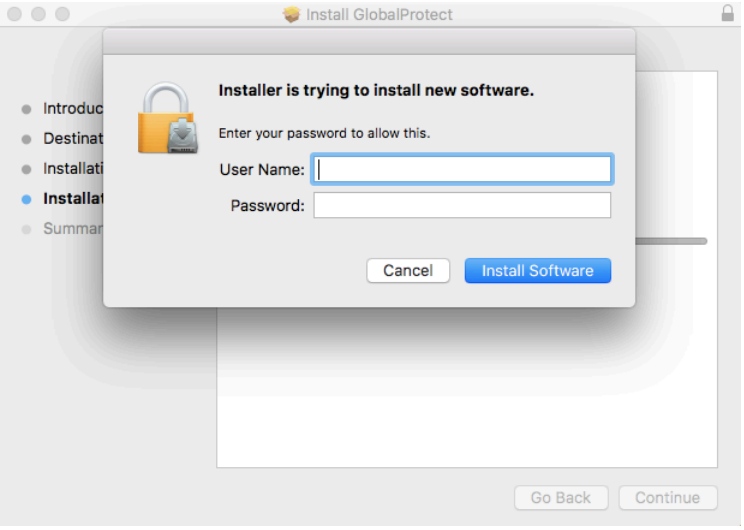


2. On the **Destination Select** screen, click **Continue**.
3. On the **Installation Type** screen, select the **Uninstall GlobalProtect** check box, and then click **Continue**.

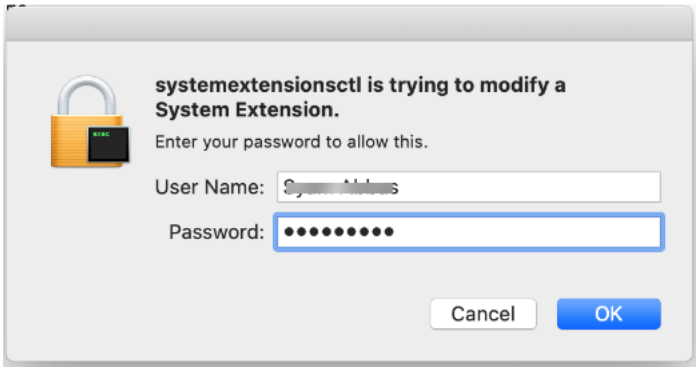


4. Click **Install** to confirm that you want to remove the GlobalProtect app.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to uninstall GlobalProtect.

 ©2023 Palo Alto Networks, Inc.



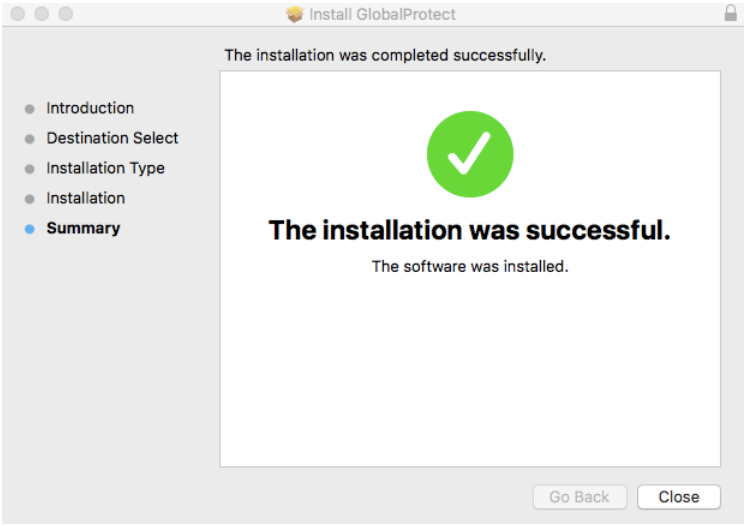
6. If your system administrator has enabled the macOS system extensions during the GlobalProtect app 5.1.4 installation running macOS Catalina 10.15.4 or later, the pop-up prompt appears for you to uninstall the system extensions. When prompted, enter your **User Name** and **Password**, and then click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



 ©2023 Palo Alto Networks, Inc.

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.



 ©2023 Palo Alto Networks, Inc.

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.

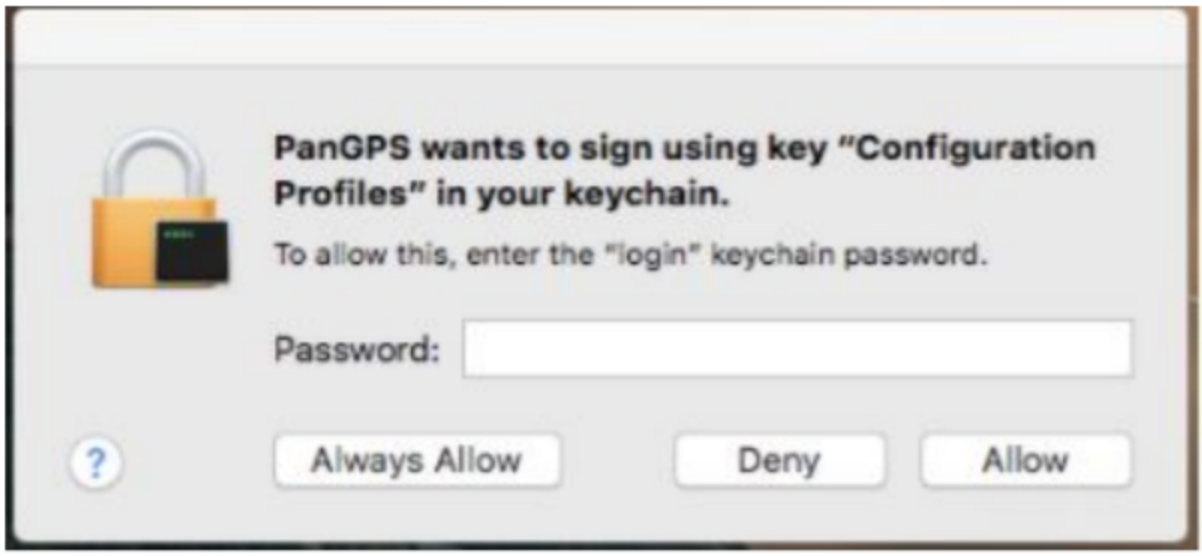
 ©2023 Palo Alto Networks, Inc.

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.*

 ©2023 Palo Alto Networks, Inc.

GlobalProtect App for iOS

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 iOS:

- Download and Install the GlobalProtect App for iOS
- Use the GlobalProtect App for iOS
- Uninstall the GlobalProtect App for iOS

Download and Install the GlobalProtect App for iOS

Before you can connect your iOS endpoint to the GlobalProtect network, you must download and install the app. If your iOS endpoint is managed by a mobile device management (MDM) system, your administrator may have automatically pushed the GlobalProtect app to your endpoint and configured the VPN settings. If you do not already have the GlobalProtect app on your iOS endpoint, you can download it from the App Store.

Before you download the 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. If your administrator has allowed you to use biometric (fingerprint or, for macOS X devices only, face ID) 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.

After you gather the required information, you can download and install the app as follows:

STEP 1 | Launch the App Store.

STEP 2 | **Search** for **`GlobalProtect`**.

STEP 3 | From the search results, select **GlobalProtect™**.

STEP 4 | From the GlobalProtect app product page, tap **GET**.

STEP 5 | **Install** the app.

STEP 6 | When prompted, **Sign In** with Apple ID.

 ©2023 Palo Alto Networks, Inc.

Use the GlobalProtect App for iOS

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).

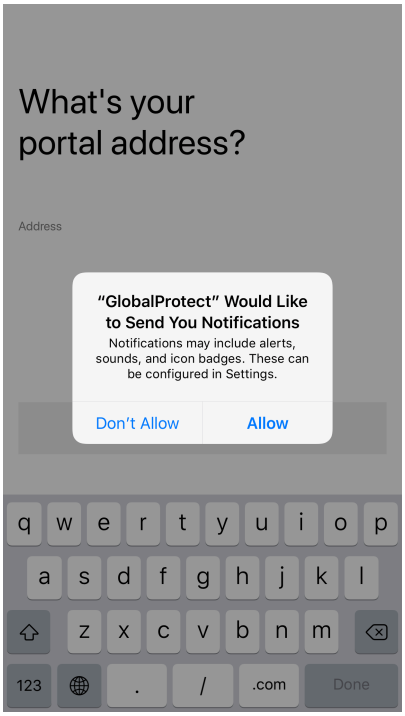
We typically recommend that organizations allow its GlobalProtect users to log in transparently following app installation. After you log in to an endpoint with transparent GlobalProtect login, the GlobalProtect app automatically initiates and connects to the corporate network without further user intervention.

