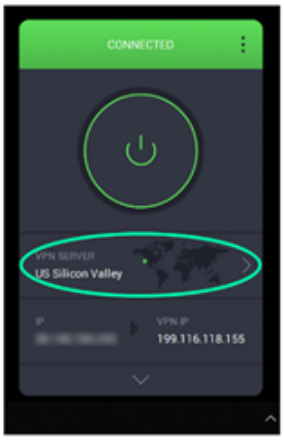
Understanding Advanced Settings on the Desktop PIA Client

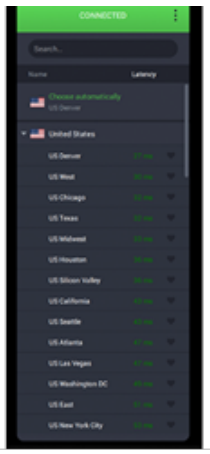
Travis - 2022-08-12 - Application & Features

SERVERS/REGIONS AND FAVORITES

The most commonly adjusted setting for most users is the region they are connecting to. To access a complete list of the region selections available to you, click on the VPN SERVER widget, shown circled in the image below.

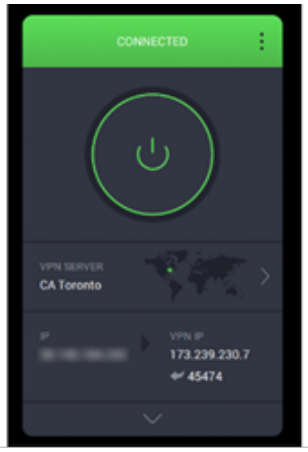


Clicking on the VPN SERVER selection shown above will present you with a full list of servers, as shown below. You can minimize or expand countries with the arrow next to a country's name. The latency shown next to each region is an indicator of the efficiency of the pathway between your device and the server. By default, the application is set to ‘Choose Automatically’ which is the option visible at the top of the server list; this option will connect to the server with the lowest latency. The heart next to each server can be used to indicate the region as a favorite. This will add the option to the QUICK CONNECT menu. Clicking on the left-pointing arrow at the top left of this interface will return you to the settings interface.



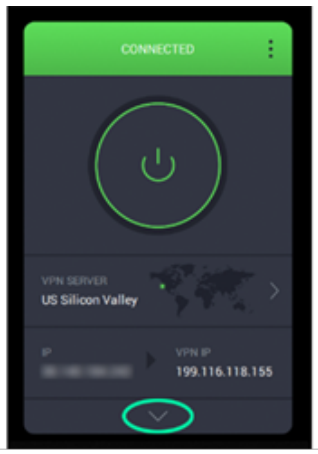
IP WIDGET

The IP widget will display your actual IP, and when connected, will also display the IP you are being masked with. If you are using the Port Forwarding feature, the forwarded port will also be shown here.



BASIC/EXPANDED DISPLAY

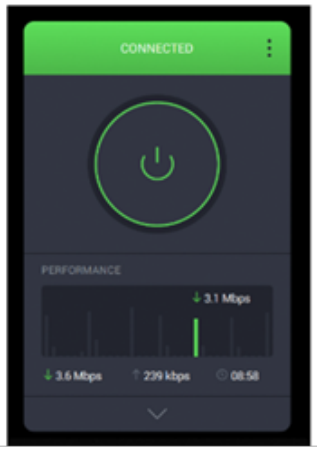
Returning to the DEFAULT DISPLAY, there is an arrow at the bottom that will open the EXPANDED DISPLAY. This is what you will use to customize the DEFAULT DISPLAY as well as change advanced settings.



Clicking on this will display the EXPANDED DISPLAY which will look similar to the image shown below. We will systematically go over everything shown, starting with how to customize the DEFAULT DISPLAY. There is a switch that can be toggled in the top right of each widget, below the VPN SERVER and IP widgets are marked as favored, while QUICK CONNECT, PERFORMANCE, USAGE, QUICK SETTINGS, SUBSCRIPTION, and SNOOZE are not. If a widget is marked as favored, it will also be shown in the DEFAULT DISPLAY.

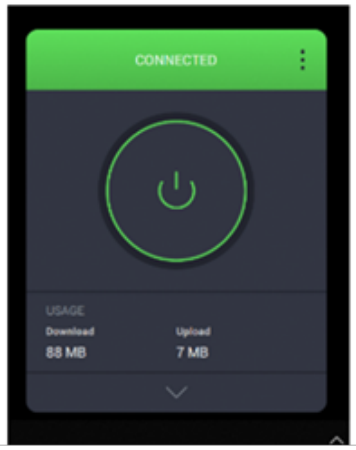
PERFORMANCE WIDGET

The PERFORMANCE widget will show your history of data that flows through the application. Every five seconds the display will update, showing how much was downloaded over the past five seconds. The numeric display at the bottom of the widget shows live download and upload traffic, as well as the duration of the connection. Please be aware, this is the traffic that has and is occurring, not a speed test.



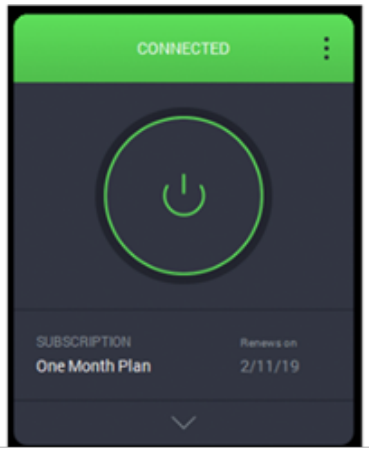
USAGE WIDGET

The USAGE widget shows the total amount you have downloaded and uploaded since establishing the connection.



SUBSCRIPTION WIDGET

The SUBSCRIPTION widget will display the status of the subscription logged into the app.

