Firefly CAP100

User Manual

The complete guide to your Firefly device: the network it runs, the cameras it watches, the devices it connects, and the sensors it reports.

Applies to Firefly CAP100 / CAP100-W **Revised** 18 September 2026

Screenshots from a live device, privacy-redacted

CONTENTS

PART ONE · GETTING STARTED

1 What this device is

The Firefly CAP100 is four things in one box, and you can use as many or as few of them as you like:

ROLE	WHAT IT MEANS
A router and access point	It shares an internet connection, hands out addresses, runs a Wi-Fi hotspot, filters and shapes traffic.
A camera recorder	It watches RTSP or ONVIF cameras, recognises people, vehicles and animals on the device itself, and notifies you by rules you write.
A hub for other devices	It relays Bluetooth audio to two headphones, and collects readings from IoT sensors.
A monitored endpoint	It watches its own health, checks targets you name, reads a temperature and humidity sensor, and can report to a GEN2 server.

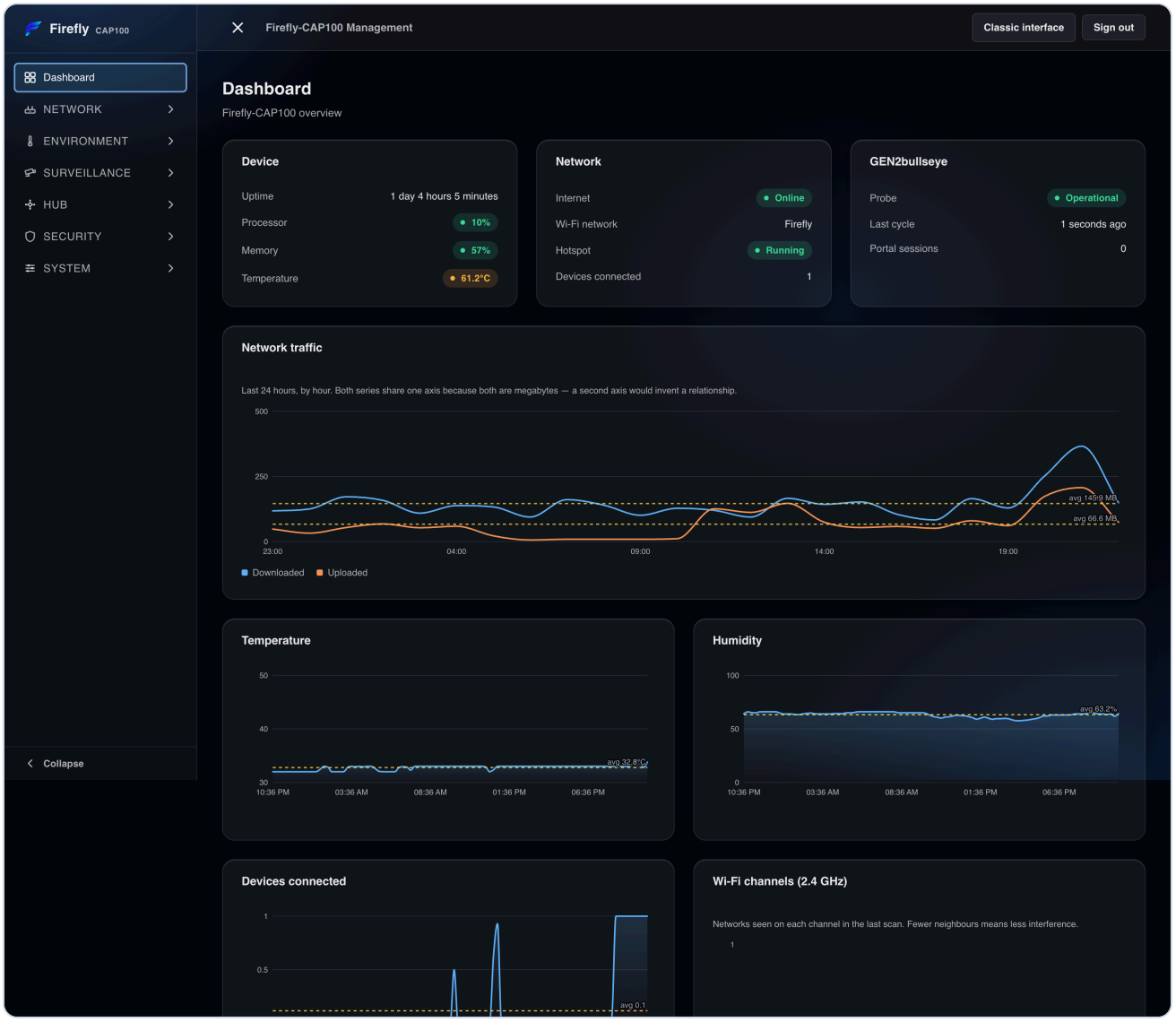
> **Everything runs on the device.** Video is never uploaded, the AI runs locally, and the only things that leave are the reports and notifications you configure.

2 Signing in and finding your way

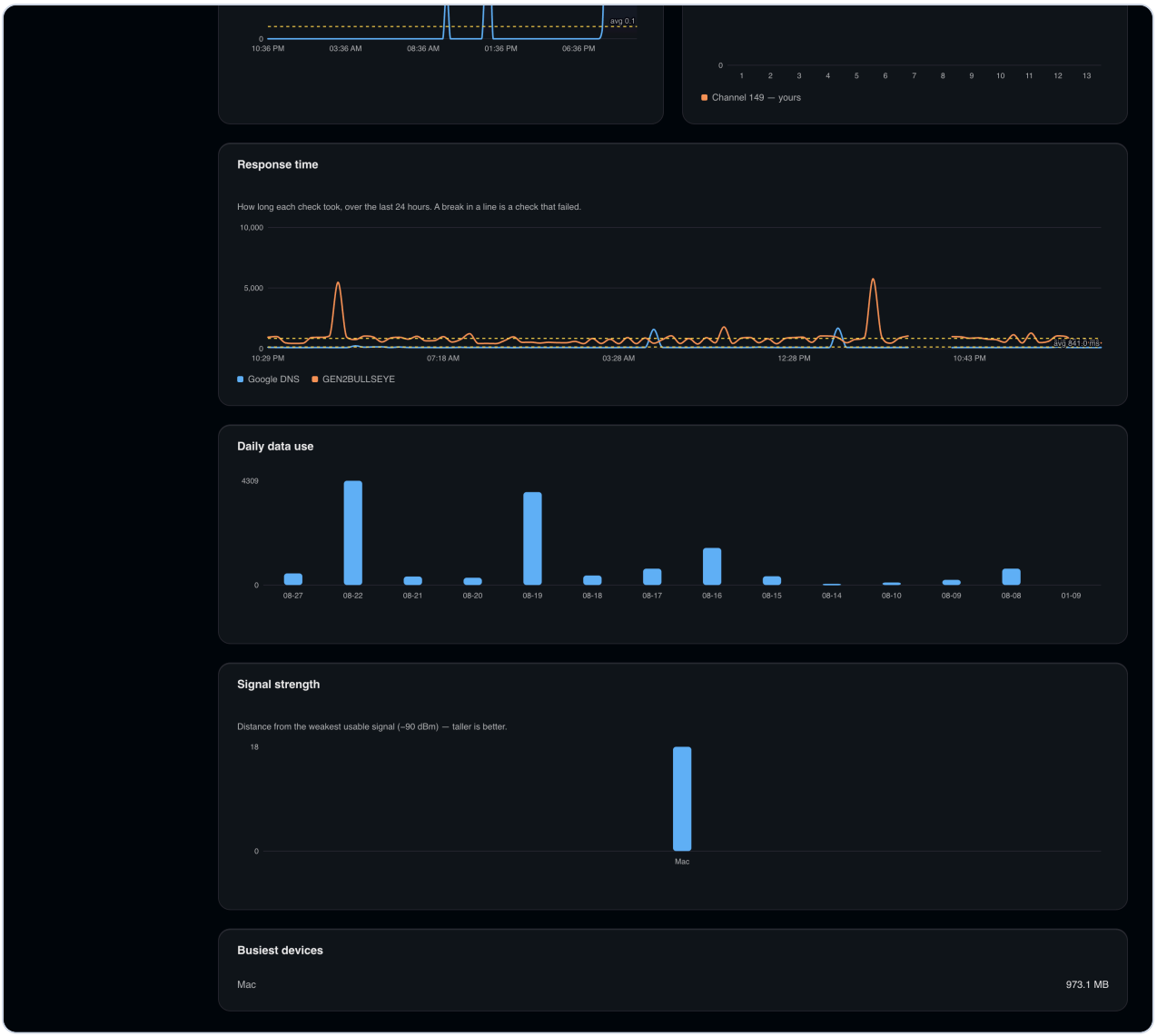
Open the device's address in a browser and sign in. The menu down the left side groups every page into six sections; **Collapse** at the bottom narrows it to icons. **Classic interface** at the top right opens the older administration pages, and **Sign out** ends your session.