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

STEP 1 | Connect to the GlobalProtect portal or gateway.

Use one of the following workflows to connect to the GlobalProtect portal or gateway:

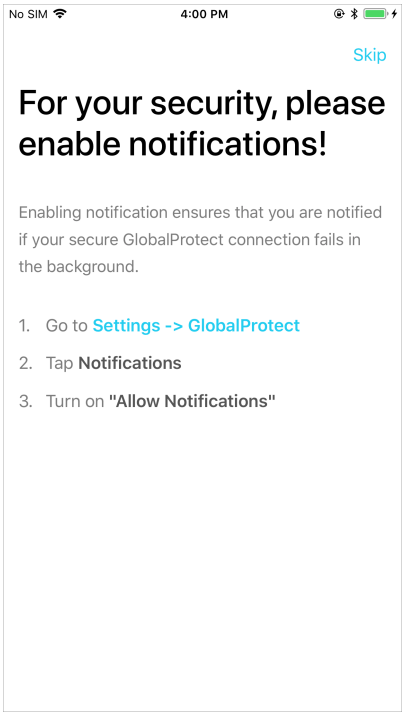
- First time connection experience:
  1. Launch the GlobalProtect app.
  2. (Optional) If you have not enabled GlobalProtect notifications on your endpoint, a notification permission dialog appears. **Allow** GlobalProtect to send you notifications.



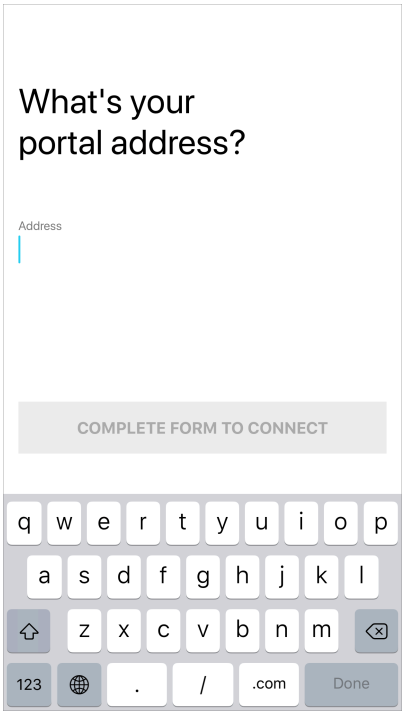
If you **Don't Allow** GlobalProtect to send you notifications, a reminder appears the next time you launch the app. Tap the **Settings -> GlobalProtect** link to go to the notification

 ©2023 Palo Alto Networks, Inc.

permission screen, where you can enable notifications. If you still do not want to enable notifications, **Skip** this screen.



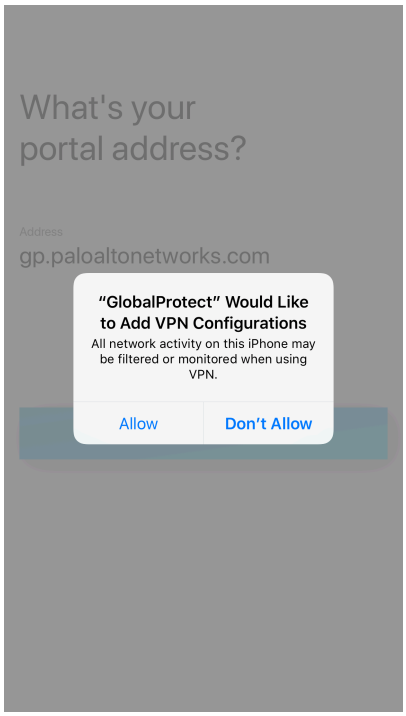
3. Enter the GlobalProtect portal address.



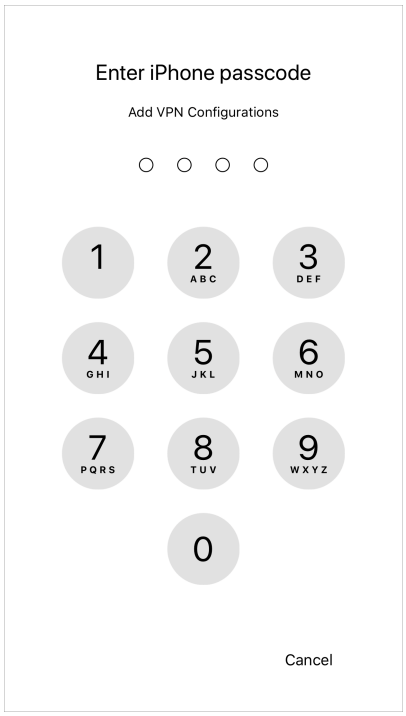
4. (Optional) Depending on the connection mode, tap **Connect** to initiate the connection.
5. When the `"GlobalProtect" Would Like to AddVPN Configurations` message appears, use the following steps to add VPN configurations to your endpoint:

 ©2023 Palo Alto Networks, Inc.

1. **Allow** GlobalProtect to add VPN configurations to your endpoint. This setting enables GlobalProtect to filter and monitor network activity on the endpoint when you are using the VPN.



2. Enter your iPhone or iPad passcode to confirm that you want to add VPN configurations to your endpoint.



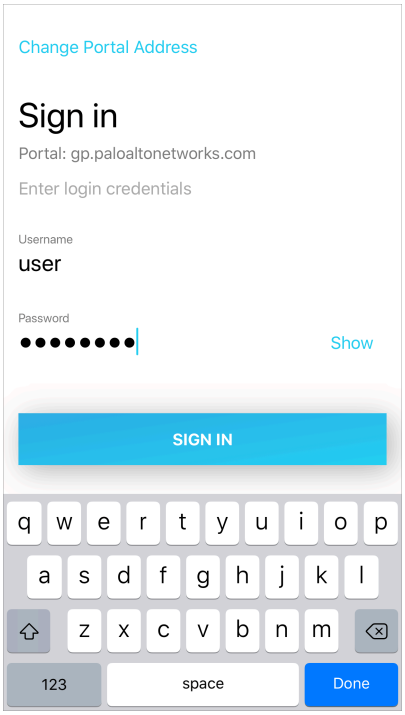
 ©2023 Palo Alto Networks, Inc.

6. (Optional) If your endpoint is unable to verify the identity of the GlobalProtect portal using the portal server certificate, the `Cannot Verify Server Identity` message appears. If you trust the certificate, tap **Continue** to proceed with the connection.
7. (Optional) If prompted, enter your **Username** and **Password** and then **SIGN IN**.

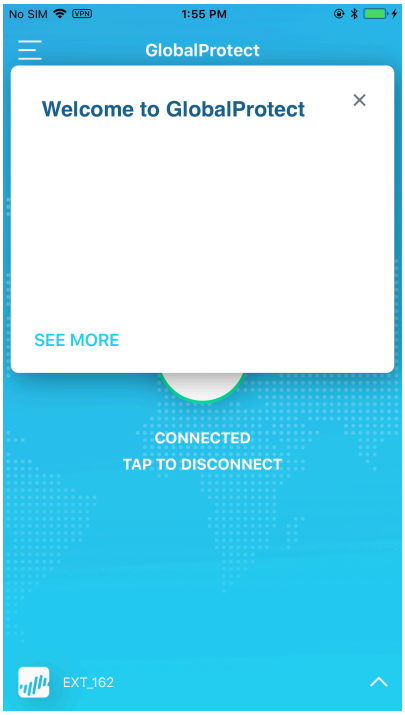
   If your administrator has allowed you to use biometric (fingerprint or, for iOS X devices only, face ID) information to sign in, you need to first sign-in with a username and

 ©2023 Palo Alto Networks, Inc.

password twice (once to save it and again to authenticate); you can then use biometric information to sign in.

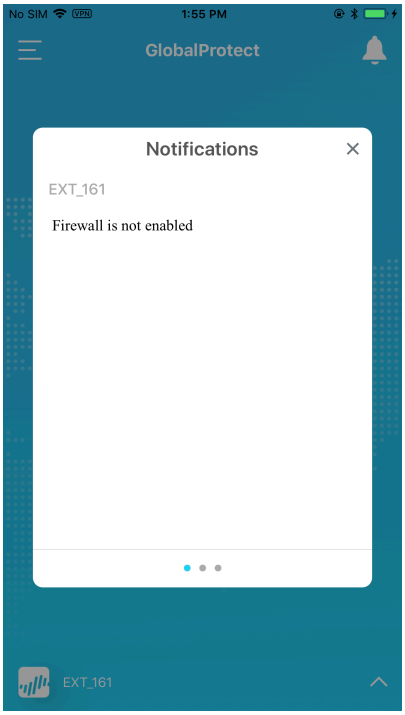


8. (Optional) If you are using multi-factor authentication, enter the GlobalProtect verification **Code** that is sent to your endpoint after you sign in, and then tap **Continue**.
9. (Optional) If your administrator configures the GlobalProtect app to display a welcome message, the welcome message appears upon successful connection. Close the welcome message to proceed to the home screen.