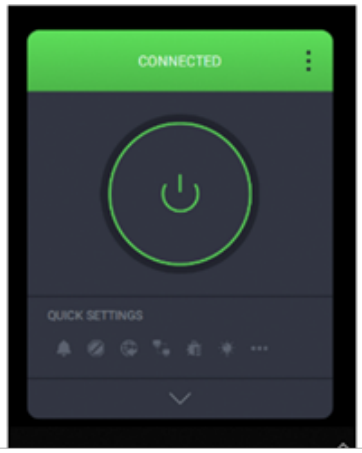


VPN SNOOZE WIDGET

The VPN SNOOZE widget allows you to specify a planned pause of the VPN connection, temporarily stopping the connection and starting it again after the duration specified. More details about the VPN Snooze feature are available here.

QUICK SETTINGS WIDGET

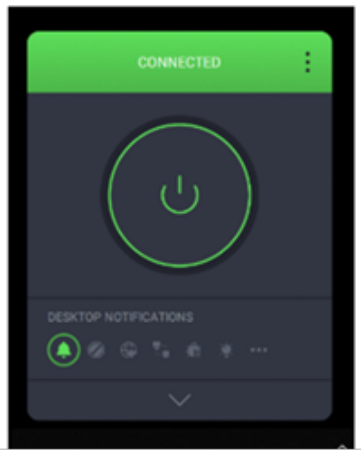
In this section of the guide, we will go over each of the options available in the SETTINGS widget. This will cover all the extra features available in the new PIA Client application.



Desktop Notifications

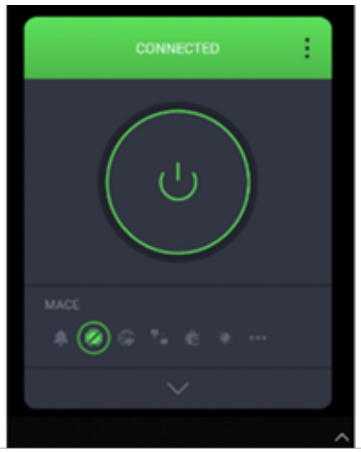
In the image below, the Desktop Notifications option is turned on. Desktop Notifications will

provide pop-up text boxes in the corner of your screen to notify you of any changes to your connectivity, such as an unexpected disconnection.



MACE

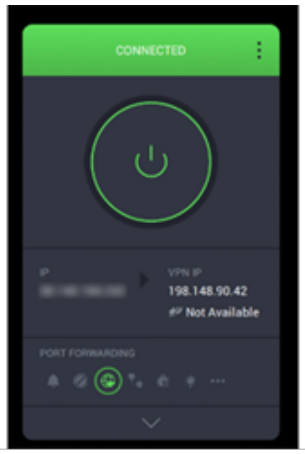
In the image below the MACE, the feature is turned on. MACE is a DNS-based ad blocker that blocks known advertising and malware domains. As it operates at the DNS level, it can only block entire domains and as such won't block ads that are served from the same domain as legitimate websites. Inversely, it can also in some situations end up blocking an entire website because it tried blocking an ad. A famous case of this is https://www.google-analytics.com/ which is used by the sponsored links in Google searches. As a result, some users complain about not being able to access Google results. More details about MACE are available here.



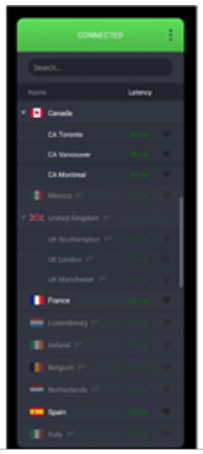
Port Forwarding

In the image below, the Port Forwarding feature is enabled. The Port Forwarding option can

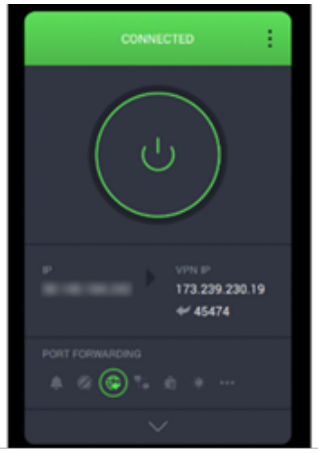
be used to potentially optimize torrent performance. To use this feature, you must connect to a server on which port-forwarding is enabled. In the image below, in the IP widget, the message Not Available is displayed, indicating that port-forwarding is not available on this particular server. The next image will show how to identify servers that can use port forwarding.



With the Port Forwarding feature turned on, expanding the VPN SERVER widget again will show a minor change. When Port Forwarding is enabled, servers that can be utilized for the feature will show in a brighter white text, while those that can not port-forward be grayed out and have an icon next to them indicating port forwarding is not available from that region.

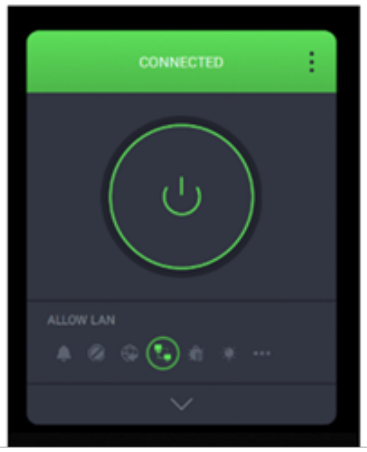


With Port Forwarding enabled, and a server that supports the feature selected, the application will display the forwarded port that has been assigned to your connection. You can then input this information into your torrent client, or any other implementation.



Allow LAN

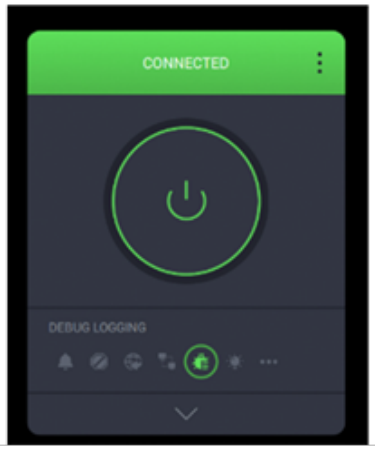
In the following image Allow LAN is turned on. If your network is properly configured to facilitate LAN communication, turning on the Allow LAN feature will allow you to do so with the VPN connected.



