GlobalProtect App User Guide

4.1

paloaltonetworks.com/documentation

techDOCS paloalto NETWORKS

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 www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

May 6, 2019

Table of Contents

GlobalProtect App for Windows

GlobalProtect™ is a program 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 traffic and allows you to connect to your corporate network to access your company's resources from anywhere in the world.

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

Download and Install the GlobalProtect App for Windows

Before connecting to the GlobalProtect network, you must download and install the GlobalProtect app on your Windows endpoint.

To download and install the app, you must obtain the IP address or fully qualified domain name (FQDN) of the GlobalProtect portal from the administrator. The administrator should also verify the username and password that you can use to connect to the portal. In most instances, you can use 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 4.1, Windows endpoints require Visual C++ Redistributables 12.0.3 for Visual Studio 2013. If you have not already installed any redistributable packages on your endpoint, the GlobalProtect app installs Visual C++ Redistributables 12.0.3 automatically. If you have already installed Visual C++ Redistributables 12.0.2 or an earlier release, you must either uninstall the existing redistributable packages from your endpoint or upgrade to Visual C++ Redistributables 12.0.3 prior to installing the GlobalProtect app.

STEP 1 | Log in to the GlobalProtect portal.

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

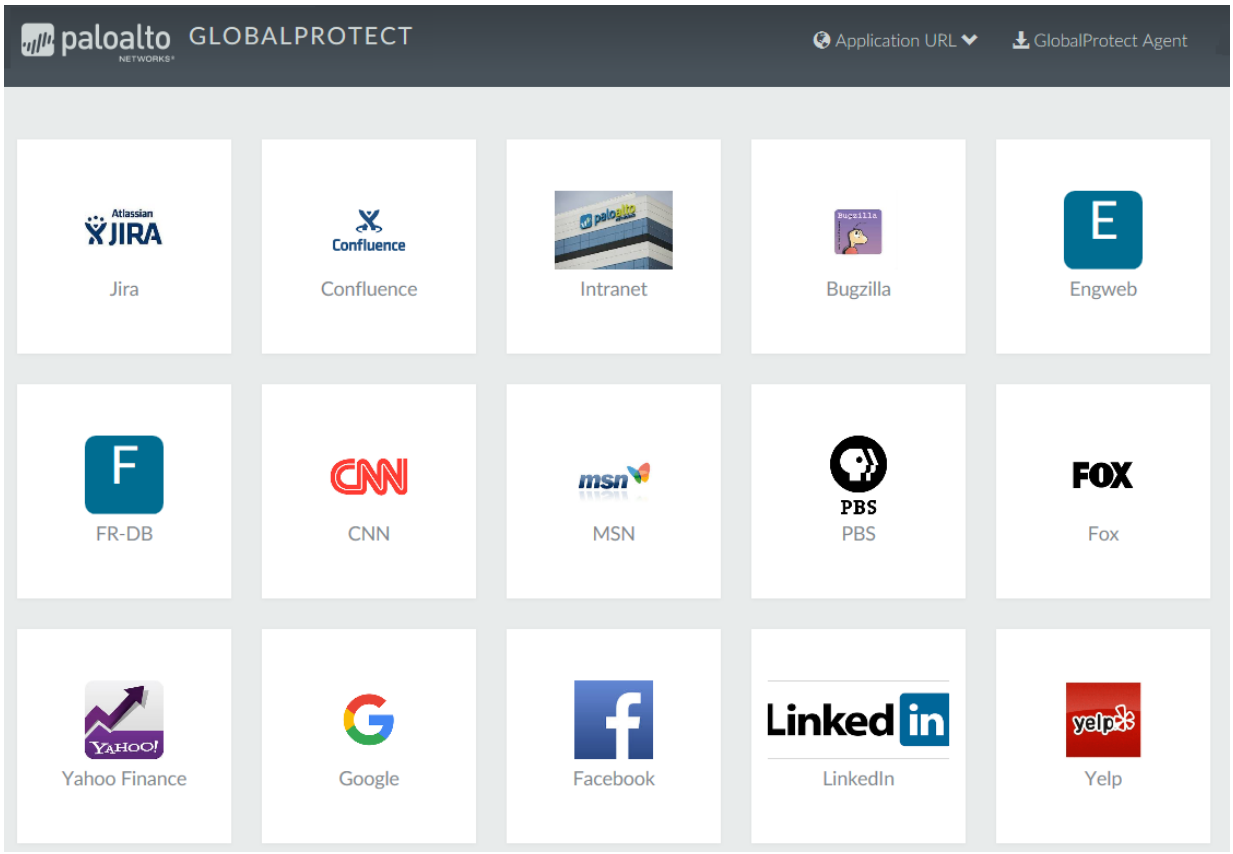
   `https://<portal IP address or FQDN>`

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

STEP 2 | Navigate to the app download page.

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

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



STEP 3 | Download the app.

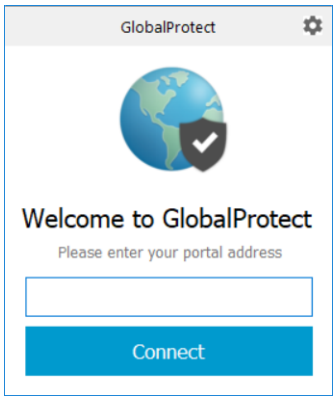
1. To begin the download, click the software link that corresponds to the operating system running on your computer. If you are not sure whether the operating system is 32-bit or 64-bit, ask your system administrator before you proceed.

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

STEP 4 | Complete the GlobalProtect app setup.

1. In the GlobalProtect Setup Wizard, click **Next**.
2. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks \GlobalProtect), or click **Browse** to select a new location and then click **Next** twice.
3. After installation is complete, **Close** the wizard.

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 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.

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 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.
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**.

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.

