



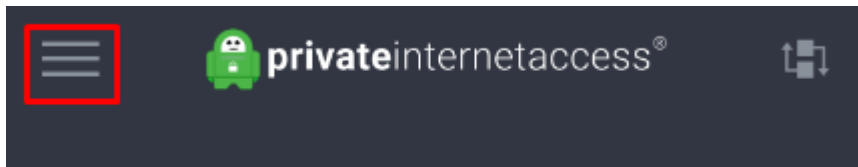
Knowledgebase > Technical > Application Settings and Features > Application & Features
> Understanding iOS Settings and Protocols

Understanding iOS Settings and Protocols

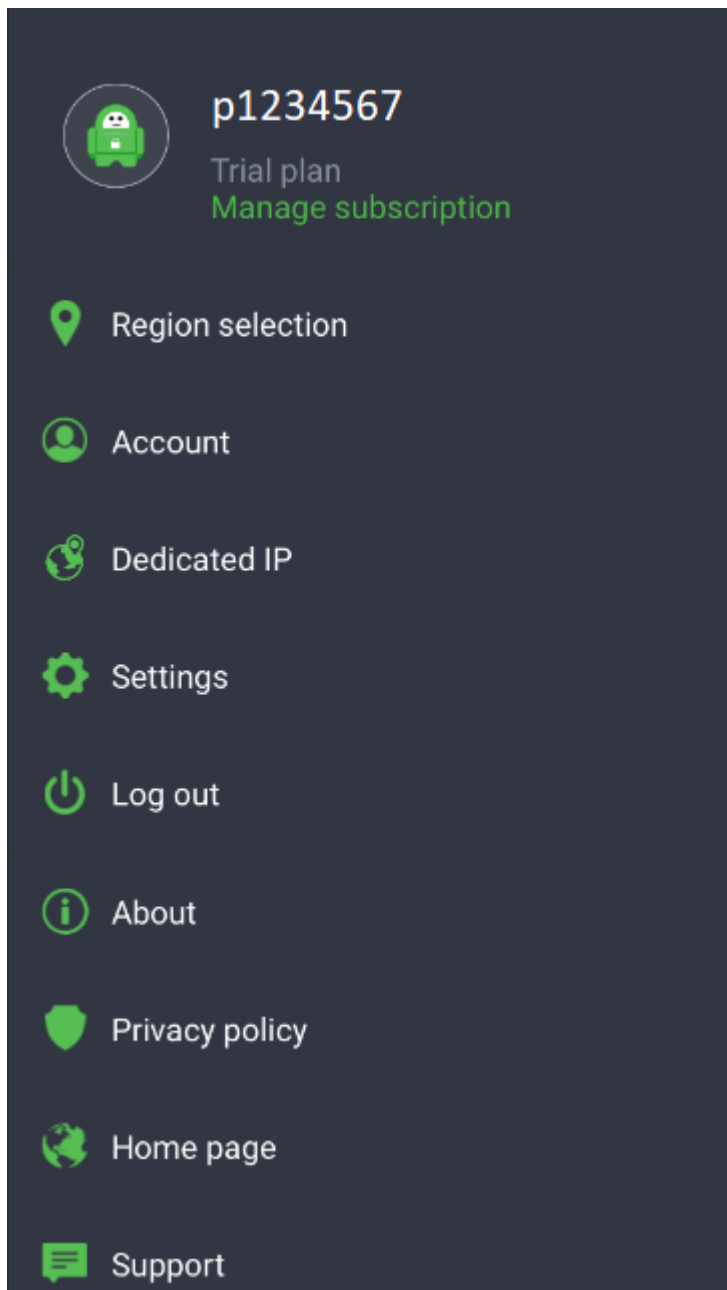
Kaneesha D. - 2021-06-11 - Application & Features

Now that you have the VPN installed on your iOS devices, you may be interested in the settings and features available in the iOS application.

To access the iOS settings select the (3) horizontal lines in the top left corner.

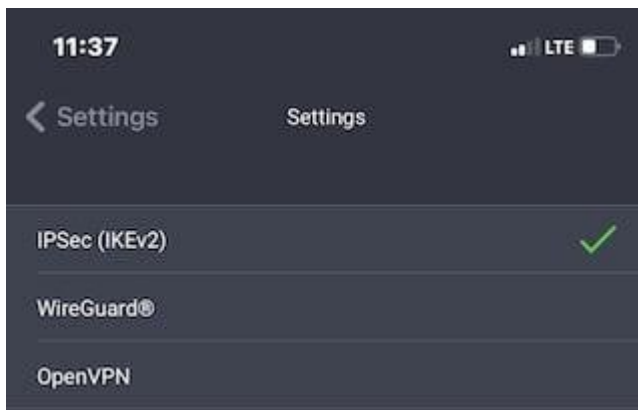


Here you will be able to access several options such as: Region Selection, Account, Settings, Log out, and more.