SECTION	PAGES
Network	WAN · LAN · DHCP Server · Wi-Fi · Wi-Fi Client · Clients · Bandwidth Shaper
Environment	Monitors
Surveillance	Live View · Detections · Rules · Cameras
Hub	BT-Splitter · IoT Gateway
Security	Firewall · Parental Control · Ad Blocking · Captive Portal
System	Device · Account · Services · Logs · Diagnostics · Monitoring

3 Dashboard



Dashboard, upper half. A single view of the device's health, its network, and the last 24 hours of activity.



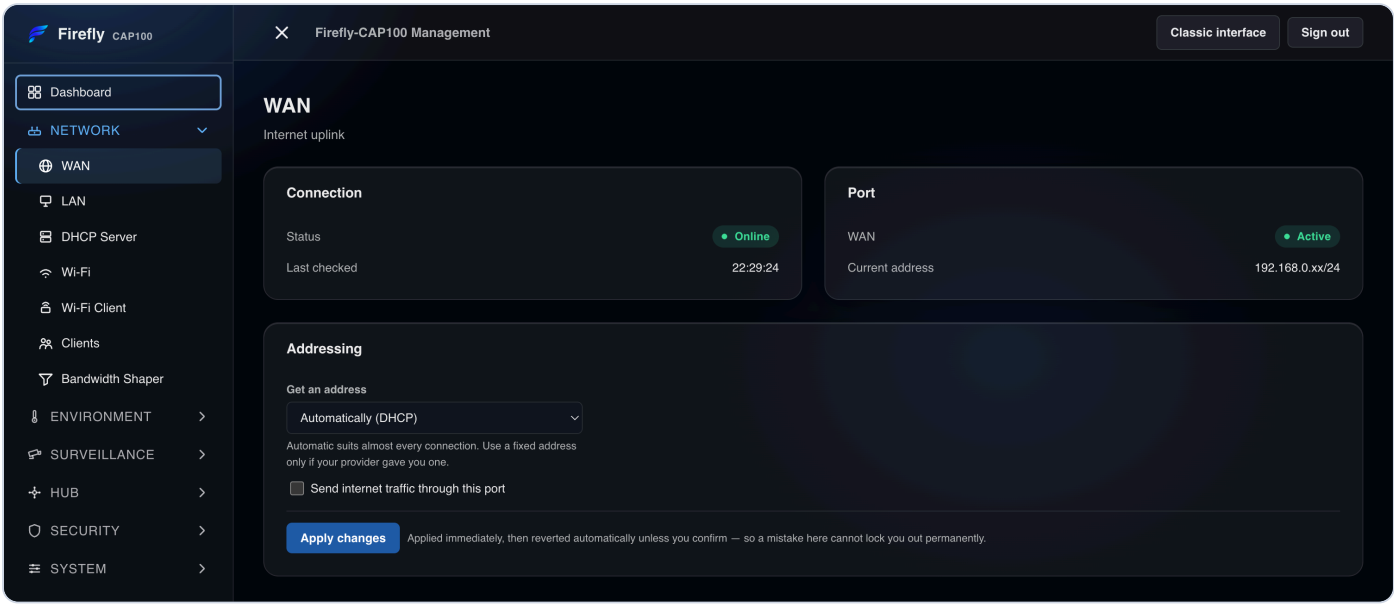
Dashboard, lower half. Response time, daily data use, signal strength and the busiest devices.

The cards cover the device itself, the network, recent traffic by hour, temperature and humidity, connected devices, Wi-Fi channel occupancy, response times for the targets being monitored, daily data use, signal strength, and the busiest devices.

> **Reading the charts honestly.** Traffic in and out share one axis because both are megabytes. A break in a response-time line is a check that failed, not missing data. Signal strength is drawn as distance above the weakest usable signal (−90 dBm), so taller is better.

PART TWO · NETWORK

4 WAN — the internet connection



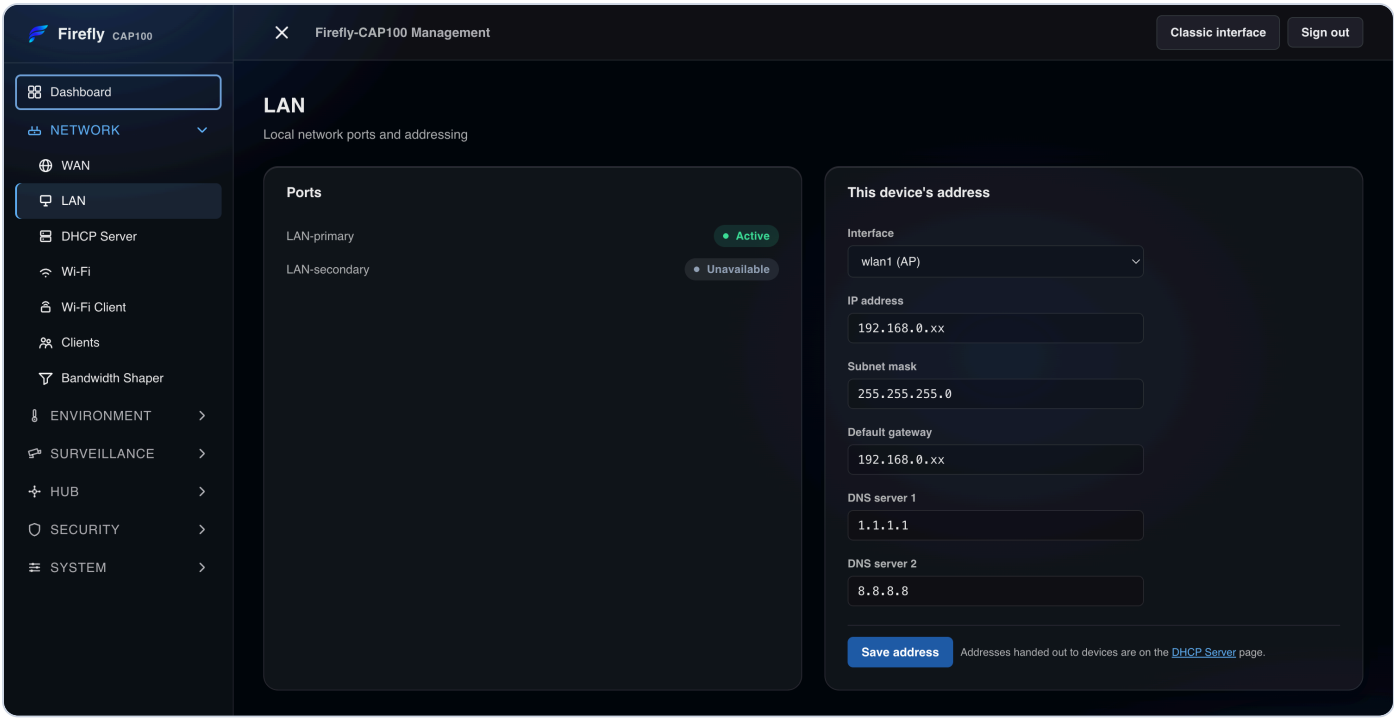
Network → WAN.