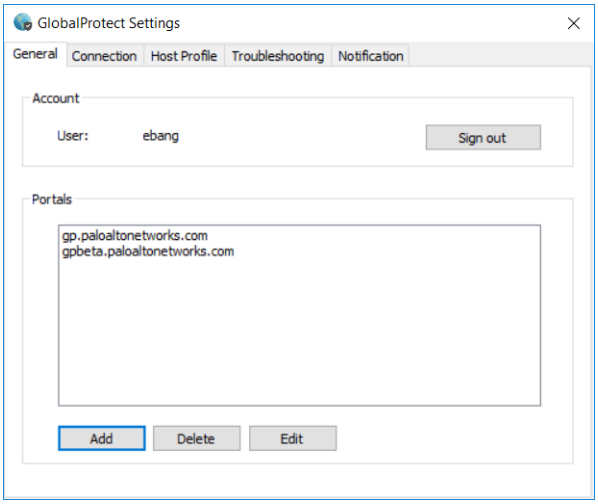
STEP 2 | Open the GlobalProtect app.

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

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).

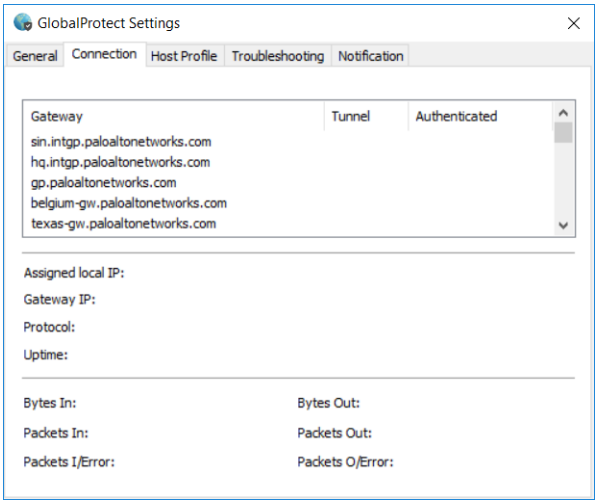


Figure 1: Connection Tab When In Internal Mode

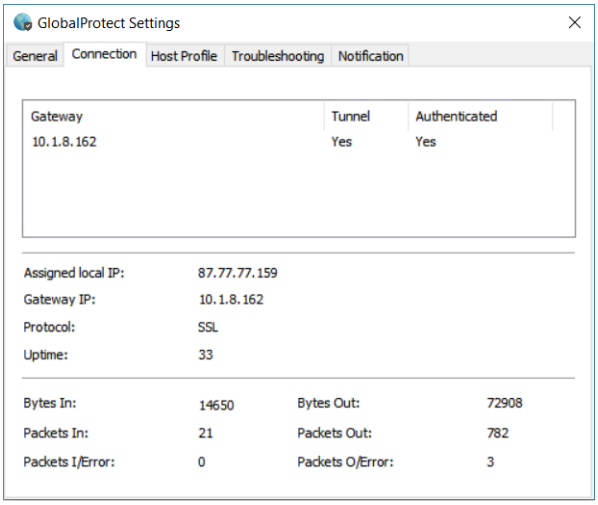
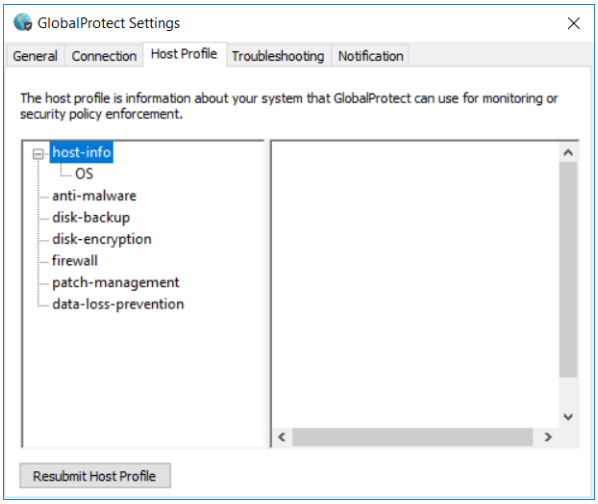


Figure 2: Connection Tab When In External Mode

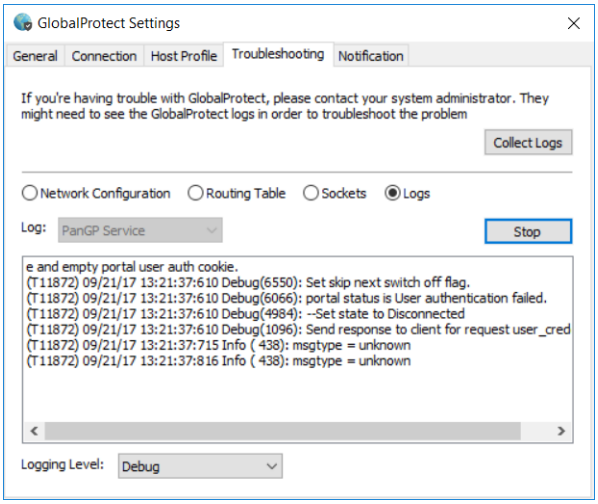
- **Host Profile**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile (HIP). Click **Resubmit Host Profile** to manually resubmit HIP data to the gateway.

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*
-2	*Not Available*
-1	*Unknown*
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.



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.

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.

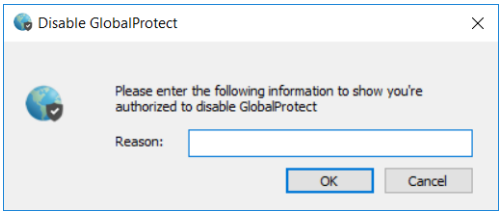
1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the settings icon (⚙) to open the settings menu.
3. Select **Disable**.

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.

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**.