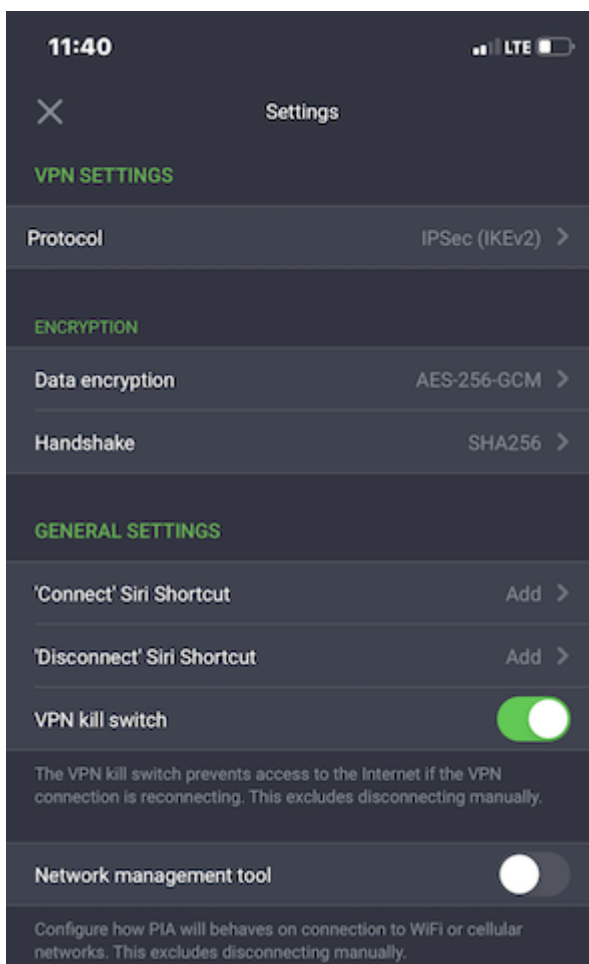
Once you are in the Settings menu you will be able to access and change several features depending on the protocols that your application is connecting to. Below we outline what each protocol's settings are available and what they do.

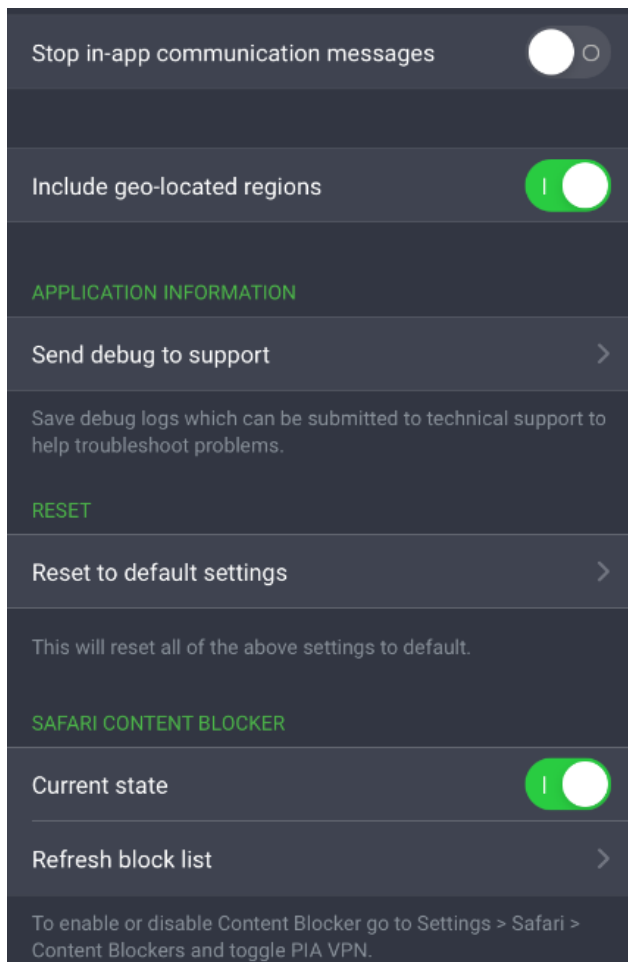
The Protocols that you can connect to are: **WireGuard, OpenVPN and IKEv2**



The protocol selected will change the settings that you can select.