Three cards: **Connection** shows the current state, **Port** selects which physical port carries internet traffic, and **Addressing** decides how this device gets its own address on that connection.

SETTING	MEANING
Get an address	*Automatically (DHCP)* for most connections, or *Use a fixed address* when your provider gave you one.
Send internet traffic through this port	Which interface is treated as the way out.

Apply changes commits them. Expect a short interruption while the connection is re-established.

5 LAN — this device's address

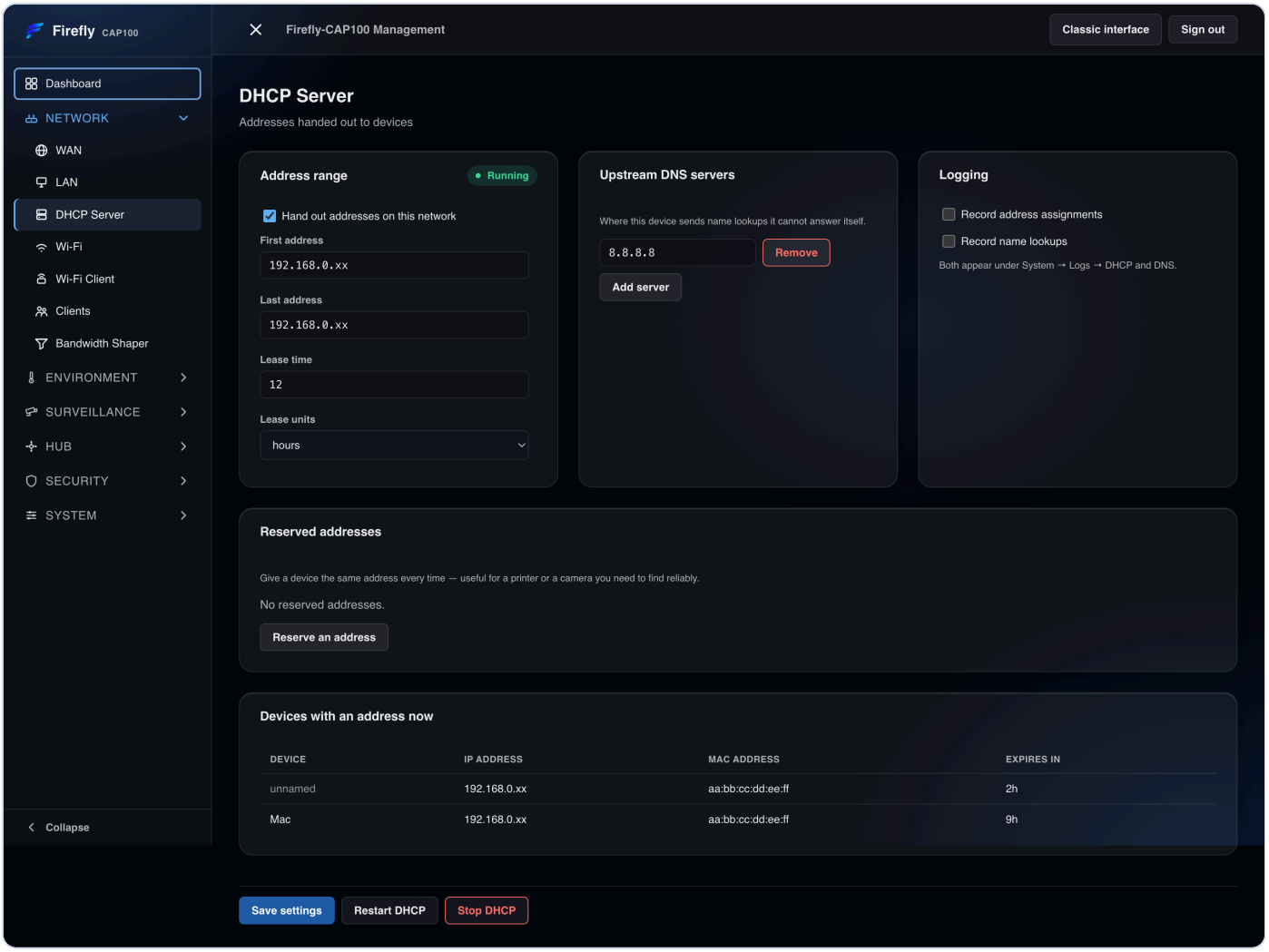


Network → LAN.

Ports lists the interfaces this unit has. **This device's address** sets the address for a chosen interface: IP address, subnet mask, default gateway, and two DNS servers. The interface list names each one by role — for example the Wi-Fi client radio, the access-point radio, and the loopback.

> **Change this carefully.** The address you are connected to *is* this address. If you change it, your browser will lose the page and you must reconnect on the new one.

