

PuriFi™

TAKE BACK YOUR PRIVACY



Owner's Manual

Read this before you plug anything in.

Model: PuriFi V1

Document revision A — August 2026

Contents

Setting up

1. What's in the box	5
2. Meet your PuriFi	6
3. Set up in three steps	9
4. Alternative setup: DNS server mode	14
5. Reading the screen	20
6. Your first five minutes	24

Using it

7. Everyday use	26
The main screen	26
Device settings	27
Finding a setting	28
Pausing and resuming protection	29
Lockdown	29
Checking it is really working	30
Advanced security	30
Content controls	31
Allowing a site that PuriFi blocked	32
Query logging and your privacy	34
Hiding your address from trackers	35
Your Daily Recap	35
Private VPN	36
Sharing with your household	39
Alerts	42
Renaming, unlinking, and starting over	43
8. Profiles and per-device rules	45
Which devices PuriFi can tell apart	45
Seeing every device on your Wi-Fi	46
Making a profile	47

What a profile controls	48
Pausing and scheduling	50
Deleting a profile	51
Your devices	51
New devices	53
9. Your account	55
What is on the page	55
Your name and photo	56
Setting a password	58
Linked accounts	59
Your phone number and text alerts	59
Where you are signed in	60
Getting a copy of your data	61
Signing out, and deleting	61
10. What PuriFi does not do	62
It does not block every ad	62
It does not make you anonymous	62
Double NAT	62
It cannot filter a phone away from home	63
It is not a commercial VPN service	63

When something is wrong

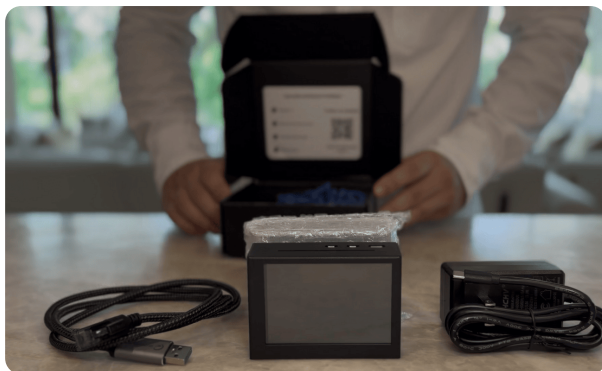
11. Troubleshooting	64
The screen never shows READY TO PAIR	64
A red arrow and blinking X	64
The app cannot find my device	64
“Device did not respond”	65
“This device hasn’t finished connecting yet”	65
“Registration blocked”	65
The picture is dimmed	65
A website or app has stopped working	65

The app says my device is offline	66
Nothing here helped	66
12. Care and safety	67

The small print

13. Specifications	68
14. Warranty and returns	69
15. Your privacy	72
16. Regulatory information	74
17. Open-source notices	76
18. Getting help	78

1. What's in the box



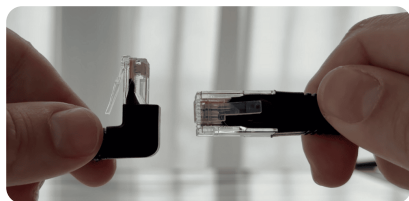
The device, its power supply and the USB-to-Ethernet cable. The Ethernet cable is not shown here.

PuriFi device — the unit with the small screen on the front.

Power supply — 27 W USB-C.

USB-to-Ethernet cable — USB on one end, Ethernet on the other. This is PuriFi's second network connection.

Ethernet cable.



Ethernet cable — an Ethernet plug on both ends.

One is right-angled to sit flat against the device.



USB-to-Ethernet cable — a USB plug on one

end, an Ethernet plug on the other.

Between them, the two cables cover both of the connections PuriFi needs. You do not need to buy anything, and you will not need the cable currently joining your modem to your router — you can unplug it and put it away.

There is no printed manual in the box. The QR code inside the lid brings you here, so this manual is always the current one — worth a bookmark.

You will also need

A phone, iPhone or Android, with Bluetooth switched on and the PuriFi app installed. Get it at **purifi.io/download**.

A way to sign in. You will create a PuriFi account during setup. Signing in with Google — or with Apple, on an iPhone — is the quickest route and needs nothing else. If you would rather use an email address and password, you will be sent a link to confirm the address, so pick an inbox you can check while standing next to the device.

Your Wi-Fi password, but only if you plan to connect PuriFi wirelessly rather than by cable — see page 16.

NOTICE

PuriFi is set up entirely from the phone app. There is no web page to log into, no setup wizard on a computer, and no code to type in from the box.

2. Meet your PuriFi

PuriFi sits between your modem and your router and checks every request your home makes before it leaves the house. Because it sits in the middle, it protects everything — phones, laptops, televisions, speakers, game consoles, doorbells — without you installing anything on them.

The two network connections

This is important, so it is worth thirty seconds.

PuriFi has **two** network connections and they are not interchangeable:

The built-in Ethernet port is the **modem** side. The cable from your modem plugs in here.

The USB-to-Ethernet cable is the **router** side. Its USB end plugs into one of PuriFi's USB ports, and its Ethernet end goes to your router.

Everything in your home stays connected to your router exactly as it is now. Nothing changes on your phones, and nothing changes in your router's settings.



Modem into the built-in Ethernet port; USB-to-Ethernet cable into a USB port.

The screen

The screen on the front is a touchscreen. It is not decorative — it tells you what PuriFi is doing at a glance, and it is the fastest way to diagnose a problem. Section 5 explains every state it can show.

Touch is reserved for features arriving in a later update. For now the screen is there to be read, not tapped.

The power button

There is a soft button on the right-hand side of the case. Press it once and PuriFi shuts down. Press it again to start it back up.

A press shuts PuriFi down properly rather than cutting the power, so it is the right way to switch the device off. You will not need it in normal use — PuriFi is meant to stay on, and it starts by itself whenever it has power.

NOTICE

Use the button rather than pulling the power lead out. Cutting power while PuriFi is writing to its memory card is the one thing most likely to damage it.

What PuriFi does not have

No reset button. If you ever need to reset it, you do that from the app — see page 43.

NOTICE

Do not remove the memory card. The card holds everything that makes your PuriFi yours, including the credential that links it to your account. Removing or reformatting it will unregister the device permanently.

Three ways to connect it

There is more than one way to set up PuriFi, and each comes with its own advantages.

1 Inline — the standard setup

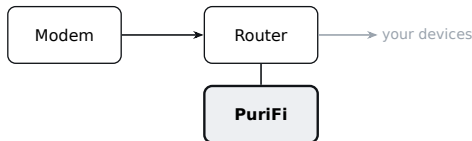


Pros Plug and play, best protection

Cons Double NAT, no per-device configurations

Putting your router into access point mode solves both issues. This is the optimal way of using PuriFi — see page 13.

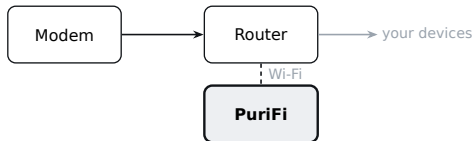
2 DNS server mode, wired



Pros No double NAT, per-device configurations

Cons One router setting to change; devices with their own DNS slip past

3 DNS server mode, over Wi-Fi



Pros No cable to PuriFi, no double NAT, per-device configurations

Cons Less steady than a wire; devices with their own DNS slip past

Section 3 covers the first. Section 4 covers the other two.

3. Set up in three steps

Step 1 — Put PuriFi between your modem and your router

1. Unplug the Ethernet cable that runs from your modem to your router — take it out at both ends and put it aside. You will not need it.
2. Take the **Ethernet cable** from the box. Plug one end into your modem, and the other into PuriFi's **built-in Ethernet port**.
3. Take the **USB-to-Ethernet cable** from the box. Plug the USB end into one of PuriFi's USB ports.
4. Plug its Ethernet end into your router's internet port — the one you just emptied. It is nearly always a different colour from the rest and labelled Internet or WAN.



2. The Ethernet cable goes into PuriFi's built-in port.



3. The USB-to-Ethernet cable goes into a USB port.



4. Its other end goes into your router's Internet port — the odd-coloured one, set apart from the LAN ports beside it.

NOTICE

PuriFi has to sit *between* your modem and your router. Plugging it into a spare port on the side of your router will not protect your home — traffic would never pass through it.

Step 2 — Plug in the power

Connect the power supply to PuriFi and to a wall outlet. PuriFi starts on its own.

Here is what you should see, and when:

When	On the screen
Straight away, for about 3 seconds	The screen lights up bright and blank
Then	Black, for a few seconds
Within about 20 seconds	The word PuriFi in cyan
Between 60 and 90 seconds	The full animation, with a pulsing green READY TO PAIR along the bottom



First few seconds. A bright, blank screen here is not a fault.



About 20 seconds in. The PuriFi name means it is starting up.



Pulsing green along the bottom of the screen.

When **READY TO PAIR** is pulsing on the screen, PuriFi is waiting for your phone. If you do not see it after a few minutes, go to page 64.

Step 3 — Pair with the app

1. Open the PuriFi app and create your account. You can use an email address and password, sign in with Google, or on an iPhone sign in with Apple.
2. If you used an email address and password, check your email and click the link to confirm your address — the app will notice on its own and move you along. Signing in with Google or Apple skips this step.
3. On the main screen, drag the panel at the bottom upwards, then tap **Add Device**.
4. Allow Bluetooth when your phone asks. PuriFi is set up over Bluetooth, so stay near the device.
5. Your PuriFi appears in a list, named **PuriFi** followed by a short code. Tap **Continue**.
6. The app checks the device's internet connection and shows **Internet Connection OK**.
7. If the app offers to remember your home Wi-Fi name, say yes. This lets Private VPN pause itself automatically when you are at home. You can skip it and set it later.
8. Tap **Register Device** and wait. You will see it work through **Registering your device...** and then **Your PuriFi is linked!**
9. Tap **Done**. Protection takes about another minute to arm itself. You can close the app — it finishes on its own.



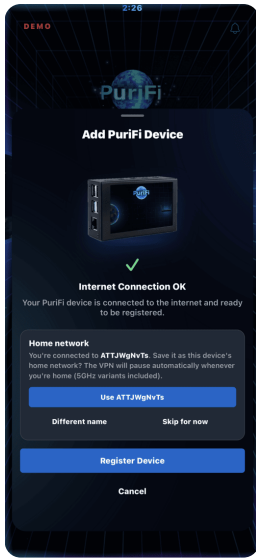
Steps 3-4

Drag the panel up, then tap Add Device.



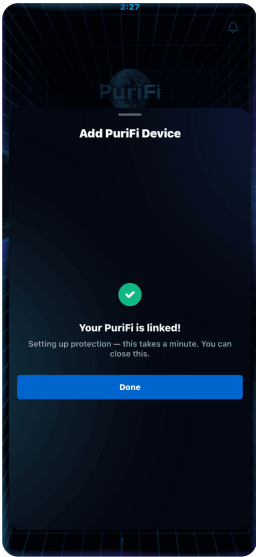
Step 5

Your PuriFi appears. Tap Continue.



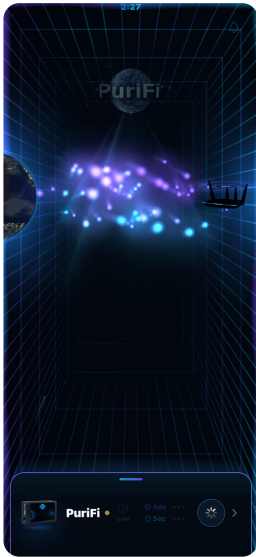
Steps 6-8

Internet checked. Save your home Wi-Fi, then register.



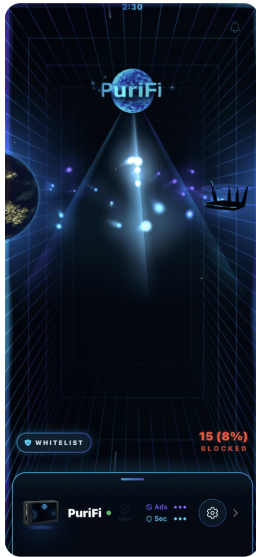
Step 9

Linked. Tap Done.



Right after Done

An amber dot means protection is still arming.



About a minute later

A green dot, and the counter starts moving.

How you know it worked. The green **READY TO PAIR** banner disappears from the screen within about five seconds of a successful pairing. That is PuriFi confirming it, independently of the app.



Armed and working. The pairing banner is gone, a blocked name is showing along the bottom, and the counter in the corner is running.

Registration usually takes under a minute. On some routers the secure connection can take up to three minutes to establish the first time — this is normal and needs no action from you. Keep your phone near the device while it works.

Two things you will notice. Before you add a device, the app runs a demonstration — the numbers you see are examples, not your household. And for about a minute after linking, the dot beside your device name is **amber** and the **Ads** and **Sec** indicators are greyed out while protection arms itself. When the dot turns **green** and the blocked counter starts moving, you are protected.

Worth ten minutes: access point mode

PuriFi and your router are both handing out addresses. That is what puts your home behind two layers of address translation, and why PuriFi sees your household as one device rather than as your phones, TVs and consoles. Handing both jobs to PuriFi fixes both.

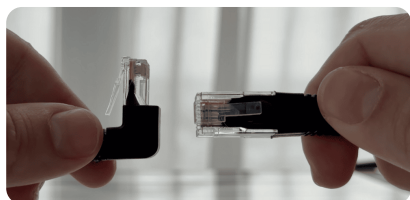
In your router's settings find Operation Mode — usually under Advanced or System — and choose Access Point. Keep the same Wi-Fi name and password so your devices reconnect on their own. Then move PuriFi's cable out of the router's Internet port into one of its numbered LAN ports: in access point mode the Internet port is unused. Per-device profiles (page 45) then work for everything in the house.

4. Alternative setup: DNS server mode

Almost everyone should use the inline setup in Section 3. It protects every device in the house, needs no changes to your router, and cannot be worked around.