Debug Logging

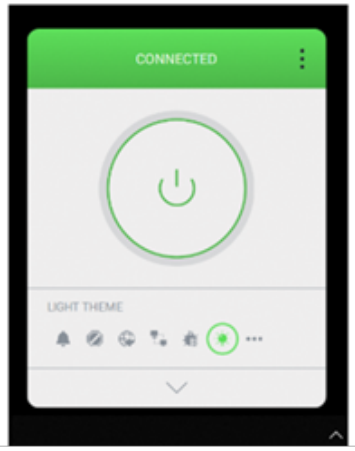
In the image below the Debug Logging feature is turned on. This feature is important if you find that you are experiencing problems. This will allow the application to collect connectivity and functionality logs. In the event you need to contact customer support, this can be helpful for the support team and they may request you provide them with the Client logs. Rest assured, these logs are not traffic logs, PIA does not monitor, restrict, or block web traffic, not on our servers and not on your system; the logs this feature generates are exclusively for troubleshooting purposes and contain no information which may identify a

user upon submission.



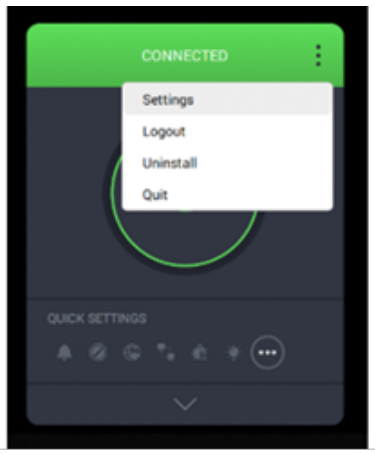
Light Theme

The image below is a demonstration of the Light Theme feature. As you can see, this largely inverts the color scheme of the PIA Client. This feature is purely cosmetic.



More Settings...

In the following image More Settings... has been highlighted in the SETTINGS widget, additionally, the top-right menu has been expanded to show another way to access the same thing. This option opens the most extensive menu of the client, containing all the settings available in the EXPANDED DISPLAY as well as a few more advanced settings.

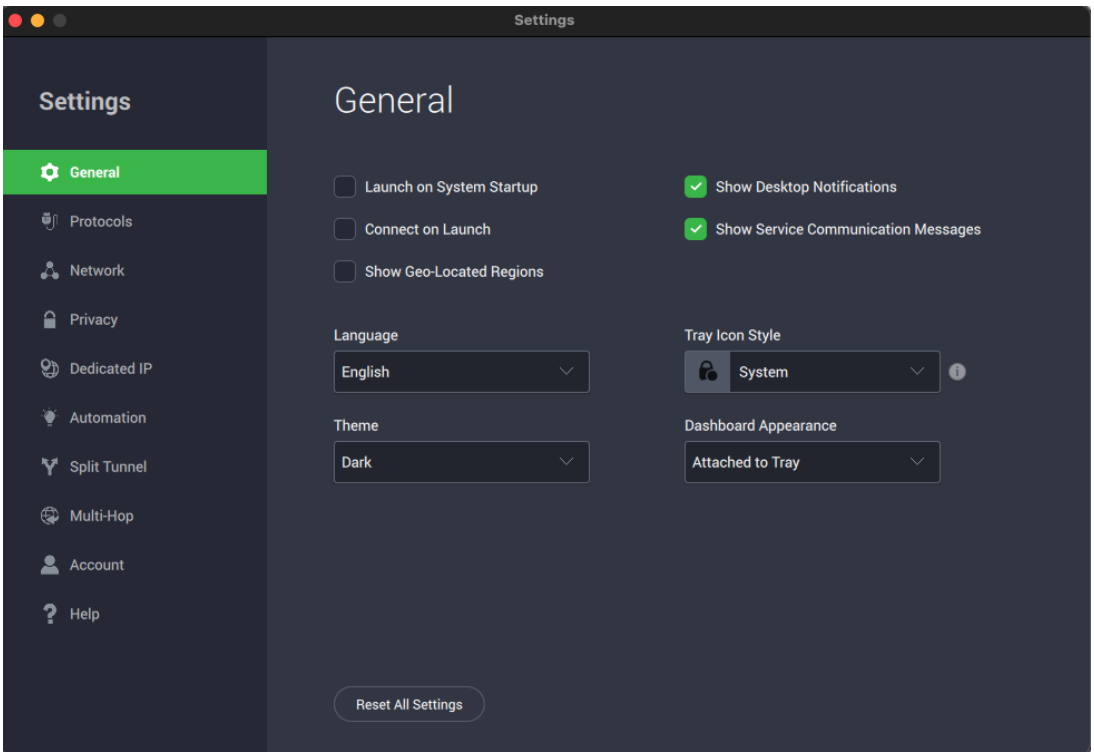


PREFERENCES

General

The first section of the settings interface is General, which controls the basic functions of the VPN and some graphical settings.

- Launch on System Startup: This will ensure that the application is launched upon boot.
- Connect on Launch: This will instruct the VPN to attempt to connect to a specified region on connect.
- Show Desktop Notifications: This was already explained in the section above.
- Language: will specify what language the application interface displays.
- Theme: This allows for selection of Dark or Light, demonstrated in the explanation of the Light Theme option above and System (Windows only and automatically sets the theme based on how it is set in Windows).
- Tray Icon Style: This allows users to select a particular icon based on needs.
- Dashboard Appearance: This allows you to choose how the application displays when the GUI is open. The GUI is attached to the icon when Attached to Tray is enabled. A window will detach the GUI from the tray and allow for a more mobile experience.