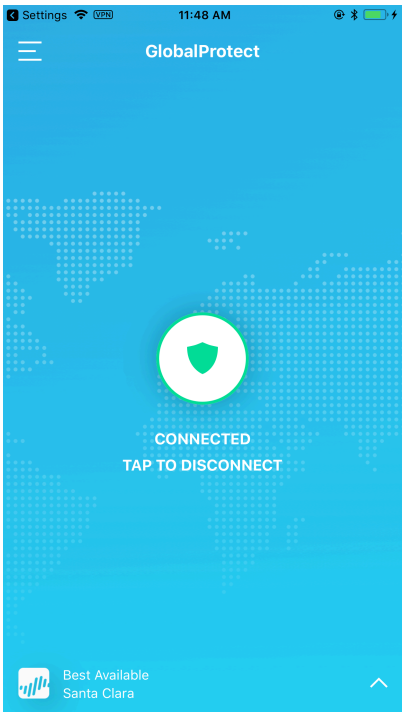


 ©2023 Palo Alto Networks, Inc.

10. (Optional) If there are notifications on your app, the Notifications dialog appears upon successful connection. Close the Notifications dialog to proceed to the home screen.



11. When the home screen appears, verify that your connection has established successfully. If the connection is successful, the home screen displays the **CONNECTED** state.

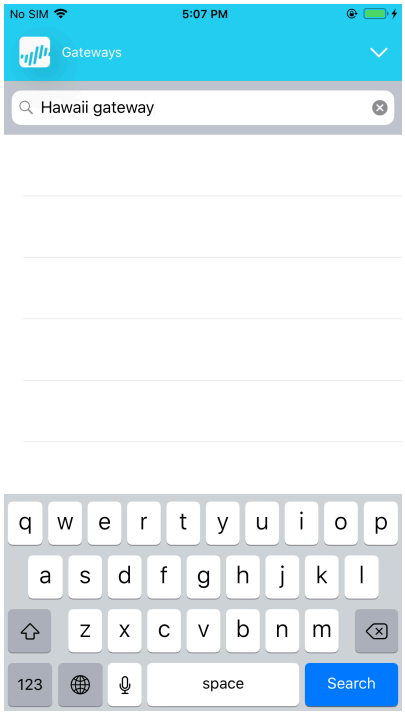


12. (Optional) By default, the endpoint automatically connects to the **Best Available** gateway based on the configuration that the administrator defines and the response times of the

 ©2023 Palo Alto Networks, Inc.

available gateways. To connect to a different gateway, tap the gateway drop-down at the bottom of the home screen and then use one of the following options:

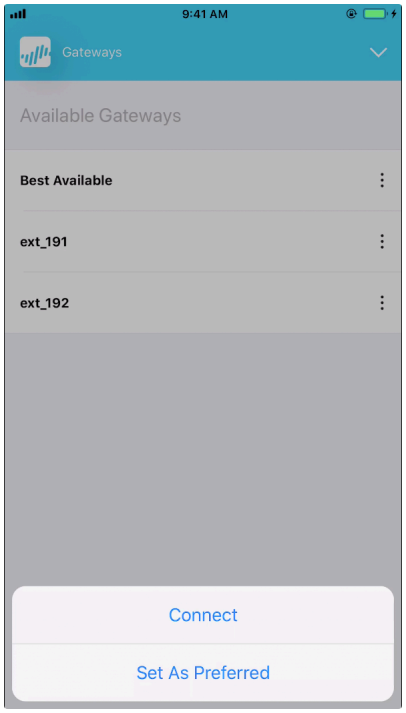
- Select a gateway manually (external gateways only). If your administrator configures more than 10 manual external gateways in your portal agent configuration, you can also locate a specific gateway using the gateway search option.



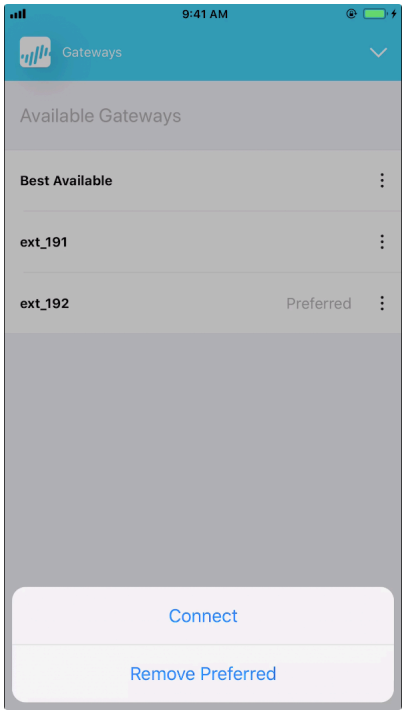
- Assign and automatically connect to a preferred gateway by tapping the More Options (⋮) icon for the gateway that you want to set as the preferred gateway and

 ©2023 Palo Alto Networks, Inc.

then **Set As Preferred**. Alternatively, you can long-press (tap and hold) the gateway and then **Set As Preferred**.



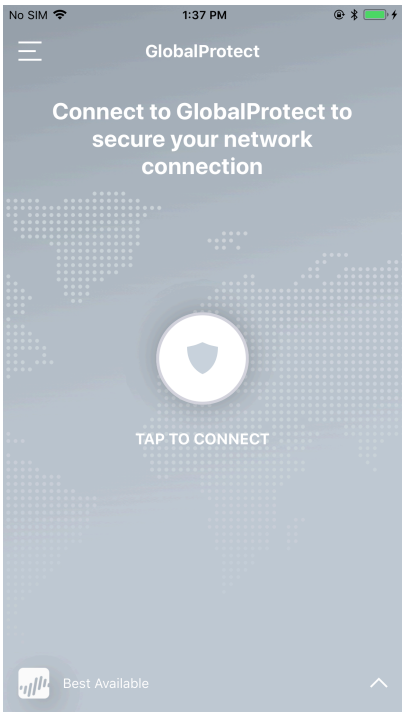
To remove the preferred gateway assignment, tap the More Options (⋮) icon for the preferred gateway and then **Remove Preferred**. Alternatively, you can long-press (tap and hold) the gateway and then **Remove Preferred**.



- On-Demand (Remote Access VPN) connection experience:

 ©2023 Palo Alto Networks, Inc.

When GlobalProtect administrator configures GlobalProtect with the **On-Demand** connect method, you must launch the GlobalProtect app to initiate the connection manually. After the connection initiates, you can **TAP TO CONNECT** to establish the GlobalProtect connection. If your administrator enables GlobalProtect to **Save User Credentials**, the connection establishes without requiring further user interaction. If your administrator does not enable GlobalProtect to **Save User Credentials**, you must sign in to establish the connection.



- Always On connection experience

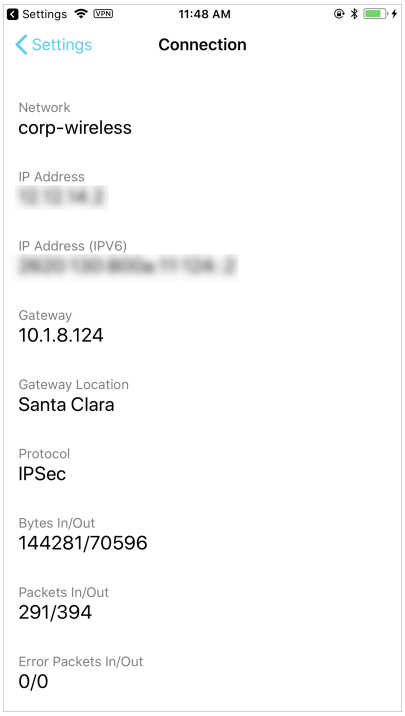
  When your GlobalProtect administrator configures GlobalProtect with the **Always On** connect method, the connection initiates automatically. Depending on whether your administrator configures the GlobalProtect app to **Save User Credentials**, you can establish the GlobalProtect connection without launching the app. If your administrator enables GlobalProtect to **Save User Credentials**, the connection establishes automatically without requiring any user interaction. If your administrator does not enable GlobalProtect to **Save User Credentials**, you must sign in through the app to establish the connection.

 ©2023 Palo Alto Networks, Inc.

STEP 2 | View information about your GlobalProtect connection.

After you establish the GlobalProtect connection, launch the GlobalProtect app. Tap the settings icon to open the settings menu. From the settings menu, tap **SETTINGS** to view information about your connection, including the **Portal** address and connection **Status**.

