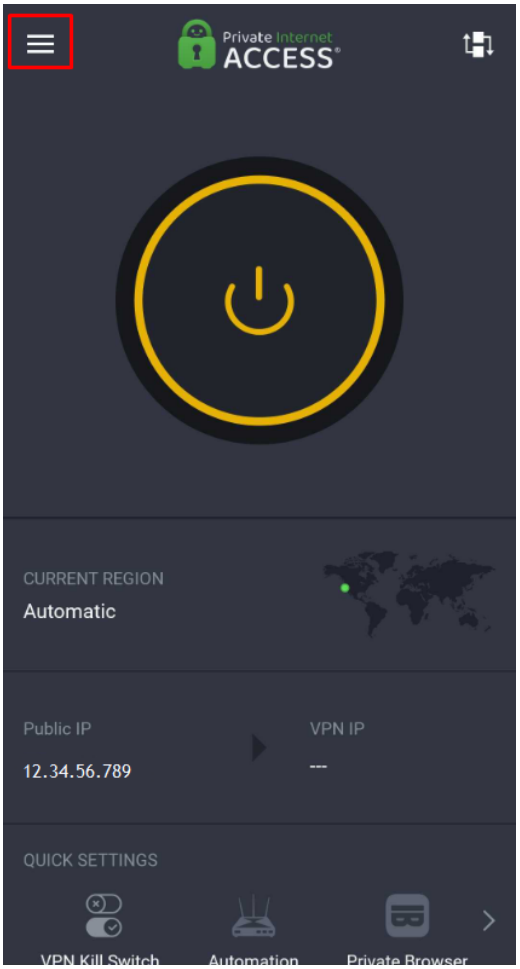
Understanding Android Settings and Protocols

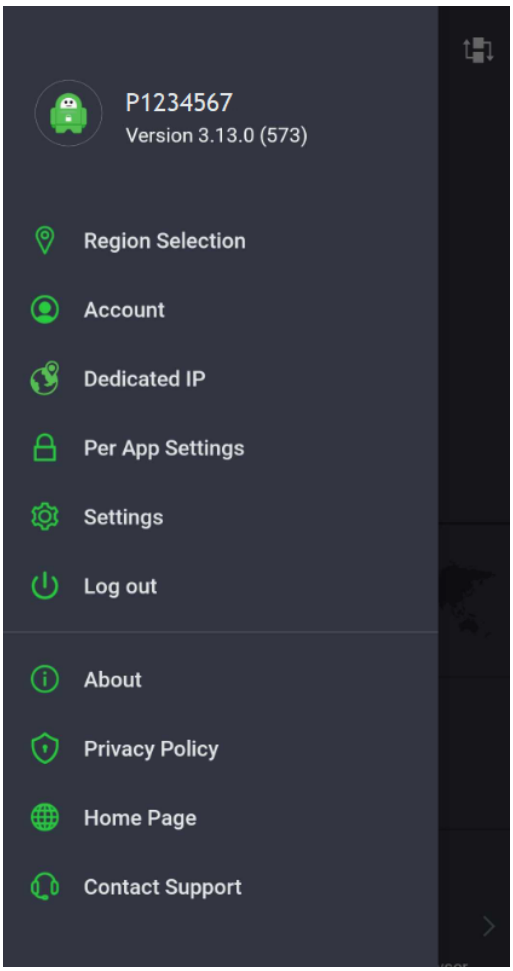
Travis - 2022-06-28 - Application & Features

We typically recommend the default settings for the application for the majority of our users, however at times, specific settings need to be adjusted in order to resolve connection issues or invoke extra security.