But if you would rather not put PuriFi between your modem and your router, there is a second way to run it. In DNS server mode, PuriFi hangs off one of your router's LAN ports and acts purely as your home's DNS server. Your traffic no longer flows through it — your router simply asks PuriFi to look addresses up.

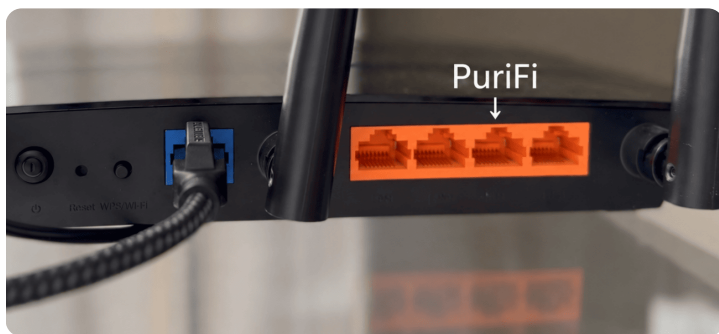
DNS server mode uses one cable — the plain Ethernet cable from the box. The USB-to-Ethernet cable is not used at all.



1. The Ethernet cable from the box. Use the right-angled end at the device.



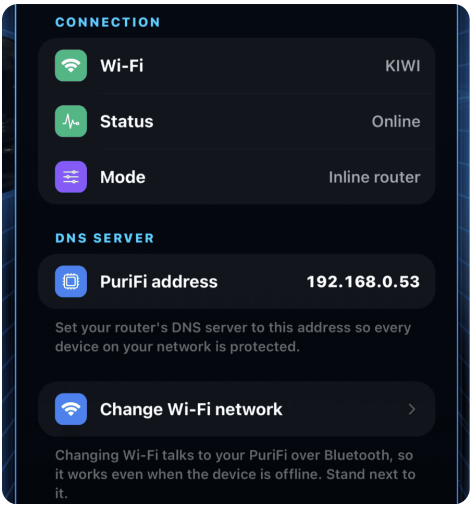
2. Into PuriFi's built-in Ethernet port.



3. The other end goes into any LAN port on your router — one of the numbered ones. Leave the Internet port alone; your modem stays plugged into it.

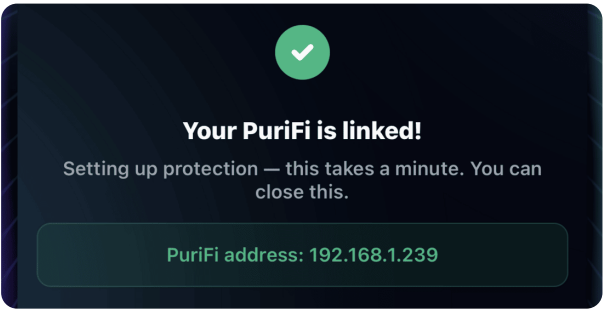
PuriFi tells you its address

You do not have to work this out yourself. Open **Network** in the device's settings and it is there under **DNS SERVER**, labelled **PuriFi address**.

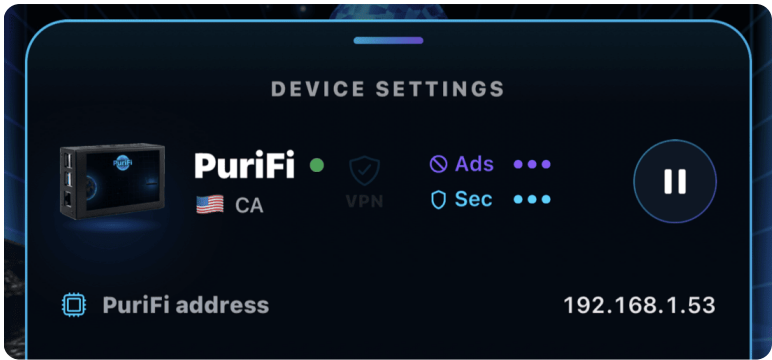


The **Network** page. **Mode** tells you which of the three setups this PuriFi is running.

The same address also appears in two other places:



At the end of pairing, under the confirmation.



And any time afterwards, at the top of **DEVICE SETTINGS** for that device.

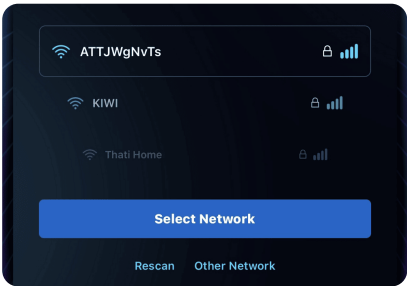
Use the one in DEVICE SETTINGS. That is the address PuriFi holds on to deliberately so it does not change — it usually ends in **.53**, after the numbered port that DNS runs on. Once your router is pointed at it you can leave it alone.

If you ever swap routers, PuriFi takes a new address on the new network. Open **DEVICE SETTINGS** again at that point and update your router to match.

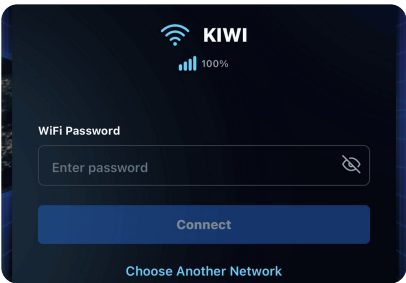
No cable? Use Wi-Fi instead

PuriFi does not have to be wired at all. If you leave its Ethernet port empty, it can join your home Wi-Fi like any other device and serve filtered DNS over that instead. Everything else in this section applies unchanged — it still takes an address, you still point your router at it.

The app offers this during setup when it sees the Ethernet port is empty. Pick your network, enter the password, and PuriFi joins. Your phone talks to it over Bluetooth while it does, so this works before PuriFi has any internet of its own.



1. Choose your network from the ones PuriFi can see.



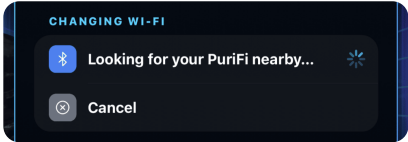
2. Enter the password and tap Connect.

Changing the network later

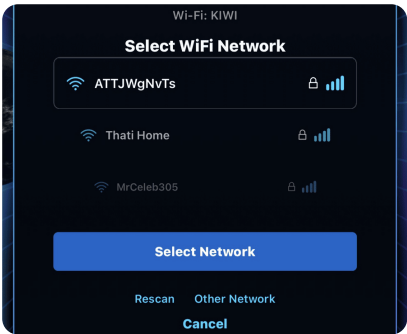
Open your device's settings, find **Network**, and tap **Change Wi-Fi network**. The page says the same thing this manual does — it talks to your PuriFi over Bluetooth, so it works even when the device is offline, and you need to be standing next to it.



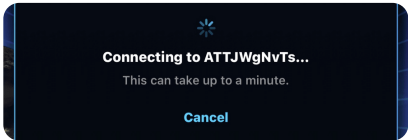
1. In **Network**.



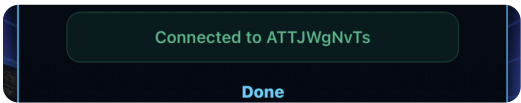
2. Your phone finds the device over Bluetooth.



3. The networks PuriFi can see. The one it is on now is named at the top.



4. It joins. This can take up to a minute.



5. Done.

NOTICE

Stand next to your PuriFi for this. Changing the network happens over Bluetooth, not over the internet, so your phone has to be within range of the device. That is also what makes it work when PuriFi has no working connection at all — which is exactly when you need it, if the password was wrong or your Wi-Fi has changed.

Joining can take up to a minute. The app shows **Connecting to Wi-Fi...** while it works, and tells you plainly if the password was refused.

NOTICE

A wired connection is steadier than Wi-Fi, and every device in your home depends on this one for name lookups. Use the cable where you reasonably can, and keep Wi-Fi for the places a cable cannot go.

One red arrow is normal here

Because the USB-to-Ethernet cable is not used in this mode, PuriFi shows a red arrow and a blinking red X for that unused connection, permanently. That is expected — it is the device telling you a port has nothing plugged into it, not a fault.

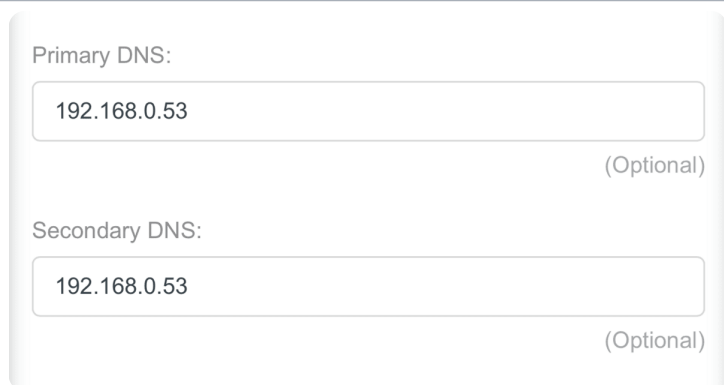


One red arrow, and nothing else wrong.

Everything else works normally. Setup, pairing and filtering all behave exactly as they do in the inline setup. If you see **two** red arrows, the cable to your router has come out.

Point your router at it

In your router's settings, find the DNS server fields. They are usually under LAN, DHCP, or Internet, and there are normally two of them. Set **both** the primary and the secondary to PuriFi's address.



Primary DNS:

192.168.0.53

(Optional)

Secondary DNS:

192.168.0.53

(Optional)

One router's DNS fields, with the same address in both. Yours will look different, and your address will not be this one — use the one from **DEVICE SETTINGS**.

NOTICE

Put the same address in both fields. If you leave your internet provider's DNS in the secondary field, your devices will quietly fall back to it whenever PuriFi is busy — and everything that goes through that fallback is unfiltered, with no indication that anything has changed.

Save the settings, then restart your devices or wait for them to pick up the change on their own. Most do within a day; restarting is faster.

What is different in this mode

Better: no second layer of address translation, so Plex, remote play, port forwarding and game servers behave as they did before. PuriFi also sits on the same network as everything else, so it can tell your devices apart — per-device profiles work for televisions and consoles, not just phones (page 45).

Worse: coverage depends on your router passing PuriFi's address to your devices. Anything with a DNS server built into it — some smart TVs, streaming sticks and IoT gadgets — ignores your router and slips past. Inline, those are caught anyway.

Switching between setups

You do not have to pair again to change your mind. Open **Network** in the device's settings: under **SETUP** there are two rows, **Inline Mode** and **Sidcar Mode**, with a check on the one you are running. Tap the other one and PuriFi walks you through it. It takes about a minute, and your router's DNS address stays the same when PuriFi is on your Wi-Fi.

To Inline Mode — wire first, then tap. Plug the modem into PuriFi's built-in Ethernet port and the USB-to-Ethernet cable into your router's Internet port, exactly as in Section 3. Then tap **Inline Mode**. PuriFi checks the wiring before it changes anything: if the USB adapter is missing, the modem is not on its Ethernet port, or the adapter's cable is on a LAN port instead of Internet, it tells you and leaves everything as it was. Your saved Wi-Fi keeps working as Wi-Fi discovery (page 45); turn it off any time under **Household**.

To Sidecar Mode — tap first, then wire. Tap **Sidecar Mode** while PuriFi is still wired inline (once the modem cable is moved, the app cannot reach it). Then move the modem cable back to your router's Internet port and plug PuriFi's Ethernet cable into any LAN port — or leave it on your Wi-Fi. Your home is offline between the tap and the re-wire, about a minute. Until you re-wire, **Mode** still says **Inline**; the note under **SETUP** reminds you what to move.

5. Reading the screen

The screen shows one of a few things. Learning these three-second checks will save you almost every support call.

What you see	What it means	What to do
Bright and blank	Powering up	Wait. It lasts about 3 seconds.
The word PuriFi in cyan on black	Starting up	Wait. About 20 seconds in.
The animation, with a pulsing green READY TO PAIR	Running, but not yet linked to an account	Open the app and tap Add Device
The full-brightness animation, with a count in the bottom-right corner	Working normally and protecting your home	Nothing
The whole picture dimmed , with red dots reaching the router	Filtering is off. Your internet works, but nothing is being blocked	Usually temporary — see page 65
A red arrow and a blinking red X	A network connection is unplugged, or the USB adapter is not working. In DNS server mode, one arrow is normal — see page 18	Check both cables — page 64



A working screen. Blue dots are ordinary requests on their way out; red ones are being shot down. The name along the bottom is what was just blocked, and the corner keeps the running count.

Give the screen a day to settle. The display calibrates itself over its first 24 hours, and it keeps improving for a while after that.

The moving picture

The animation is a live view of your home's internet activity, not a screensaver.

Each dot travelling from the globe to the router is one real request from a device in your home. Dots that turn **red** and get shot down are requests PuriFi blocked. Dots that pass through untouched are ordinary traffic being allowed. When your household is quiet, the screen is quiet.



The earth on the left is the internet, the router on the right is your home. The ball in the middle is PuriFi, catching what should not get through.

The counter

The number in the bottom-right corner is how many requests PuriFi has blocked today, followed by what share of all traffic that represents.



Protection off: the picture dims and red dots reach the router untouched.

If you have turned query logging off (page 34), the counter disappears entirely rather than showing a misleading zero.

Names on the screen

When PuriFi blocks something, the name of the company behind it appears briefly along the bottom of the screen, with the reason underneath. Each name stays for about five seconds.



This is the same information the app shows under **Recently Blocked**, just faster to glance at.

6. Your first five minutes

Protection turns itself on

There is nothing to switch on. About a minute after pairing finishes, PuriFi arms itself and starts filtering — the dot beside your device name turns from amber to green, and the blocked counter starts moving.