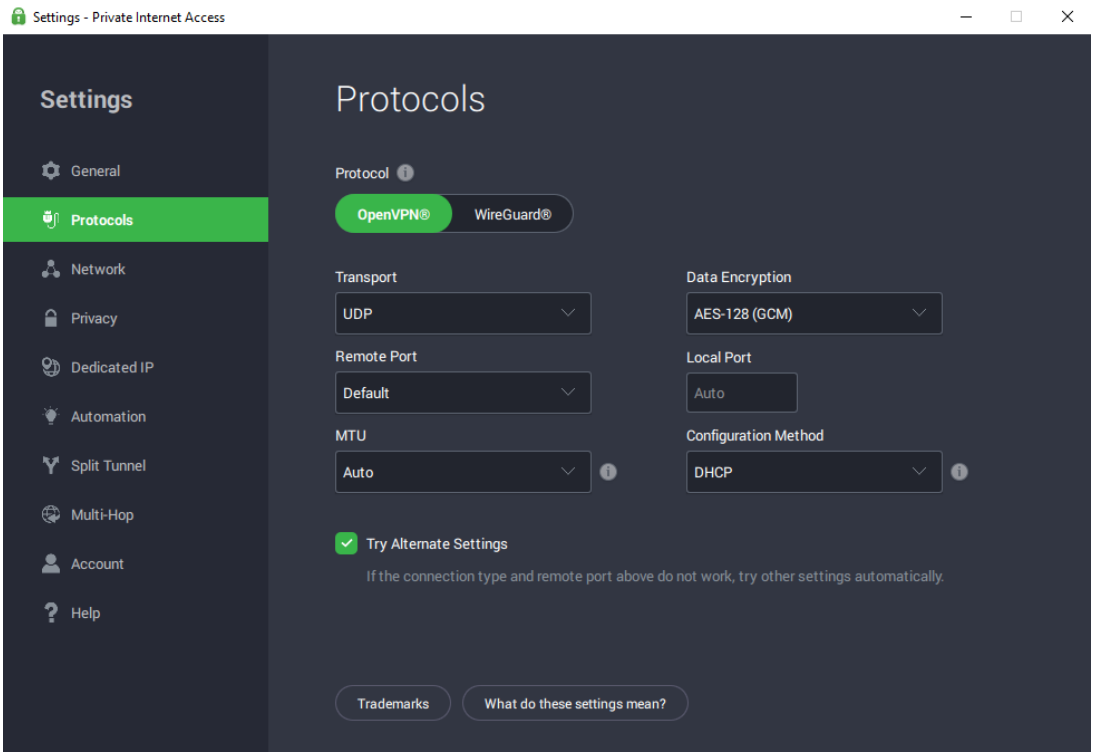


Protocols

The next section is Connection. This section contains specific settings which can be altered to either troubleshoot a connectivity issue or provide additional support and security.

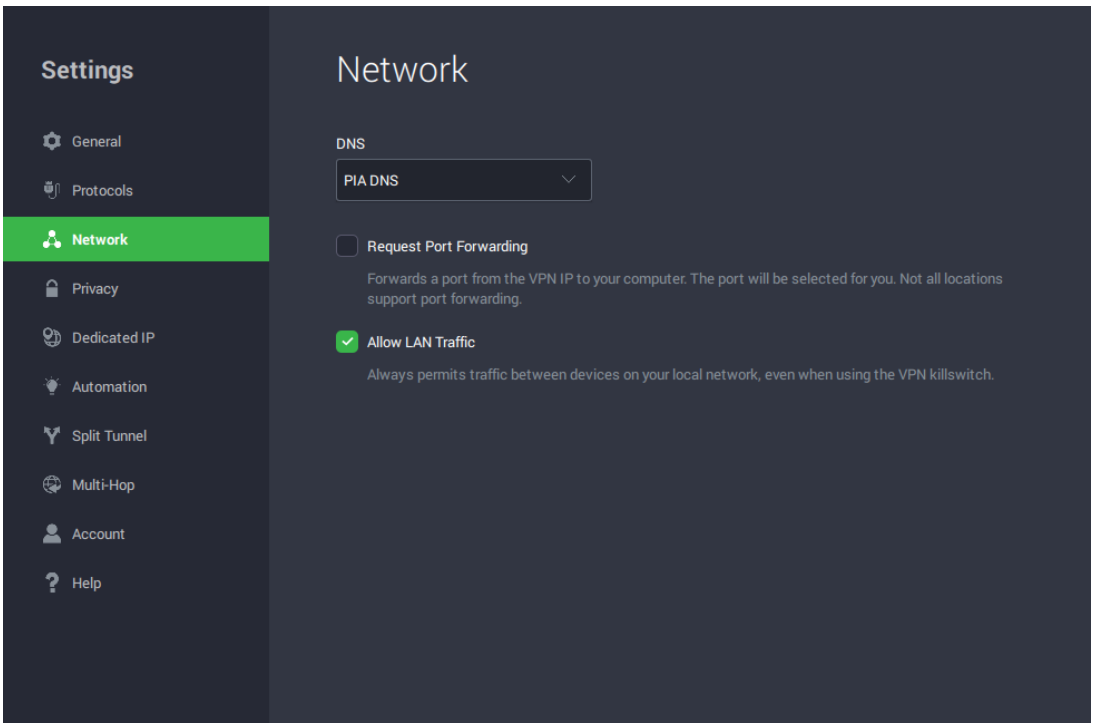
- Protocol: The protocol toggle allows you to choose between the Wireguard and OpenVPN protocols.
- Transport: This setting will allow you to specify the use of UDP or TCP. In general, UDP will usually provide the best performance for most users, but TCP may be necessary for certain networks.
- Data Encryption: There are four available options, GCM and CBC for both AES-128 and AES-256 encryption. PIA exclusively uses encryption that has not been cracked and is known to be secure. All of these options will provide you security, but the higher levels of encryption will have a greater impact on performance.
- Remote Port: This setting allows specification of the specific port to be used in association with the connection type. For security reasons, the PIA VPN service only allows traffic on certain ports. Some users may need to specify a certain port for performance issues related to restrictions on the network they are connecting from.
- MTU: This option determines the maximum packet size allowed through the tunnel and offers three settings: Auto, Large Packets, and Small Packets. Auto detects automatically and is best for most connections. Large Packets can be considered the most efficient if the connection is reliable. Small Packets is less efficient but is best for unreliable connections.