- If you want to connect to a different GlobalProtect portal, tap the **Portal** address. When prompted, enter a new portal address and then tap **CONNECT**.
- If you are connected to an external gateway, tap the connection **Status** to view additional details about your connection (including the network SSID and gateway IP address/FQDN).



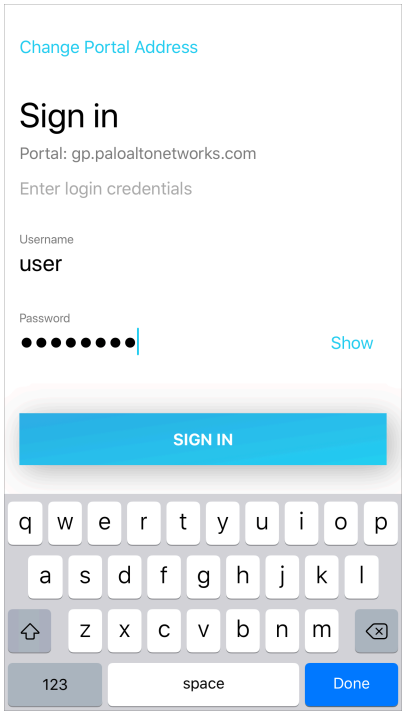
STEP 3 | (Optional) Change your saved password.

If your GlobalProtect administrator configures the GlobalProtect portal agent to **Save User Credentials**, your credentials are automatically saved to the GlobalProtect app. When your password expires or a RADIUS or AD administrator requires a password change at the next login, you can update your password on the app. This feature is enabled only when you are

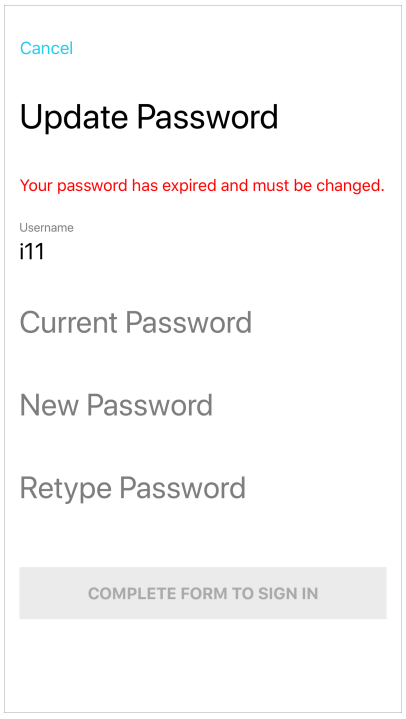
 ©2023 Palo Alto Networks, Inc.

authenticated with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).

1. Launch the GlobalProtect app.
2. From the home screen, **TAP TO CONNECT**.
3. (Optional) If prompted, enter your *old* **Username** and **Password**, and then **SIGN IN**.



4. When the GlobalProtect app prompts you to `Update Password`, enter your **Current Password** followed by your **New Password**.

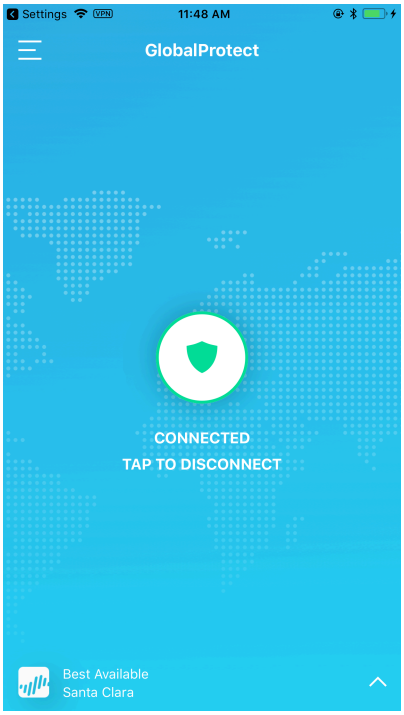


 ©2023 Palo Alto Networks, Inc.

5. **Retype Password** to confirm your new password.
6. **SIGN IN** to reconnect to GlobalProtect with your new password.

STEP 4 | (Optional) Disconnect from GlobalProtect.

If your administrator configures GlobalProtect with the **On-Demand** connect method, you can **TAP TO DISCONNECT** from the home screen.



 ©2023 Palo Alto Networks, Inc.

Uninstall the GlobalProtect App for iOS

Use the following steps to uninstall the GlobalProtect app from your iOS 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.

STEP 1 | Tap and hold the GlobalProtect app icon until the icon jiggles.

STEP 2 | Tap the **X** on the top-left corner of the icon.

STEP 3 | When prompted, **Delete** GlobalProtect.

STEP 4 | Tap **Done** or press the home button to return to the home screen.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

GlobalProtect App for Android

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 Android:

- Download and Install the GlobalProtect App for Android
- Download and Install the GlobalProtect App for Android on Chromebooks
- Use the GlobalProtect App for Android
- Disable the GlobalProtect App for Android
- Uninstall the GlobalProtect App for Android
- Uninstall the GlobalProtect App for Android from Chromebooks

Download and Install the GlobalProtect App for Android

Before you can connect your Android endpoint to the GlobalProtect network, you must download and install the app. If your Android endpoint is managed by a mobile device management (MDM) system, your administrator may have automatically pushed the GlobalProtect app to your endpoint and configured the VPN settings. If you do not already have the GlobalProtect app on your Android endpoint, you can download it from Google Play.

Before you download the 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.

After you gather the required information, you can download and install the app as follows:

STEP 1 | Launch Google Play.

STEP 2 | **Search** for **`GlobalProtect`**.

STEP 3 | From the search results, select **GlobalProtect**.

STEP 4 | From the GlobalProtect app product page, tap **Install**.

STEP 5 | When prompted, review and **Accept** the information for which GlobalProtect needs access.

 ©2023 Palo Alto Networks, Inc.

Download and Install the GlobalProtect App for Android on Chromebooks

To use the GlobalProtect app for Android on a Chromebook, you must download and install the app. If your Chromebook is managed by Workspace ONE or the Google Admin console, your administrator may have automatically pushed the GlobalProtect app to your endpoint and configured the VPN settings. If you do not already have the GlobalProtect app for Android on your Chromebook, you can download it from the Google Play Store.

Before you download the 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.

After you gather the required information, you can download and install the app as follows:

The GlobalProtect app for Android is supported only on certain Chromebooks. If you were using version 4.1.x of the GlobalProtect app for Chrome OS, the app is no longer available. Consider upgrading to a Chrome OS system that supports Android Apps and use the GlobalProtect app for Android.

STEP 1 | Enable the Google Play Store app on your Chromebook.

1. (Optional) If your Chromebook is running Chrome OS version 52 or earlier, update your Chromebook operating system.
2. From your Chromebook, click your account photo at the bottom right corner of the screen.
3. Select **Settings**.
4. In the Google Play Store area, **Enable Google Play Store on your Chromebook**.

   If this option is not available, your Chromebook does not support Android apps.
5. When prompted, click **Get Started** to launch the Google Play Store.
6. **Agree** to the Terms of Service.
7. On the Welcome page, **SIGN IN** to the Google Play Store.
8. **Accept** the Google Play Terms of Service.

STEP 2 | Download and install the GlobalProtect app for Android endpoints on your Chromebook.

1. Open the Google Play Store app.
2. Search for **`GlobalProtect App`**.
3. Click the GlobalProtect app icon.
4. Click **INSTALL**, and then follow the on-screen instructions to complete the app installation.

 ©2023 Palo Alto Networks, Inc.

Use the GlobalProtect App for Android

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.

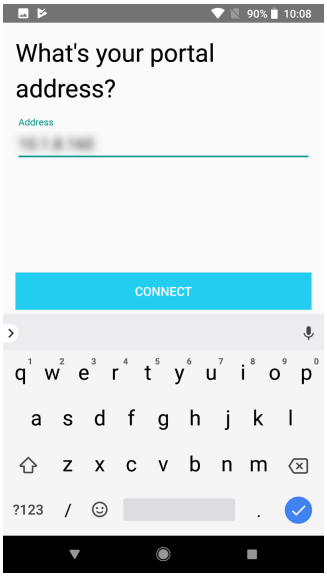
If your setup requires you to enter your GlobalProtect credentials, follow the applicable steps below.

 ©2023 Palo Alto Networks, Inc.

STEP 1 | Connect to the GlobalProtect portal or gateway.