6 DHCP server

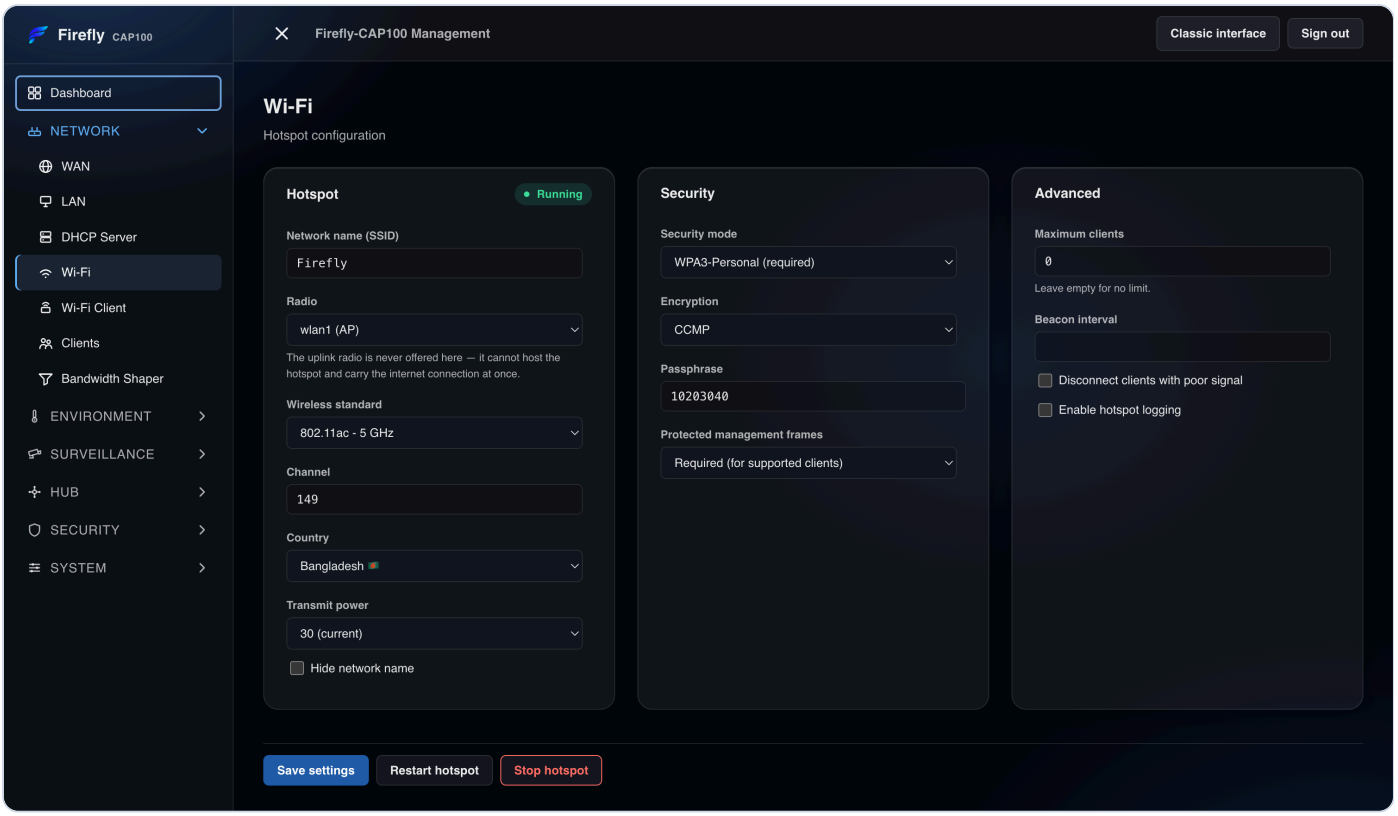


Network → DHCP Server. Addresses currently handed out are listed at the bottom.

CARD	WHAT IT DOES
Address range	Whether this device hands out addresses at all, the first and last address of the pool, and how long a lease lasts (minutes, hours, days, or never expiring).
Upstream DNS servers	Where name lookups go when this device cannot answer them itself. Add or remove as many as you need.
Logging	Record address assignments, and record name lookups. Both appear under **System → Logs**.
Reserved addresses	Give a device the same address every time — worth doing for a printer, or a camera you need to find reliably.
Devices with an address now	Live list: device name, address, hardware address, and when the lease expires.

Reserve addresses for cameras. Surveillance refers to cameras by address. A camera that moves to a different address after a power cut stops working until you correct it — a reservation prevents that.

7 Wi-Fi hotspot



Network → Wi-Fi. The network this device broadcasts.

Hotspot

Network name (SSID), which radio carries it, the wireless standard (b/g/n through ax and be), channel, country, transmit power, and whether the name is hidden.

Set the country correctly. It governs which channels and power levels are legal where you are. A wrong country can make your network unreachable for some devices.

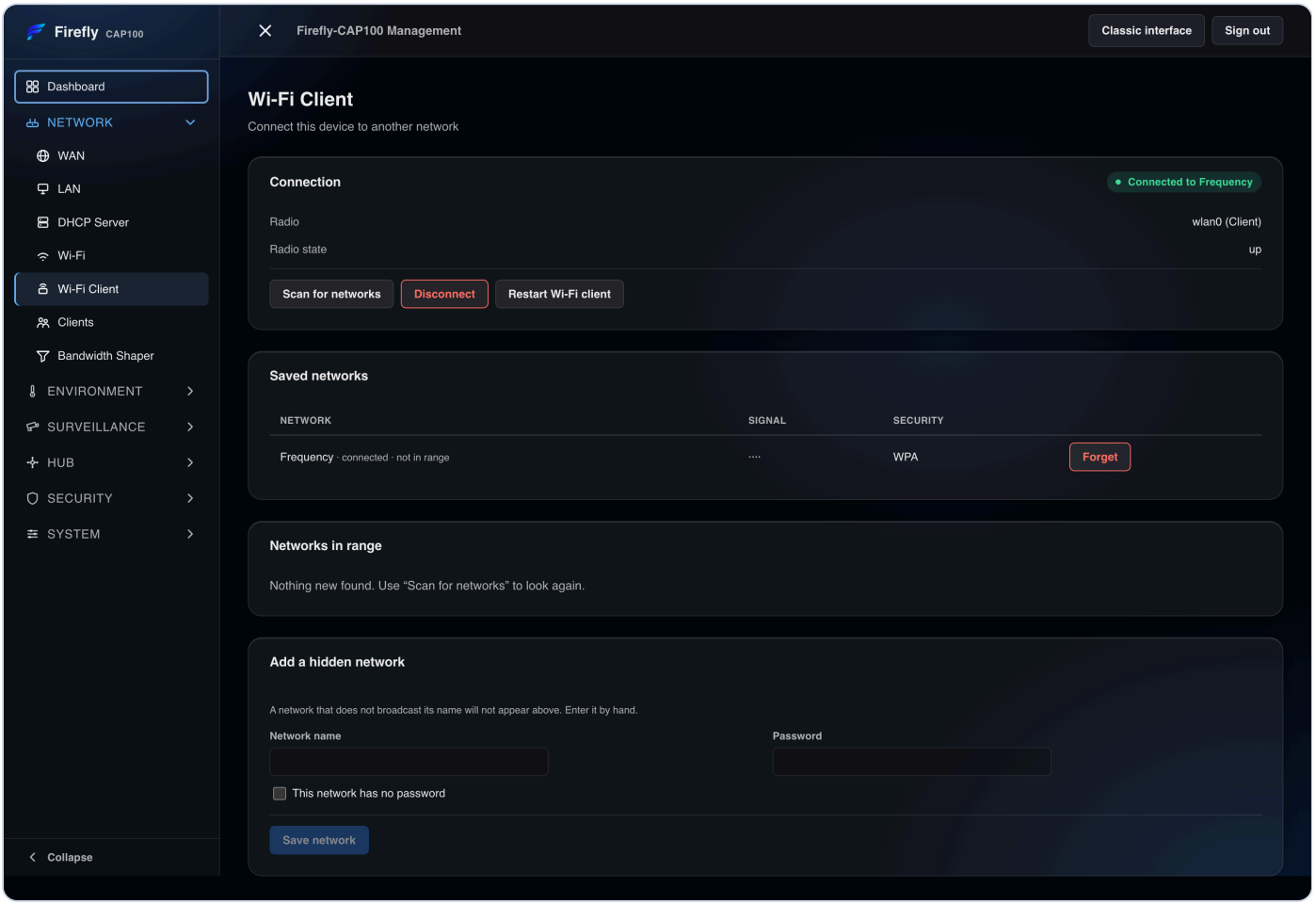
Security

SETTING	GUIDANCE
Security mode	*WPA2 and WPA3-Personal (transitional)* suits mixed households. *WPA3-Personal (required)* is stronger but excludes older devices. *None* leaves the network open.
Encryption	CCMP for anything modern. TKIP exists only for legacy equipment.
Passphrase	The Wi-Fi password.
Protected management frames	Enabled for supported clients, required, or disabled. *Required* is part of WPA3.

