PrivateCloud Setup Manual

PrivateRouter LLC
618 E. South St, Suite 500,
Orlando, FL 32801 USA

v1 2023-8

Trademarks

TorGuard is a trademark of VPNetworks LLC. "WireGuard" and the "WireGuard" logo are registered trademarks of Jason A. Donenfeld. Other brand names and products are registered trademarks of their respective holders.

Statement of Conditions

In the pursuit of enhancing internal architecture, operational performance, and/or dependability, PrivateRouter LLC reserves the right to modify the products detailed in this document at any time without prior notice. PrivateRouter LLC does not assume any responsibility for any liabilities that may arise from the usage or implementation of the product(s) or circuit configuration(s) described herein.

Chapter 1
Getting Started

This chapter outlines the steps for plugging in your PrivateCloud device and establishing an Internet connection through it.

What's in the box?

The following items should be included in the product box:

- x86 or ARM PrivateCloud Device
- x1 LAN Cable
- x1 AC Adapter
- x1 WiFi USB Adapter for WiFi HotSpot

If you find any components to be incorrect, missing, or damaged, get in touch with PrivateRouter or TorGuard customer service. Retain the box and all original packaging materials in case you need to send the product back for repairs or replacement.

The PrivateCloud Router Ports

Based on the model you have, your PrivateRouter will either come with two LAN ports or one LAN port along with a USB LAN adapter. In the OpenWRT configuration, the first port is designated as the LAN, while the second port serves as the WAN (Internet) connection. If your setup includes a USB LAN adapter, this will act as your WAN port.

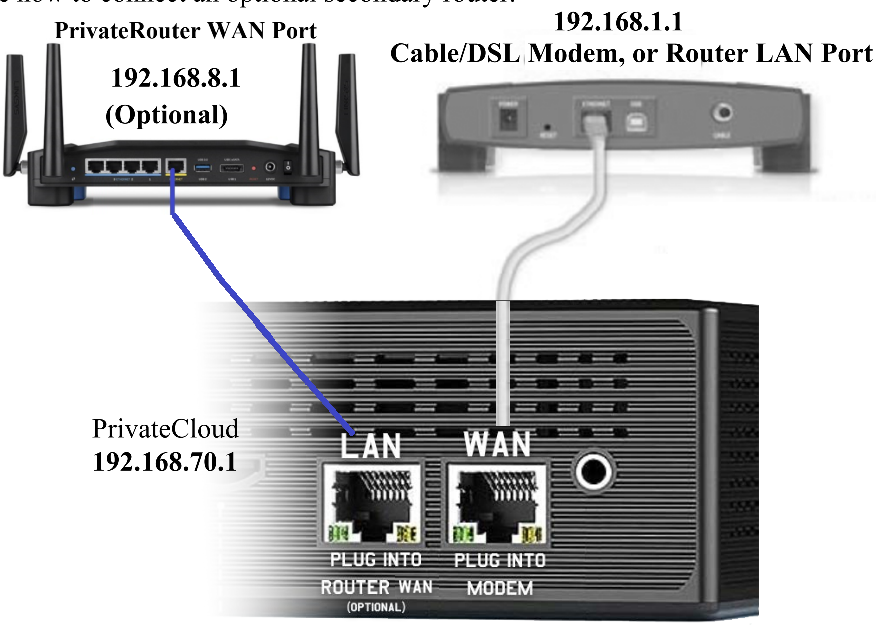
To get started, connect the WAN port to a router or modem with internet access, and link the LAN port to a computer. Additionally, you can use the provided USB WiFi adapter to set up the "PrivateCloud_Wifi" hotspot.

Figure 1-1

Option 1: Set Up PrivateCloud as a WiFi Router

The primary method to connect is by utilizing the PrivateCloud device as a WiFi router. Moreover, if you want to tap into the functionalities of the PrivateCloud remote VPN access feature, you can connect an auxiliary router or another PrivateRouter device through the LAN port.

In this setup scenario, we'll guide you on linking the PrivateCloud device to a current modem and demonstrate how to connect an optional secondary router.



Kindly note that the default IP address for standard PrivateRouter VPN WiFi devices is **192.168.8.1**, while the default IP address for PrivateCloud devices is **192.167.70.1**

After Connecting Your PrivateCloud Device Power Cycle All Devices

- Power off your ISP modem and PrivateCloud
- Power on your ISP modem or router and wait for it to fully boot up.
- Power on your PrivateCloud.
- Connect to the PrivateCloud device by plugging a computer's LAN cable into the PrivateCloud LAN port. Enter the default password “torguard” and browse to **192.168.70.1**

After setting up your PrivateCloud device by connecting a computer to its LAN port, you have the option to add a secondary router, as demonstrated in this example. This configuration is particularly useful if you've enabled a PrivateCloud WiFi hotspot or have configured the PrivateCloud device to serve as a Remote VPN access gateway.