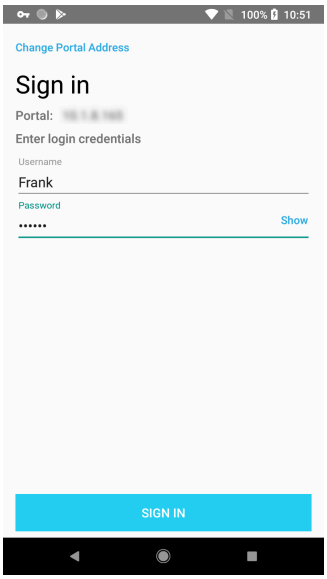
Use one of the following workflows to connect to the GlobalProtect portal or gateway:

- First time connection experience:
  1. Launch the GlobalProtect app.
  2. Enter the GlobalProtect portal address.



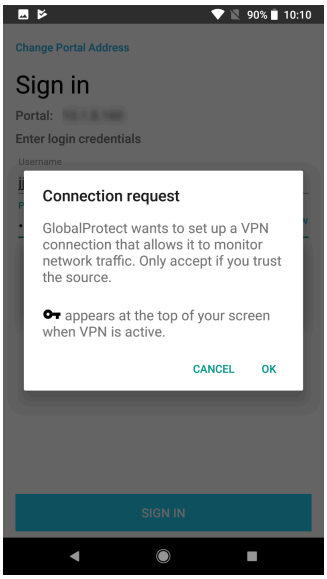
  3. (Optional) Depending on the connection mode, tap **Connect** to initiate the connection.
  4. (Optional) If your endpoint is unable to verify the identity of the GlobalProtect portal using the portal server certificate, the `Cannot Verify Server Identity` message appears. If you trust the certificate, tap **Continue** to proceed with the connection.
  5. (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; you can then use biometric information to sign in.

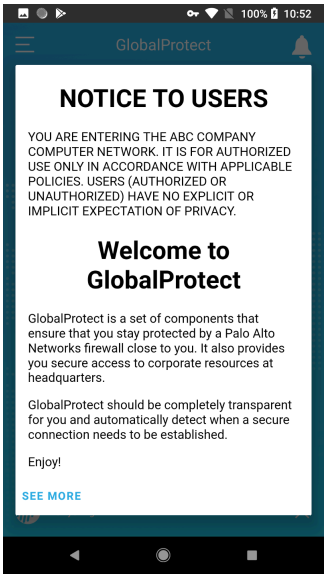


 ©2023 Palo Alto Networks, Inc.

6. When the `Connection request` message appears, tap **OK** to allow GlobalProtect to set up a VPN connection on your endpoint.

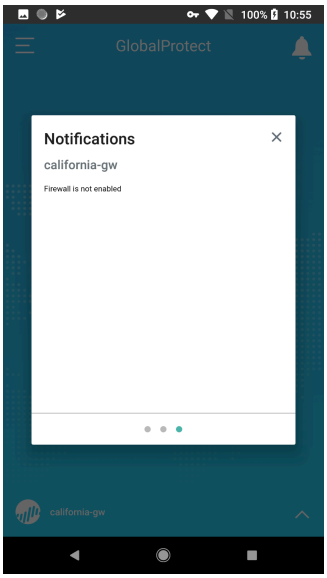


7. (Optional) If you are using multi-factor authentication, enter the GlobalProtect verification **Code** that is sent to your endpoint after you sign in, and then tap **Continue**.
8. (Optional) If your administrator configures the GlobalProtect app to display a welcome message, the welcome message appears upon successful connection. Tap outside of the welcome message to proceed to the home screen.

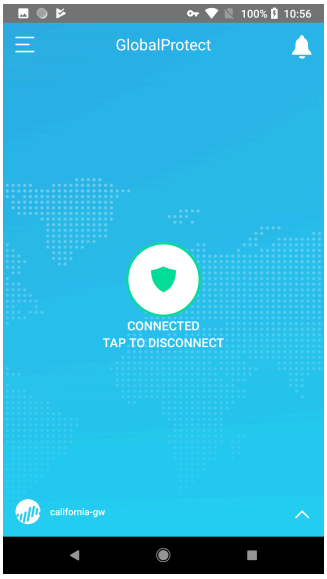


9. (Optional) If there are notifications on your app, the Notifications dialog appears upon successful connection. Close the Notifications dialog to proceed to the home screen.

 ©2023 Palo Alto Networks, Inc.



10. When the home screen appears, verify that your connection has established successfully. If the connection is successful, the home screen displays the **CONNECTED** state.



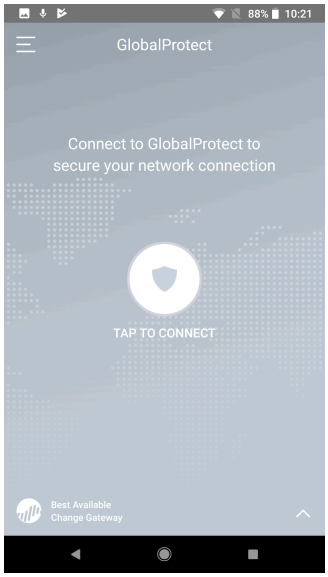
11. (Optional) By default, the endpoint automatically connects to the **Best Available** gateway based on the configuration that the administrator defines and the response times of the available gateways. To connect to a different gateway, tap the gateway drop-down at the bottom of the home screen, and then select a gateway from the list (external gateways only).

- On-Demand (Remote Access VPN) connection experience:

  When your GlobalProtect administrator configures GlobalProtect with the **On-Demand** connect method, you must launch the GlobalProtect app to initiate the connection manually. After the connection initiates, you can **TAP TO CONNECT** to establish the GlobalProtect connection. If your administrator enables GlobalProtect to **Save User Credentials**, the connection establishes without requiring further user interaction. If your

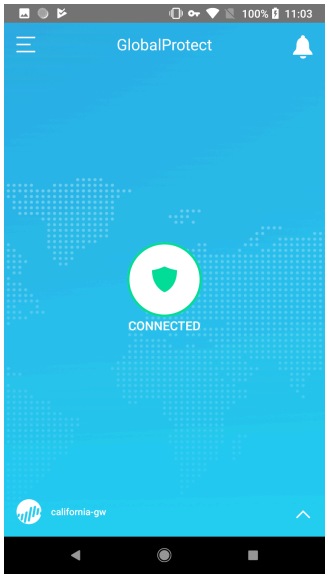
 ©2023 Palo Alto Networks, Inc.

administrator does not enable GlobalProtect to **Save User Credentials**, you must sign in to establish the connection.



- Always On connection experience:

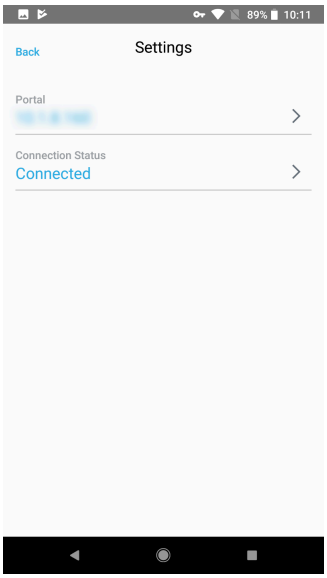
  When your GlobalProtect administrator configures GlobalProtect with the **Always On** connect method, the connection initiates automatically. Depending on whether your administrator configures the GlobalProtect app to **Save User Credentials**, you can establish the GlobalProtect connection without launching the app. If your administrator enables GlobalProtect to **Save User Credentials**, the connection establishes automatically without requiring any user interaction. If your administrator does not enable GlobalProtect to **Save User Credentials**, you must sign in through the app to establish the connection.



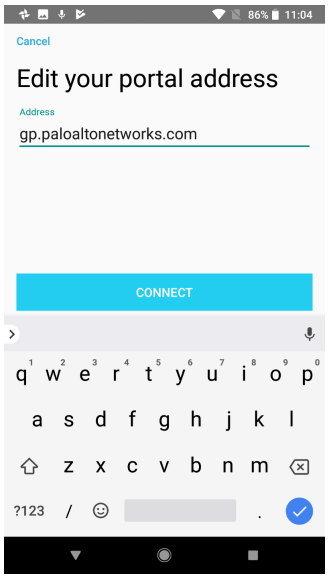
 ©2023 Palo Alto Networks, Inc.

STEP 2 | View information about your GlobalProtect connection.

After you establish the GlobalProtect connection, launch the GlobalProtect app. Tap the settings icon to open the settings menu. From the settings menu, tap **SETTINGS** to view information about your connection, including the **Portal** address and connection **Status**.

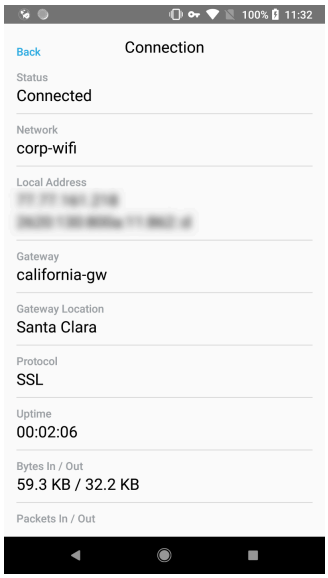


- If you want to connect to a different GlobalProtect portal, tap the **Portal** address. When prompted, enter a new portal address and then tap **CONNECT**.