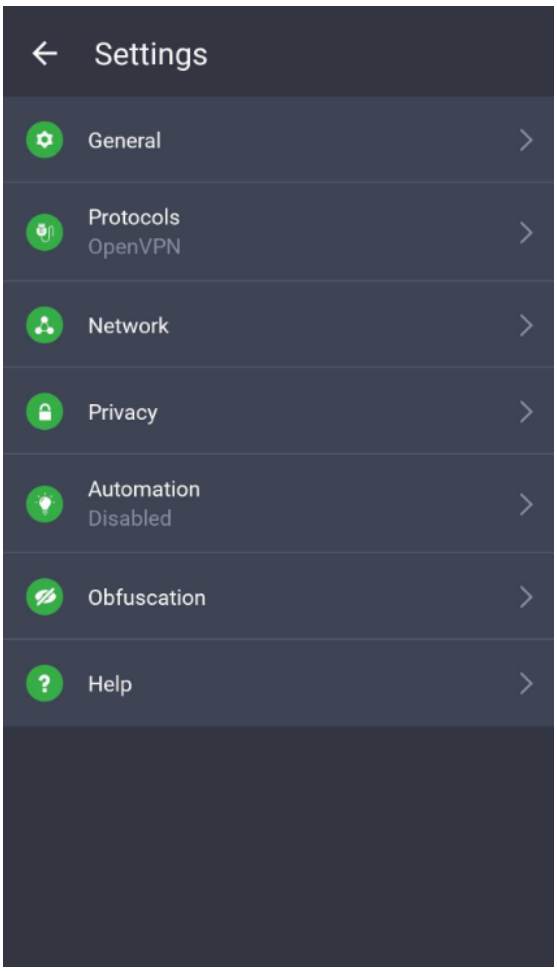
To access the app's Settings, first open the app, then tap the icon that looks like three horizontal lines in the top left corner of the main menu.



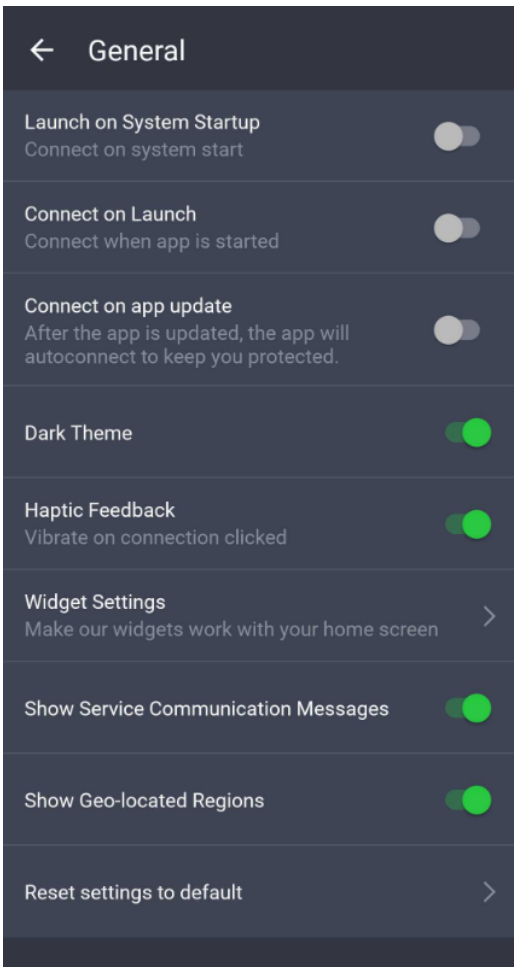
The main menu settings should now display, tap **Settings**



VPN Settings


Settings
General
Protocols
OpenVPN
Network
Privacy
Automation
Disabled
Obfuscation
Help

General



Launch on System Startup- This feature will cause the app to start and initiate a connection once your phone has been turned on.

Connect on Launch - This allows the VPN to connect after opening the application.

Connect on app update - This feature will connect the VPN immediately after updating the application.

Dark Theme - This feature will change the colors of the app to use dark gray as the background. Some users find this easier on their eyes. This is a purely cosmetic feature.

Haptic Feedback - This feature will cause your device to vibrate as a notification of connectivity.