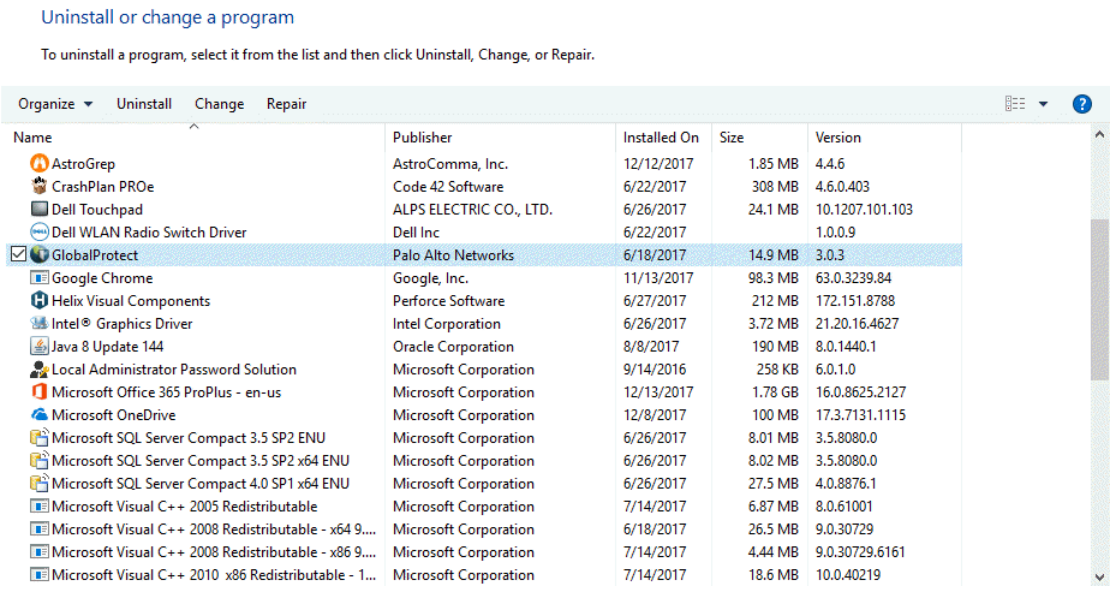
Uninstall the GlobalProtect App for Windows

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

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

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

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



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

Fix a Microsoft Installer Conflict

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

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

STEP 1 | Restart the endpoint.

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

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

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

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

GlobalProtect App for Mac

GlobalProtect™ is a program 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 traffic and allows you to connect to your corporate network to access your company's resources from anywhere in the world.

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

Download and Install the GlobalProtect App for Mac

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. The administrator should also verify the username and password that you can use to connect to the portal. In most instances, you can use 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:

STEP 1 | Log in to the GlobalProtect portal.

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

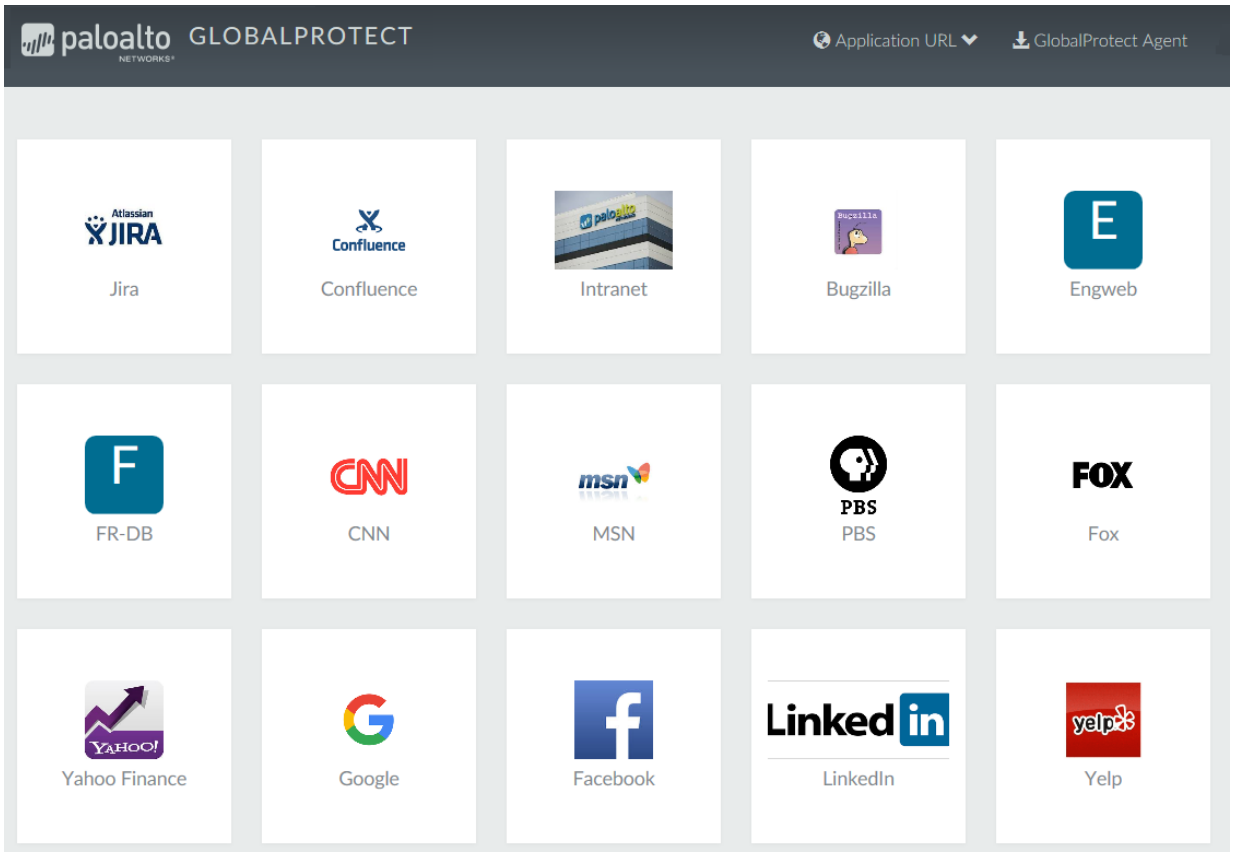
   `https://<portal IP address or FQDN>`

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

STEP 2 | Navigate to the app download page.