Option 2: Set Up Your PrivateCloud in Side Router Mode

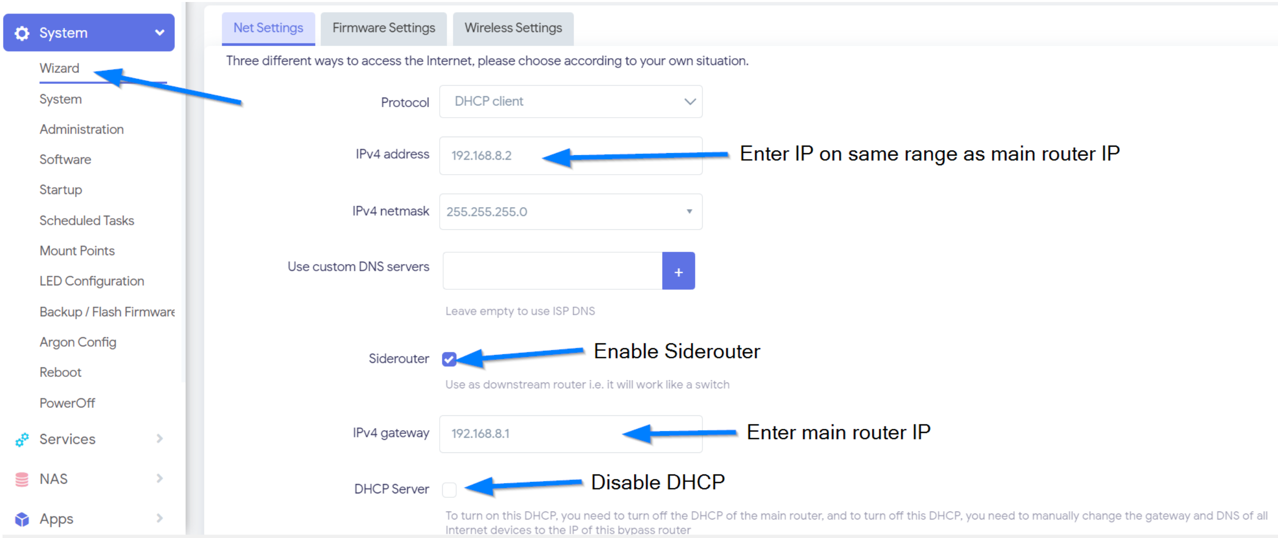


Figure 1-3

In this scenario, we'll be configuring the PrivateCloud device in "Side Router" mode. This allows you to connect to your PrivateCloud through an existing PrivateRouter or another WiFi router. To activate Side Router mode, navigate to the '**System**' tab and click on '**Wizard**.' Check the '**Side Router**' option and input the IP address of your main router. For the 'IPv4 Gateway,' enter the main PrivateRouter's IP, which in this case is **192.168.8.1**. Make sure to disable the DHCP option. For the 'IPv4 Address,' change the PrivateCloud device's IP to **192.168.8.2** so that it becomes accessible through your main WiFi router. **Click Save and Apply then reboot**.

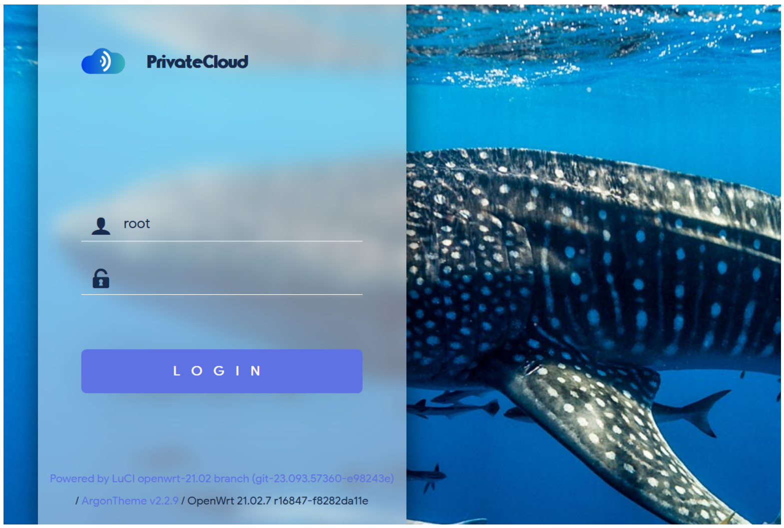
Plug Your PrivateCloud LAN Port into the PrivateRouter LAN Port

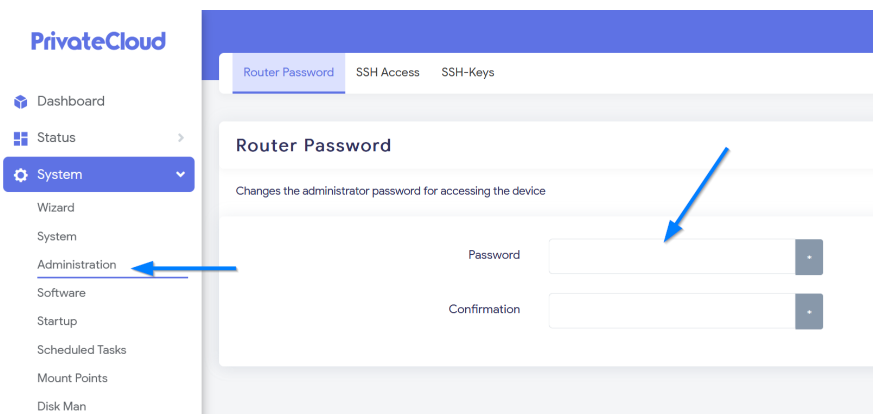
Make sure to restart your devices after plugging in your PrivateCloud device

After enabling Side Router mode and connecting the LAN ports of both devices, you can now access your PrivateCloud device at the IP address 192.168.8.2 when you're connected to the main PrivateRouter WiFi network.

Setting a Secure Admin Password

To access the PrivateCloud administrative interface, first connect to the PrivateCloud WiFi network or plug your computer into via LAN cable. Once connected, open a web browser and navigate to: 192.168.70.1. The default username is "root," and the default admin password is "torguard". Input these credentials and then click the LOGIN button.





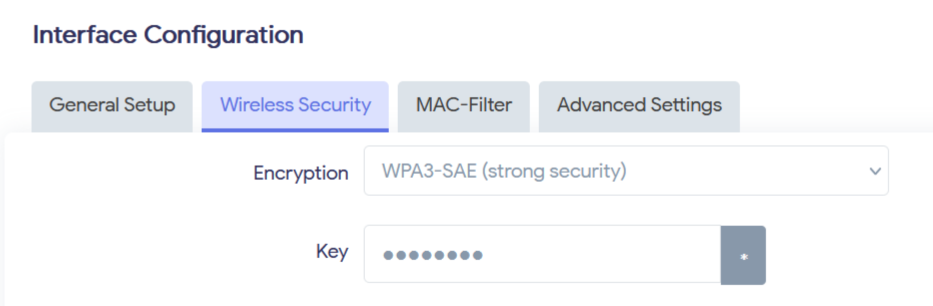
In the side menu, select the "System" option, followed by clicking on "Administration." In the password text field, enter your new, secure admin password. Confirm the password by retyping it in the box provided below. It's crucial to choose a secure password that is different from your WiFi password, as this will be the password you use to access the administrative interface at 192.168.70.1. Finally, click the Save button to finalize the changes.