Advanced

Maximum simultaneous clients, beacon interval, whether to disconnect clients with poor signal, and hotspot logging.

8 Wi-Fi client

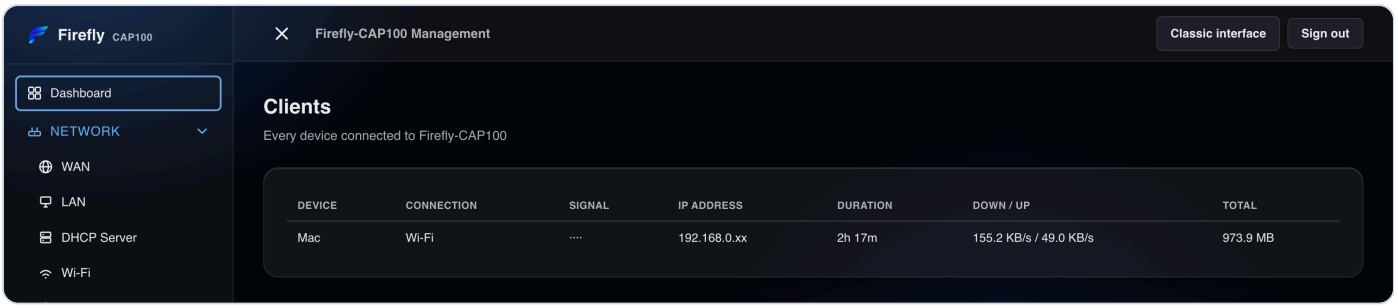


Network → Wi-Fi Client. Connects this device *to* an existing network.

This is the opposite of the hotspot: it joins this device to somebody else's Wi-Fi, which is how a CAP100-W can reach the internet without a cable.

- **Scan for networks** lists what is in range with signal and security.
- **Saved networks** are remembered and rejoined automatically; **Forget** removes one.
- **Add a hidden network** is for networks that do not broadcast their name — type it in by hand.
- **Disconnect** and **Restart Wi-Fi client** are the recovery buttons when a connection misbehaves.

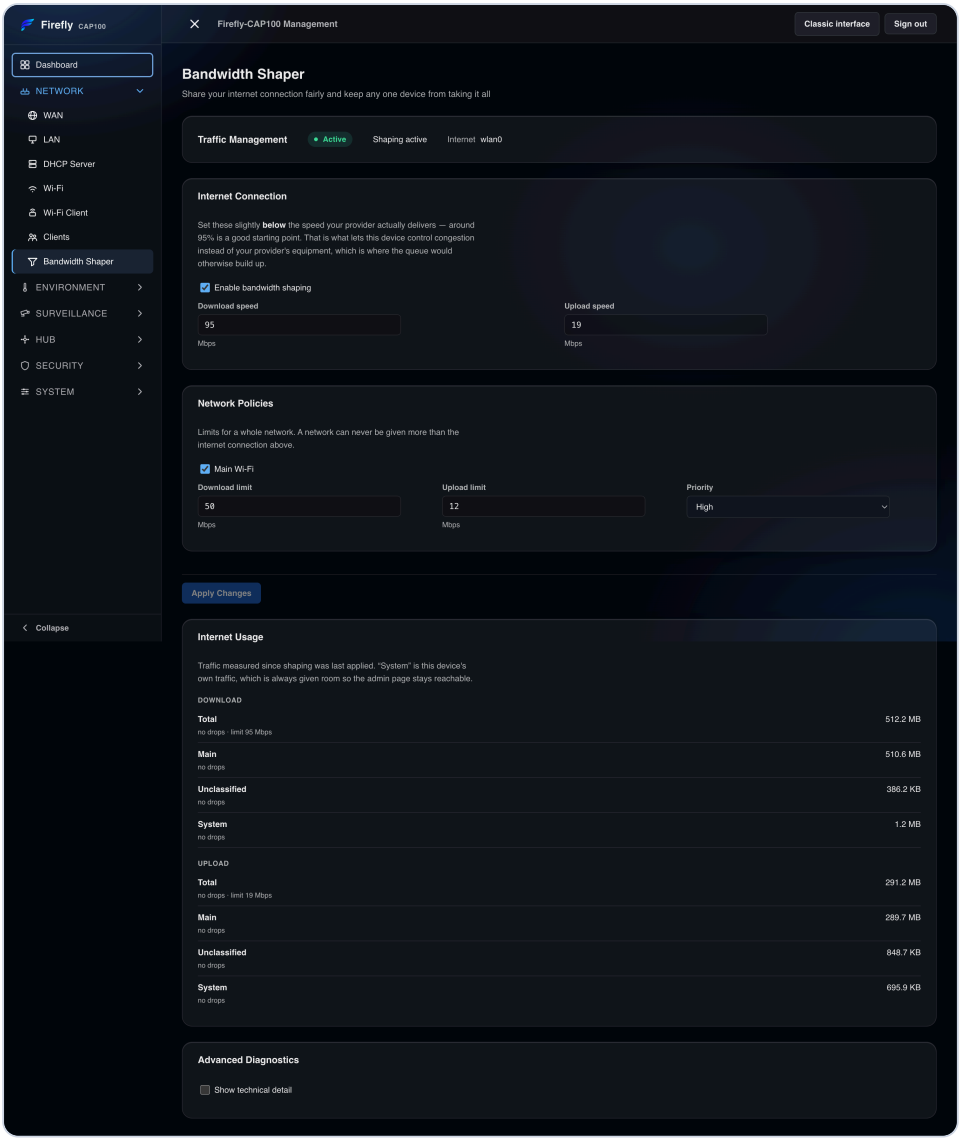
9 Clients



Network → Clients. Everything currently on the network.

A live list of connected devices — what they are called, their addresses, and how they are connected. This is the page to check when you want to know whether something is actually on the network before hunting elsewhere.

10 Bandwidth shaper



Network → Bandwidth Shaper.