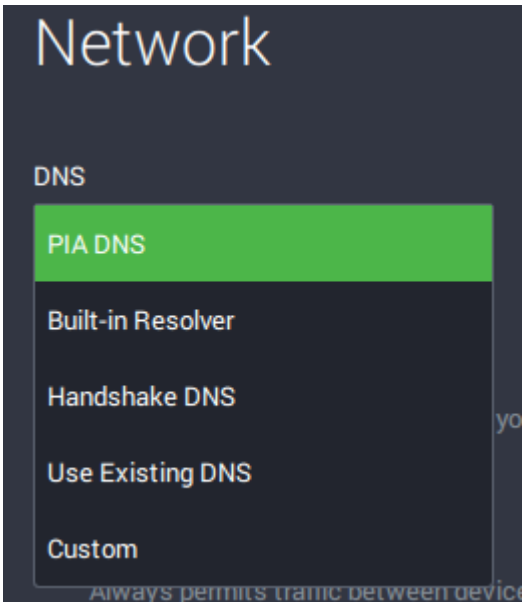
- Data Encryption: Upon changing the Data Encryption setting, the available options within Data Authentication will change. The GCM Data Encryption settings must utilize GCM Data Authentication.
- Local Port: By default, the application will randomly select the local port used; the vast majority of users will never need to modify this setting. Advanced users operating with highly restrictive firewalls may utilize this setting to specify a port that will work with their configuration.
- Use Small Packets: This setting will cause the connection to modify the MTU setting of the connection, effectively changing the packet size of the traffic occurring over the connection — this can be used to resolve packet loss issues.
- Try Alternate Settings: When checked, the application will by default, change the connection type and remote port until a connection is established.



Network

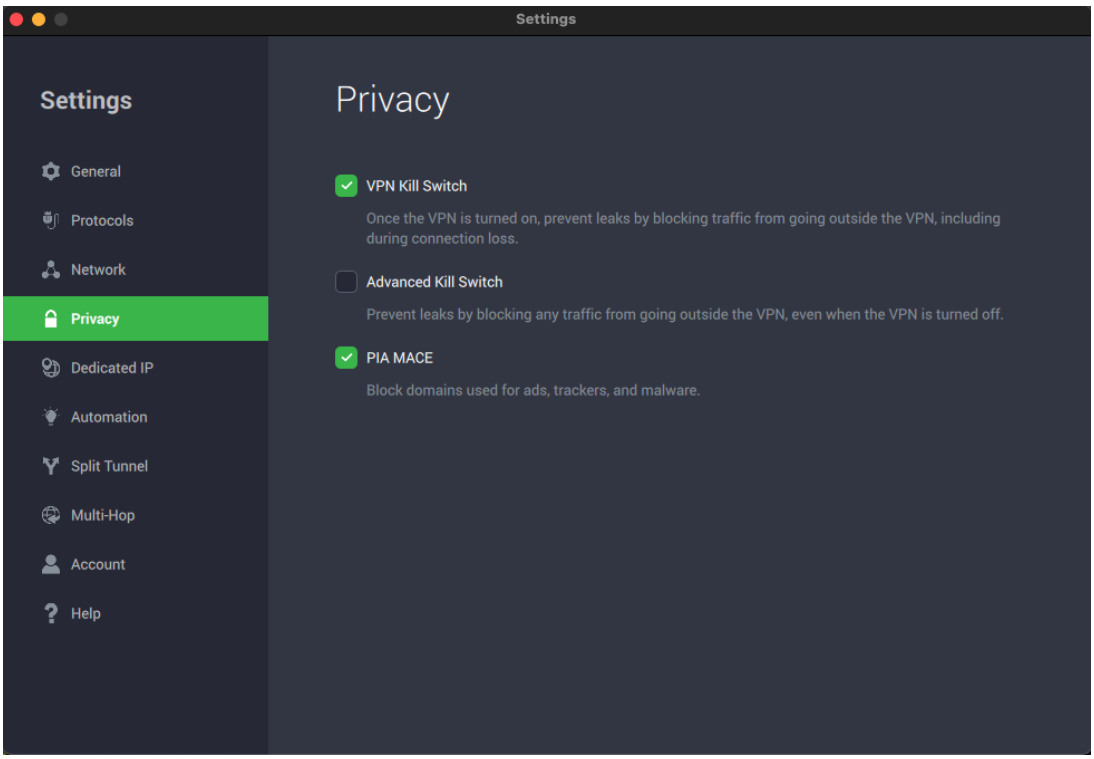
The next section is Network. The PIA Client will auto-connect you to PIA's DNS Servers. It will also allow you to choose to use your device's existing DNS, Handshake DNS, Built-in-Resolver, or to set up a custom DNS server. Also within this section, you will also find another area to toggle the Port Forwarding and Allow LAN Traffic features, also available in the SETTINGS widget.