- If you are connected to an external gateway, tap the connection **Status** to view additional details about your connection (including the network SSID and gateway IP address/FQDN).

 ©2023 Palo Alto Networks, Inc.



STEP 3 | (Optional) Change your saved password.

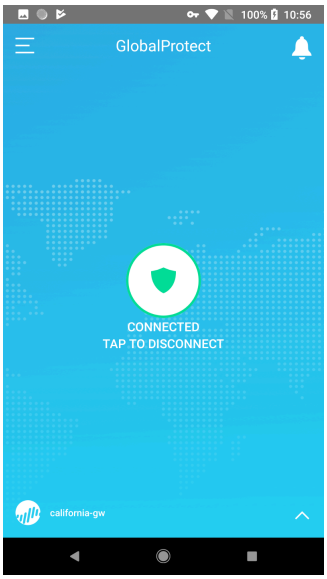
If your GlobalProtect administrator configures the GlobalProtect portal agent to **Save User Credentials**, your credentials are automatically saved to the GlobalProtect app. When your password expires or a RADIUS or AD administrator requires a password change at the next login, you can update your password on the app. This feature is enabled only when you are authenticated with a RADIUS server using the Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).

1. Launch the GlobalProtect app.
2. From the home screen, **TAP TO CONNECT**.
3. (Optional) If prompted, enter your *old* **Username** and **Password**, and then **SIGN IN**.
4. When the GlobalProtect app prompts you to `Update Password`, enter your **Current Password** followed by your **New Password**.
5. **Retype Password** to confirm your new password.
6. **SIGN IN** to reconnect to GlobalProtect with your new password.

 ©2023 Palo Alto Networks, Inc.

STEP 4 | (Optional) Disconnect from GlobalProtect.

If your administrator configures GlobalProtect with the **On-Demand** connect method, you can **TAP TO DISCONNECT** from the home screen.



 ©2023 Palo Alto Networks, Inc.

Disable the GlobalProtect App for Android

If your administrator configures the GlobalProtect connect method as **Always On**, you can disable the GlobalProtect app. For example, you might want to disable 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 disabling 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 disable the GlobalProtect app depends on how the administrator configures your GlobalProtect service (PanGPS). This configuration can prevent you from disabling the app entirely or allow you to disable 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 disable 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.

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

STEP 1 | Disable the GlobalProtect app.

1. Launch the GlobalProtect app.
2. Tap the settings icon to open the settings menu.
3. From the settings menu, tap **DISABLE**.

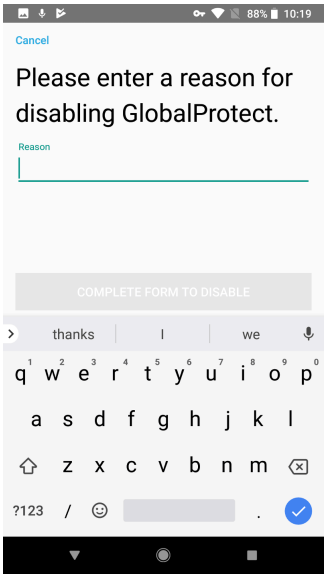
*The **Disable** option is visible only if your GlobalProtect agent configuration allows you to disable the app. If the configuration allows you to disable the GlobalProtect app without requiring you to respond to a challenge, the GlobalProtect app closes without requiring further action.*

 ©2023 Palo Alto Networks, Inc.

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

If prompted, provide the following information:

- **Reason**—Your reason for disabling 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 disable the app.

 ©2023 Palo Alto Networks, Inc.

Uninstall the GlobalProtect App for Android

Use the following steps to uninstall the GlobalProtect app from your Android 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.

STEP 1 | Launch the Settings app.

STEP 2 | Tap **Apps & notifications**.

STEP 3 | Tap **GlobalProtect**.

STEP 4 | Tap **Uninstall**.

 ©2023 Palo Alto Networks, Inc.

Uninstall the GlobalProtect App for Android from Chromebooks

Use the following steps to uninstall the GlobalProtect app for Android from your Chromebook . 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.

STEP 1 | Open the Google Play Store app.

STEP 2 | Click the menu button (☰) next to the Google Play search bar.

STEP 3 | Select **Apps & games** > **My apps & games**.

STEP 4 | Select **INSTALLED**.

STEP 5 | From the On this device area, select **GlobalProtect**.

STEP 6 | Click **UNINSTALL**.

 ©2023 Palo Alto Networks, Inc.

 ©2023 Palo Alto Networks, Inc.

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
- 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.

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-5.1.0.tgz
         ./
         ./GlobalProtect_deb-5.1.0.0-62.deb
         ./GlobalProtect_deb_arm-5.1.0.0-62.deb
         ./GlobalProtect_rpm-5.1.0.0-62.rpm
         ./GlobalProtect_rpm_arm-5.1.0.0-62.rpm
         ./GlobalProtect_tar-5.1.0.0-62.tgz
         ./GlobalProtect_tar_arm-5.1.0.0-62.tgz
         ./GlobalProtect_UI_deb-5.1.0.0-62.deb
         ./GlobalProtect_UI_rpm-5.1.0.0-62.rpm
         ./GlobalProtect_UI_tar-5.1.0.0-62.tgz
         ./manifest
         ./relinfo
```

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.

 ©2023 Palo Alto Networks, Inc.

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 | (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.
```

STEP 4 | Install the GUI version of the GlobalProtect app for Linux.

Install the app using root privileges and use an installation method that will automatically add any missing packages that are required by the GlobalProtect app.

For Debian and Ubuntu, use the **sudo apt-get install <*gp-app-pkg*>** command.

For CentOS and Red Hat, use the **sudo yum install <*gp-app-pkg*>** command.

 ©2023 Palo Alto Networks, Inc.

STEP 5 | Use the GUI version of the GlobalProtect App for Linux.

After installation completes, the GlobalProtect app automatically launches. Specify your portal address and enter your credentials when prompted to begin the connection process.

Because the GlobalProtect service supports only one socket connection to the GlobalProtect agent and to the GUI version of the GlobalProtect app, you must either log out of the Linux operating system or the SSH session depending on the installation method used as a root user after installing the app. You must log back in to the Linux endpoint as another user with non-privileged user privileges and the app launches.

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-5.1.0.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-5.1.0.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

 ©2023 Palo Alto Networks, Inc.

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.

There are two app packages available for GlobalProtect:

- CLI version (for example GlobalProtect_deb-5.1.0.0-19.deb)—Use either the **sudo dpkg -i *<gp-app-pkg>*** or **sudo apt-get install *<gp-app-pkg>***
- UI version (for example GlobalProtect_UI_deb-5.1.0.0-19.deb)—Install using the **sudo apt-get install *<gp-app-pkg>*** command.

where ***<gp-app-pkg>*** is the path of either the CLI or UI distribution package for your Linux version.

```
user@linuxhost:~$
      sudo dpkg -i GlobalProtect_deb-5.1.0.0-19.deb
      Selecting previously unselected package GlobalProtect.

      (Reading database ... 67776 files and directories currently
 installed.)
      Preparing to unpack GlobalProtect_deb-5.1.0.0-19.deb ...
      Start installing gp...
      Unpacking GlobalProtect (5.1.0-19) ...
      Setting up GlobalProtect (5.1.0-19) ...
      Enable gp service...
      Starting gp service...
      Create symlink for gp cli...
```

```
user@linuxhost:~$
      sudo apt-get install GlobalProtect_deb-5.1.0.0-23.deb
      [sudo] password for gpqa:
      Reading package lists... Done
      Building dependency tree
      Reading state information... Done
```

 ©2023 Palo Alto Networks, Inc.

```
      Note, selecting 'globalprotect' instead of '/home/gpqa/
Downloads/GlobalProtect_deb-5.1.0.0-24.deb'
      The following packages were automatically installed and are
 no longer required:
      linux-headers-5.10.0-28 linux-headers-5.10.0-28-generic
 linux-image-5.10.0-28-generic linux-image-extra-5.10.0-28-generic
      Use 'sudo apt autoremove' to remove them.
      The following NEW packages will be installed:
      globalprotect
      0 upgraded, 1 newly installed, 0 to remove and 73 not
 upgraded.
      After this operation, 0 B of additional disk space will be
 used.
      Get:1 /home/gpqa/Downloads/GlobalProtect_deb-5.1.0.0-24.deb
 globalprotect all 5.1.0-24 [1,334 kB]
      E: read, still have 59 to read but none left
      E: Error reading archive member header
      E: Prior errors apply to /home/gpqa/Downloads/
GlobalProtect_deb-5.1.0.0-24.deb
      debconf: apt-extracttemplates failed: No such file or
 directory
      Selecting previously unselected package globalprotect.
      (Reading database ... 247210 files and directories currently
 installed.)
      Preparing to unpack .../GlobalProtect_deb-5.1.0.0-24.deb ...
      Start installing gp...
      Unpacking globalprotect (5.1.0-24) ...
      Setting up globalprotect (5.1.0-24) ...
      Enable gp service...
      Starting gp service...
      Create symlink for gp cli...
```

The GlobalProtect app for Linux installs to the `/opt/paloaltonetworks/globalprotect` directory. After GlobalProtect first runs, the app also creates a GlobalProtect user folder `$HOME/.globalprotect` to save user registry configuration and other CLI related settings.