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

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

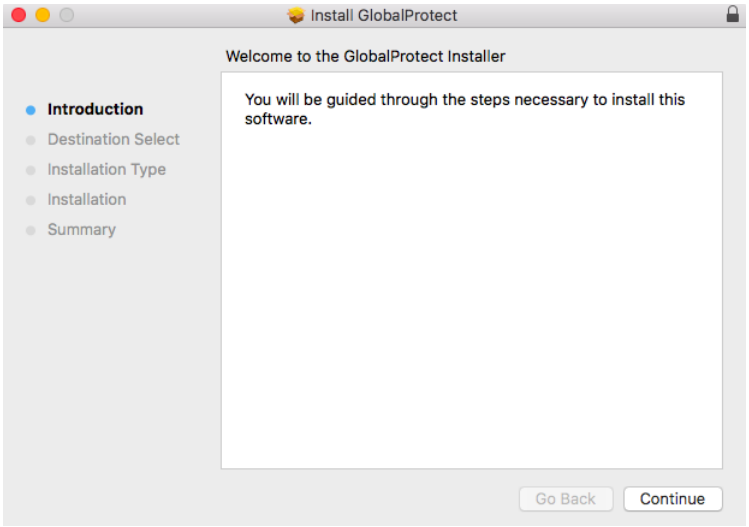


STEP 3 | Download the app.

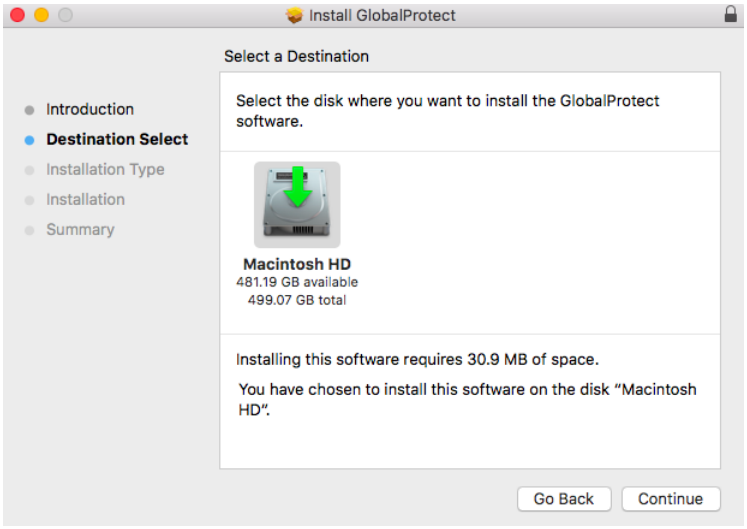
1. Click **Download Mac 32/64 bit GlobalProtect agent**.

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

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



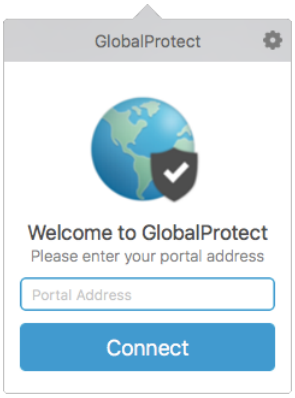
1. From the GlobalProtect Installer, click **Continue**.
2. On the **Destination Select** screen, select the installation folder for the GlobalProtect app, and then click **Continue**.



3. On the **Installation Type** screen, select the **GlobalProtect** installation package check box, and then click **Continue**.
4. Click **Install** to confirm that you want to install GlobalProtect.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to begin the installation.
6. After installation is complete, **Close** the installer.

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 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.

Use the GlobalProtect App for Mac

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.

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 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.
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**.

   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.

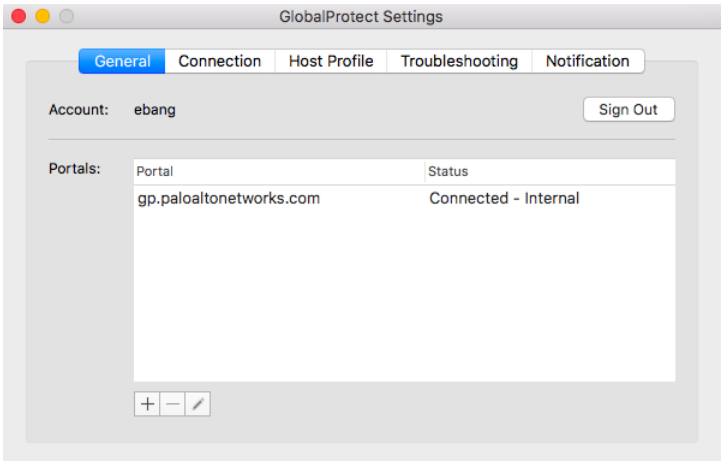
STEP 2 | Open the GlobalProtect app.

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

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).