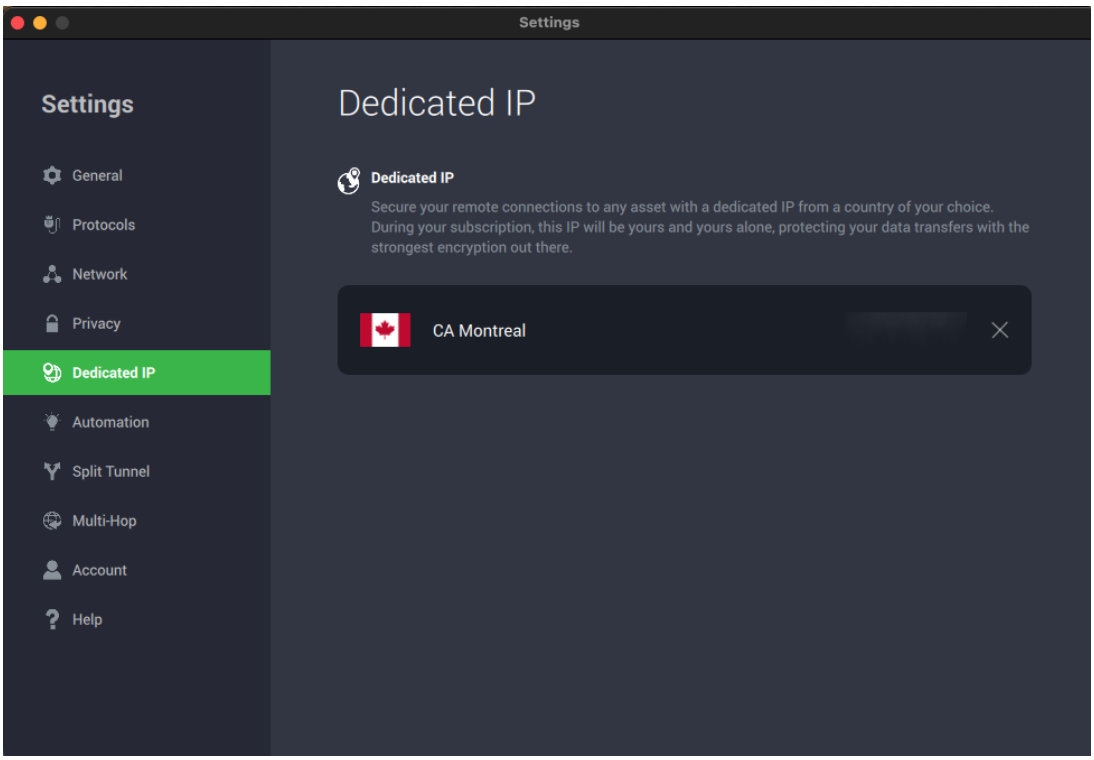


Privacy

The following section is Privacy. This allows access to the VPN Killswitch feature, which will prevent web traffic outside the VPN tunnel. You can also turn MACE on or off, which is a DNS level ad-blocker and can be easily accessed from the SETTINGS widget.



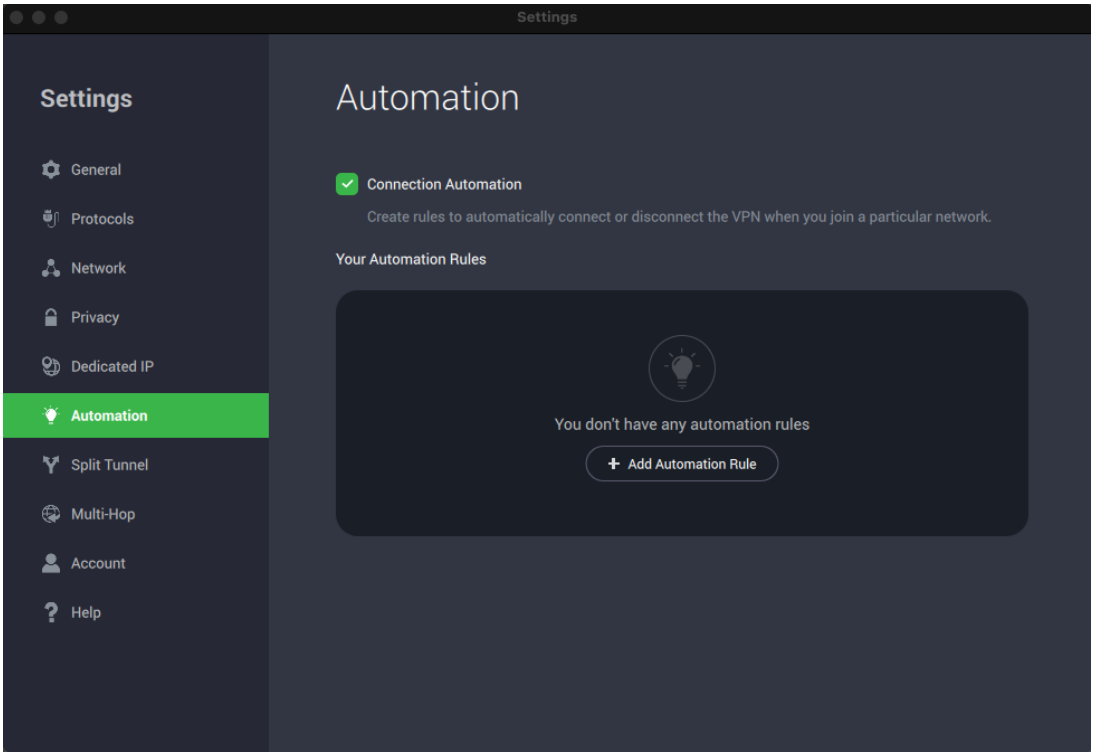
Dedicated IP



The Dedicated IP tab is where you will see the Dedicated IP you have purchased either through the client control panel or when you first signed up for the application. For more information regarding Dedicated IPs, please see the article Do you offer dedicated IP addresses?