Setting a Secure WiFi Password

Changing the PrivateCloud WiFi password is essential for security. To do so, initially access the administrative interface by navigating to **192.168.70.1**. In the left-hand panel, select the "Network" menu and then choose "Wireless." From the Wireless Overview menu, identify the

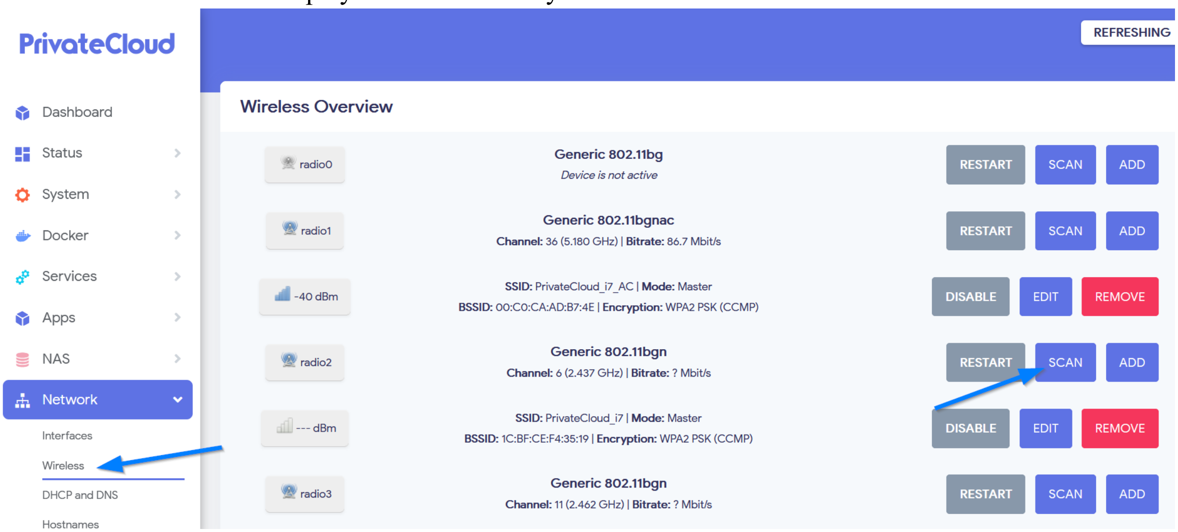
Enter a Secure WiFi Password

To set a new PrivateCloud WiFi password, navigate to the security tab within the WiFi network menu. Choose the WiFi encryption method you prefer, although we recommend WPA2 or WPA3 encryption for optimal security. In the "Key" field, input your new WiFi password. This will be the password you use to connect to the PrivateCloud WiFi network. Click the "SAVE" button and return to the Wireless Overview menu. To finalize your changes, click "SAVE" followed by "APPLY CHANGES."



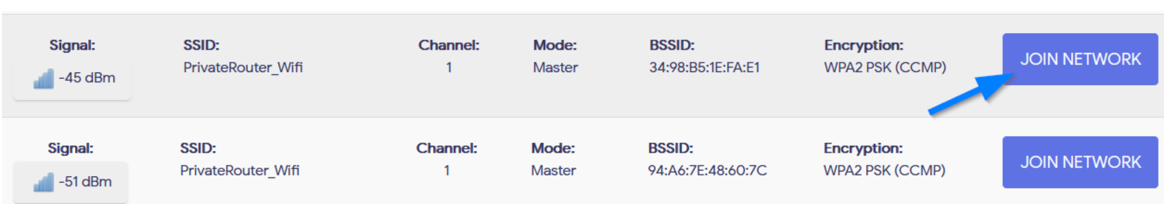
Connect to the Internet Through an Existing WiFi Network

In situations where WAN plugin access is unavailable, you can link your PrivateCloud to a pre-existing WiFi network for internet connectivity. If you can't physically connect a LAN cable to an existing router, you have the option to connect your PrivateCloud to an available WiFi network. To do so, navigate to the "Network" tab and then choose "Wireless." Hit the "Scan" button on your WiFi Radio device to display a list of all nearby WiFi networks.



Join a WiFi Network to Gain Internet Access

Wait briefly as your PrivateCloud completes its scan for nearby WiFi networks. Select the network you want to join and click on "JOIN NETWORK." In the subsequent screen, you'll be prompted to input the WiFi network's passphrase into a text field. Enter the required password and click "SAVE." To finalize the settings, go back to the Wireless Overview menu, click "SAVE," and then hit "APPLY SETTINGS."



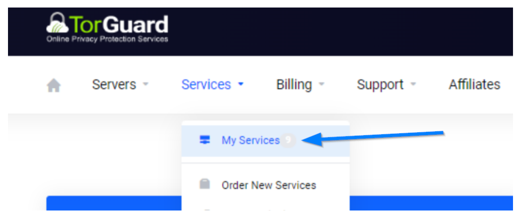
PrivateCloud VPN Access with TorGuard

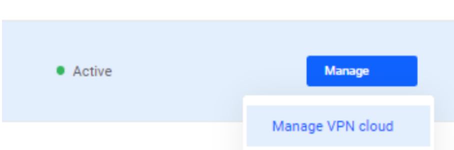
The most common use case for PrivateCloud is setting up remote access VPN with TorGuard. This enables you to utilize your local IP address from anywhere through a secure WireGuard connection, giving you full access to your network on any device as if you were physically present. This is especially useful for securely accessing Docker apps on your PrivateCloud device without exposing them to the public internet. In this example, a PrivateRouter OpenWRT device is operating as the WireGuard gateway. Any additional WireGuard peers you create will connect through this gateway device, gaining access to any local IP address connected to the PrivateRouter network at 192.168.70.1/24.

Option 1: Setup Remote Access Wireguard for your devices

This setup requires a TorGuard Private VPN Cloud account.

To setup Remote Access through Wireguard first you have to create a Wireguard config in the TorGuard member's area. Navigate to the "Active Products and Services" section or go to the Service menu and select "My Services."