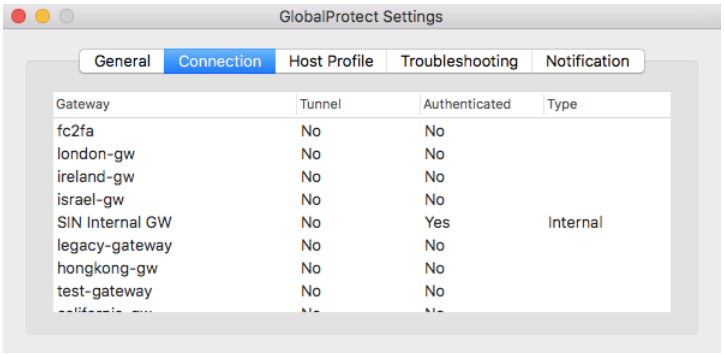


Figure 3: Connection Tab When In Internal Mode

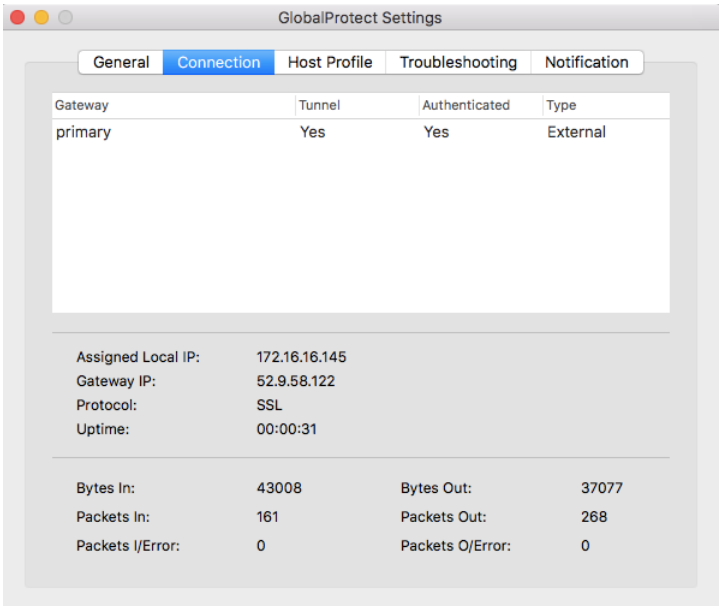
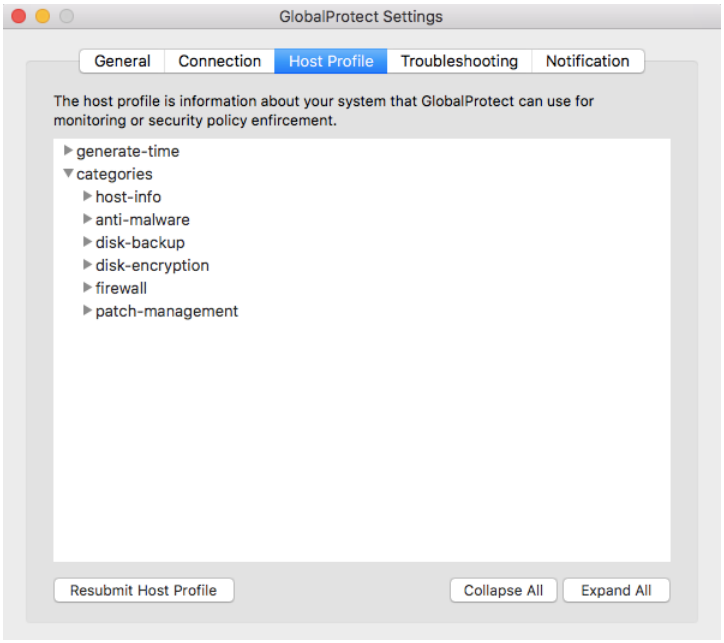


Figure 4: Connection Tab When In External Mode

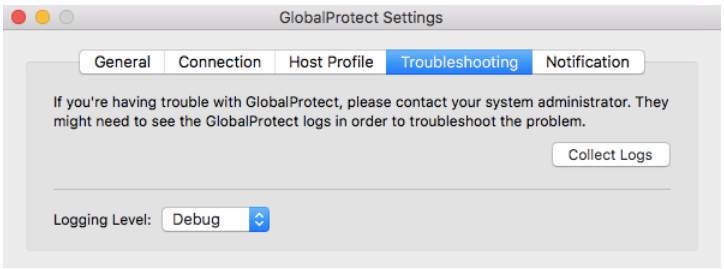
- **Host Profile**—Displays the endpoint data that GlobalProtect uses to monitor and enforce security policies using the Host Information Profile (HIP). Click **Resubmit Host Profile** to manually resubmit HIP data to the gateway.

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*
-2	*Not Available*
-1	*Unknown*
0	*Low*
1	*Moderate*
2	*Important*
3	*Critical*



- **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.

Disable the GlobalProtect App for Mac

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.

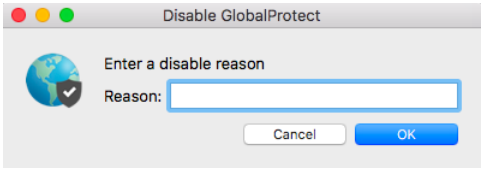
1. Launch the GlobalProtect app by clicking the GlobalProtect system tray icon. The status panel opens.
2. Click the settings icon (⚙) to open the settings menu.
3. Select **Disable**.

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.

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**.

Uninstall the GlobalProtect App for Mac

Use the following steps to uninstall the GlobalProtect app from your Mac 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 Mac endpoints.

On Mac endpoints, you can use the Mac 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 install the **Uninstall GlobalProtect** package. After you install the **Uninstall GlobalProtect** package successfully, the GlobalProtect app is removed from the endpoint.

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

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

STEP 1 | Log in to the GlobalProtect portal.

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

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

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

STEP 2 | Navigate to the app download page.

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

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

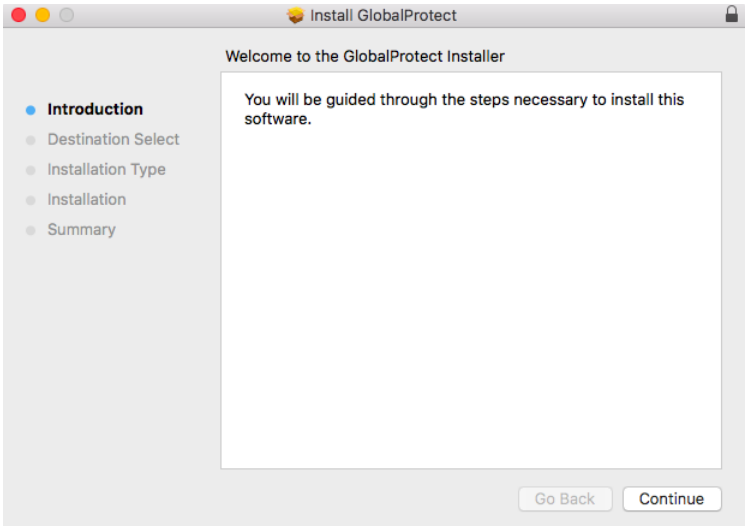
STEP 3 | Download the app.

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

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

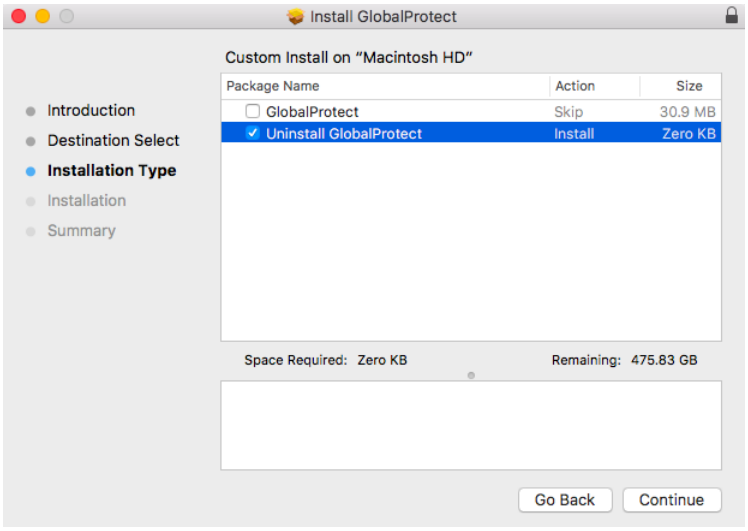
STEP 4 | Uninstall GlobalProtect.