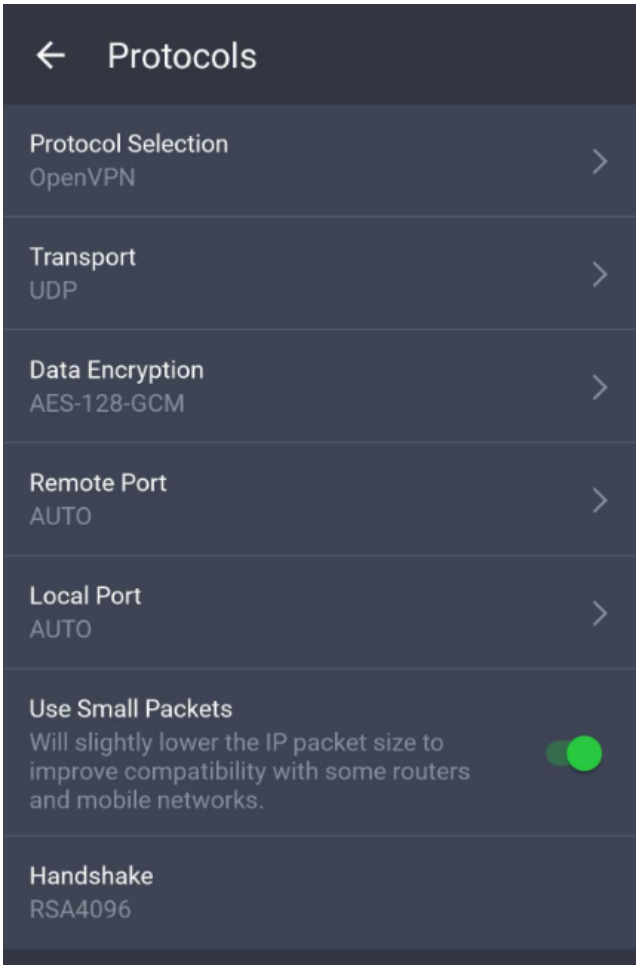
Widget Settings - This will open a section with settings to allow for cosmetic adjustment of the available widgets for the PIA App

Show Service Communication Messages - Enabling this feature allows the in-app messages to be displayed.

Show Geo-located Regions – This feature includes our geo-located server options in the server selection.

Reset Settings to Default - This will reset all settings back to the original default settings.

Protocols



Protocol Selection – Switch between OpenVPN and WireGuard.

Transport - Switch between TCP and UDP.

Data Encryption - This will specify AES-128-GCM, or AES-256-GCM. These are the two types of encryption that the PIA VPN uses. By default, the app will use AES-128-GCM, which is very secure.

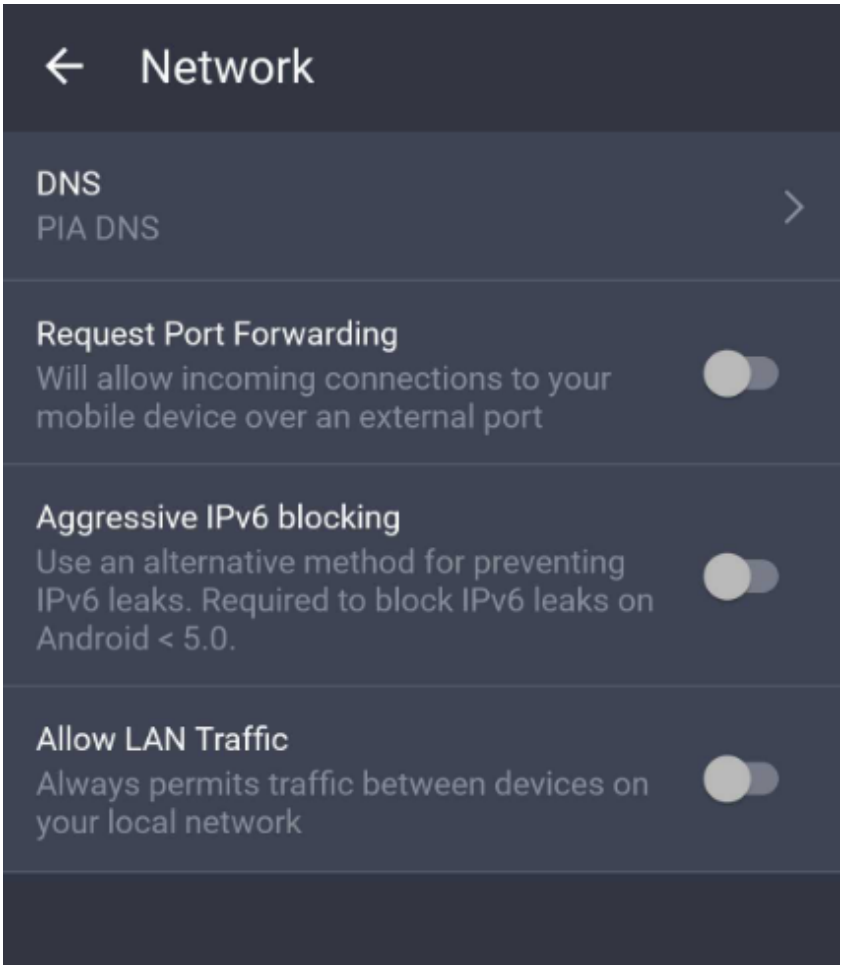
Remote Port - This specifies what port the VPN's external connection will use for traffic. The allowed ports for our VPN are; UDP: 8080, 853, 123, and 53 --- TCP: 80, 443, 853 and 8443. To learn more about these protocols/ports and why they would be changed visit the article here.