IPsec (IKEv2) settings: IKEv2 is an advanced VPN protocol that provides a balance between security and speed by using the UDP socket and port 500 for lower latency communication. Additionally, you are able to toggle the Data encryption level as well as the Handshake.





OpenVPN settings: OpenVPN gives the most flexibility when encountering connection issues as different Sockets and Port combinations can resolve them. Not only are you able to toggle your encryption settings, but you have the option to enable the 'Use small packets' feature.

11:43

LTE



Settings

VPN SETTINGS

Protocol	OpenVPN >
Socket	Automatic >
Remote port	Automatic >
DNS	PIA DNS >

ENCRYPTION

Data encryption	AES-128-GCM >
Data authentication	GCM >
Handshake	RSA-2048 >

Use small packets

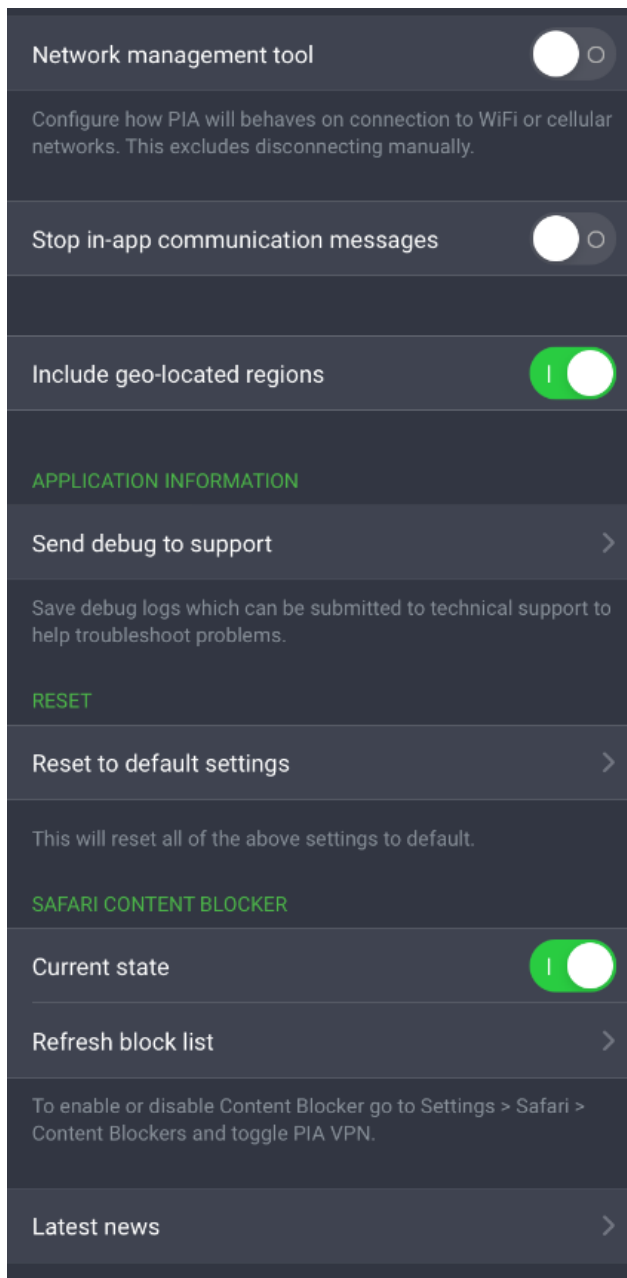
Will slightly lower the IP packet size to improve compatibility with some routers and mobile networks.

GENERAL SETTINGS

'Connect' Siri Shortcut	Add >
'Disconnect' Siri Shortcut	Add >

VPN kill switch

The VPN kill switch prevents access to the Internet if the VPN connection is reconnecting. This excludes disconnecting manually.



WireGuard settings: WireGuard which is optimized to be the best pre-configured option for speed and security, connects over the TCP socket with port 1337 in use. Similar to our other pre-configured option, IPsec, you have the basic settings to choose from with the exception of the ability to change your encryption settings.