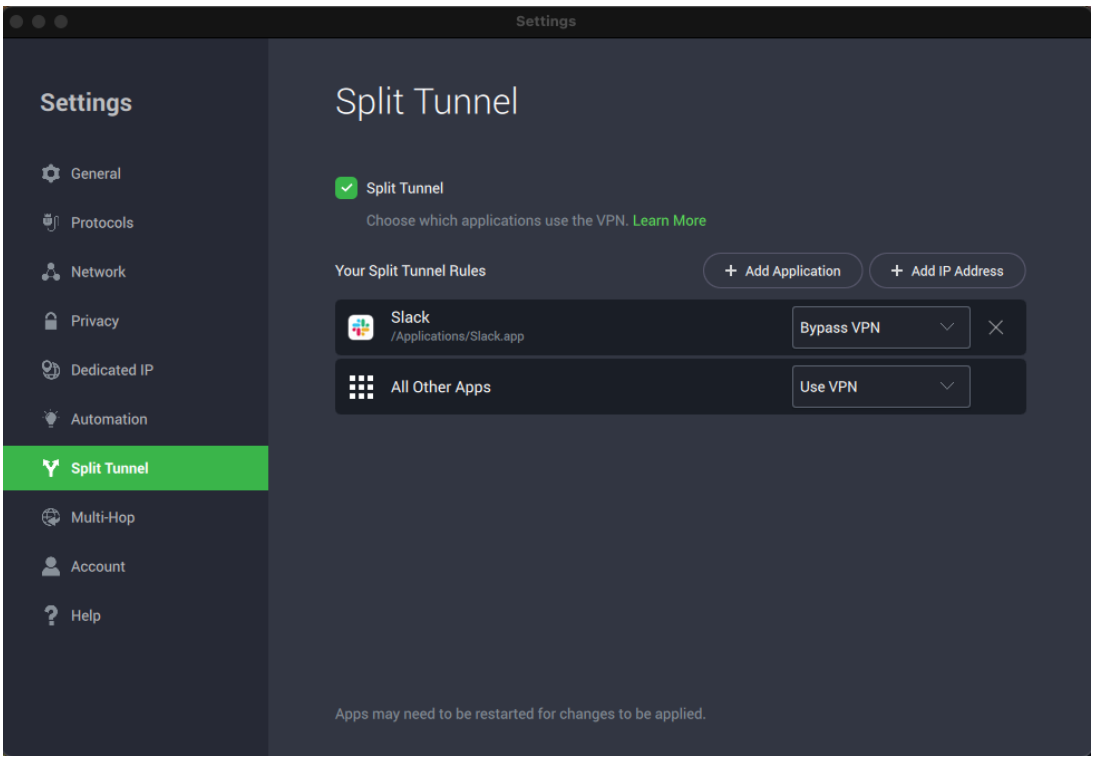
Automation

The automation tab will allow you to determine how the VPN reacts to certain conditions. This includes whether or not the VPN should connect on open WiFi Networks, Protected Networks or the Network to which you connect in your home. More details about this feature are available here.



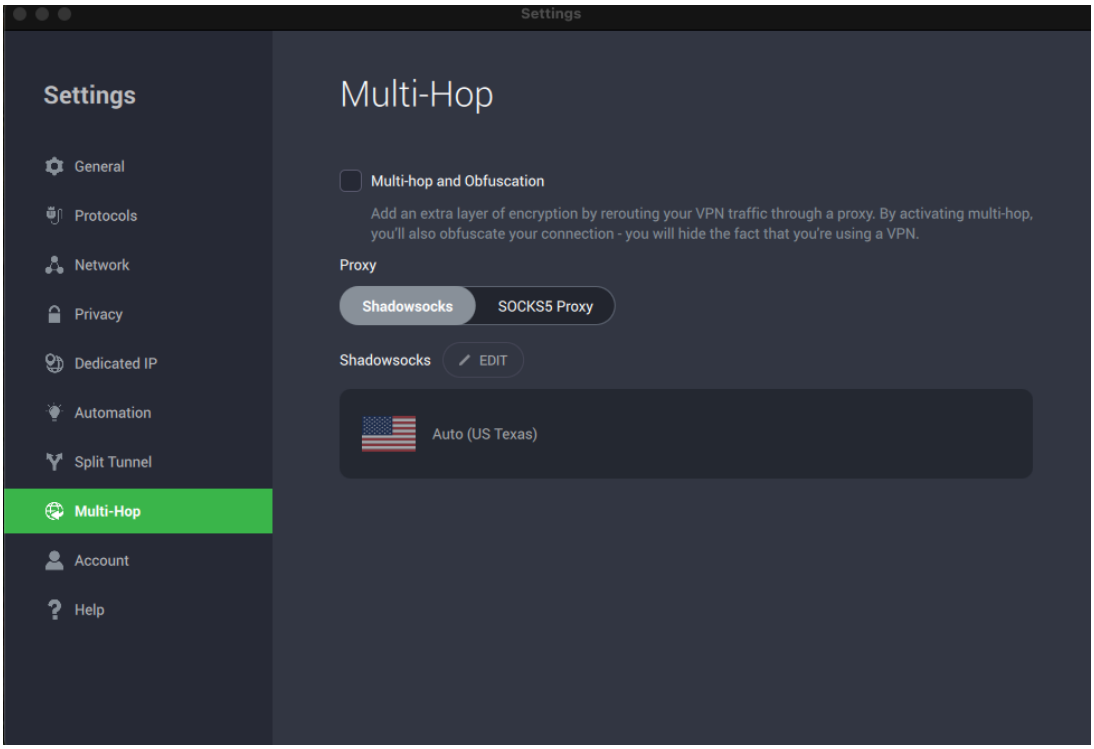
Split Tunnel

The Split Tunnel feature, when enabled, allows you to “exclude” specific applications or IPs. When excluded, these applications and IPs will operate outside of the encrypted tunnel. You can read more about our Split Tunneling feature here.