Local Port - This specifies the port used for internal communication on your device. This only needs to be adjusted in very specific situations and is not suggested.

Use Small Packets - This will reduce the MTU/reduce the IP packet size on your device which can sometimes aid with some connectivity issues. Specifically, if packet issues are seen in a debug log.

Handshake - This will specify what certificate to use when establishing a connection to the VPN server.

Network



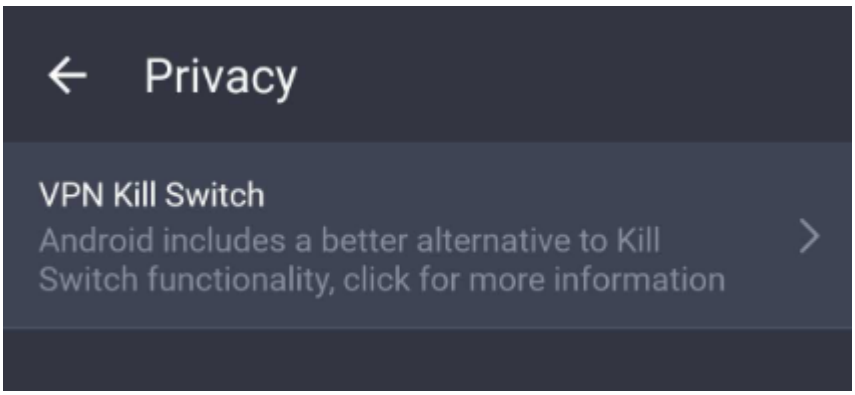
DNS - This specifies what DNS servers are used with the VPN. By default, they use PIA's DNS servers. If you are experiencing connection issues or wish to use different servers, you can tap this setting and select Custom DNS to change them.

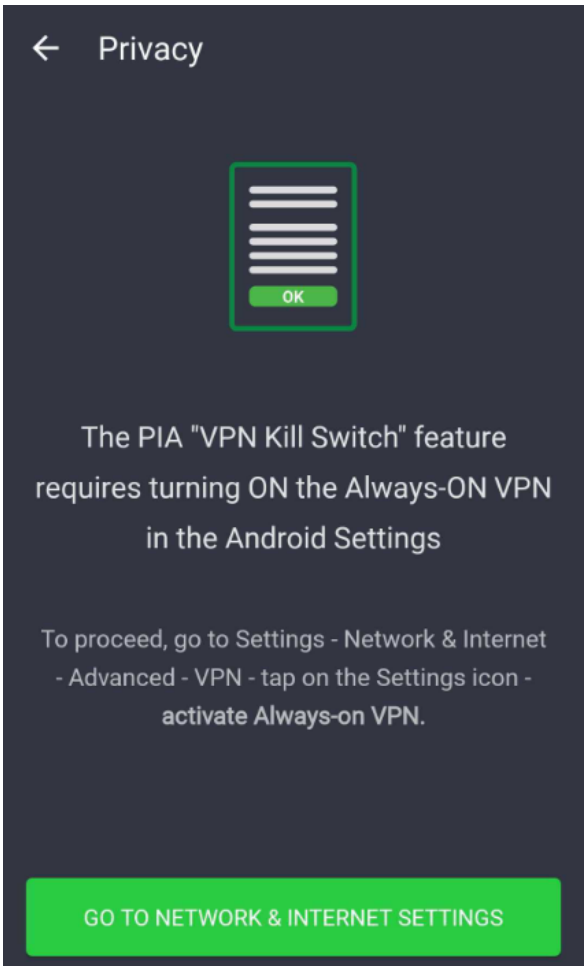
Request Port Forwarding - This will allow incoming connections to connect to your mobile device via an external port. This is sometimes helpful if an ISP is blocking or restricting specific ports. Also, for those who wish to torrent, this is a recommended setting.