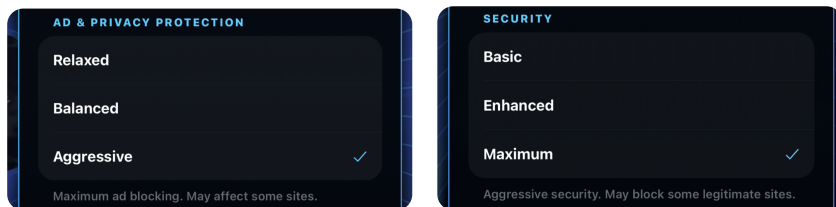
It arms at the strongest settings, so you are fully protected without touching anything.

Before it is paired, PuriFi does not filter. It passes your traffic straight through. That is deliberate — your home has working internet from the moment you plug the device in, even before you have paired it, and even if pairing fails.

Changing your levels

PuriFi arrives already set to **Aggressive** and **Maximum**, and you do not have to touch either. You only need this if you want to dial the strength up or down.

In the app, open your device's settings and find the **BLOCKING** section. There are two lists. Tap the level you want in each; a tick marks the one in use, and the line underneath tells you what it does.



Ad & Privacy Protection — how hard PuriFi blocks advertising and tracking.

Security — how hard it blocks dangerous sites.

A tick marks the level in use, and its description sits underneath. Both arrive at the strongest setting.

There is a short pause before a change takes effect. After you tap a level, PuriFi waits about three seconds before applying it — so you can change your mind, or set both rows, without it rebuilding twice. Every new tap starts those three seconds again. When you stop tapping, the change goes live.

Ad & Privacy Protection decides how aggressively PuriFi blocks advertising and tracking:

Level	What the app says
Relaxed	Light ad blocking. Most sites work normally.
Balanced	Blocks ads, trackers, and telemetry.
Aggressive	Maximum ad blocking. May affect some sites.

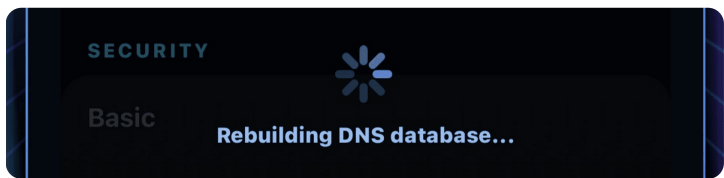
Security decides how aggressively PuriFi blocks dangerous sites:

Level	What the app says
Basic	Blocks known malware and phishing domains.
Enhanced	Blocks malware, phishing, scams, and C2.
Maximum	Aggressive security. May block some legitimate sites.

If a site you trust stops working, you do not need to turn protection down — just add that one site to your allowed list (page 32). That keeps everything else at full strength.

What happens next

While it arms itself, PuriFi downloads and builds its block list. This takes up to about five minutes the first time, and again whenever you change a level.



The app shows this while the new list is built.

The screen may dim while the list builds. Building the list is the one moment where blocking is briefly switched off, so the screen honestly shows protection as off until it finishes. Your internet keeps working throughout. When it is done, the picture returns to full brightness and you will see PuriFi start shooting down red dots.

Depending on the levels you choose, PuriFi will be checking against somewhere between a few hundred thousand and several million known advertising, tracking and malicious addresses. It refreshes that list every day on its own.

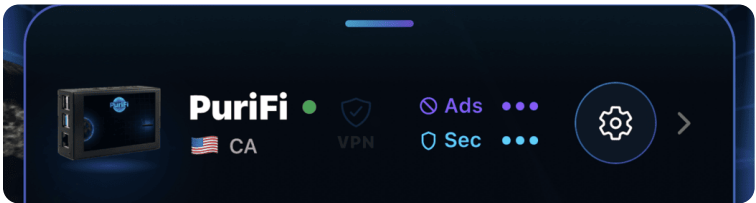
7. Everyday use

The main screen

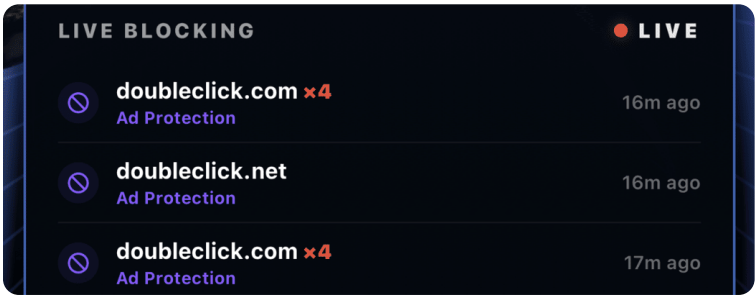
Opening the app lands you on the same portal animation your PuriFi is showing, driven by the same live traffic. Two things sit on top of it: the **blocked count** in the corner, which opens your Daily Recap, and the **WHITELIST** pill, which opens the allowlist.

Everything else is in the panel along the bottom. Drag it upwards and it expands.

Your device sits at the top — name, whether it is protecting, and the pause button. Tap the arrow beside the name to open **DEVICE SETTINGS**, which is where the rest of this section lives.



LIVE BLOCKING is a running feed of what PuriFi is stopping, as it happens, each entry labelled **Ad Protection**, **Security** or **Protection**. Tap any domain to allow it. When your household is quiet it simply says it is waiting.



A count beside a name means it was blocked more than once. **LIVE** means the feed is connected.

PURIFI PROTECTION is the summary: a badge reading **Healthy**, **Degraded** or **Offline**, the word **Active** or **Passthrough**, today's queries and blocks, and a link to the Daily Recap.

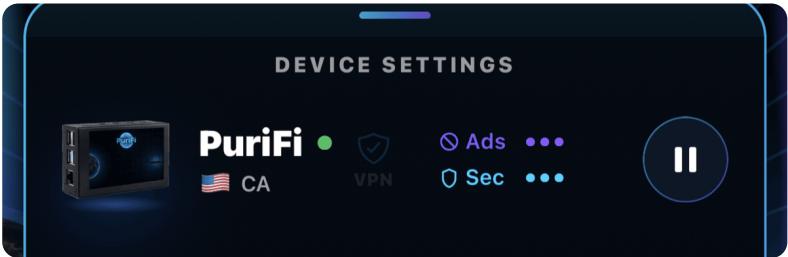


Remote access is Private VPN — see page 36.

Passthrough means PuriFi is passing traffic through without filtering. That is normal while a blocklist rebuilds, and it is what you see before the device has been set up. If it stays that way, see page 65.

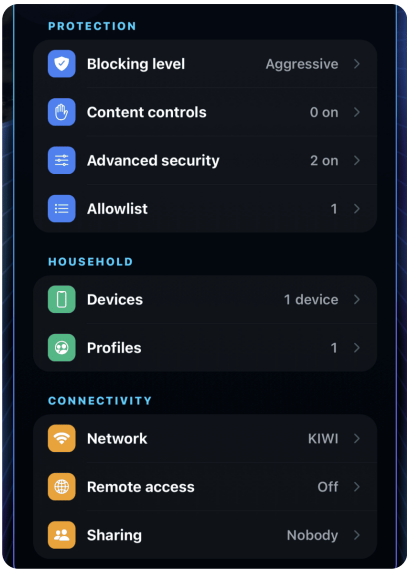
Device settings

Everything from here on lives one level deeper. Tap the arrow at the right of the device band and **DEVICE SETTINGS** opens — a separate screen, with the same band across the top so you know which device you are working on.

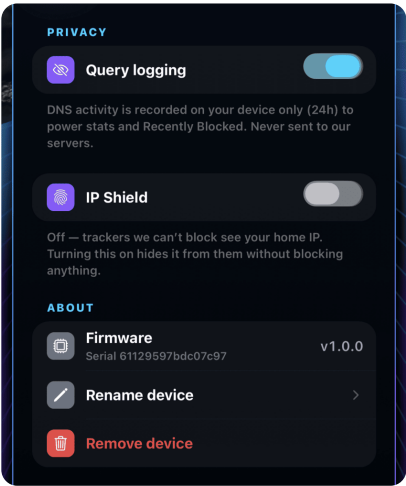


The same band, now at the top of its own screen.

Below it, every setting is grouped under headings. This is the map for the rest of the section.



PROTECTION, HOUSEHOLD and
CONNECTIVITY.



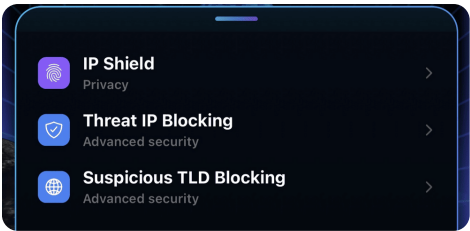
Further down: **PRIVACY** and **ABOUT**, with your
firmware version and serial number.

Finding a setting

There are a lot of switches in here. Rather than hunting through the menus, tap **Search settings** at the top of **DEVICE SETTINGS** and type what you are after.



Search matches more than the exact wording — looking for “ads”, “porn” or “bedtime” will find the right switch even though none of those is what it is called. Each result shows where it lives, so you learn the layout as you go.



Typing ip finds three different settings, each labelled with the section it belongs to.

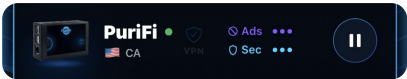
Tap one and PuriFi takes you straight there, with the setting highlighted so you can see which one it meant.



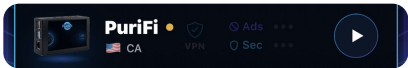
Search covers the settings themselves, not your content — it will not find a particular device, profile or allowed domain by name. It also only shows settings you can actually reach: switches that are unavailable, for a guest or while protection is paused, stay out of the results rather than appearing and doing nothing.

Pausing and resuming protection

The round button at the right of the device band switches filtering on and off. Your internet keeps working either way — pausing only stops the blocking.



Protecting. Green dot, **Ads** and **Sec** lit, and a pause button.



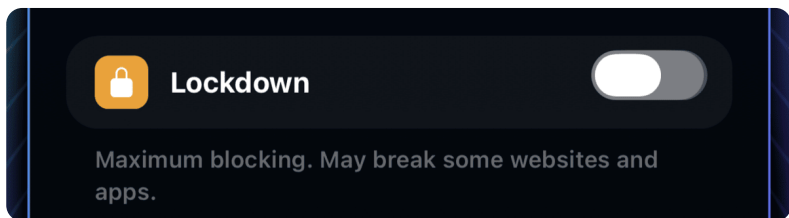
Paused. Amber dot, the levels greyed out, and a play button to start again.

Use it when you want to check whether PuriFi is the reason something is not loading. Pause, retry, and if the problem goes away you have found your answer — then add that site to your allowed list rather than leaving protection off.

Lockdown

LOCKDOWN turns everything on at once: every security option, every content control, maximum levels. The app warns you plainly —

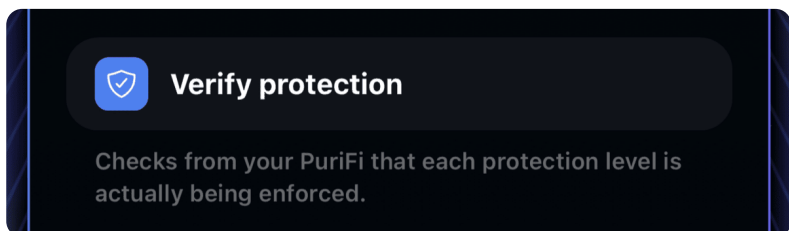
Maximum blocking. May break some websites and apps. — and it is not exaggerating.



While Lockdown is on, the individual switches are held on and cannot be changed. Turn Lockdown off to get back to your own settings, which are remembered.

Checking it is really working

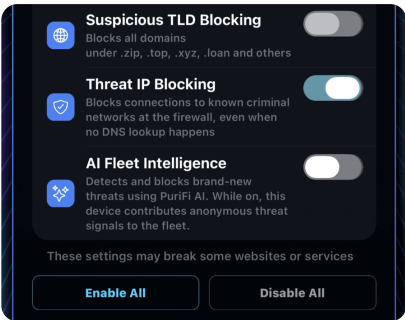
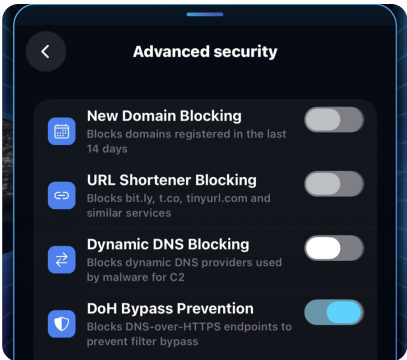
Verify protection asks the device itself, rather than trusting the app's own idea of what it sent. In the app's words, it *Checks from your PuriFi that each protection level is actually being enforced.*



Worth a tap after you change something, or any time you want reassurance that what the app is showing you is what the device is doing.

Advanced security

These are off unless you turn them on. They live on their own **Advanced security** screen, which carries the warning *These settings may break some websites or services.* **Enable All** and **Disable All** at the bottom switch the whole set at once.



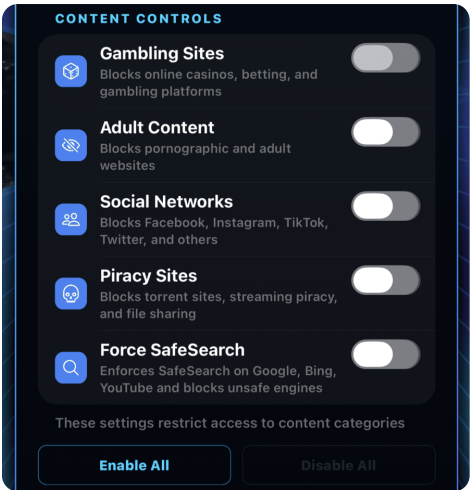
Setting	What it does
New Domain Blocking	Blocks domains registered in the last 14 days
URL Shortener Blocking	Blocks bit.ly, t.co, tinyurl.com and similar services
Dynamic DNS Blocking	Blocks dynamic DNS providers used by malware for C2
DoH Bypass Prevention	Blocks DNS-over-HTTPS endpoints to prevent filter bypass
Suspicious TLD Blocking	Blocks all domains under .zip, .top, .xyz, .loan and others
Threat IP Blocking	Blocks connections to known criminal networks at the firewall, even when no DNS lookup happens
AI Fleet Intelligence	Detects and blocks brand-new threats using PuriFi AI. While on, this device contributes anonymous threat signals to the fleet.