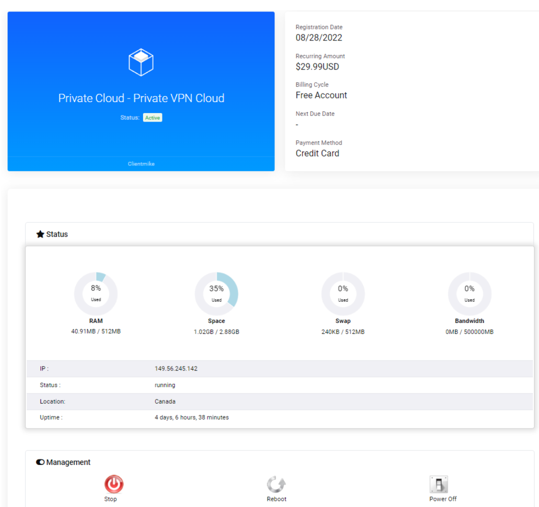




Locate your specific service, click on "Manage" to access the dropdown menu, and then select "Manage VPN Cloud."

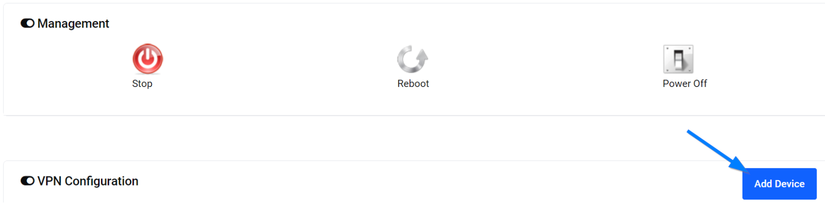
You're now in the Cloud VPN Control Panel. At the top, you'll find information about your current service and billing details. Below that, you'll see your VPN information and status, along with options to stop, start, or reboot your VPN server if you encounter issues like server unreachability.

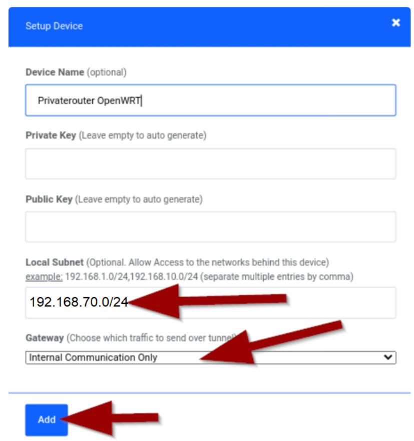
Next, we'll set up the primary Wireguard gateway configuration for your PrivateCloud device. Following that, you'll be able to create additional peer configurations for all your other devices, such as laptops and smartphones. This will allow you to connect all these devices through Wireguard, giving them the same local IP address and providing access to your local network, Docker apps, and other network services.



Generate Your PrivateCloud Wireguard config

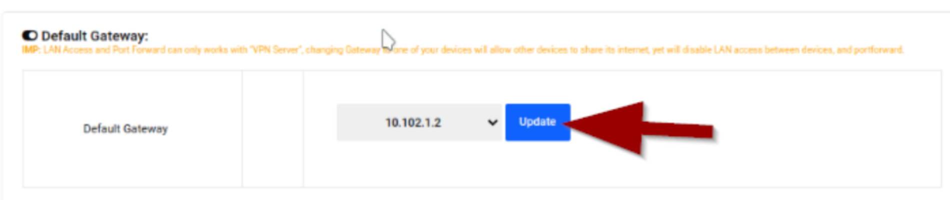
Start by clicking the "Add device" button to include the PrivateRouter OpenWRT as your gateway. Name this configuration "PrivateRouter OpenWRT."



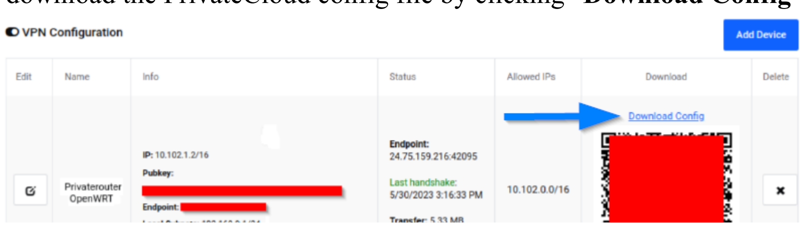


Since the router operates on the local IP 192.168.70.1 and we aim to connect to all computers on this network via Wireguard, enter 192.168.70.0/24 under 'Local Subnet.' We're setting up remote VPN access that employs the local IP as a gateway, so select "Internal Communication Only" under 'Gateway.' Click 'Add.'

Next, set the Default Gateway for other Wireguard peers you'll create later. Scroll to "Default Gateway" and select the Wireguard peer IP address just created, which in this example is 10.102.1.2 (your IP may differ). Click 'Update.'