Aggressive IPv6 Blocking - This feature will protect users from leaks caused by the use of IPv6. Traffic that occurs over an IPV6 address is not protected as currently, the PIA VPN operates exclusively on IPV4.

Allow LAN Traffic - This will allow access to your local network devices. If you are on a public network, this is not suggested.

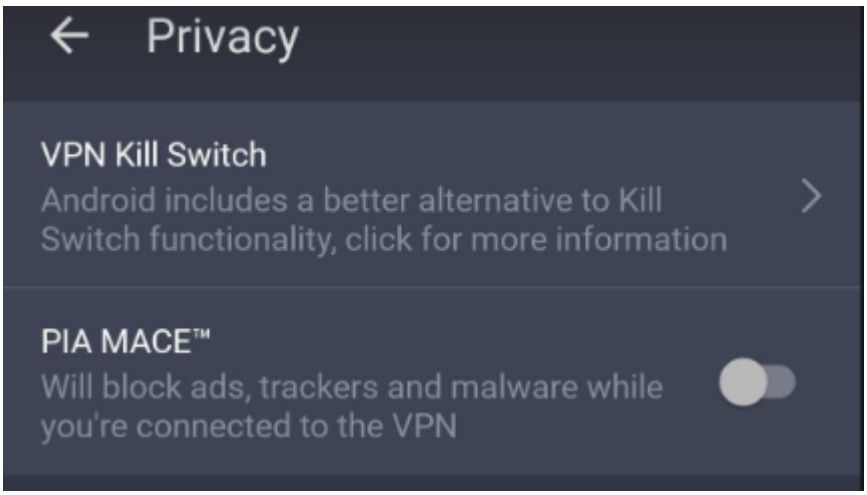
Privacy



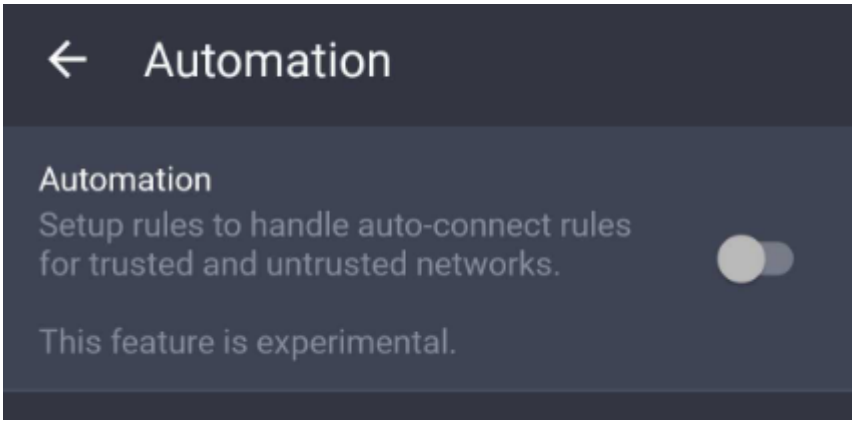


VPN Killswitch - This feature will prevent internet traffic if the VPN becomes disconnected. This is a good utility in general for making sure your traffic does not leak when your traffic absolutely requires protection. This uses the built in Android OS "Killswitch". Android 8.0 and later includes this feature which blocks connections when a VPN is not connected. This is better integrated compared to the PIA Killswitch as it is deeply integrated with Android OS.

PIA MACE (APK only) - This enforces the use of MACE, which blocks ads, malware, and trackers. If you are having trouble accessing specific content/websites, sometimes it is because the source of this content is being blocked by MACE.