NOTICE

DoH Bypass Prevention stops Apple iCloud Private Relay from working. It also switches browsers that were using encrypted DNS back to ordinary DNS, so that PuriFi can see and filter their requests. Both effects are intended — they are how the setting prevents devices from routing around your filtering — but if iCloud Private Relay stops working after you enable this, now you know why.

Content controls

Also off by default. These block categories of content rather than threats, and carry their own warning — *These settings restrict access to content categories*. As with advanced security, **Enable All** and **Disable All** switch the set at once.



Setting	What it does
Gambling Sites	Blocks online casinos, betting, and gambling platforms
Adult Content	Blocks pornographic and adult websites
Social Networks	Blocks Facebook, Instagram, TikTok, Twitter, and others
Piracy Sites	Blocks torrent sites, streaming piracy, and file sharing
Force SafeSearch	Enforces SafeSearch on Google, Bing, YouTube and blocks unsafe engines

The switches here apply to everything in your home. If you would rather set different rules for different people or devices — stricter for the kids, looser for you — use profiles instead, on page 45.

NOTICE

Content filtering is a useful layer, not a guarantee. No filter catches everything, and it should not be the only thing standing between a child and the internet.

Allowing a site that PuriFi blocked

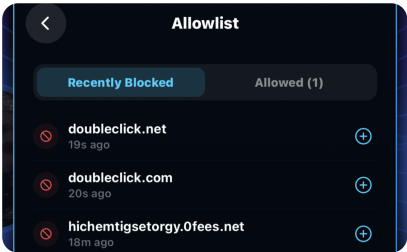
If something you trust stops working, allow it rather than turning protection down.



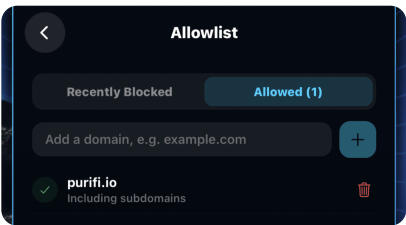
On the main screen.

Open **Allowlist** from the device's settings, or tap the **WHITELIST** pill on the main screen — both open the same place. It has two tabs.

Straight from the live feed. Drag the panel at the bottom of the main screen upwards and **LIVE BLOCKING** shows what PuriFi is stopping as it happens. Tap any domain in that list and the allowlist opens already asking whether to allow that one — useful the moment you notice something being blocked that you wanted.

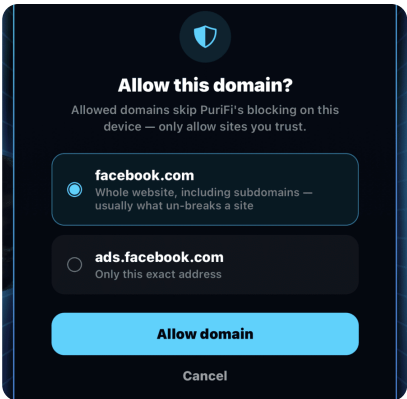


Recently Blocked lists what PuriFi has just stopped. Tap + beside anything you recognise.

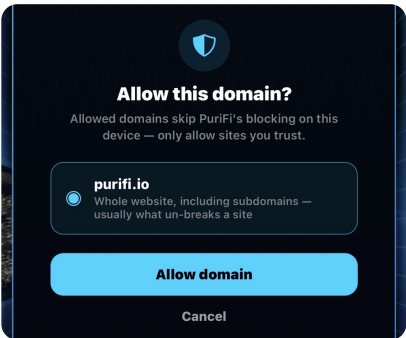


Allowed is what you have let through. You can also type a domain in by hand.

Either way, PuriFi asks how much to allow:



Where the blocked address is a subdomain, you choose between the whole website and that one address.



Where it is already a plain domain, there is only one thing to allow.

The first option — *Whole website, including subdomains* — is usually what un-breaks a site, and it is preselected. Pick the exact address only when you want to allow one thing and nothing else.

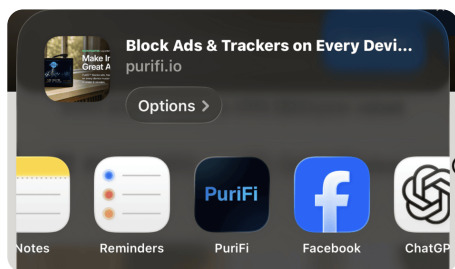
NOTICE

Allowing a site takes about a minute to take effect while PuriFi rebuilds its blocklist. The entry appears in **Allowed** straight away, but give it a moment before you decide it has not worked.

Remove anything you have allowed with the bin icon beside it.

Allowing a site without opening the app

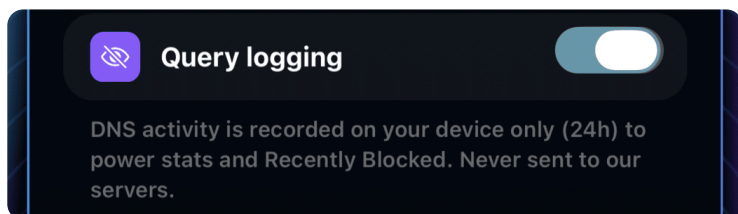
You do not have to go looking for the address. In your browser, tap Share and choose **PuriFi** — the app opens straight on the confirmation step for whatever site you were on.



PuriFi appears in the share row like any other app.

Query logging and your privacy

PuriFi keeps a short record of the addresses your household looks up, so it can show you statistics and the **Recently Blocked** list. In the app's words:



DNS activity is recorded on your device only (24h) to power stats and Recently Blocked. Never sent to our servers.

You can switch it off. Under **PRIVACY**, turn off **Query Logging** and PuriFi stops recording and permanently deletes what it has already stored:

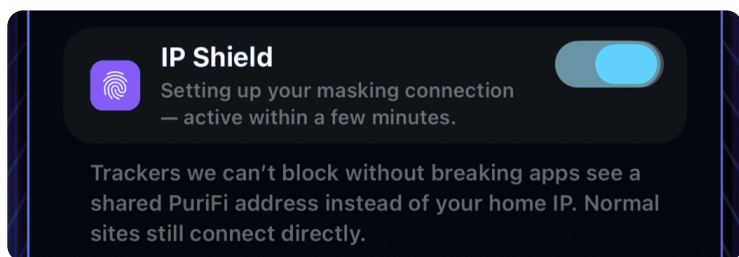
Off — nothing is recorded. Stats and Recently Blocked are unavailable; blocking keeps working.

Blocking is unaffected. What you give up is the statistics, the Daily Recap, the Recently Blocked list, and AI Fleet Intelligence, which needs the log to work.

Hiding your address from trackers

Some tracking companies cannot be blocked outright without breaking the apps they are built into. **IP Shield**, under **PRIVACY**, deals with those differently:

Trackers we can't block without breaking apps see a shared PuriFi address instead of your home IP. Normal sites still connect directly.



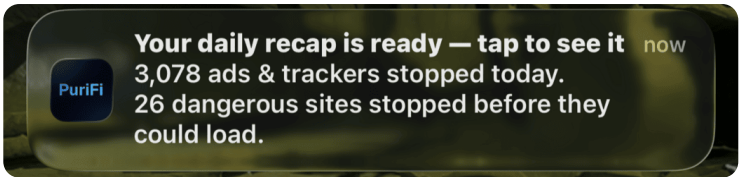
Just switched on. It takes a few minutes to become active.

It is off unless you turn it on. Ordinary browsing is unaffected — this only changes what a short list of tracking endpoints can see.

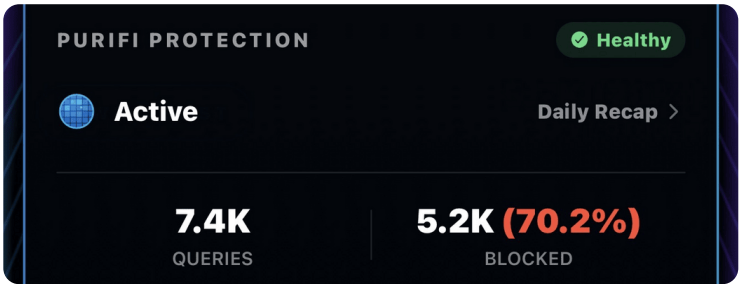
Your Daily Recap

Once a day PuriFi sends you a summary — how much junk it stopped, what percentage of your traffic that was, which company was the worst offender, and your busiest hour.

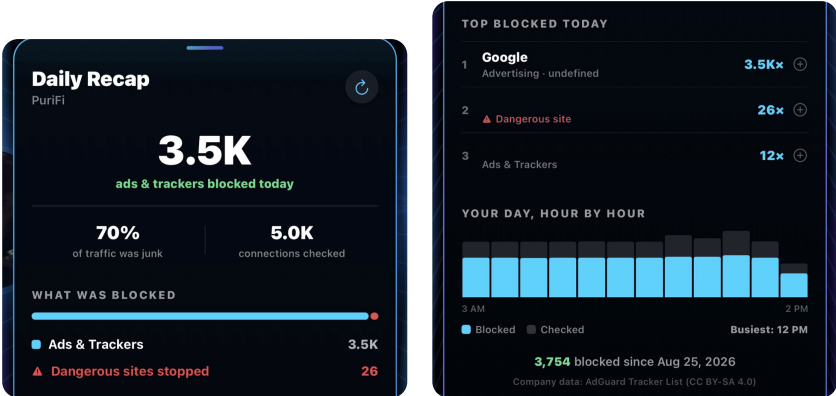
It arrives as a notification on your phone. Tap it and the report opens in the app. You can also just tap the blocked count on the main screen — the number in the corner is a button.



If you missed it, you can find the same report any time on the main screen: drag the panel at the bottom upwards and tap **Daily Recap** in the **PURIFI PROTECTION** panel.



The panel also shows whether protection is **Healthy**, and today's running totals.



How much was stopped, and what share of your traffic that was.

Who was responsible, and your day hour by hour.

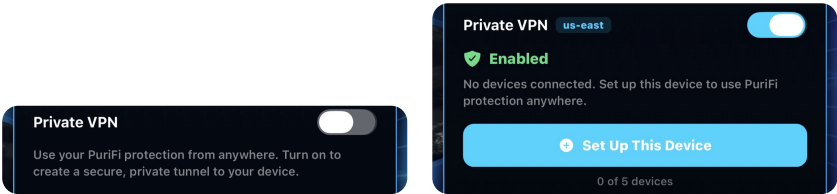
Tapping any company in that list takes you straight to the allow flow, in case something on it turns out to be a site you actually wanted.

Private VPN

At home, everything is protected. The moment you walk out of the door with your phone, it is not.

Private VPN fixes that by building an encrypted connection from your phone back to **your own PuriFi**, so that your phone keeps the same filtering anywhere in the world. Your traffic goes to the device in your house, not to a company's server.

Open **DEVICE SETTINGS** and find it under **Remote access**.



Off. The switch turns the feature on for the household.

On, with nothing connected yet. The badge names the relay region nearest you.

Tap **Set Up This Device** to add the phone in your hand. It will ask permission to add a VPN configuration — this is normal, and PuriFi's filtering at home keeps working whether you allow it or not.



Each PuriFi supports up to **five** connected phones and laptops in total, shared across everyone in the household. Remove one with the bin icon beside it.

Knowing it is on

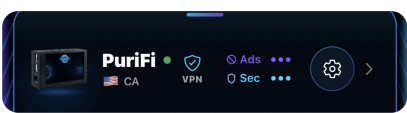
The status line tells you how the tunnel is carrying your traffic. There are two answers, and both are fine.



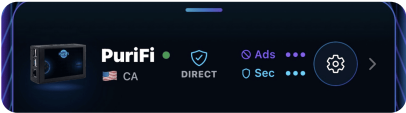
Direct connection. Your phone reaches your PuriFi straight, with nothing in between.

Routing through relay. The same tunnel, taking a slightly longer path.

The device band tells you the same thing at a glance.



VPN — a tunnel is live.

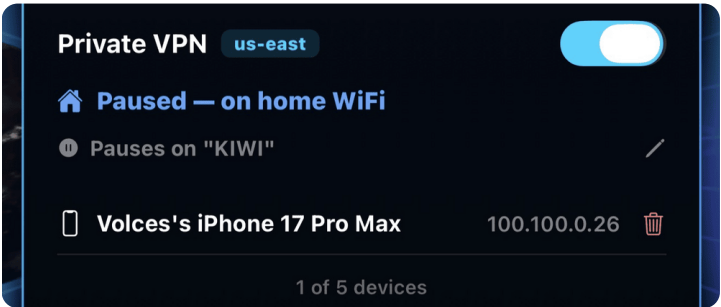


DIRECT — and it is a direct one.

Neither is better for your privacy. PuriFi prefers a direct connection, but many networks will not allow one — so it falls back to a PuriFi relay. Either way the tunnel is encrypted end to end and nobody in the middle can read it. The relay only forwards, it cannot see inside.

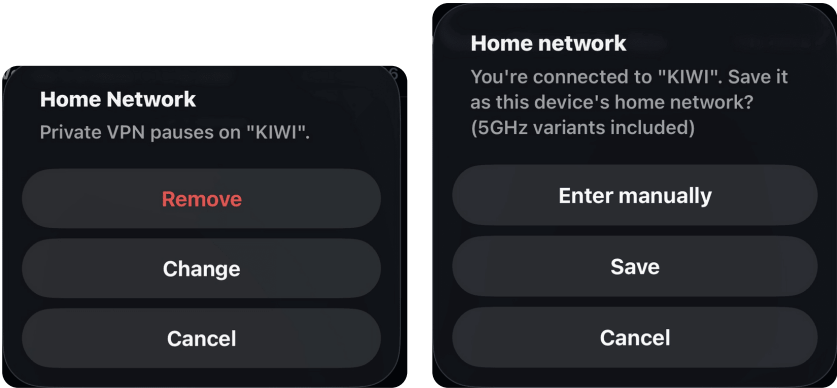
Auto-pause at home

You do not need the tunnel while you are sitting on your own network, so PuriFi switches it off there and back on when you leave.