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:~$
   ```

 ©2023 Palo Alto Networks, Inc.

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

Prompt mode:

```
>>
      help
      Usage: only the following commands aresupported:
      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.

 ©2023 Palo Alto Networks, Inc.

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.

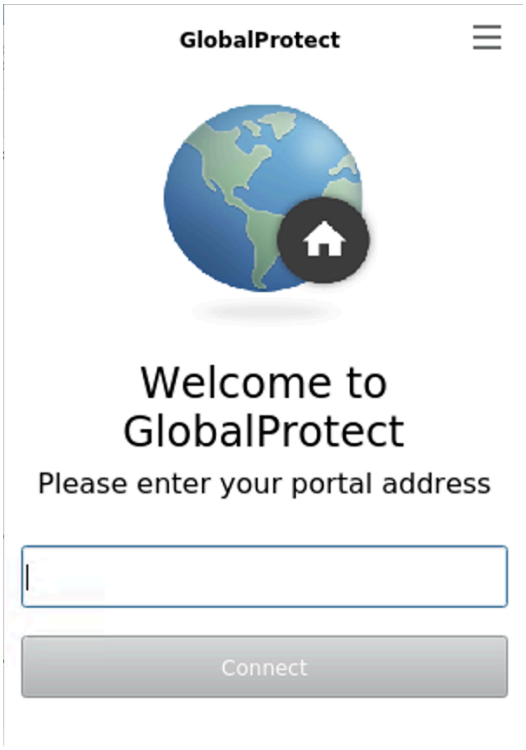
- Use the GUI Version of the GlobalProtect App for Linux
- Use the CLI Version of the GlobalProtect App for Linux

Use the GUI Version of the GlobalProtect App for Linux

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

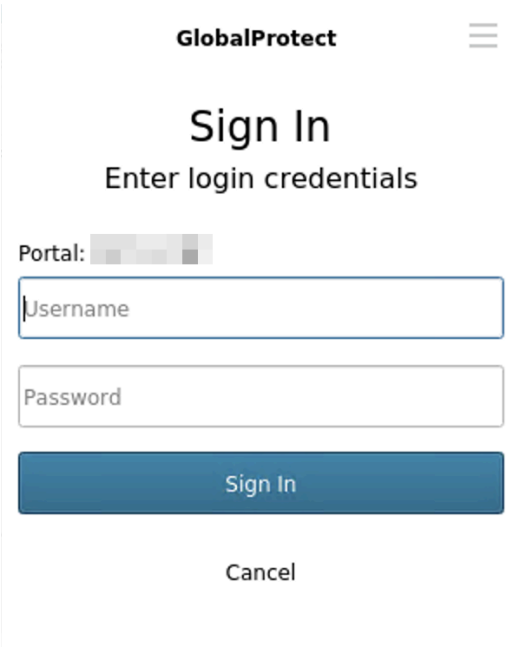
 ©2023 Palo Alto Networks, Inc.

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.

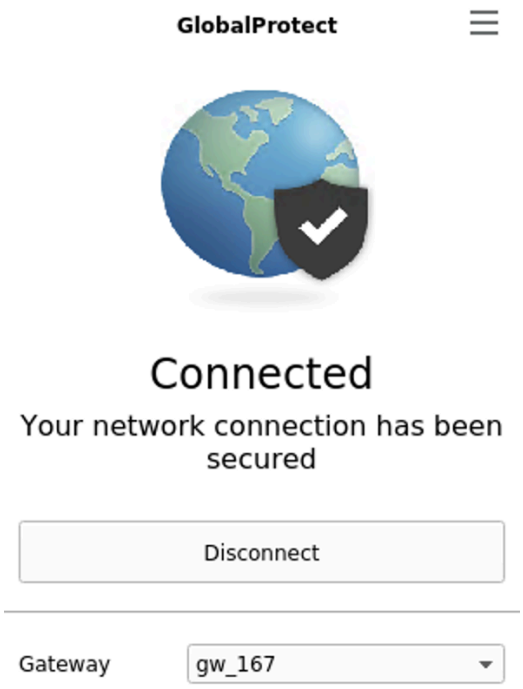
1. (Optional) If multiple portals are saved on your app, select a portal from the **Portal** drop-down. By default, the most recently connected portal is pre-selected from the **Portal** drop-down.



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

 ©2023 Palo Alto Networks, Inc.

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**.



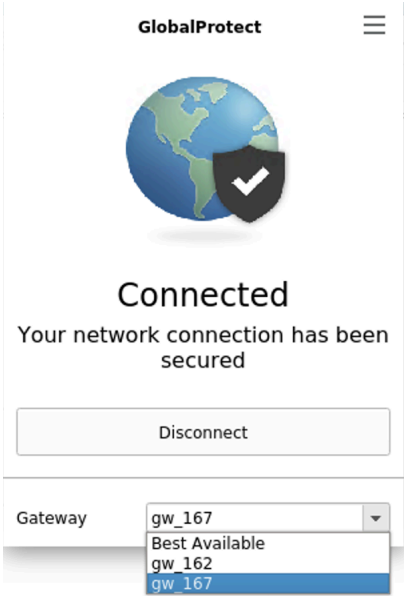
3. (Optional) By default, you are automatically connected to the **Best Available** gateway, based on the configuration that the administrator defines and the response times of the

 ©2023 Palo Alto Networks, Inc.

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

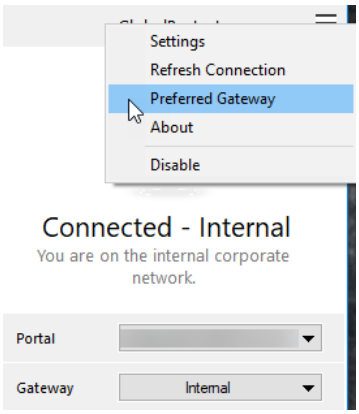
- Select a gateway manually (external gateways only).

  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.

 ©2023 Palo Alto Networks, Inc.

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.

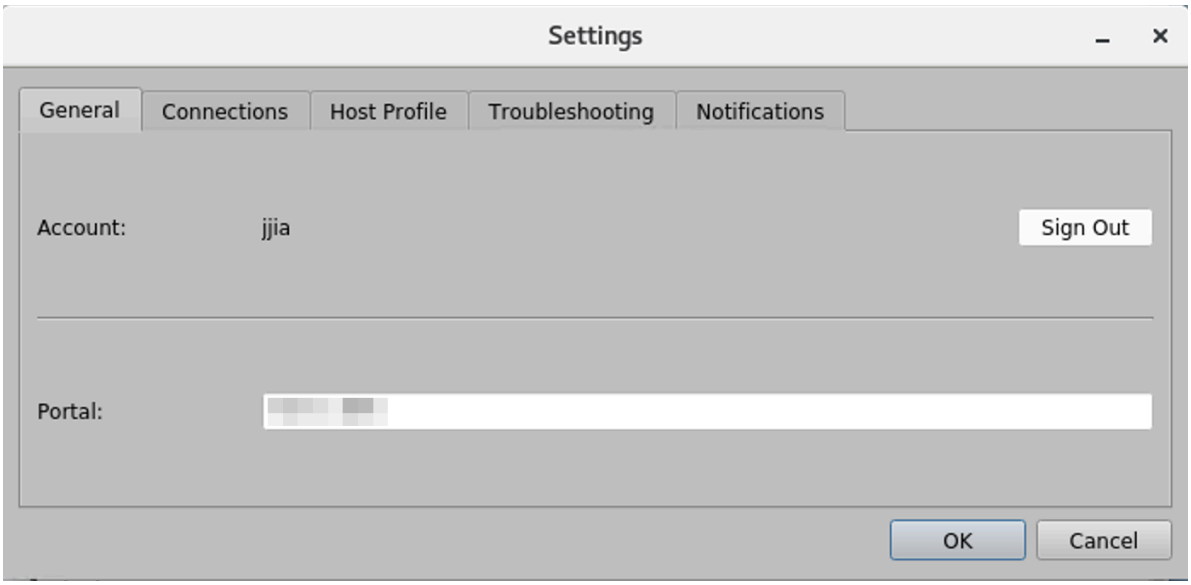
Click the GlobalProtect system tray icon to launch the app interface.