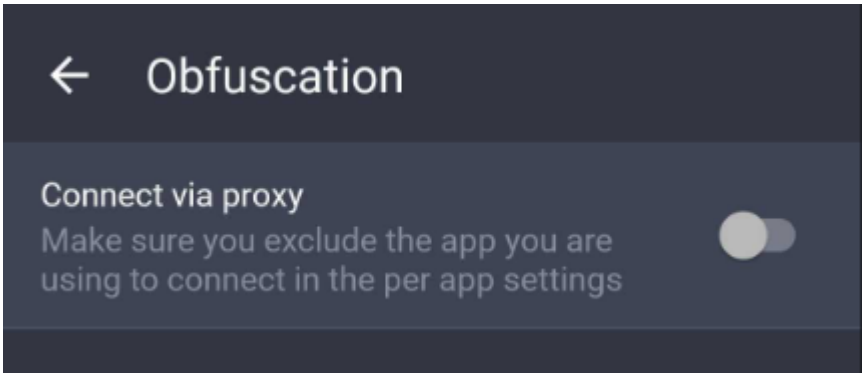


Automation



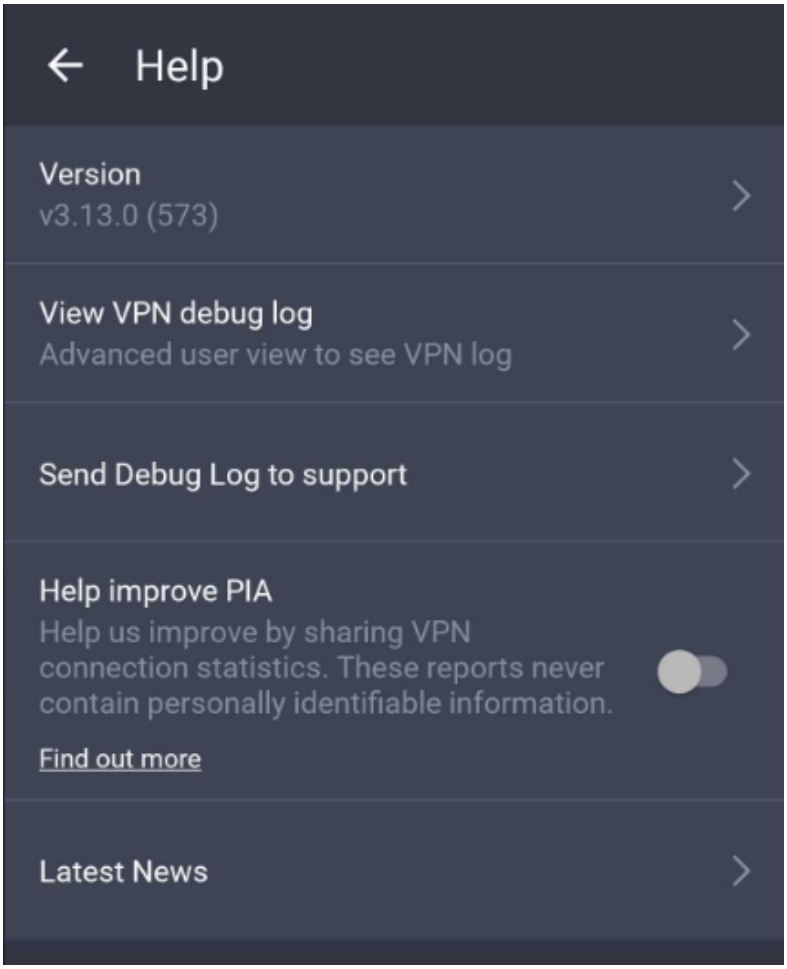
Automation - This feature will keep the VPN connected unless you are using a Wi-Fi or Mobile network that you have listed as "Trusted"

Obfuscation



Connect via Proxy - this allows you to connect certain apps through the PIA App Proxy, i.e. torrent apps.

Help



Version - This lists the version of the application currently installed on your device.

View VPN Debug Log - This will show the debug log for the VPN connection. For most users, if assistance is needed, we suggest contacting our support team. However, if you would like to review the log to search for the cause of an issue you are experiencing, you may do so with this option.

Send Debug Information to Support - This will generate a debug log ID for you to submit to the support team via support ticket (use the Contact Us tab above to submit a ticket)

Help improve PIA - Helps improve the VPN by sharing anonymous connection statistics.

Latest news - Opens the latest news regarding new additions to the app and to PIA.