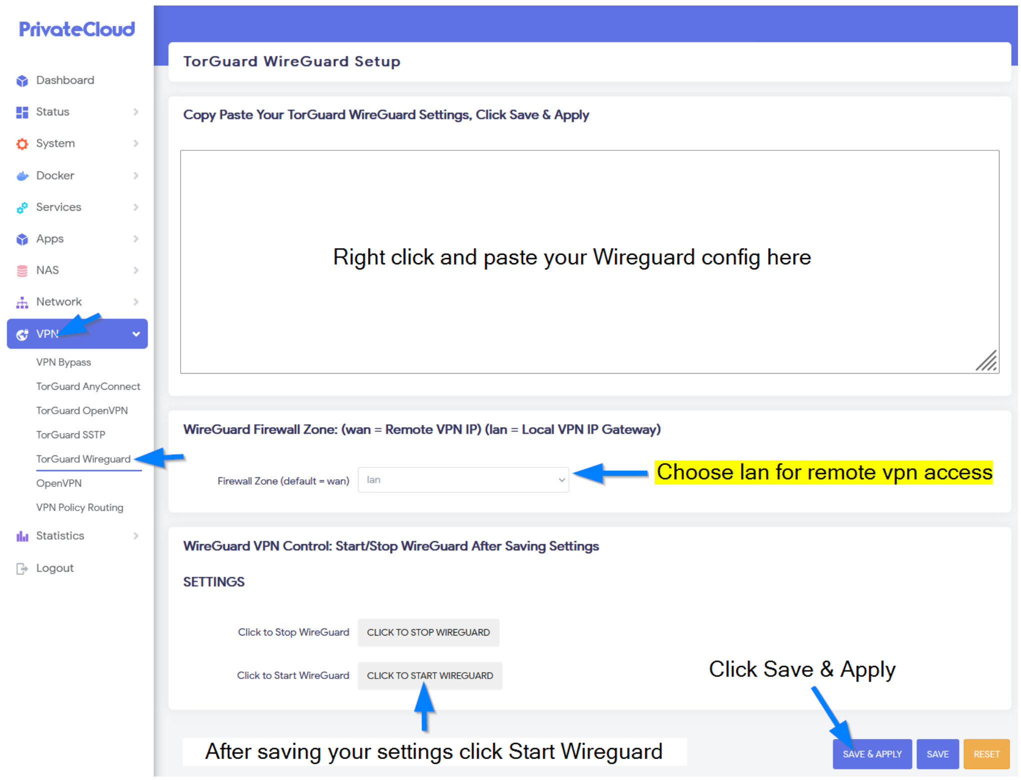


You've now added a Wireguard config for PrivateCloud and set a default gateway for your peers. To proceed, download the PrivateCloud config file by clicking "**Download Config**"



Add Your Local IP WireGuard config to PrivateCloud

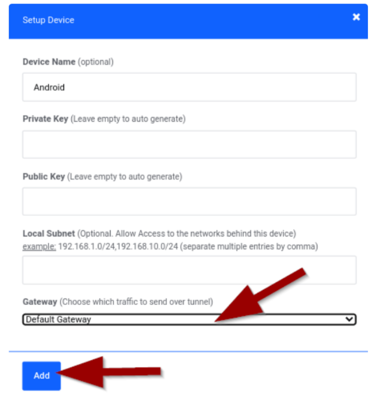
Connect to your PrivateCloud via Wi-Fi or a LAN cable. Navigate to 192.168.70.1 in a browser, go to the **VPN** tab, and select '**TorGuard Wireguard'** from the left panel. Open the downloaded Gateway Wireguard config and paste its entire contents in the provided text area. **For remote access VPN, choose "lan" from the dropdown menu** and click the "Save & Apple" button. Finally, click "Start Wireguard."



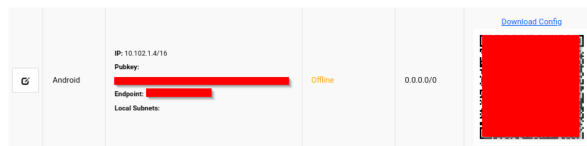
To confirm the Wireguard connection, go to the 'Network' tab and select 'Interfaces.' Under the "WG" interface, you should see RX and TX packets, indicating an active connection.

Create Wireguard Peers for your devices

It's time to add our first Wireguard peer. Back in the TorGuard Member's Area service panel Click "**Add device**," give it a name—in this example, "Android," as we're connecting a mobile device to the router. Under 'Gateway,' choose "**Default Gateway**," so the peer will connect to the OpenWRT Wireguard gateway. Click 'Add.' (Repeat this for additional devices.)

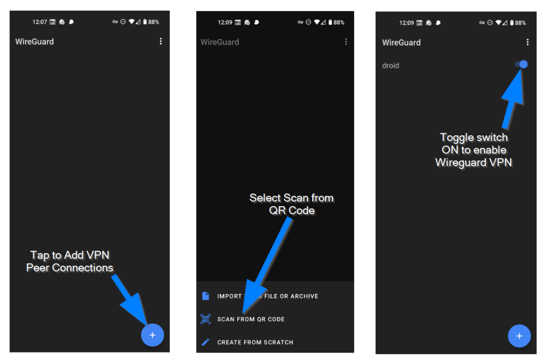


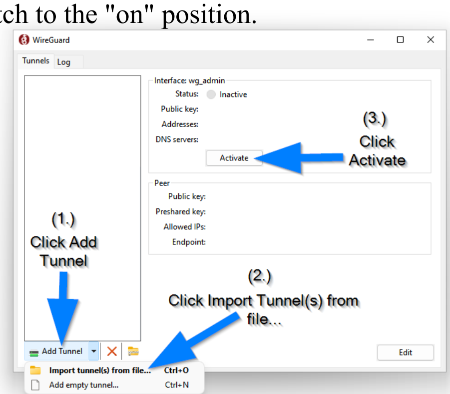
You will see a newly added peer in your TorGuard service panel:



Connect to WireGuard on Mobile and Desktop

To set up your new VPN connection on a mobile device, first grab the Wireguard client app from Google Play or the Apple App Store. Once installed, open the app and tap the "+" symbol to initiate adding a new VPN peer. Choose the 'Scan from QR Code' option thereafter. On your computer, locate the QR code option within your TorGuard Wireguard management panel. Point your mobile device's camera at this enlarged QR code to automatically input the Wireguard settings into your app. To activate your Wireguard VPN connection, simply toggle the switch to the "on" position.





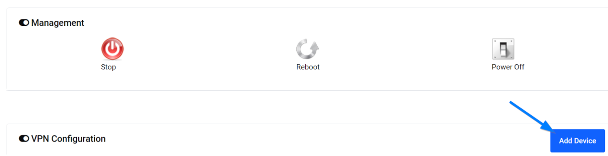
To set up a new VPN on your desktop, download the Wireguard client for Windows or MacOS. From your management panel, click 'Download Wireguard config' and save it. Open the Wireguard app, click 'Add Tunnel,' and choose 'Import Tunnel(s) from file.' Locate the downloaded config file and click 'OK.' Your new connection will appear; click 'Activate' to connect.