 ©2023 Palo Alto Networks, Inc.

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:

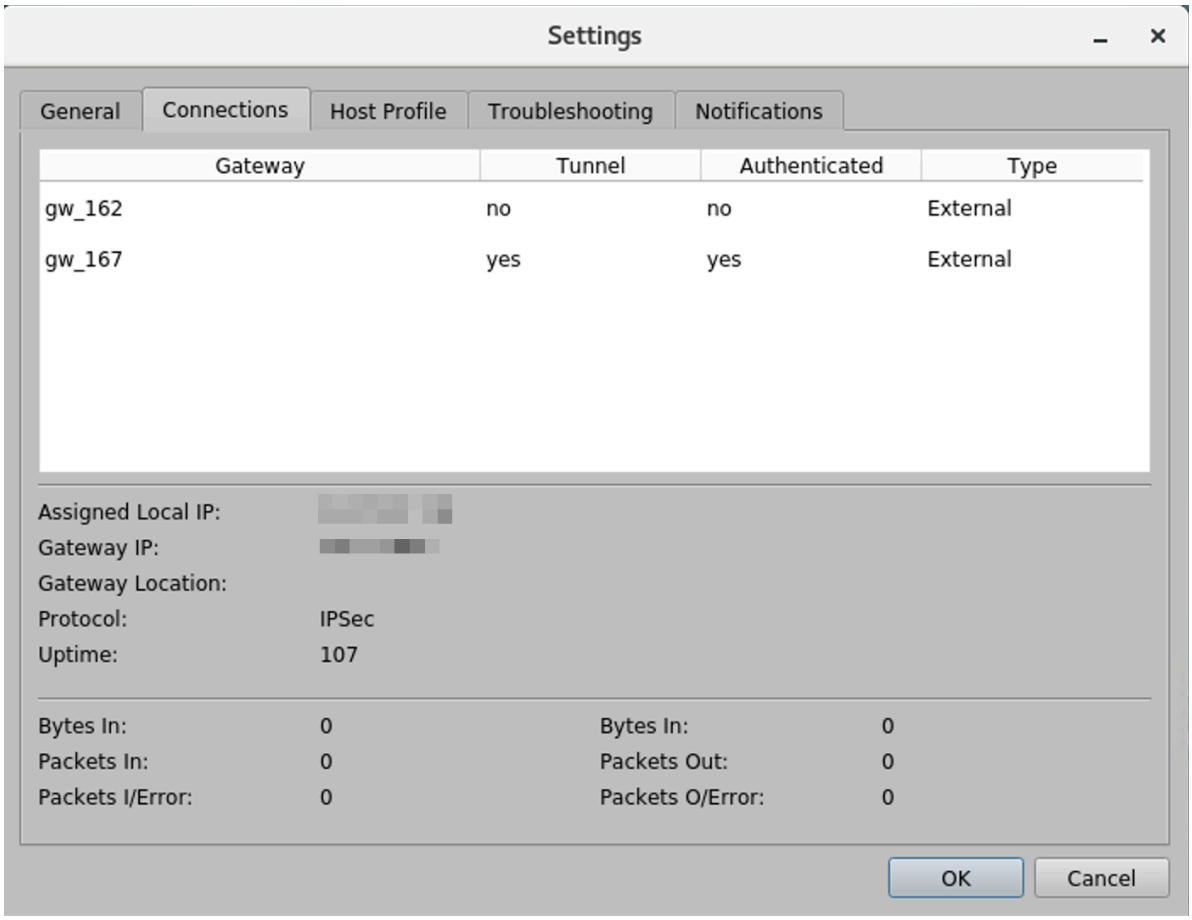
- **General**—Displays the username and portal(s) associated with the GlobalProtect account. You can also add, delete, or modify portals from this tab.



- **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)

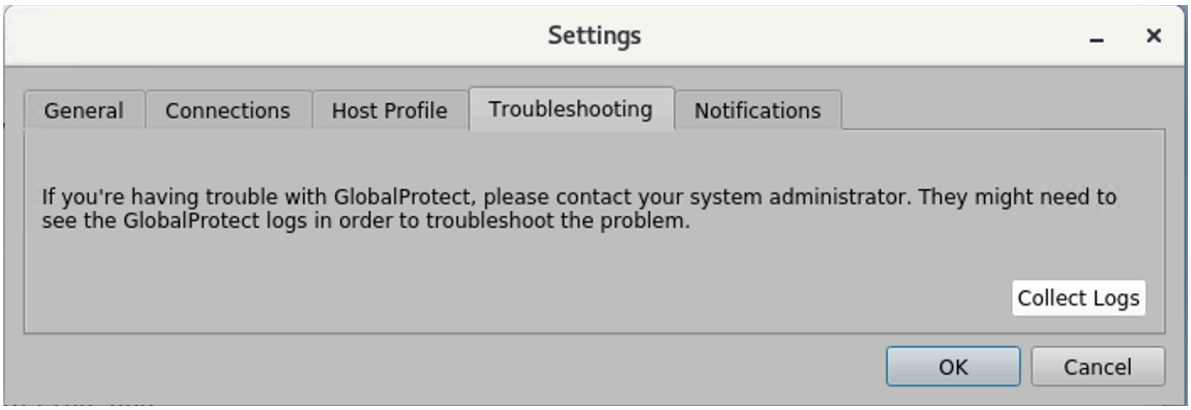
  *For internal mode, the **Connection** tab displays the entire list of available gateways. For external mode, the **Connection** tab displays only the gateway to which you are connected and additional details about the gateway (such as the gateway IP address, location, and uptime).*

 ©2023 Palo Alto Networks, Inc.



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

 ©2023 Palo Alto Networks, Inc.



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).

 ©2023 Palo Alto Networks, Inc.

- 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
```

  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...
```

 ©2023 Palo Alto Networks, Inc.

```
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
```

 ©2023 Palo Alto Networks, Inc.

- 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
```

 ©2023 Palo Alto Networks, Inc.

```
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.

 ©2023 Palo Alto Networks, Inc.

- 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: 4.1.0-23
Copyright(c) 2009-2017 Palo Alto Networks, Inc.
```

 ©2023 Palo Alto Networks, Inc.

Disable the GlobalProtect App for Linux

If your administrator configures the GlobalProtect connect method as **Always On**, you can disable the GlobalProtect app. For example, you might want to disable 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 disabling 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 disable the GlobalProtect app depends on how the administrator configures your GlobalProtect service. This configuration can prevent you from disabling the app entirely or allow you to disable 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 disable 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.

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

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

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

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

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

  Use the **`globalprotect disable`** command to disconnect and disable the GlobalProtect app. If your configuration requires it, you must also specify a reason (using the **`--reason "<reason>"`** option) or a passcode (using the **`--passcode <passcode>`** option).

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

  ```
  user@linuxhost:~$ globalprotect disable --reason "This is my reason
   for disabling GlobalProtect"
  ```

  ```
  user@linuxhost:~$ globalprotect disable --passcode ITp@ssw0rd
  ```

 ©2023 Palo Alto Networks, Inc.

Uninstall the GlobalProtect App for Linux

You can uninstall the GlobalProtect app for Linux using either the dpkg and the apt-get utility. To uninstall the GlobalProtect app, you must run the command with root permissions:

- Begin the uninstallation process by entering the **sudo dpkg -P globalprotect** command.

```
user@linuxhost:~$ sudo dpkg -P globalprotect
(Reading database ... 209181 files and directories currently
 installed.)
Removing globalprotect (4.1.0-12) ...
gp service is running and we need to stop it...
Disable service...
Removing gp service...
gp service has been removed successfully
Removing configuration...
```

- Uninstall the GlobalProtect app for Linux by entering the **sudo apt-get remove globalprotect** command.

 ©2023 Palo Alto Networks, Inc.

GlobalProtect for IoT Devices

GlobalProtect™ is an application that runs on your endpoint (desktop computer, laptop, or server, or IoT device) to protect you by using the same security policies that protect the sensitive resources in your corporate network. For IoT devices, GlobalProtect™ secures traffic to and from the device to any source or destination anywhere on the internet or within your corporate network.

You can install GlobalProtect on IoT devices that are embedded within the following operating systems:

- IoT on Android
- IoT on Raspbian
- IoT on Ubuntu
- IoT on Windows

 ©2023 Palo Alto Networks, Inc.