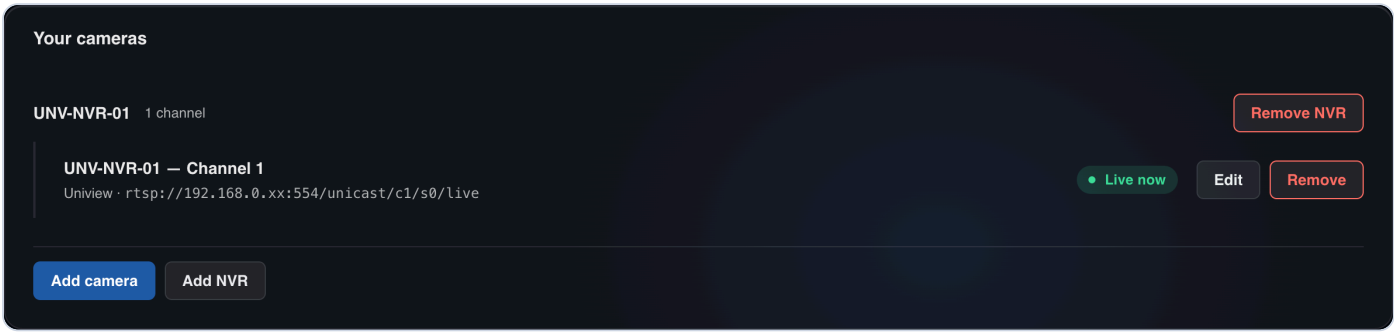
Shaping stops one download from ruining everyone else's video call. It works by holding traffic slightly below what the line can carry, so the queue forms here — where it can be managed — rather than at your provider.

CARD	WHAT TO DO WITH IT
Internet Connection	Turn shaping on and enter your real download and upload speeds. Set them **around 95%** of what the line actually delivers.
Network Policies	Per-network limits and a priority of High, Normal or Low. A network can never be given more than the connection above.
Internet Usage	Traffic since shaping was last applied. The **System** row is the device's own traffic, always given room so this admin page stays reachable.
Advanced Diagnostics	Technical detail for when something is not behaving.

> **Guessing the speeds too high defeats the whole mechanism.** If you enter more than the line delivers, the queue forms upstream again and shaping stops helping. Measure first, then subtract a little.

PART THREE · SURVEILLANCE

11 Adding cameras



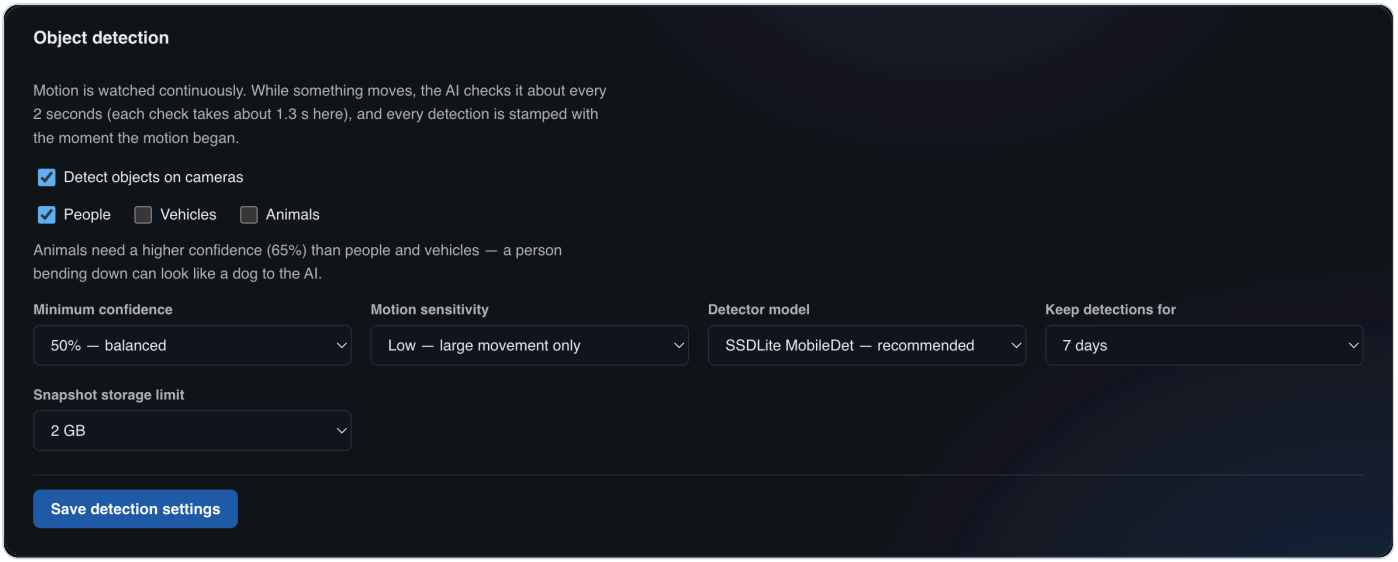
Surveillance → Cameras. Channels imported from an NVR are grouped under its name. **Live now** means the relay currently has a picture.

Add camera and choose the brand: the preset fills in that vendor's stream paths, so you supply an address and login rather than an RTSP URL. Choose **Other** to paste a full address. Always press **Test connection** first — it probes the camera exactly as it would be saved and reports the codec and resolution found.

Add NVR imports every channel at once as one camera per channel, grouped together. Each channel can be previewed before saving.

> **Use the NVR's own address, not this device's.** Entering the Firefly address produces a *connection refused* error, because nothing serves camera streams there.
>
> Detection starts **off** for imported NVR channels — otherwise a 16-channel import would start sixteen AI workloads at once. Turn it on per channel.

12 Detection settings



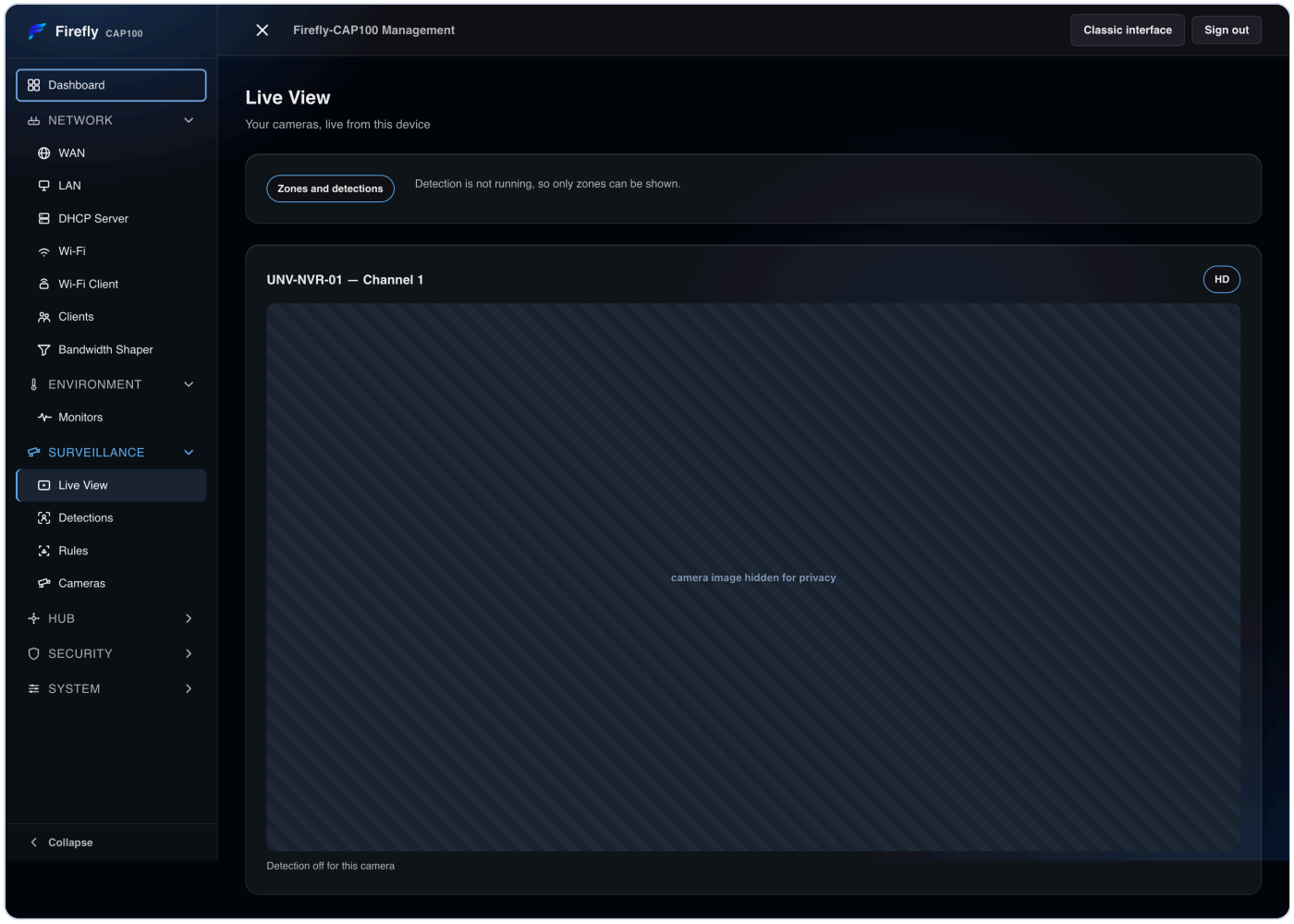
Surveillance → Cameras → Object detection. These apply to every camera with detection turned on.