Paused because the phone is on the saved home network.

If you saved your home Wi-Fi name during setup this already works. To change it, tap the pencil beside **Pauses on**.



Change picks up the network you are on now; **Remove** turns auto-pause off. Saving the network you are on. 5 GHz variants are matched too.

If you would rather type it, **Enter manually** takes the name — and it is case-sensitive, so it has to match your Wi-Fi exactly.

If your PuriFi goes offline

The tunnel runs to the device in your house, so a power cut or an internet outage at home leaves it with nothing to reach. You do not have to do anything about it.

When PuriFi stops answering but your phone’s own connection is fine, the tunnel steps aside on its own so your phone keeps working normally. It says so plainly rather than leaving you guessing.



Paused — PuriFi is offline. The band shows **PAUSED** and a crossed-out cloud.

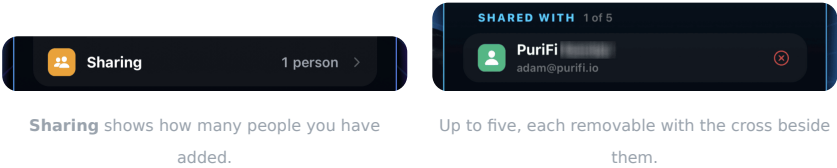
When your PuriFi comes back, the tunnel comes back with it — no tapping required. You will also get a message when it goes offline and another when it returns.

Sharing with your household

Other people can use your PuriFi’s Private VPN without having any control over your settings. They get protection on the road; you keep the keys.

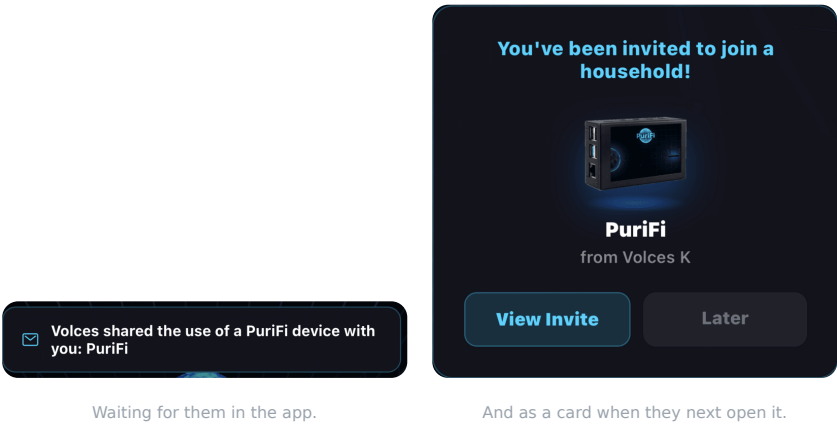
Inviting someone

Open **Sharing** in your device's settings and enter their email address.

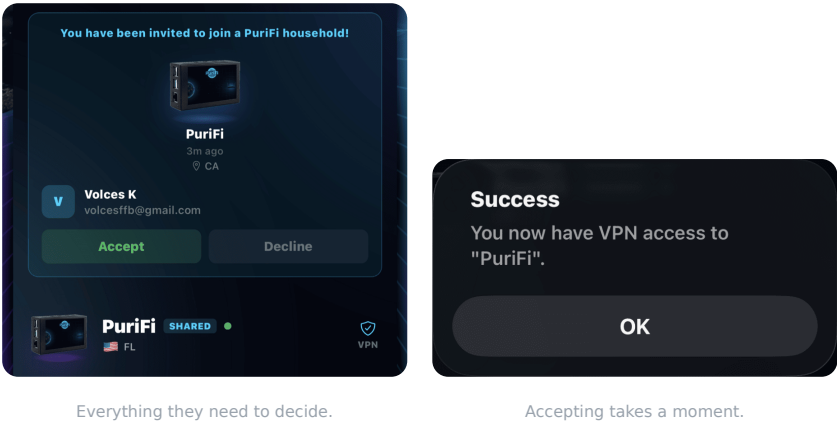


What they see

They get an email, and a notice in the app if they already have it installed — the bell on the main screen picks up a red dot.



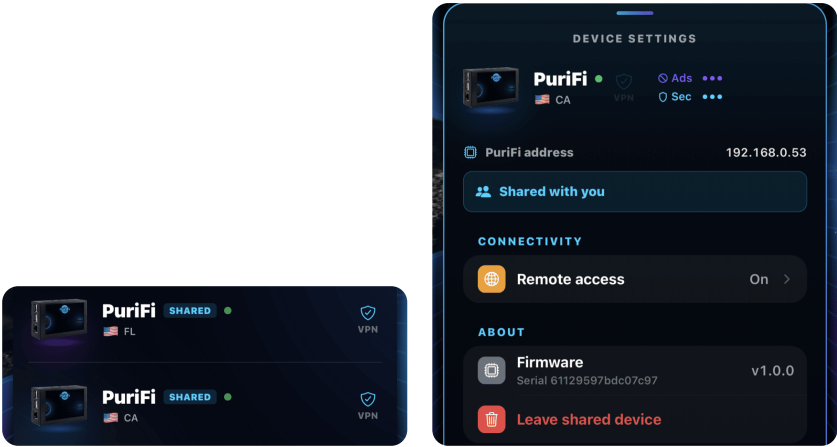
Opening the invitation shows them which device it is, who sent it, and two buttons.



Invitations expire after **seven days**. You can renew or cancel one at any time.

What a guest can and cannot do

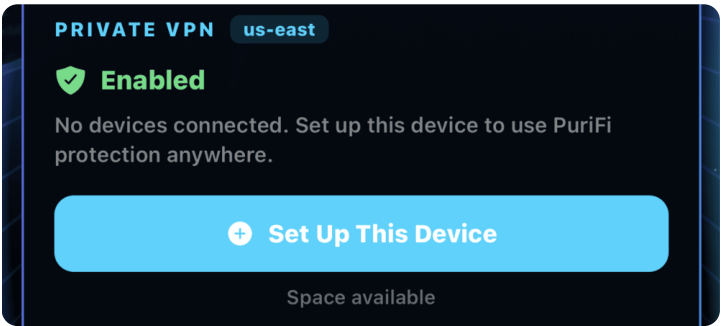
The device appears in their list with a **SHARED** badge, and their settings screen is much shorter than yours: **Shared with you** at the top, remote access, and a way out.



Shared devices are labelled in the list.

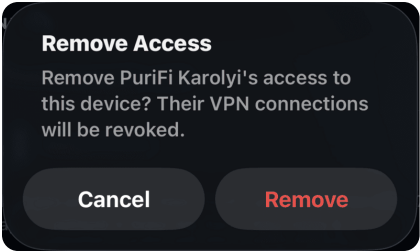
A guest's settings: no blocking, no household, no profiles.

They set up their own phone exactly as you did, and the counter tells them whether there is room.



Guests cannot see your statistics, change your blocking, or invite anyone else. The five connected devices are shared across everyone, not five each.

Leaving is theirs, removing is yours. A guest can walk away at any time with **Leave shared device**. You can take access back with the cross beside their name — either way their tunnel stops working immediately.



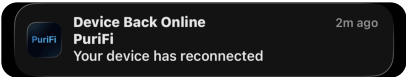
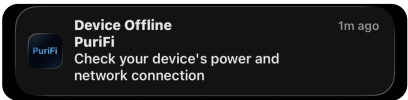
PuriFi asks before it does it, and tells them afterwards.

Alerts

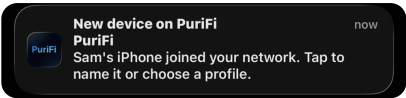
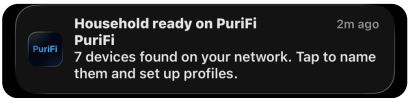
PuriFi tells you when something needs your attention.

In the app. Your Daily Recap arrives once a day (page 35). The rest come in three groups.

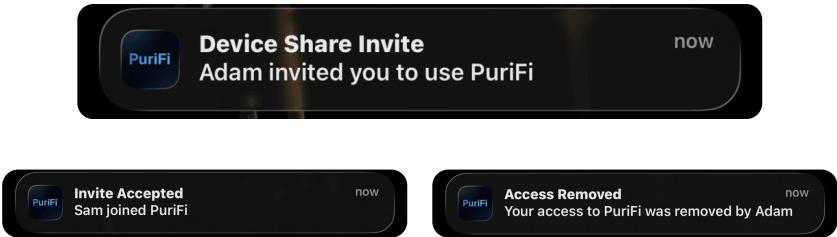
Is my PuriFi working? — if it stops answering for more than about ten minutes, and again when it recovers.



Something joined the house. — once, when PuriFi first maps your network, and then whenever something new appears. Both open straight onto the device so you can name it or put it on a profile (page 45).

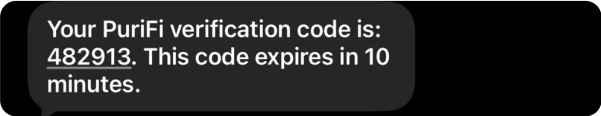


Sharing. — the first goes to the person you invited; the other two come back to you, so you always know where your device stands.



By text message, if you want it — useful precisely when your PuriFi is unreachable and a notification in the app might not arrive.

Add and verify your phone number under **Account** → **Profile**, then switch on **Text me about my device**. Both steps are required — verifying your number alone does not sign you up. Verifying sends you a code:



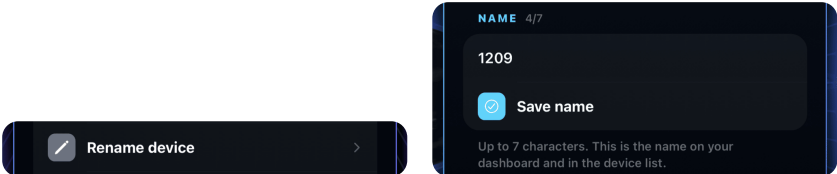
After that you get the same two messages the app sends, by text.



Reply STOP to any of them to opt out. Message and data rates may apply.

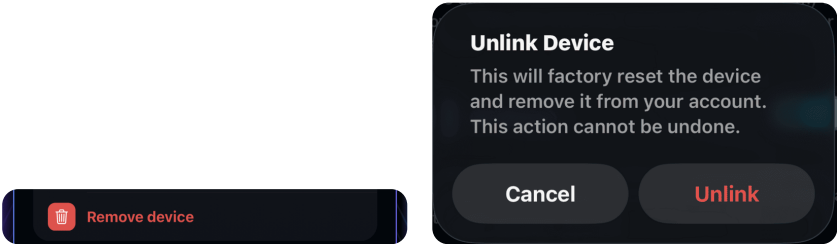
Renaming, unlinking, and starting over

Rename device is in the **ABOUT** section. Names are limited to seven characters — the name has to fit on the device’s own screen — and the counter beside the field shows how many you have left.



Remove device removes the device from your account and factory-resets it. Use this when you sell or give away your PuriFi, or if you

want to start again from scratch. The device must be online for this to work.



At the foot of **ABOUT**, in red.

The confirmation calls it *unlinking* — same thing.

NOTICE

This erases your settings, your allowed sites, and your history from the device, and returns it to **READY TO PAIR**. Your household stays online throughout — PuriFi keeps passing traffic through, just without filtering. It cannot be undone.

8. Profiles and per-device rules

Everything so far applies to your whole home at once. Profiles let you set different rules for different people and devices — stricter for the kids, quieter for the smart TV, ordinary for you.

Open your device's settings in the app and find the **HOUSEHOLD** section.

Which devices PuriFi can tell apart

Before you set profiles up, it is worth knowing which of your devices PuriFi can recognise individually. That depends on how you wired it in.

Phones and laptops using Private VPN are always recognised, in every setup. If what you actually want is different rules for the family's phones, you have that today and nothing needs to change.

Everything else — TVs, consoles, tablets, speakers — depends on the wiring. In the standard setup your router hands out your home's addresses, and PuriFi sees the traffic arriving as one stream from the router rather than from each device. It cannot tell a tablet from a television, so **HOUSEHOLD** shows a single entry for the router.

How you wired it in decides what PuriFi can tell apart:

Setup	Tells devices apart	Catches devices with built-in DNS	Double NAT
Standard, inline (Section 3)	Phones on Private VPN only	Yes	Yes
Standard, inline + Wi-Fi discovery <i>(tap the unlock card in HOUSEHOLD and point your router's DNS at your PuriFi)</i>	Yes, at the DNS layer	Yes	Yes
DNS server mode (Section 4)	Yes	No	No
Inline, with your router as an access point <i>(the standard setup with one router setting changed)</i>	Yes, and enforced instantly	Yes	No

Access-point mode gives up nothing. If you put your own router into bridge or access-point mode — a setting in its admin page, usually ten minutes' work — PuriFi becomes the only thing handing out addresses. It then sees every device by name, keeps catching the ones with a DNS server built into them, and the double-NAT trade-off on page 62 disappears, because only PuriFi is translating. Router makers all call it something slightly different; look for Bridge Mode, AP Mode or Access Point Mode.

Seeing every device on your Wi-Fi

If PuriFi is wired inline and **HOUSEHOLD** only shows your router, there is a way out that changes nothing about your router: let PuriFi join your Wi-Fi as well.

Both cables keep doing exactly what they were doing. PuriFi simply also joins your home network the way a laptop would, and from there it can see the devices on it.

% FIGURE: the unlock card in **HOUSEHOLD** — “See every device on your Wi-Fi”

The app offers this itself. When it can help, a card appears at the top of **HOUSEHOLD** — *See every device on your Wi-Fi* — and tapping it takes you to the Wi-Fi setup you already know from page 16. Pick your network, enter the password, done.