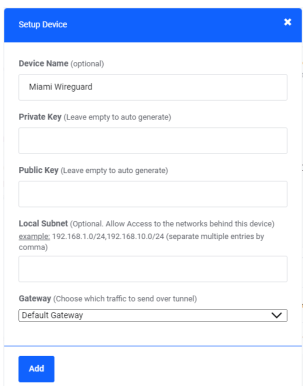
Option 2: Use Wireguard with an External VPN Server IP

Utilizing your external IP address via Wireguard, as opposed to your local IP, is another typical configuration. This enhances your IP privacy, as your PrivateCloud device will employ your external VPN server IP rather than your local one. Although this mode doesn't permit remote access for other peers, it does offer the flexibility to configure both internal and external Wireguard firewall port rules if you choose.. This is particularly useful if you opt to self-host services behind a domain secured with SSL.

Generate Your PrivateCloud Wireguard config

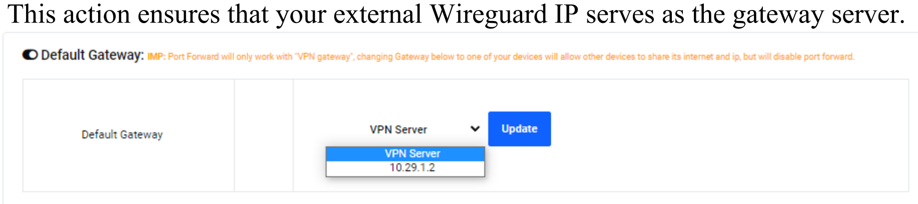
Start by clicking the "Add device" button to setup a PrivateRouter Wireguard connection to use your external Wireguard server IP address.



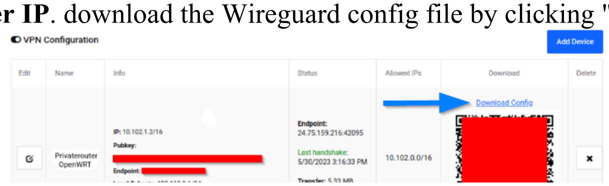


We're setting up an **external VPN IP connection**, so select "Default Gateway" under 'Gateway.' Click 'Add.'

Lastly, choose 'VPN Server' as your default gateway and click the 'Update' button. This action ensures that your external Wireguard IP serves as the gateway server.

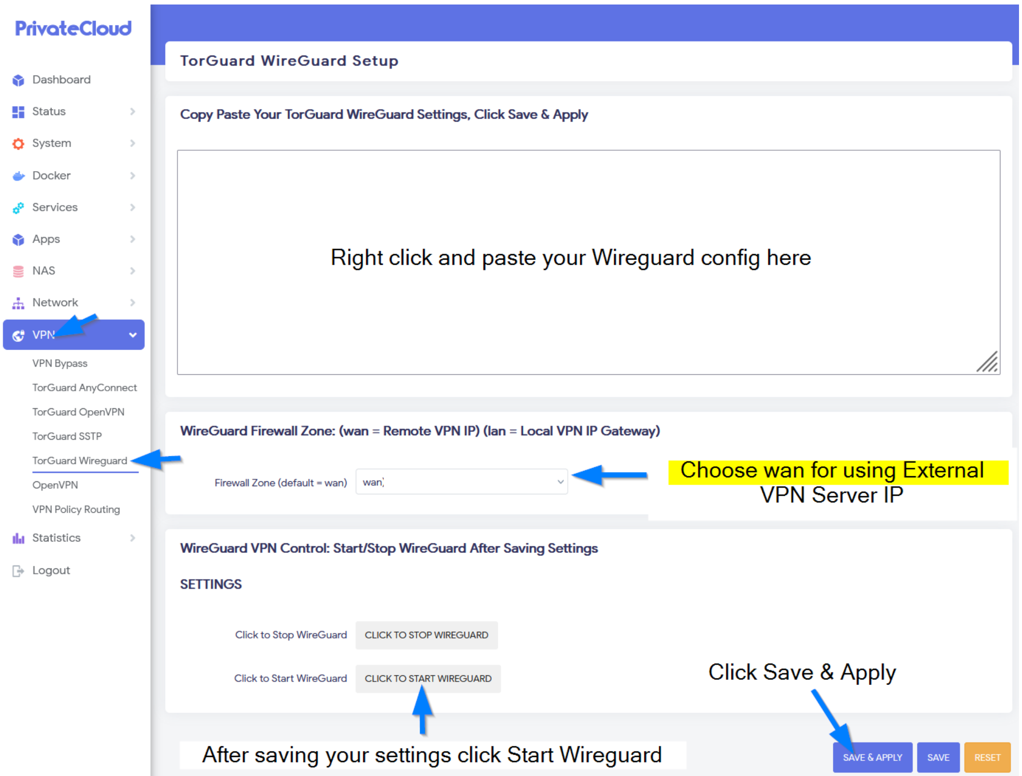


You've now added a Wireguard config for PrivateCloud and set a default gateway to use the **External VPN Server IP**. download the Wireguard config file by clicking "**Download Config**"

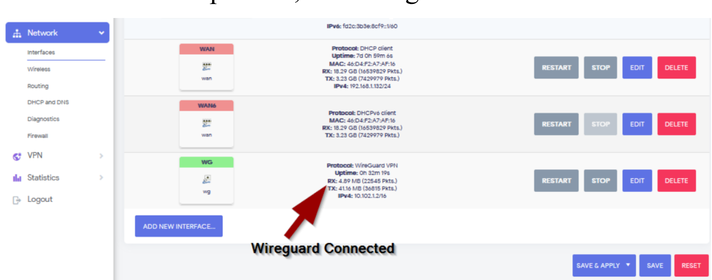


Adding the Wireguard config for External IP VPN

Connect to your PrivateCloud via Wi-Fi or a LAN cable. Navigate to 192.168.70.1 in a browser, go to the VPN tab, and select 'TorGuard Wireguard' from the left panel. Open the downloaded Gateway Wireguard config and paste its entire contents in the provided text area. For using the External Wireguard server IP, choose "wan" from the dropdown menu and click the "Save & Apply" button. Finally, click "Start Wireguard."



To confirm the Wireguard connection, go to the 'Network' tab and select 'Interfaces.' Under the "WG" interface, you should see RX and TX packets, indicating an active connection.

