We are proud to announce the release of version 1.5.1 for all supported Desktop operating systems. Among the new features and changes introduced in this release is split tunneling, which allows applications to bypass the VPN using the App Exclusions feature. When used, this will allow applications to circumvent the encrypted tunnel and connect directly to the internet. While not all applications can be excluded, currently, a wide variety of apps, including those found within the Windows 10 Store, can be added to the exclusions list. Below is the full change log from this release:

* Split tunneling allows applications to bypass the VPN using the App Exclusions feature.
* Excluded applications bypass the VPN and connect directly to the Internet.
* Mac: This feature currently requires macOS 10.13.
* Linux: This feature currently requires iptables 1.6.1 with systemd network control groups on Linux.

Additionally, in order to assist with any issues you may experience while using this feature, we have included a help link to the App Exclusions which leads you to the following knowledgebase article:

Split Tunnel Application Examples

As the title indicates, this article provides examples of applications that you might wish to exclude and how to exclude those programs that may be considered less common.

In order to gather feedback on this feature and to continue improving functionality, please visit our Reddit on split-tunneling, which can be found here:

Announcing: Split-Tunneling (Reddit)

Additionally, as the split-tunneling feature is currently in beta, and as we work to ensure users who experience these issues are assisted as quickly as possible, you can reach out to our desktop development team via the following email addresses:
Windows: beta-feedback-win@privateinternetaccess.com
Mac: beta-feedback-mac@privateinternetaccess.com
Linux: beta-feedback-linux@privateinternetaccess.com

We hope you enjoy the split-tunneling feature and don't hesitate to contact us should you experience any issues.