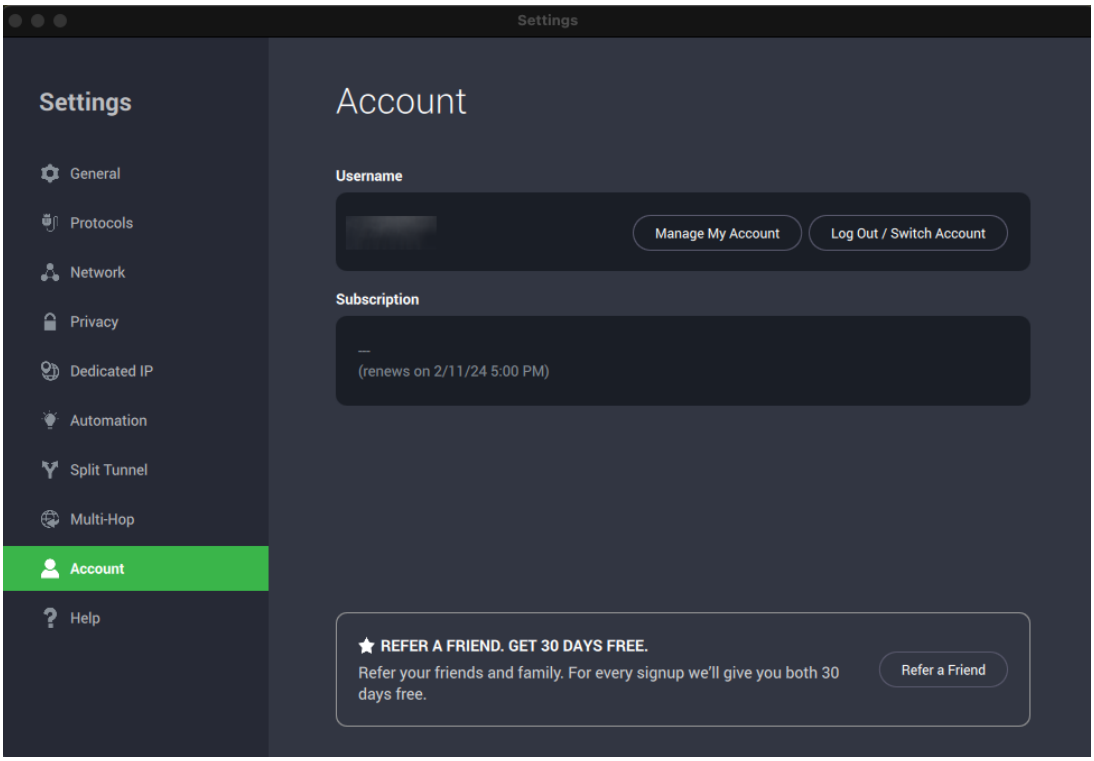
Multi-Hop

Want to create a circuitous route to your destination of choice? We recommend using the Multi-Hop and Obfuscation checkbox to create a Multi-Hop setup and run your connection through two different servers (one a proxy).



Account

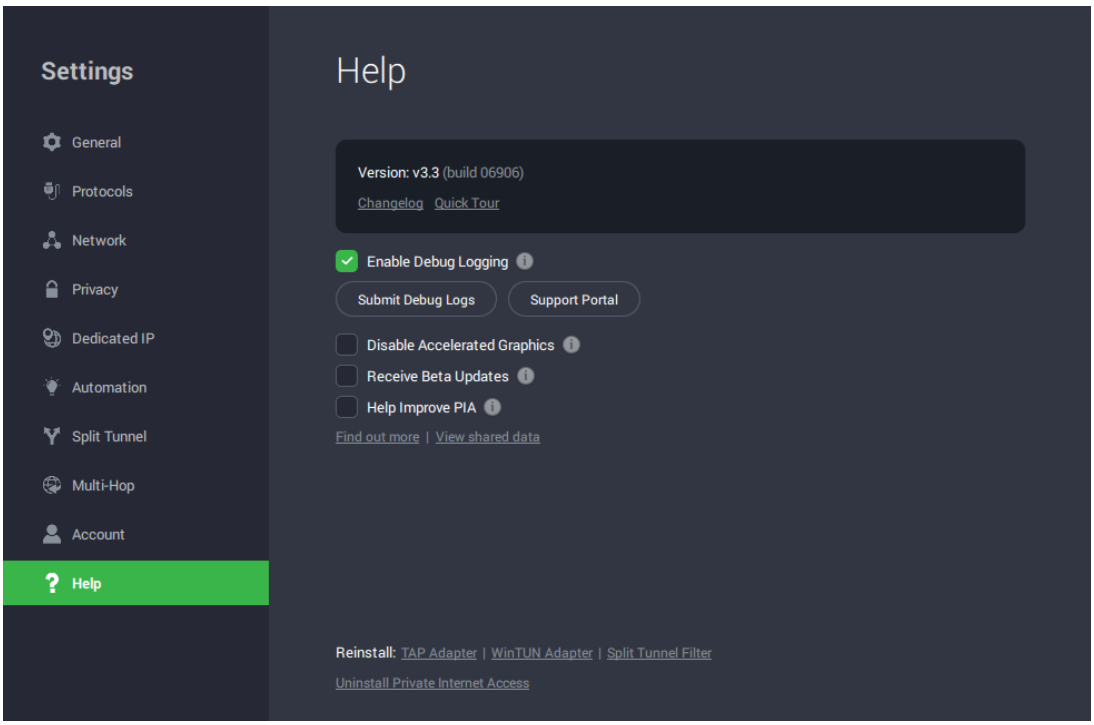
The next section is Account. This contains details about the subscription of the account you are logged in on in the application.



Help

The final section is Help. In addition to being another location to toggle the Debug Logging feature, you can also find a shortcut to the Support Portal, and see the version of the application you are using. In the Help tab, you will also find the following features:

- Disable Accelerated Graphics (Windows and Linux only): Checking this box will disable the apps graphical effects the can have a higher impact on CPU usage.
- Receive Beta Updates: When checked you will be prompted, within the application, to install the latest beta version when it becomes available.
- Show service communication messages: When toggled to the off position, this will limit the communication you receive from the application
- Help Improve PIA: This feature helps ensure the service performance by sharing anonymous connection stats with PIA. The reports do not contain any personally identifiable information.



Submit Debug Logs

If you select the Submit Debug Logs option, you will see a window like the one shown below. You can enter details about what you are experiencing in the text box at the top of the right side. Upon clicking Send a Reference ID will be generated, click Copy to clipboard and paste this Reference ID in a response to customer support.