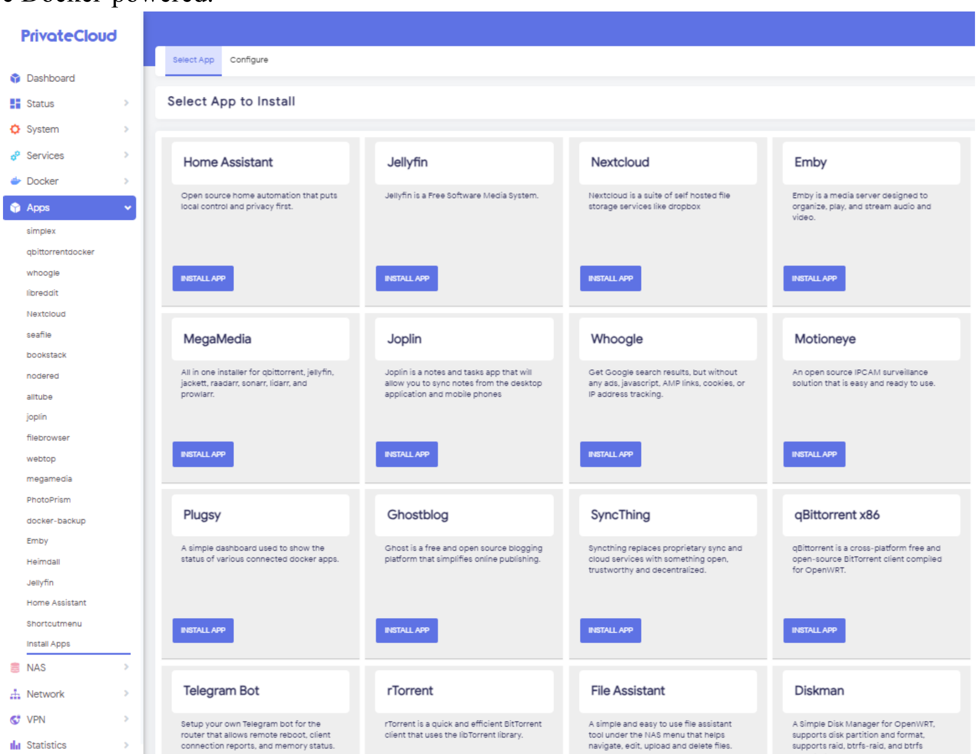


Chapter 2
PrivateRouter Apps

PrivateRouter OpenWRT features an enhanced storage build, offering 4GB for package storage and over 900GB+ of extra docker app storage. This allows for the installation of numerous third-party apps that wouldn't typically fit on the router's built-in storage.

Install PrivateRouter Apps

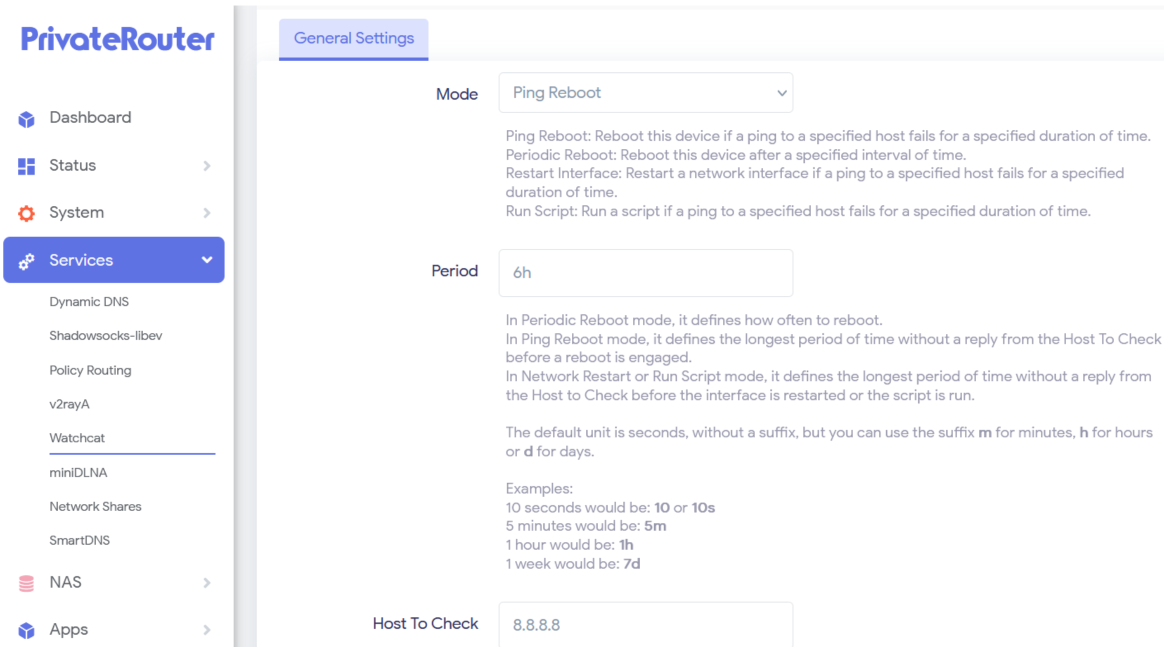
To add more third-party apps to your PrivateRouter, first navigate to the "Apps" option in the side menu and choose "Install Apps." For standard PrivateRouters, a list of all compatible apps will be displayed. If you're using a PrivateRouter Cloud device, you'll have the option to access over 100 apps that are Docker-powered.



After selecting the "Install App" button, scroll down to monitor the installation log and confirm that the app has been successfully installed. Once the app is added, you'll notice it appears in your side menu. For certain apps, you may need to log out and log back into the PrivateRouter menu to complete the process.

Configure Watchcat App to Minimize Downtime

To safeguard your network from unexpected ISP disruptions or VPN disconnections, you can utilize OpenWRT's Watchcat module to routinely ping a specific IP address. If there's no response, you can set a time duration for Watchcat to restart your router. Often, a simple reboot solves most connectivity issues.