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

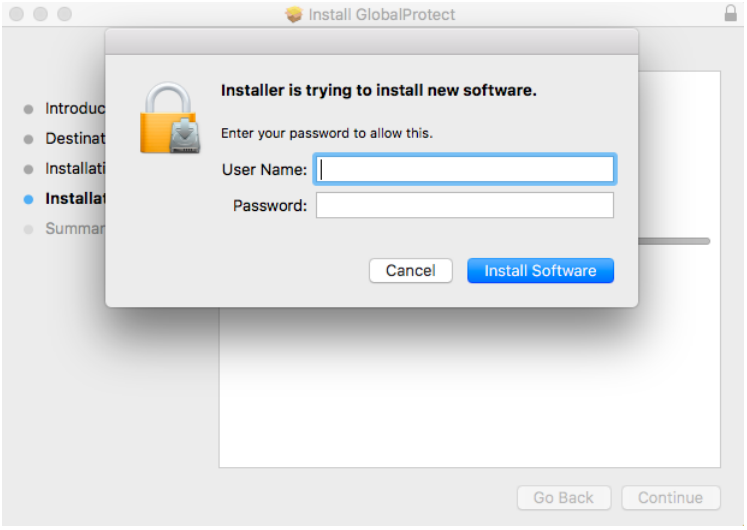


2. On the **Destination Select** screen, click **Continue**.

3. On the **Installation Type** screen, select the **Uninstall GlobalProtect** package check box, and then click **Continue**:

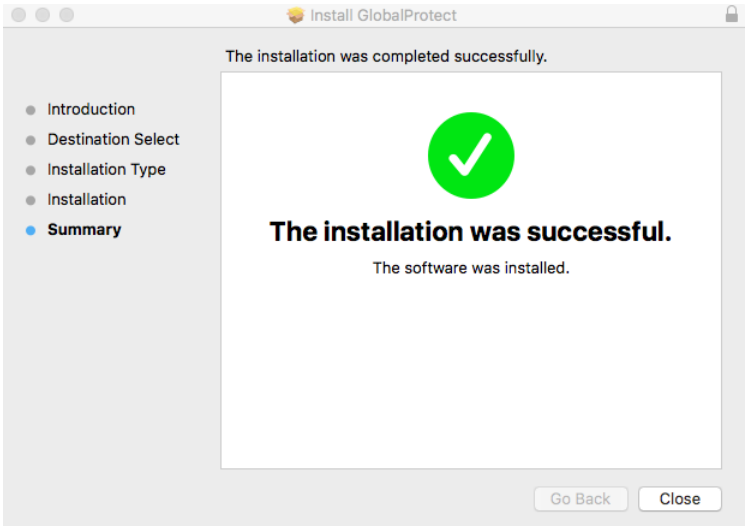


4. Click **Install** to confirm that you want to remove the GlobalProtect app.
5. When prompted, enter your **User Name** and **Password**, and then click **Install Software** to uninstall GlobalProtect.



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

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



Remove the GlobalProtect Enforcer Kernel Extension

When you uninstall the GlobalProtect app for Mac, 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 Mac 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 Mac 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 Mac hard disk:

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

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

GlobalProtect App for Chrome OS

The GlobalProtect™ app for Chrome OS is a software program that runs on your Chromebook, protecting you with the same security policies that protect the sensitive resources on your corporate network. You can use the GlobalProtect app to connect to your corporate network and access your company's internal resources from anywhere in the world.

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

Download and Install the GlobalProtect App for Chrome OS

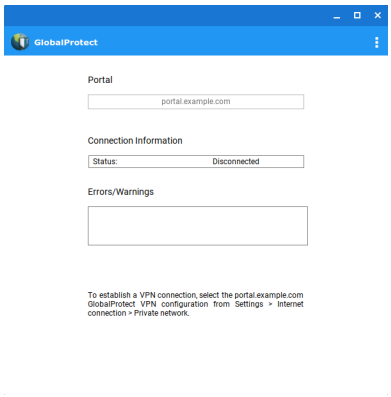
Before you can connect your Chromebook to the GlobalProtect network, you must download and install the app. If your Chromebook is managed by the Chromebook Management Console, your administrator may have automatically pushed the GlobalProtect app to your device and configured the VPN settings. If you do not already have the GlobalProtect app on your Chromebook, you can download it from the Chrome Web Store.

After downloading the app, you will need the IP address or FQDN of the GlobalProtect portal, which you can get from your administrator. In addition, your administrator should verify which username and password you should use to connect to the portal and gateways. Usually this is the same username and password 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 | Download the app from the Chrome Web Store. If you already have the app, skip to 2.

1. If you haven't already, add a Google account on your Chromebook.
2. Search for the app in the Chrome Web Store or go directly to the GlobalProtect app page.
3. Click **Add to Chrome** and then follow the prompts to download and install the app.
4. When successfully installed, the Chrome App Launcher displays the GlobalProtect icon in the list of apps.

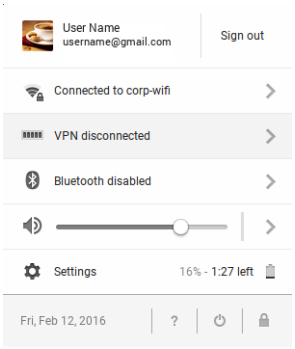
STEP 2 | Configure your VPN settings.



1. In the launcher, click the GlobalProtect icon to launch the app.
2. On the initial setup screen, enter the IP address or FQDN of the GlobalProtect portal supplied by your GlobalProtect administrator.
3. Click **Add Connection** to add the GlobalProtect VPN configuration.