That alone fills in **HOUSEHOLD**: you get names, makers and addresses instead of one line saying *router*. To go further and give each device its own rules, point your router's DNS at PuriFi as well — the address is on page 14, and it is the same one-field change described there.

% FIGURE: the **WI-FI DISCOVERY** group, switched on, with the Turn off control

NOTICE

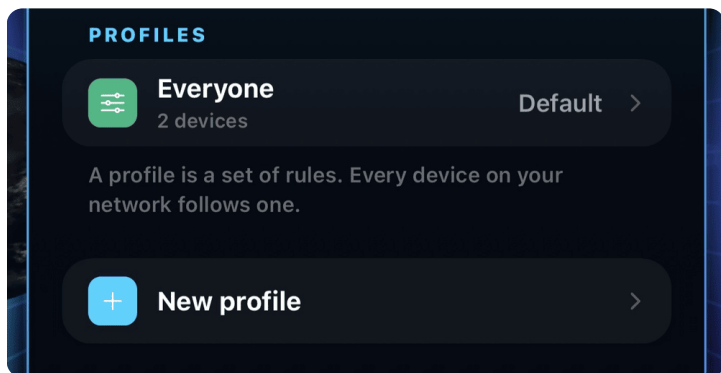
This is about names, not traffic. PuriFi is on your Wi-Fi to see what is connected — as the app puts it, *name, address and maker only, never traffic*. Nothing about what those devices do is collected because PuriFi joined your network.

It is optional and it is reversible. Nothing switches on by itself. Once it is running, **WI-FI DISCOVERY** in **HOUSEHOLD** shows what it found and offers **Turn off**, which puts everything back.

How it fits together

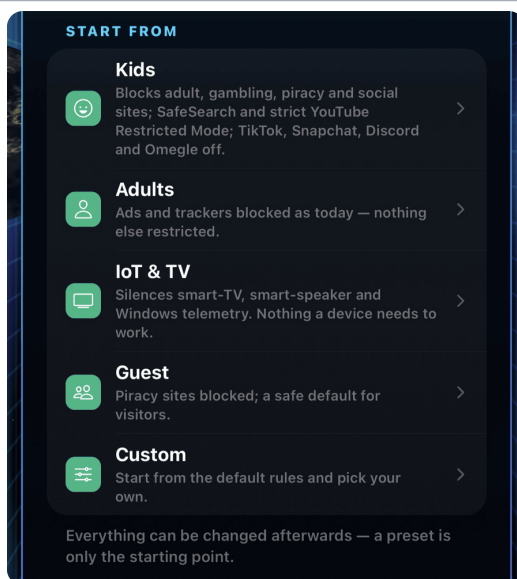
The app puts it in one line: *a profile is a set of rules, and every device on your network follows one.*

Everything starts on a single profile called **Everyone**, marked **Default**, which applies to any device that has not been given one of its own. Nothing changes until you add a second.



Making a profile

Tap **New profile** and pick something to start from. The app describes each one, and says plainly that *everything can be changed afterwards* — *a preset is only the starting point.*



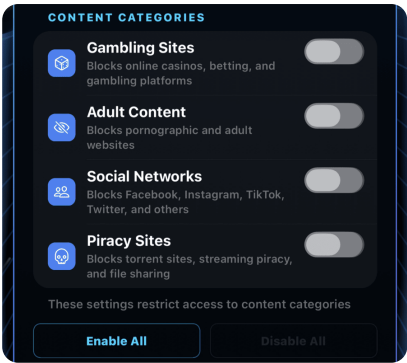
You can have up to **eight** profiles.

What a profile controls

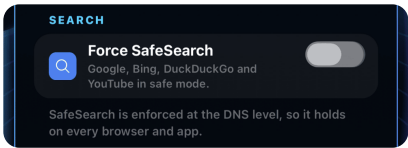
Each profile has its own copy of everything below, so tightening the rules for one changes nothing for anyone else.

Content categories and search. The same four categories as the household-wide controls, plus SafeSearch — which the app notes is *enforced at the DNS level, so it holds on every browser and app*, not just the ones that offer their own setting.

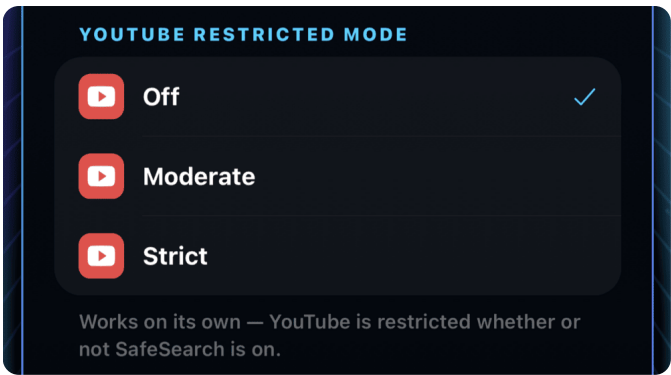
YouTube Restricted Mode, with three settings rather than a switch: **Off**, **Moderate** and **Strict**. It does not depend on SafeSearch — as the app puts it, *YouTube is restricted whether or not SafeSearch is on*.



Content categories, per profile.

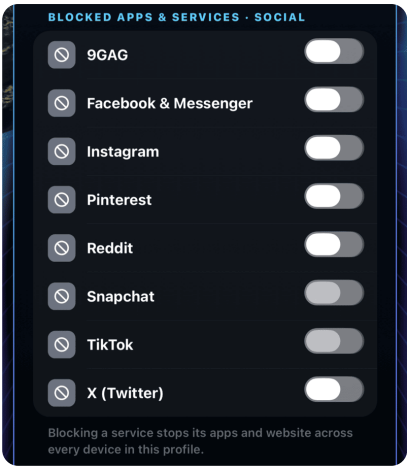


SafeSearch, with the reason it is hard to dodge.

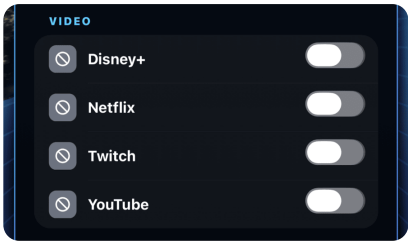


Three settings, not a switch — and it works on its own.

Blocked apps and services, grouped by what they are: social, shopping, messaging, video, gaming, dating, telemetry and music. Blocking one *stops its apps and website across every device in this profile* — not just the browser.

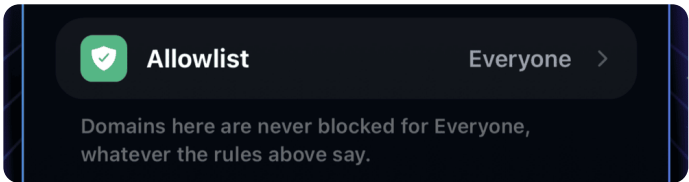


Social — eight services.

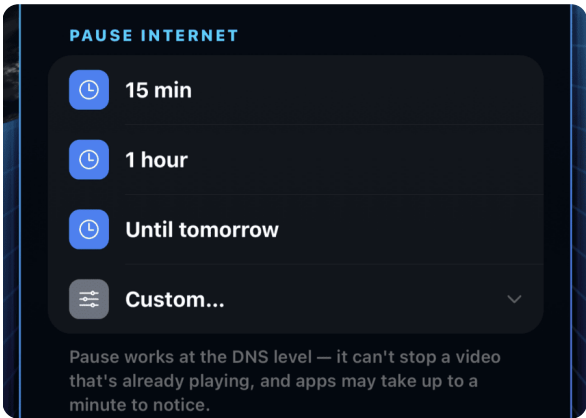


Video — and seven more categories like it.

Its own allowed list. Domains added here are never blocked for that profile, whatever the rules above say. Allowing a homework site for the kids does not allow it for the whole house.



Pausing and scheduling

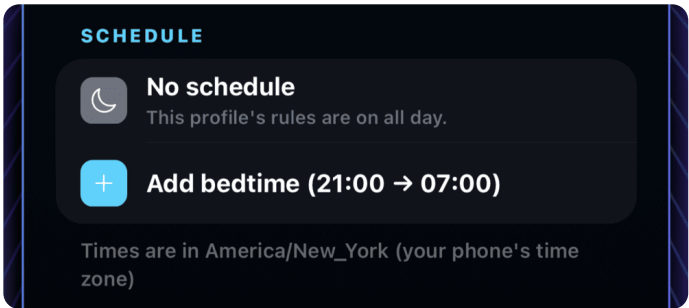


PAUSE INTERNET stops a profile reaching the internet — **15 min, 1 hour, Until tomorrow**, or a time you choose. A pause on one device beats a pause on its profile, which beats the schedule, and everything resumes on its own.

NOTICE

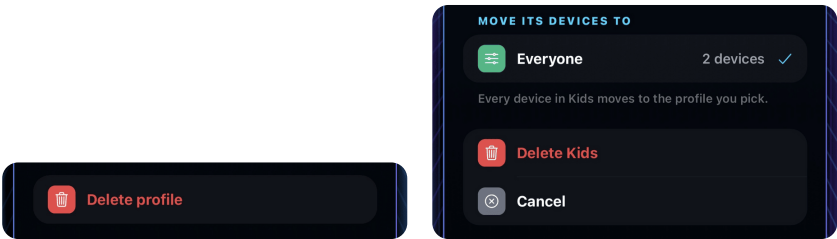
Pause works at the DNS level. It cannot stop a video that is already playing, and apps may take up to a minute to notice. It is for the next thing they try to open, not the thing on screen.

Under **SCHEDULE**, **Add bedtime** sets 21:00 to 07:00 in one tap, or you can build your own. Times follow your phone's time zone, which the app names underneath so there is no doubt.



Deleting a profile

A profile cannot simply vanish while devices are on it, so PuriFi asks where they should go first.



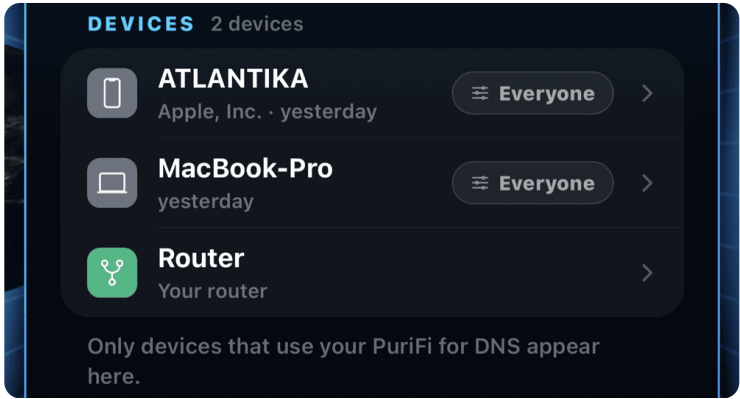
At the foot of the profile.

Its devices move to the profile you pick.

Your devices

Devices lists everything PuriFi has seen, with what it is, when it was last around, and which profile it follows. Only devices that use your

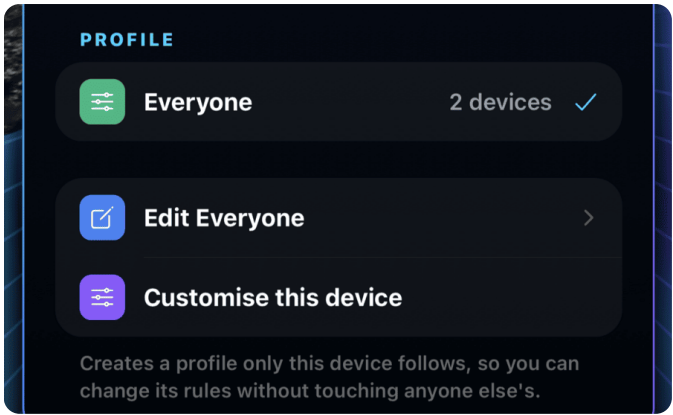
PuriFi for DNS appear here — which is why the list looks different depending on how you wired it in (page 45).



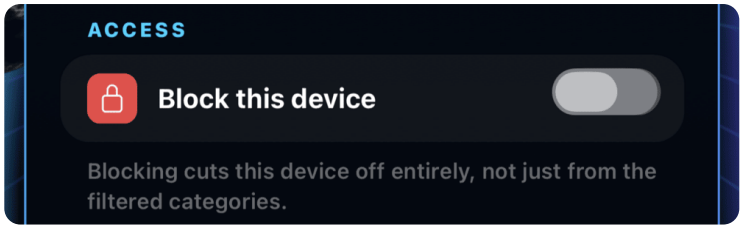
Tap one to open it. You can give it a name you will recognise, and PuriFi shows what it already knows — maker, hostname, addresses, and when it first and last appeared.



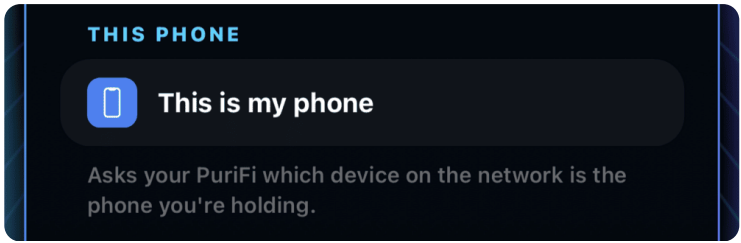
PROFILE is where you move it to a different profile, or give it rules of its own with **Customise this device** — which quietly creates a profile only that device follows, so you can change its rules without touching anyone else's.



Block this device is the blunt instrument.