SETTING	WHAT IT CHANGES
Detect objects on cameras	The master switch.
People / Vehicles / Animals	What is recorded at all. Unticking one also hides it from rules.
Minimum confidence	How sure the AI must be. Lower catches more and mistakes more.
Motion sensitivity	How much must move before the AI is asked. **Low** ignores small movement — useful where foliage moves constantly.
Detector model	**SSDLite MobileDet** is the default and recommended. **YOLOX-Nano** is offered for comparison only.
Keep detections for	1–90 days, after which entries and their snapshots are removed.
Snapshot storage limit	A disk ceiling; the oldest days go first.

> **Animals are held to a higher bar automatically** — your confidence plus 15 points, never below 65%. A person bending down is easily mistaken for a dog by this class of model.

> **YOLOX is experimental, and that is not a formality.** In testing it missed people that MobileDet found, and each check costs more time. Switch to it only to compare on your own footage, and switch back if detections start being missed. Changing model restarts the detector; past detections are unaffected.

13 Live View



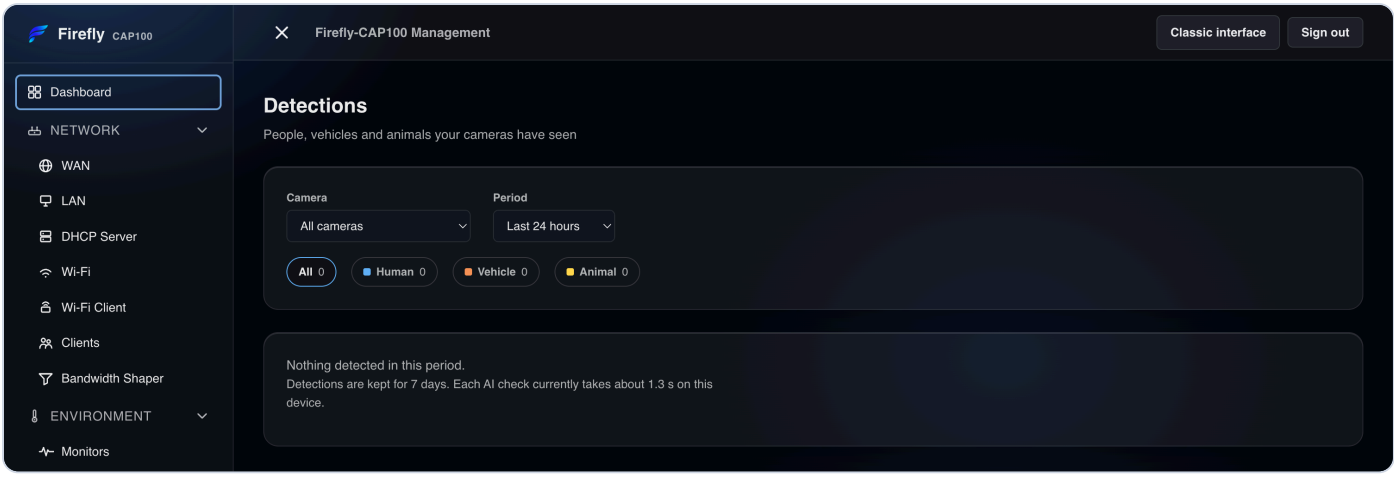
Surveillance → Live View. Camera imagery is hidden throughout this manual.

Each camera gets a tile. One camera plays its full-resolution stream; with several, tiles start on the smaller sub stream to spare your Wi-Fi, and each has its own **HD / SD** button. The badge reads **Live**, **Connecting…**, **Paused** (the tab is in the background, so the camera is not held open for nobody), **Offline**, or **Can't play here**.

The **Zones and detections** toggle draws your zones as dashed outlines and each detection as a coloured box — blue for people, orange for vehicles, yellow for animals.

> **Boxes lag the picture by a second or two**, because that is how long a check takes, and they fade rather than vanish. If detection is off, zones still draw but no boxes appear.

