Getting started

tunnel64 — your own routed network, one per device

Most VPNs put you behind one shared address along with everyone else. This one hands each of your devices its own routed IPv6 `/64` — a whole network, not an address — and optionally a public IPv4 that belongs to you alone.

This guide takes about ten minutes and covers everything you are likely to need.

1 Add a device

Sign in with your email address — we send a link, there is no password to remember. In your panel, type a name for the device and press **Add device**.

> **The configuration is shown once**
>
> It contains a private key that we never store and cannot recover. Download it or copy it somewhere safe before closing the dialog. If you lose it, press **new config** on that device and set it up again — nothing else is lost.

2 Install the WireGuard app

We use WireGuard, which has official apps for every platform. Get it from `wireguard.com/install` or your app store.

Platform	What to do
iPhone, iPad, Android	Open the app, tap **+**, choose **Create from QR code** and scan the code in your panel. Fastest way by far.
macOS, Windows	Open the app, choose **Import tunnel(s) from file**, and pick the **.conf** file you downloaded.
Linux	Save the file as `/etc/wireguard/wg0.conf`, then `sudo wg-quick up wg0`. Enable it at boot with `sudo systemctl enable wg-quick@wg0`.
Routers (OpenWrt, MikroTik, pfSense)	All support WireGuard. Use the values from the config file: the interface address, the peer key, and the endpoint.

3 Turn it on and check

Switch the tunnel on, then visit `https://ifconfig.co` in a browser. It should show one of our addresses rather than your own.

```
curl -4 ifconfig.co # our IPv4
curl -6 ifconfig.co # an address inside your own /64
```

Your addresses

Your account holds a block of IPv6 space, and each device you add takes its own **/64** out of it. A /64 contains 18,446,744,073,709,551,616 addresses. You can use as many of them as you like, at once, without asking us.

Device	Its own network
laptop	`2a10:fa80:4200:10::/64`
phone	`2a10:fa80:4200:11::/64`
home router	`2a10:fa80:4200:12::/64`

That last one matters: because a router receives a whole /64 rather than a single address, it can hand real, publicly reachable IPv6 addresses to every machine behind it. No NAT, no port forwarding.

Why each device needs its own configuration

> **Do not copy one configuration onto two devices**
>
> It will look like it works and then behave strangely. Traffic can only be delivered to one of them, and it will be whichever connected most recently — so the other stops receiving anything, with no error. It reads as an intermittent fault and it is not.
>
> Add a second device instead. Your plan allows 5 on standard and 10 on dedicated, and each one gets its own /64.

IPv4

On the standard plan your IPv4 traffic shares an address with other customers, which is how every VPN works. On the dedicated plan you get a public IPv4 that is yours alone, and incoming connections to it reach you.

Running something people can reach

A server, a game, a webcam, anything that has to accept incoming connections rather than start them.

Over IPv6

Your /64 has no NAT in front of it, so this works directly — but incoming connections are blocked by default, because most people do not expect their laptop to be reachable from the internet. Turn on **Let the internet start connections to this device** in your panel.

> **Understand what that switch does**
>
> While it is on, **every port on that device is reachable**, including things your operating system is listening on that you may not know about. Turn it on only if you know what is running. Replies to connections *you* start always work either way, so ordinary browsing needs nothing changed.

Over IPv4

This needs the dedicated plan. A shared address cannot forward incoming connections to any one customer — there is nothing to distinguish them by. With a dedicated address, incoming traffic is delivered to **one** of your devices: whichever is marked **inbound** in your panel. Press **inbound** next to a different device to move it.

Reverse DNS

You can set the reverse DNS (PTR) for your own addresses from the panel. This is what makes a mail server's name match its address, and it is what most receiving mail servers check first.

You hold	You can name
Your IPv6 block	Any address inside it.
A dedicated IPv4	That address.
A shared IPv4	Nothing — it is shared with other customers, so no single name would be right.

Changes usually appear within a few minutes.

Sending email

Outbound port 25 is blocked by default on every account. This is not about you: an address range that emits spam gets onto blocklists within hours, and then nobody's mail works. Ask us and we will usually open it — tell us briefly what you are sending and roughly how much.

> **Ports 587 and 465 are never blocked**
>
> If you are sending through a provider like Gmail, Fastmail or your own hosting, you are already using one of those and nothing is in your way. Port 25 only matters if you are running a mail server that delivers directly to other servers.

When something is wrong

What you see	What it usually is
It will not connect at all	The endpoint is UDP. A few hotel and corporate networks block UDP entirely; try a phone hotspot to tell the difference in a minute.
Connects, but nothing loads	Almost always MTU. Set the interface MTU lower in the app — try 1380. Ours defaults to 1420, which suits most links but not all.
Some sites work, others do not	Also MTU, and the same fix.
It connects but nothing loads *at all*, on every site	Different from the MTU case, where some things work. If nothing works and it just connected for the first time, tell us — it is usually something at our end, not yours.
It worked, then stopped	Check whether your subscription expired — we email you 7 days before, 1 day before, and once after. Nothing is deleted; renewing brings the same addresses back.
Two devices, one keeps dropping	The same configuration is on both. Add a second device instead.

What you see	What it usually is
Works on WiFi, not on mobile (or the reverse)	If your panel offers **automatic / IPv4 / IPv6** for a device, try pinning it to the other one. Some networks have one of the two badly broken, and your device keeps choosing it. Everything still goes through the tunnel either way.
A site says “VPN detected”	Some services block VPN address ranges. Nothing we can do at our end — turn the tunnel off for that site.
IPv6 does not work on some network	Some networks and sites still have no IPv6. Your IPv4 keeps working.

If none of that fits, email support@tunnel64.net with your account address and what you tried. Never send us your private key — we do not need it and we do not want it.

Billing

- Pay by card or crypto. Access starts as soon as the payment confirms.
- **Nothing renews automatically.** You are never charged without choosing to pay.
- We email you 7 days before your access ends, again the day before, and once after.
- Time you buy is added to what you already have, so renewing early never costs you days.
- Payments are final. There are no refunds, including for unused time — so if you are unsure, buy the shortest period first.

What we can and cannot see

The honest version, which is shorter than most:

We do not record	We do record
The content of your traffic. Where you connect to — no destinations, no domains, no URLs. Your DNS queries. Any connection or flow logs.	Your email address — that is your whole account. How many bytes moved, per device. When you last connected, and the address you last connected *from* — most recent only, overwritten each time. Payment records, as accounting law requires.

On a **shared IPv4**, many customers leave from the same address at once and we do not record which connection belonged to whom — so we could not tell anyone, including ourselves. On **your IPv6** or a **dedicated IPv4**, those addresses belong to your account, so they could be linked to your email address. Nothing else about you exists to link.

> **A VPN is not anonymity**
>
> It changes where your traffic emerges. It does not protect you from a compromised device, an account you are logged into, or a browser that identifies you. Anyone selling you anonymity is selling you something they cannot deliver.
>
> The full terms are at `www.tunnel64.net/terms`.

Anything else?

support@tunnel64.net