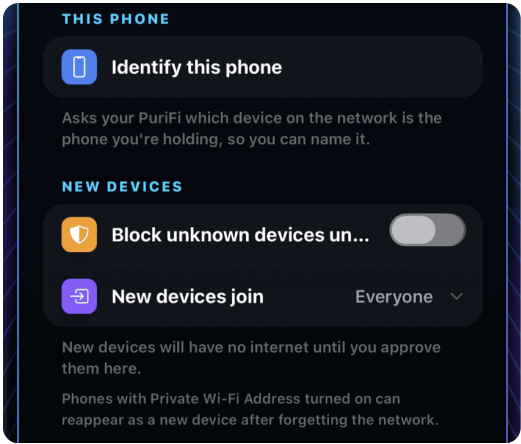
Which one is my phone? Device names come from the network and are often useless. Open any device and tap **This is my phone** — PuriFi works out which one you are holding by checking where the request came from, and you can name it there and then.



New devices

When something joins that PuriFi has not seen before, it appears in the list and you get a notification. You choose which profile new

arrivals land on, and you can hold them back until you have looked at them.



With **Block unknown devices** on, anything new has no internet at all until you approve it. It is off unless you turn it on, so nothing in your home will stop working unexpectedly.

NOTICE

A phone with Private Wi-Fi Address switched on can come back as a brand-new device after it forgets and rejoins your network. If a familiar phone reappears as a stranger, that is why — name it again, or turn that setting off on the phone.

9. Your account

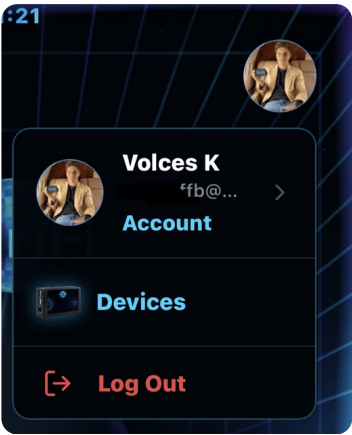
Everything so far has been about your PuriFi. This section is about the account you sign in with — your name and photo, how you sign in, your phone number, and where you are currently signed in.

NOTICE

None of this touches your PuriFi. Your device keeps filtering whatever you do on this page, including if you sign out of the app entirely.

Getting there

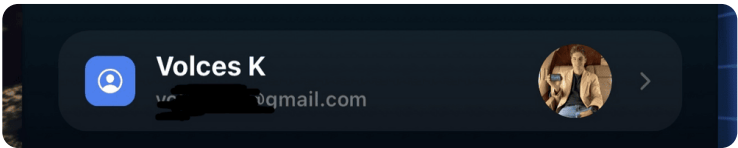
Tap your photo in the top right of the main screen. **Account** is the first entry.



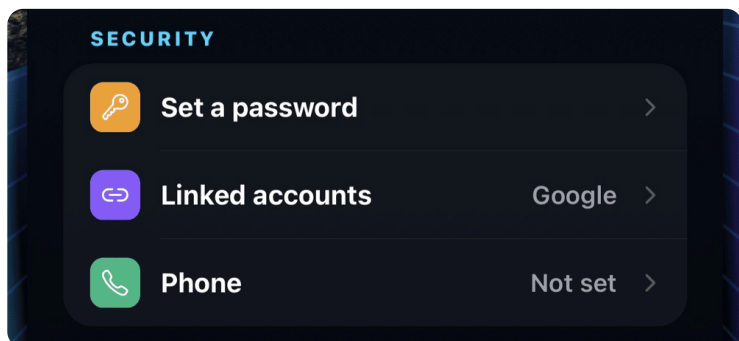
Your photo, top right, opens this.

What is on the page

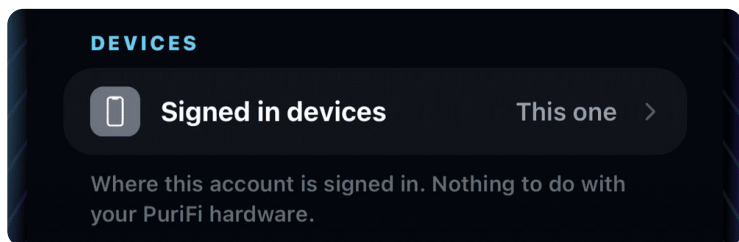
The top of the page is you — your name, the email you sign in with, and your photo. Tap it to change any of them.



Below that, **SECURITY** holds the three things that control how you get into your account: a password, the Google or Apple account you signed up with, and your phone number.



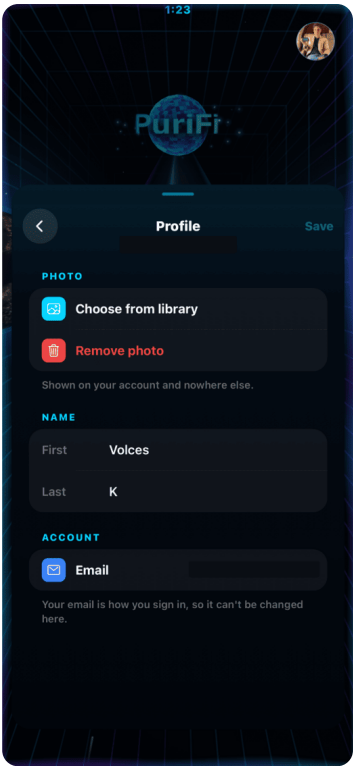
DEVICES is one entry, and the app is careful to say what it is not:



Under that sit the three things you do to the account as a whole: ask for a copy of your data, sign out, and delete the account.

Your name and photo

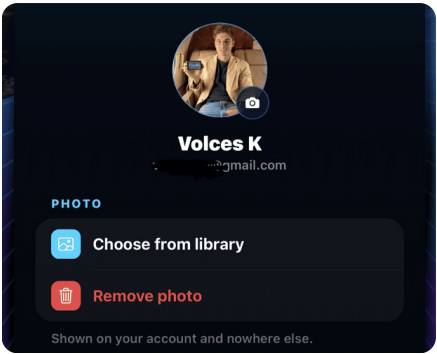
Tap the band at the top of the account page and you land on **Profile**. Your photo, your name, and the email you sign in with are all here.



Tap **Save** in the top right when you are done. Nothing is stored until you do.

The whole **Profile** page.

Your photo comes from your phone's library, and PuriFi is direct about where it goes: *shown on your account and nowhere else*. There is no profile anyone else can see.



Your name is free text, in two fields, and nothing depends on it.

NAME

First

Volces

Last

K

Your email is the one thing on this page you cannot change:

ACCOUNT

 Email

Your email is how you sign in, so it can't be changed here.

If you need to move your account to a different address, email support@purifi.io.

Setting a password

If you signed up with Google or Apple you never chose a password, and you do not need one. This is here in case you want a second way in — if you ever lose access to the Google or Apple account you signed up with, a password is what gets you back.

NEW PASSWORD

Password

At least 8 characters



Confirm

Repeat it



 Set password

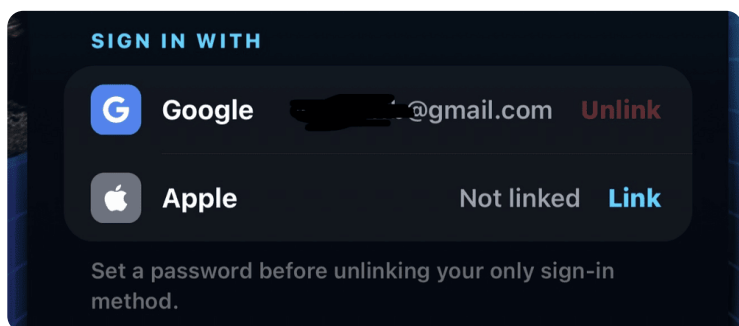
You signed up with Google or Apple. A password gives you a second way in.

Eight characters or more. The eye reveals what you have typed.

Set a password before you unlink anything. If Google or Apple is your only way in and you unlink it without setting a password first, you lock yourself out. The app warns you about this on the **Linked accounts** page.

Linked accounts

Linked accounts shows which sign-in services your account is attached to. Linking a second one gives you another way in; unlinking removes it.



One linked, one not. The address beside a linked service is the account it is linked to.

Apple hides your real address after the first time you sign in with it, so an account linked through Apple may show no address at all. That is Apple's doing, not a fault — the link still works.

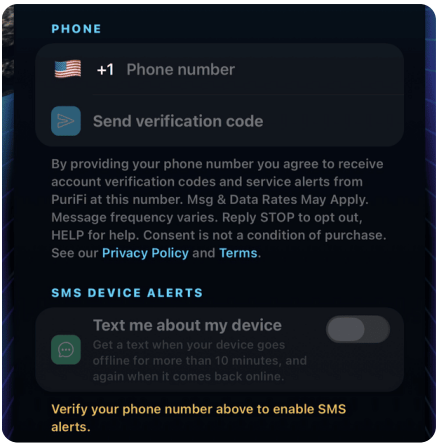
⚠ CAUTION

Do not unlink your only way in.

If Google or Apple is the only way you sign in and you have not set a password, unlinking it locks you out of your own account. Set a password first — page 58.

Your phone number and text alerts

Adding a phone number does two things: it lets us send you a verification code, and it turns on text alerts about your PuriFi.



The order matters. Enter the number, tap **Send verification code** and confirm it first — until the number is verified, the **Text me about my device** switch stays greyed out and the page says so in yellow.

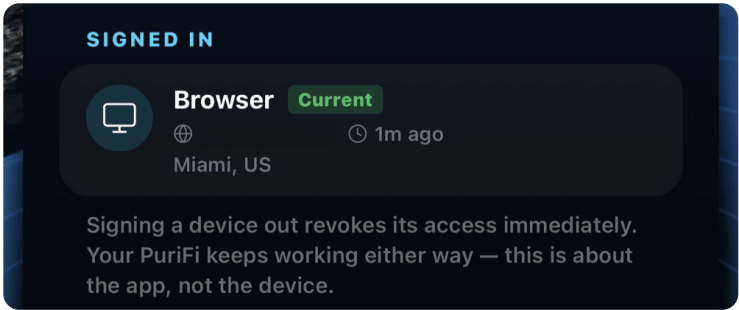
With both done, you get a text when your PuriFi goes offline for more than ten minutes, and another when it comes back. That is the same pair of alerts described on page 42, delivered by text instead of a notification.

NOTICE

Verifying your number and switching on text alerts are separate steps. Verifying alone does not sign you up for anything — the switch is what does. Reply STOP to any message to stop them. Message and data rates may apply.

Where you are signed in

Signed in devices lists every phone, tablet and browser your account is currently signed in on, with roughly where and when each one was last used. The one you are holding is marked **Current**.



Sign a session out and its access stops immediately. This is worth doing if you have signed in somewhere you no longer control — an old phone, a shared computer.

Getting a copy of your data

Export My Data sends you everything we hold about your account. Tap it and we email a file to the address your account is under — usually within a minute or two.

The file is JSON, which any text editor will open. Inside is your profile, the PuriFis on your account, your orders, your account activity, the emails we have sent you, your VPN clients, any device you have shared or been given, and your app notification registrations. Your password and your sign-in tokens are not in it, and neither is anything belonging to anyone else. Your browsing is not in it either, because we do not keep it.

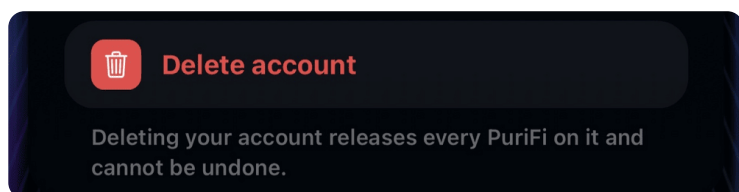
It goes to your account's email address rather than downloading to the phone on purpose: that way it reaches you, and not whoever happens to be holding your phone.

Signing out, and deleting

Sign out ends the session on this phone. Your account and your PuriFi are untouched, and you can sign back in whenever you like.



Delete account is the other thing entirely. It releases every PuriFi on the account — they go back to **READY TO PAIR** and can be claimed by someone else — and starts the deletion of your data.



 CAUTION**Deleting your account releases your devices.**

You are signed out everywhere straight away and every PuriFi on the account is released. Your data is permanently deleted after 30 days — until then, email support@purifi.io and we can restore it. After 30 days it is gone.

10. What PuriFi does not do

Every product like this has limits. Here are ours, in plain language, so you are not left wondering whether something is broken.

It does not block every ad

PuriFi blocks advertising and tracking that is served from separate advertising companies — which is most of it, across most of the web and most apps.

It does **not** block ads that a platform serves from its own systems. YouTube ads, sponsored posts in Instagram or TikTok, promoted results in a search page: these arrive from the same addresses as the content you asked for, so there is nothing separate to block. No network-level blocker can remove them, ours included. Anyone who tells you otherwise is selling something.

It does not make you anonymous

PuriFi protects you from the companies watching **the network you are on**. It does not hide you from a website you have chosen to log into. If you sign into a service, that service knows who you are — that is what signing in means.

It does not change your internet speed

PuriFi handles a full gigabit. It will not slow your connection down, and it cannot raise the speed your provider sells you. Your ping does not change.

It creates a second layer of network address translation

This is the one genuine trade-off of sitting between your modem and your router. Your router ends up behind PuriFi, which means your home has two layers of address translation instead of one.

Most people will never notice. What can notice are services that need to reach into your home from outside: **Plex**, **remote play** on consoles

and handhelds, **port forwarding**, and **self-hosted game servers**. If you run any of these, expect to adjust them.

It cannot filter a phone that is not at home

A phone on mobile data is not on your network, so PuriFi cannot see or filter it. That is exactly what Private VPN is for — see page 36.

It is not a commercial VPN service

Private VPN connects you to your own device in your own home. PuriFi does not run VPN servers for general browsing.

11. Troubleshooting

The screen never shows **READY TO PAIR**

This is the most common first-run problem and it is almost always the router-side cable.

PuriFi will not offer to pair until both of its network connections are live. If either one is missing, the banner never appears.

1. Check that the USB-to-Ethernet cable is firmly seated in a PuriFi USB port.
2. Check that its far end is in your router's internet port and that the port's light is on.
3. Check the cable from your modem into PuriFi's built-in Ethernet port.
4. Restart PuriFi — press the side button to shut it down, wait a few seconds, press it again — and give it 90 seconds.