   The app displays the home screen after it adds the VPN configuration to the Internet connection settings of your Chromebook but does not initiate a connection.
4. Close the GlobalProtect app.

STEP 3 | Log in to GlobalProtect.



1. Click the status area at the bottom right corner of the Chromebook.
2. Select **VPN disconnected** and then select the portal that you or your administrator entered when configuring the GlobalProtect VPN settings. The app prompts you to enter your login credentials.

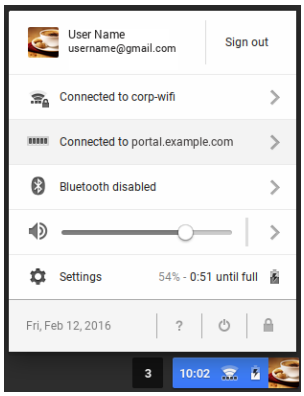
   To view VPN settings before connecting, select the portal from **Settings** > **Private network**, and then click **Connect**.
3. Enter your **Username** and **Password** for the portal and click **Connect**. Repeat this step to enter your credentials for the gateway. If your authentication is successful, you will be connected to your corporate network. If your administrator has set one up, the GlobalProtect welcome page will display. After dismissing the welcome page you can view it at any time from the GlobalProtect menu ( ).

Use the GlobalProtect App for Chrome OS

Because Chrome OS does not allow third-party applications to launch automatically, you must manually initiate a connection each time you want to connect to your corporate network.

STEP 1 | If you are not connected to GlobalProtect, connect now.

When connected to the VPN, the status area displays the VPN icon along the bottom of the Wi-Fi icon ( ). To view the portal to which you are connected, select the status area.



If you are not connected, you will see **VPN disconnected**.

1. Click the status area at the bottom right corner of the Chromebook.
2. Select **VPN disconnected** and then select the portal that you or your administrator entered when configuring the GlobalProtect VPN settings.

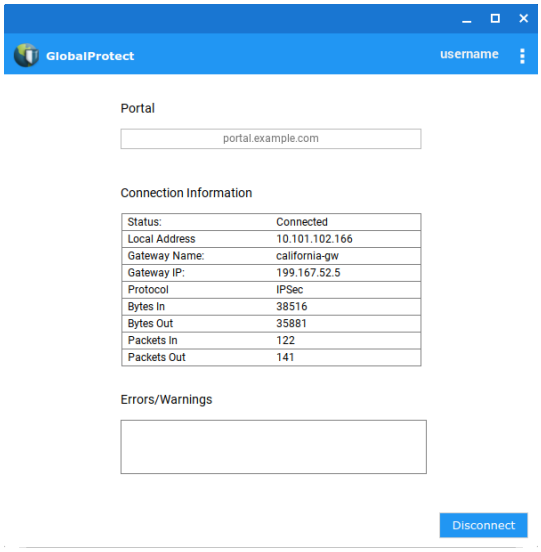
   To view VPN settings before connecting, select the portal from **Settings** > **Private network**, and then click **Connect**.
3. If prompted, enter your **Username** and **Password** for the portal and click **Connect**.
4. If prompted, enter your **Username** and **Password** for the gateway and click **Connect**. If your authentication is successful, you will be connected to your corporate network.

STEP 2 | Open the application.

From the Chrome App Launcher, click the GlobalProtect icon to launch the app.

STEP 3 | Continue to use the app to perform any of the following tasks:

- View information about your network connection.



GlobalProtect displays the following information about your network connection:

- **Portal**—Portal address or FQDN.
- **Connection Information**—Displays information about your connection, including the gateway to which you are connected.
- **Errors/Warnings**—Displays errors and warnings about your connection to help you troubleshoot any connection issues.

- Log in with a new password. If your password for accessing your corporate network changes, you will need to sign-out of GlobalProtect to clear your credentials.

  1. Click your username in the top-right corner and select **Sign-Out**. When you next log in, you must enter your credentials for the portal and gateway.
  2. Connect to the portal and gateway as described in 1.

- Reset your VPN connection settings.

  1. If connected, select **Disconnect**.
  2. Select the GlobalProtect menu (⋮) and select **Reset GlobalProtect**.
  3. Select **Yes** when asked to confirm.
  4. Enter the IP address or FQDN of the portal supplied by your GlobalProtect administrator.
  5. Connect to the portal and gateway as described in 1.

- Troubleshoot connection issues.

  Select the GlobalProtect menu (⋮) and then select either of the following options:

  - **Notifications**—Depending on how the administrator has configured GlobalProtect, you may be able to view notification messages which can include messages or instructions from the administrator.
  - **Collect Logs**—By default, GlobalProtect creates debug logs to help troubleshoot issues should they arise. Select this option to package the debug logs into a ZIP file and send them to your IT help desk so that they can identify and resolve any issues.

Disconnect from GlobalProtect on a Chromebook

You can disconnect from the GlobalProtect VPN in any of the following ways.

- Disconnect from the VPN through the GlobalProtect app for Chrome OS.

  If the GlobalProtect administrator has selected the option to save user credentials in the GlobalProtect portal configuration, the credentials are automatically saved when you disconnect from the VPN. To clear the credentials and force you to enter them when you reconnect, use the Sign-Out option.

  From the Chrome App Launcher, click the GlobalProtect icon to launch the app, and then do either of the following:

  - **Disconnect** the VPN connection but retain your user credentials. When you next log in, you will not be prompted to enter your credentials if your administrator has permitted GlobalProtect to save them.
  - Click your username in the top-right corner and select **Sign-Out** to disconnect the VPN connection and clear your user credentials. When you next log in, you must enter your credentials for the portal and gateway.

- Disconnect from the VPN through the Chromebook settings.
  1. Click the status area at the bottom right corner of the Chromebook.
  2. Select the portal to which you are connected.
  3. Next to the portal name, select **Disconnect**.

     As an alternate method, you can also select the portal from **Settings** > **Private network**, and then click **Disconnect**.

Uninstall the GlobalProtect App for Chrome OS

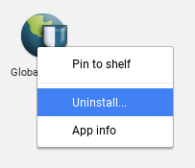
Use the following steps to uninstall the GlobalProtect app from your Chromebook. Keep in mind that by uninstalling the app, you will no longer have VPN access to your corporate network and your endpoint will not be protected your company's security policies.

