Understanding Android Settings and Protocols
Travis - 2021-06-11 - Application & Features

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

To access the Android 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 and OpenVPN
The protocol selected will change the settings that you can select.

**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.
Settings

VPN SETTINGS

Protocol
OpenVPN

Use TCP
UDP will be used to connect

Request port forwarding
Will allow incoming connections to your mobile device over an external port

Remote Port
Using automatic port selection

Local port
Using random local port for connection

DNS
PIA DNS

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

PROXY SETTINGS

Connect via proxy
Make sure you exclude the app you are using to connect in the per app settings

BLOCKING

VPN Kill Switch
Android includes a better alternative to Killswitch functionality, click for more information

Aggressive IPv6 blocking
Use an alternative method for preventing IPv6 leaks. Required to block IPv6 leaks on Android < 5.0.

Block local network
Access to local networks will be blocked

ENCRIPTION

Data encryption
AES-128 GCM

Data authentication
AEAD ciphers like AES-GCM use an integrated authentication mechanism

Handshake
rs44096
**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. With WireGuard, you have the basic settings to choose from apart from the ability to change your encryption settings, small packets, proxy settings, Killswitch, and aggressive IPv6 blocking.
Please See below for the Setting Descriptions

**Connection (Only available using the OpenVPN protocol)**

- **Use TCP** - By default, the PIA app will use the UDP protocol connection, this will specify to use the TCP protocol instead.

- **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.

- **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.

- **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.

**Proxy Settings**

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

**Blocking**

- **PIA MACE (APK version 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.

- **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.

- **Block Connections Without VPN** - 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.

- **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.

- **Block Local Network** - This will block access to your local network devices. If you are on a public network, this is suggested.

**Encryption**

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

- **Data Authentication** - This is the authentication protocol that will be used between your device and the server you are connecting to.
- **Handshake** - This will specify what certificate to use when establishing a connection to the VPN server.

**General Settings**

- **1-Click Connect** - This allows the VPN to connect after opening the application.
- **Connect on Boot** - This feature will cause the app to start and initiate a connection once your phone has been turned on.
- **Connect on App Update** - This feature will connect the VPN immediately after updating the application.
- **Network Management** - This feature will keep the VPN connected unless you are using a Wi-Fi or Mobile network that you have listed as "Trusted".

Within this tool enabled, you can manage the automation by selecting the application to protect and react over the following:

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

- **Haptic Feedback on Connect** - This feature will cause your device to vibrate as a notification of connectivity.
- **Include geo-located regions** – This feature includes our geo-located server options in the server selection.
- **Stop in-app communication messages** - Enabling this feature prevents the in-app messages from displaying.
- **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.
- **Latest news** - Opens the latest news regarding new additions to the app and to PIA.
- **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.
- **Widget Settings** - This will open a section with settings to allow for cosmetic adjustment of the available widgets for the PIA App**.
• **Reset Settings to Default** - This will reset all settings back to the original default settings.

**Application Information**

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

• **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)