To implement a Watchcat rule, go to the "Services" section in the side menu and choose "Watchcat." Choose "Ping Reboot" as the mode and specify a host IP for uptime checks.

After setting your preferences, scroll to the bottom of the page and click on "ADD" to activate the rule, followed by clicking the "SAVE AND APPLY" button. In this instance, the router will ping Google's DNS at 8.8.8.8. If there's no response after six hours, the router will automatically reboot.

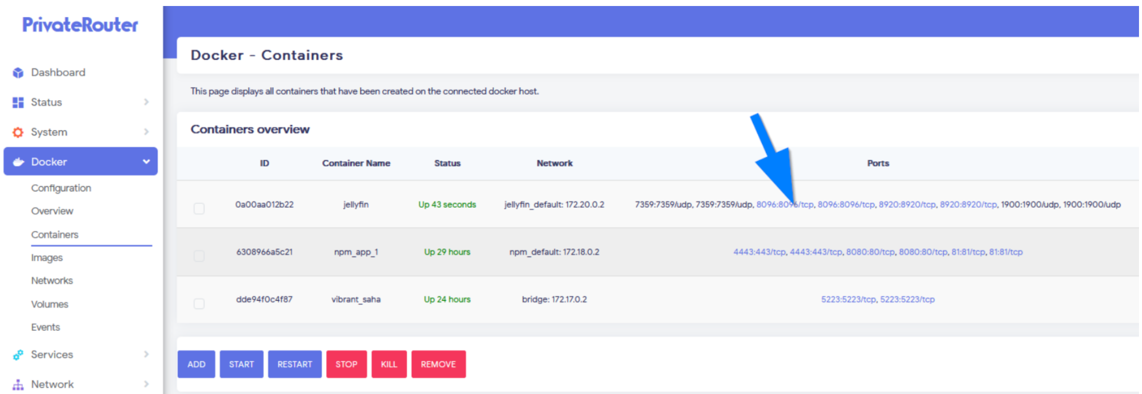
Watchcat offers additional reboot rules:

Periodic Reboot: This feature reboots the router after a set period.

Restart Interface: This setting will only reboot a specific network interface if a ping to a predetermined host goes unanswered for a specified length of time.

How to Access Docker Apps (PrivateRouter Cloud)

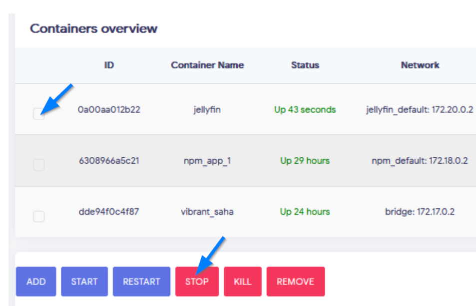
PrivateRouter Cloud x86 routers offer a simplified, one-click approach for deploying widely-used, self-hosted applications directly onto your router via Docker. Coupled with TorGuard's Private VPN Cloud service, you can effortlessly self-host apps while maintaining security through a WireGuard VPN. Jellyfin is a popular choice for a self-hosted media streaming server, providing you with control over streaming via a web interface and mobile apps for both Android and iOS.



To get Jellyfin up and running, first sign in to your PrivateRouter Cloud device. From the left-side menu, go to the "Apps" section and click on "Install Apps." Find Jellyfin in the list and click the "INSTALL" button. The installation time will vary based on your internet speed. Once the installation is finished, navigate to the "Docker" menu on the left and select "Containers." Here, you'll see all Docker apps listed as virtual containers. In this example, find the Jellyfin container and click on the TCP port 8096 to launch Jellyfin in a new browser window. Alternatively, you can manually enter the app port in a web browser by going to **192.168.70.1:8096.**

How to Start, Stop, or Remove Docker Apps

You can follow the same steps for every new Docker app you wish to install. Each application will be assigned its own unique port number, which you can find listed under the "Docker" menu in the "Containers" section. If you want to Stop, Start, or Remove any installed Docker app, simply check the box next to the specific app and then select the corresponding action button located below.

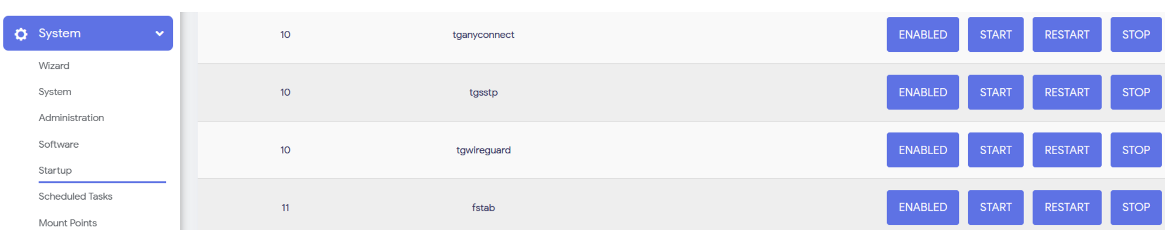


Troubleshooting the Internet Connection

TorGuard's VPN services are highly stable, often maintaining connections for months at a time without any interruptions. However, if you encounter a situation where your PrivateRouter device loses internet connectivity—especially after configuring various VPN or Router apps—you can usually resolve the issue with a few simple steps.

The quickest solution is often to reboot the router, which tends to resolve most connectivity problems. Alternatively, you can go to the "Network" tab located in the left-hand menu and select the "Interfaces" option. Here, you'll find the WAN (highlighted in red) and any VPN-specific interfaces you might have set up. Click the 'Restart' button next to each WAN interface, as well as next to the particular VPN protocol interface you're using. After waiting a few minutes, try to reconnect to the internet.

Similarly, if a particular application or service such as Samba or VPN is experiencing problems and you'd prefer not to reboot the entire router, you have the option to restart or stop that specific service individually. To do so, go to the 'System' tab in the left-hand menu and select 'Startup.' From there, find the service you want to restart and click the 'RESTART' button.



Should you continue to experience difficulties or have any inquiries regarding your PrivateRouter, you're welcome to file a support ticket on PrivateRouter.com or directly reach out to TorGuard support at **helpdesk@torguard.net**