You can uninstall the GlobalProtect app from Chromebooks only if it is installed manually or is standalone. If the app is deployed from the Google Admin console, you cannot uninstall it.

STEP 1 | Exit the GlobalProtect app.

STEP 2 | Click the Chrome App Launcher and select **All Apps**.

STEP 3 | Two-finger tap (or **Alt**-click) on the app and select **Uninstall**.



STEP 4 | When prompted to confirm the removal, click **Remove**. The Chromebook uninstalls the app and removes it from the launcher.

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 traffic and allows you to connect to your corporate network 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

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 Mac endpoint, you can open a terminal and then copy the file:

   ```
   macUser@mac:~$ scp
   ~/Downloads/PanGPLinux-4.1.0.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-4.1.0.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 proxy configuration, configure the proxy settings.

The GlobalProtect app for Linux supports only manual proxy server configuration and obtains the proxy settings from the **`https_proxy`** or **`HTTPS_PROXY`** environment variable. If you later change the system proxy configuration, verify that the terminal from which GlobalProtect runs uses the proxy environment variable. If you do not see the new settings, log out and back in to populate the new setting to the environment variable.

STEP 3 | Install the app package using either the **`sudo dpkg -i <gp-app-pkg>`** or **`apt-get install <gp-app-pkg>`** command where **<*gp-app-pkg*>** is the name of your distribution package for your Linux version.

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-4.1.0.0-19.deb
Selecting previously unselected package GlobalProtect.
(Reading database ... 67776 files and directories currently installed.)
Preparing to unpack GlobalProtect_deb-4.1.0.0-19.deb ...
Start installing gp...
Unpacking GlobalProtect (4.1.0-19) ...
Setting up GlobalProtect (4.1.0-19) ...
Enable gp service...
Starting gp service...
Create symlink for gp cli...
```

```
user@linuxhost:~$ sudo
apt-get install GlobalProtect_deb-4.1.0.0-23.deb
[sudo] password for gpqa:
Reading package lists... Done
Building dependency tree
```

```
Reading state information... Done
Note, selecting 'globalprotect' instead of '/home/gpqa/Downloads/
GlobalProtect_deb-4.1.0.0-24.deb'
The following packages were automatically installed and are no longer
 required:
  linux-headers-4.10.0-28 linux-headers-4.10.0-28-generic linux-
image-4.10.0-28-generic linux-image-extra-4.10.0-28-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-4.1.0.0-24.deb globalprotect
 all 4.1.0-24 [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-4.1.0.0-24.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-4.1.0.0-24.deb ...
Start installing gp...
Unpacking globalprotect (4.1.0-24) ...
Setting up globalprotect (4.1.0-24) ...
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:~$
```

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

Prompt mode:

```
>> help
Usage: only the following commands are supported:
collect-log            -- collect log information
connect                -- connect to server
disconnect             -- disconnect
disable                -- disable connection
```

```
import-certificate     -- import client certificate file
quit                   -- quit from prompt mode
rediscover-network     -- network rediscovery
remove-user            -- clear credential
resubmit-hip           -- resubmit hip information
set-log                -- set debug level
show                   -- show information
```

Command-line mode:

```
user@linuxhost:~$ globalprotect help
Usage: only the following commands are supported:
collect-log            -- collect log information
connect                -- connect to server
disconnect             -- disconnect
disable                -- disable connection
import-certificate     -- import client certificate file
quit                   -- quit from prompt mode
rediscover-network     -- network rediscovery
remove-user            -- clear credential
resubmit-hip           -- resubmit hip information
set-log                -- set debug level
show                   -- show information
```

STEP 6 | Use the GlobalProtect App for Linux.

Use the GlobalProtect App for Linux

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

- Connect to a GlobalProtect portal
- Import a certificate
- Connect to a gateway
- Verify the status of and view details about your connection
- Rediscover the network
- Clear the credentials for the current user
- View GlobalProtect notifications
- View the Welcome page
- View errors
- Collect logs
- Display the GlobalProtect version

- 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...
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-gateways** 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-gateways
Name                Address
-----------------------------
gw1                 192.168.1.180
gw2                 192.168.1.181
user@linuxhost:~$ globalprotect connect --gateway 192.168.1.180
Retrieving configuration...
Discovering network...
Connecting...
Connected
```

- Verify the status of and view details about your connection.

```
user@linuxhost:~$ globalprotect show --status
GlobalProtect status: Connected
user@linuxhost:~$ globalprotect show --details
Assigned IP address: 192.168.1.132
Gateway IP address: 192.168.1.180
Protocol: IPSec
Uptime(sec): 231
```

- Rediscover the network.

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

```
user@linuxhost:~$ globalprotect
rediscover-network
Disconnecting...
Retrieving configuration...
Retrieving configuration...
Discovering network...
Connecting...
Connecting...
Connected
GlobalProtect status: Connected
```

- Clear the credentials for the current user.

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

```
user@linuxhost:~$ globalprotect
remove-user
Credential will be cleared and current tunnel will be terminated.
Do you want to continue(y/n)?y
Clear is done successfully.
user@linuxhost:~$ globalprotect connect --portal 192.168.1.179
Retrieving configuration...
Disconnected
192.168.1.179 - portal:local:Enter login credentials
username:user1
Password:
Retrieving configuration...
Discovering network...
Connecting...
Connected
```

- Resubmit host information to the gateway.

  Use the **`globalprotect show --host-state`** command the current host information about your endpoint and 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 Welcome page.

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

- View errors.

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

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

- Collect logs.

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

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

- Display the version of the GlobalProtect app for Linux.

```
user@linuxhost:~$ globalprotect show --version
GlobalProtect: 4.1.0-23
Copyright(c) 2009-2017 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
```

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:

- Uninstall the GlobalProtect app for Linux using dpkg.

```
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 using ap-get.

```
user@linuxhost:~$ sudo apt-get remove GlobalProtect_deb-4.1.0.0-23.deb
Reading package lists... Done
Building dependency tree
Reading state information... Done
```