A failed or unseated USB-to-Ethernet adapter looks exactly like an unplugged cable — you will see a red arrow and a blinking red X, and no **READY TO PAIR**. If you have checked every cable and the warning persists, try the adapter in a different USB port before contacting support.

A red arrow and blinking X on the screen

One of the two network connections has dropped. The arrow points towards the side that is affected. Reseat both ends of that cable. If the modem-side connection is the problem, also power-cycle your modem and give it a couple of minutes — PuriFi will reconnect on its own once the modem is back.

The app cannot find my device

- Make sure Bluetooth is on and that you have allowed the PuriFi app to use it.
- Stand next to the device.
- Confirm the screen shows **READY TO PAIR**. If it does not, see above — the app cannot pair with a device that is not ready.
- Tap **Scan Again**.
- Close the app completely and reopen it.

“Device did not respond” or “No ethernet connection detected”

PuriFi could not reach the internet. Check the cable from your modem, and check that your modem itself is online. If your modem has just been restarted, give it a few minutes — PuriFi waits for the connection indefinitely and will pick it up on its own.

“This device hasn’t finished connecting yet”

Not a fault. Your PuriFi is still establishing its secure connection. Wait a moment and tap to try again. It typically settles within a minute.

“Registration blocked — contact support”

This one you cannot fix yourself, and retrying will not help. It means the credential tying your device to an account has been locked for security. Email support@purifi.io with your order number and we will sort it out.

The picture is dimmed and nothing is being blocked

Filtering has switched off. There are three usual reasons:

- You paused it in the app. Tap play to resume.
- The block list is rebuilding. This happens daily and after you change settings. It resolves itself within a few minutes.
- PuriFi detected a problem and stepped aside. It is designed to fall back to passing traffic through rather than leave your home without working internet. It tests itself continuously and switches filtering back on once the problem clears.

If it stays dimmed for more than about fifteen minutes, restart the device: press the button on the right-hand side to shut it down, wait a few seconds, then press it again.

A website or app has stopped working

Almost always a blocked address that the site needs.

1. Pause protection in the app and reload the page.
2. If it works, PuriFi was the cause. Resume protection and open **Recently Blocked** — the entry you need is usually near the top.
3. Tap it and choose to allow the whole website including subdomains.

If you cannot identify it, lowering **Ad & Privacy Protection** from **Aggressive** to **Balanced** resolves most cases.

If the site broke shortly after you switched on an advanced setting, that setting is the first thing to suspect — particularly **Suspicious TLD Blocking** and **New Domain Blocking**, which block by category rather than by reputation.

The app says my device is offline

Check that PuriFi has power and that its screen is lit. Check your home internet from another device. If your internet is working and PuriFi still shows offline after five minutes, restart it with the side button.

Note that while your PuriFi is offline, Private VPN cannot connect — there is nothing at home for it to reach.

Nothing here helped

Email support@purifi.io. Include your device name, roughly when the problem started, and what the screen is showing. A photograph of the screen is genuinely useful.

12. Care and safety

WARNING

Electric shock and fire hazard.

Use only the power supply provided with this product. Do not use a damaged power supply or a damaged cable. Do not open the enclosure — there are no user-serviceable parts inside, and opening it voids your warranty. If the enclosure, cable or power supply is damaged, stop using the product and contact support.

CAUTION

Hot surface.

The enclosure is a heatsink and is warm to the touch in normal operation. Do not cover it, do not place it inside a closed cabinet or on soft furnishings, and leave clear air on all sides. Keep it out of direct sunlight and away from heat sources.

NOTICE

Keep it dry. This product is for indoor use only. Do not expose it to rain, moisture, or liquids of any kind. Do not place drinks on or beside it. Liquid damage is not covered by the warranty.

NOTICE

Do not remove the memory card. It holds the credential that links this device to your account. Removing or reformatting it unregisters the device permanently.

Cleaning. Unplug the power first. Wipe with a dry, soft cloth. Do not use solvents, abrasives, or liquid cleaners, and never spray anything directly onto the device.

Ventilation. Leave clear space around the device and do not stack anything on top of it.

Children. This is not a toy. Keep the device, its power supply, and its cables out of reach of small children, and route cables so they cannot be pulled or tripped over.

13. Specifications

Product name	PuriFi™
Model	PuriFi V1
Network — modem side	Gigabit Ethernet (built in)
Network — router side	Gigabit Ethernet, via the included USB adapter
Throughput	Up to 1 Gbps
Wireless	Wi-Fi (2.4 / 5 GHz) and Bluetooth Low Energy
Display	3.5 in colour, 480 × 320
Storage	Removable memory card, not user-serviceable
Power input	USB-C, 27 W supply included
IP addressing	IPv4. IPv6 is disabled on this device.
Dimensions	3.625 × 2.5 × 1.25 in (92 × 64 × 32 mm), W × H × D
Weight	215 g (7.6 oz)
Operating temperature	0-50,°C (32-122,°F) ambient
Operating humidity	Up to 80% relative humidity, non-condensing

14. Warranty and returns

30-day returns

You may return your PuriFi device within 30 days of delivery for a full refund, provided the device is in working condition. The cost of return shipping is the responsibility of the customer. After 30 days, refunds are available only for defects covered under the hardware warranty described below.

If you bought through a crowdfunding campaign or as a pre-order, that platform's terms apply until your device is delivered. The 30-day window then starts from delivery.

PuriFi LLC Limited Hardware Warranty

PuriFi LLC warrants your PuriFi device against defects in materials and workmanship under normal use for **12 months from the date of delivery**.

Who this warranty covers. It covers the device rather than the person who bought it, and it travels with the device. If you sell or give away your PuriFi, the new owner gets whatever is left of the 12 months.

What is covered. Defects in materials or workmanship that arise under normal use conditions during the warranty period.

What is not covered:

- Physical damage, misuse, or unauthorized modifications to the device.
- Damage caused by power surges, water exposure, or conditions outside the operating temperature and humidity range on page 68.
- Normal wear and tear.
- SD card degradation resulting from normal read/write cycles over time.
- Thermal throttling experienced at elevated ambient temperatures, which is a normal protective function of the device.

How we put it right. For valid warranty claims, PuriFi will, at our discretion, replace the device with an identical or reasonably equivalent unit, or refund the purchase price. Unlike the 30-day return policy, where you pay return shipping, PuriFi provides a prepaid return shipping label for warranty claims.

How to make a claim. Email support@purifi.io with your device serial number and your order number, or write to us:

PuriFi LLC
1100 Biscayne Blvd, Unit 4201
Miami, FL 33132
United States

We will confirm the claim and send you a prepaid return shipping label with instructions.

Limits on this warranty

Any implied warranties on your PuriFi device, including the implied warranties of merchantability and fitness for a particular purpose, are limited in duration to the 12-month term of this written warranty.

NOTICE

Some States do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

Our obligation under this warranty is limited to replacing the device or refunding the purchase price, as described above. We are not liable for incidental or consequential damages arising from a defect in the device.

NOTICE

Some States do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

California residents. We do not maintain service and repair facilities in California. As permitted by California Civil Code section 1793.3, we will instead replace your device with an identical or reasonably equivalent unit, or reimburse the purchase price less an amount directly attributable to your use before the defect was discovered. Nothing in this warranty limits your rights under the Song-Beverly Consumer Warranty Act.

Your legal rights

NOTICE

This warranty gives you specific legal rights, and you may also have other rights which vary from State to State.

Nothing in this warranty affects your statutory rights as a consumer.

Getting a copy of the full terms

The complete warranty and terms of sale are published at **purifi.io/terms**. If you would prefer a paper copy at no charge, write to us at the address above or email support@purifi.io, and we will post one to you.

15. Your privacy

PuriFi is a privacy product, so it would be strange not to be direct about this.

What stays on your device and never reaches us

The addresses your household looks up. PuriFi keeps a rolling 24-hour record on the device itself, purely so the app can show you statistics and the **Recently Blocked** list. It is never uploaded. You can switch it off entirely — see page 34 — and PuriFi will delete what it has stored.

There is one exception, and only if you ask for it. **AI Fleet Intelligence** (page 30) is off unless you turn it on. With it on, your PuriFi sends us the occasional individual address — never the record, and never your ordinary browsing. An address qualifies only if your device has never seen it before, it is not among the world's hundred thousand most-visited sites, it is not on your own allowed list, and a model running on your PuriFi scores it as suspicious. Each report is attached to a code that changes every day rather than to your account or your device, and we keep it for 30 days. Turn the setting off and it stops.

The contents of anything you do. PuriFi does not inspect, log, or retain the contents of your traffic, and neither does Private VPN. When you use Private VPN, the connection runs from your phone to your own device. Our relay forwards encrypted packets and cannot read them.

NOTICE

IP Shield is the one exception to that. It is off unless you turn it on (page 35). While it is on, connections to a short list of tracking endpoints leave through a PuriFi-operated server instead of directly from your home, so those trackers see an address shared by many households rather than yours. For that traffic — and only that traffic — PuriFi is in the path. That server keeps no record of what it carries. Everything else on your network connects directly, exactly as before.

What we do hold

Your account details — name, email, and your phone number if you gave us one. Information about the device itself: its serial number, firmware version, temperature, and whether it is online. Counts of how many requests it has handled and blocked, as numbers only, never as a list of addresses. Your order and shipping details.

An approximate location is derived from your connection — state and country, nothing finer — using a database held on our own servers. Your address is not shared with anyone to do it, and we do not store it.

Your choices

You can delete your account from the bottom of the **Account** page in the app — see page 61. To get a copy of everything we hold about you, tap **Export My Data** on the same page and we will email it to you. If you would rather ask us directly, email privacy@purifi.io.

Deleting your account signs you out everywhere straight away. Your data is permanently removed 30 days later — and until those 30 days are up, you can email support@purifi.io and we will restore it.

The full privacy policy is at **purifi.io/privacy**. It is the operative document; if anything on this page appears to conflict with it, the published policy governs.

Questions about your data go to privacy@purifi.io.

16. Regulatory information

United States — FCC

FCC ID: TBD

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Radio frequency exposure

This equipment complies with FCC and ICSED Canada radiation exposure limits set forth for an uncontrolled environment. This equipment shall be installed and operated with a minimum distance of 20 cm between the radiator and all persons during normal operation.

Cet équipement est conforme aux limites d'exposition aux rayonnements de la FCC et d'ISDE Canada établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimale de 20 cm entre le radiateur et toute personne pendant le fonctionnement normal.

Canada — ISED / ISDE**IC: TBD**

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference; (2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) L'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

CAN ICES-003(B) / NMB-003(B)

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

NOTICE

No CE mark, UKCA mark, RoHS statement or WEEE symbol appears in this manual or on this product. None is substantiated, and PuriFi is not sold into those markets.

17. Open-source notices

PuriFi™ device software, Copyright © 2025–2026 ATLANTIKA SYSTEMS LLC. All rights reserved.

This product includes free and open-source software. We are grateful to the people who wrote it.

Written offer for source code

For a period of three (3) years after the last shipment of this product, ATLANTIKA SYSTEMS LLC hereby offers to any third party, for a charge no more than our cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code for the GPL- and LGPL-licensed software contained in this device, to be distributed under the terms of those licences.

To request it, write to ATLANTIKA SYSTEMS LLC at the address on the back of this manual, or email support@purifi.io with the subject line “GPL source code request”.

The same source code is also available to download, at no charge, from purifi.io/opensource.

This offer is valid for anyone who receives this notice, including anyone who obtains this device second-hand.

Tracker data

The domain-to-company mapping used by this device is adapted from the AdGuard Tracker List ([companiesdb](https://companiesdb.com)), licensed under Creative Commons Attribution-ShareAlike 4.0 International. Changes made: flattened to a domain-to-company map, PuriFi category overrides applied, entries pruned. As required by the ShareAlike condition, PuriFi's adapted version of that data is itself made available under CC BY-SA 4.0 from purifi.io/opensource or by writing to support@purifi.io.

Threat data

Malicious network ranges are sourced from Emerging Threats, Copyright © 2003–2026 Emerging Threats, used under the BSD licence. That data incorporates the Spamhaus Project DROP list, used with credit. Domain block lists are sourced from HaGeZi DNS Blocklists, licensed under GPL-3.0.

Components

WireGuard (GPL-2.0) · Linux kernel (GPL-2.0) · Raspberry Pi OS (Debian, various) · dnsmasq (GPL-2.0) · Unbound (BSD-3-Clause) · BlueZ (GPL-2.0) · NetworkManager (GPL-2.0) · systemd (LGPL-2.1) · Next.js, React, Three.js, Tailwind CSS, Node.js, Express, Expo and React Native (MIT).

Licence texts are on the device at /usr/share/common-licenses/, and the full credit list is published at purifi.io/credits.

PuriFi's DNS filtering engine is developed in-house and is proprietary software owned by ATLANTIKA SYSTEMS LLC. It is not derived from any third-party filtering project.

18. Getting help

Email

support@purifi.io — a real person answers.

For questions about your personal data, privacy@purifi.io.

We aim to reply within **three business days**, and usually much sooner. Support is by email — there is no phone line to sit on hold for.

Online

purifi.io/faq — answers to the questions we are asked most.

purifi.io/privacy — privacy policy.

purifi.io/terms — terms of service and the full warranty.

purifi.io/credits — open-source credits.

This manual lives online, at the address behind the QR code inside the lid of your box. It is updated as the product changes, so the copy you reach is always current.

What to include when you write to us

It saves a round trip if your first email has:

- Your device name, as shown in the app.
- Your order number.
- What the screen is showing — a photograph is ideal.
- What you were doing when the problem started.

PuriFi™ is a product of ATLANTIKA SYSTEMS LLC,
operated by its subsidiary PuriFi LLC.

1100 Biscayne Blvd, Unit 4201
Miami, FL 33132
United States

© 2026 ATLANTIKA SYSTEMS LLC. All rights reserved.