Settings

VPN SETTINGS

Protocol WireGuard® >

DNS PIA DNS >

GENERAL SETTINGS

'Connect' Siri Shortcut Add >

'Disconnect' Siri Shortcut Add >

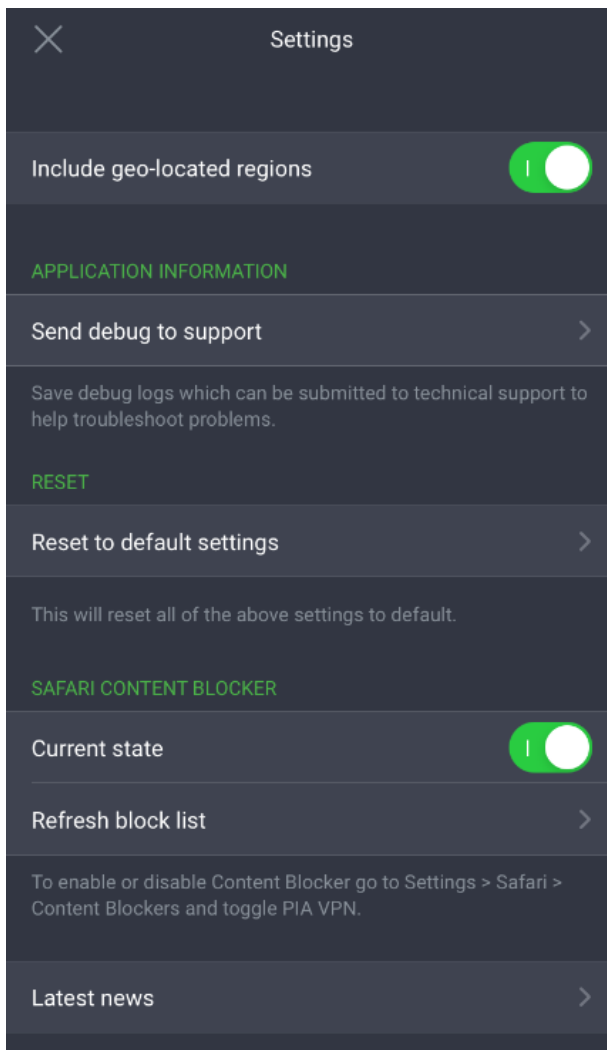
VPN kill switch

The VPN kill switch prevents access to the Internet if the VPN connection is reconnecting. This excludes disconnecting manually.

Network management tool

Configure how PIA will behaves on connection to WiFi or cellular networks. This excludes disconnecting manually.

Stop in-app communication messages



Please See below for the Setting Descriptions

Connection (Only available using the OpenVPN protocol)

- **Socket:** Allows you to choose between UDP and TCP.
- **Remote port:** Allows you to select the remote port you want to use to connect to the VPN server. If you are unable to connect, test each remote port before continuing to troubleshoot.
- **Use Small Packets:** Will slightly lower the IP packet size to improve compatibility with some routers and mobile networks.

Encryption (Only available using the IPsec & OpenVPN protocols)

- **Data Encryption:** Allows you to choose the cipher used to encrypt your traffic to the VPN server.
- **Data Authentication(OpenVPN Exclusive*):** Allows you to choose the hash function used to authenticate your encrypted traffic.
- **Handshake:** Choose the handshake used to establish a secure connection between

your device and our servers.

General Settings

- **Connect Siri Shortcut:** Allows you to record a personalized phrase that allows Siri to tell our application to Connect.
- **Disconnect Siri Shortcut:** Allows you to record a personalized phrase that allows Siri to tell our application to Disconnect.
- **VPN Kill Switch:** Prevents access to the Internet if the VPN connection is reconnecting. This excludes disconnecting manually.

Network Management Tool:

Allows you to configure how our application will behave on Connections to Wi-Fi or Cellular networks.

Within this tool you can select the application to protect and react over the following:

- Mobile Data
- Secure Wi-Fi
- Open Wi-Fi
- Specific Wi-Fi Networks

Stop in-app communication messages

- Enabling this feature prevents the in-app messages from displaying.

Include Geo-Located Regions

- Displays geo-located exit nodes in your server list.

Application Information

- **Send Debug to Support:** Allows you to send a Debug log to our support team in order for them to assist in troubleshooting issues. Only available using the OpenVPN & WireGuard protocols.

Reset

- **Reset to Default Settings:** Will reset all of the above settings to our default settings.

Safari Content Blocker

- **Current State:** On or off. You will be redirected to iOS Settings to enable or disable

this feature.

- **Refresh block list:** Updates content blocking rules to their most recent version.

Preview

- **Latest News:** Will provide you with a brief synopsis of whats new with the client, with the ability to learn more.