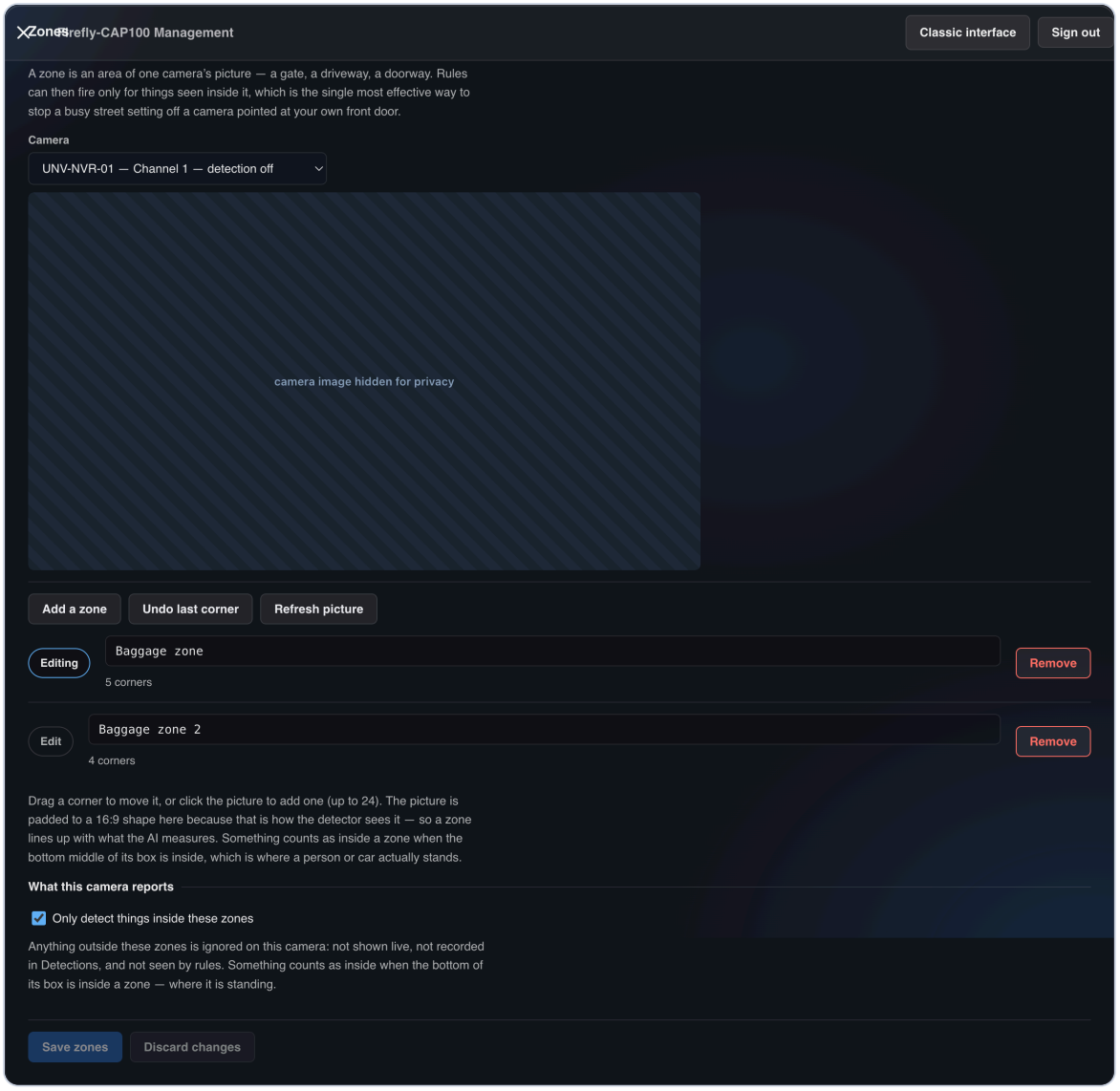
14 Detections



Surveillance → Detections. Snapshot thumbnails hidden for privacy.

Each row is an **event**, not a frame: repeat sightings of the same kind of thing on the same camera merge into one row, so somebody lingering is one entry reading *seen 4×*. The time shown is when the **motion started**. Filter by camera, period and kind; the **Rules** column shows which rules matched and whether they fired.

15 Zones



Surveillance → Rules → Zones. Drag a corner to move it; click to add one.

A zone is an area of one camera's picture — a gate, a driveway, a doorway. Up to 8 per camera, 3–24 corners each. Rules can then fire only for things inside them, which is the most effective way to stop a public footpath triggering a camera aimed at your door.

> **Two details that matter.** The picture is padded to 16:9 in the editor because that is exactly how the detector sees it, so what you draw lines up with what the AI measures. And something counts as **inside** when the **bottom middle of its box** is inside — where a person actually stands, not where their head is.

Only detect things inside these zones goes further: anything outside is not shown live, not recorded, and never seen by rules.

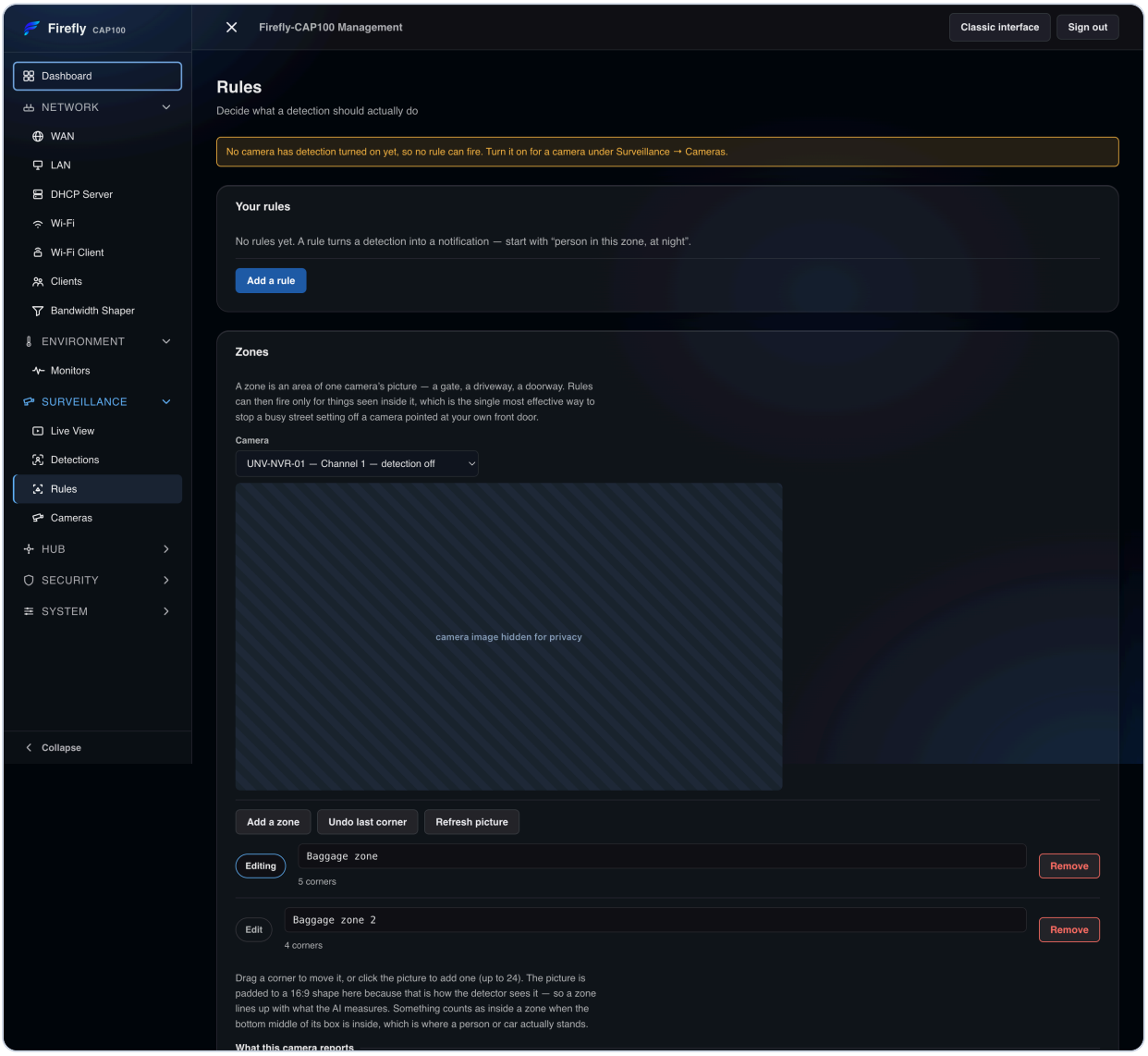
> **With no zones drawn, that setting does nothing** — deliberately. A camera set to "zones only" with no zones would see nothing at all, so it keeps watching the whole picture and says so on screen.

16 Schedules

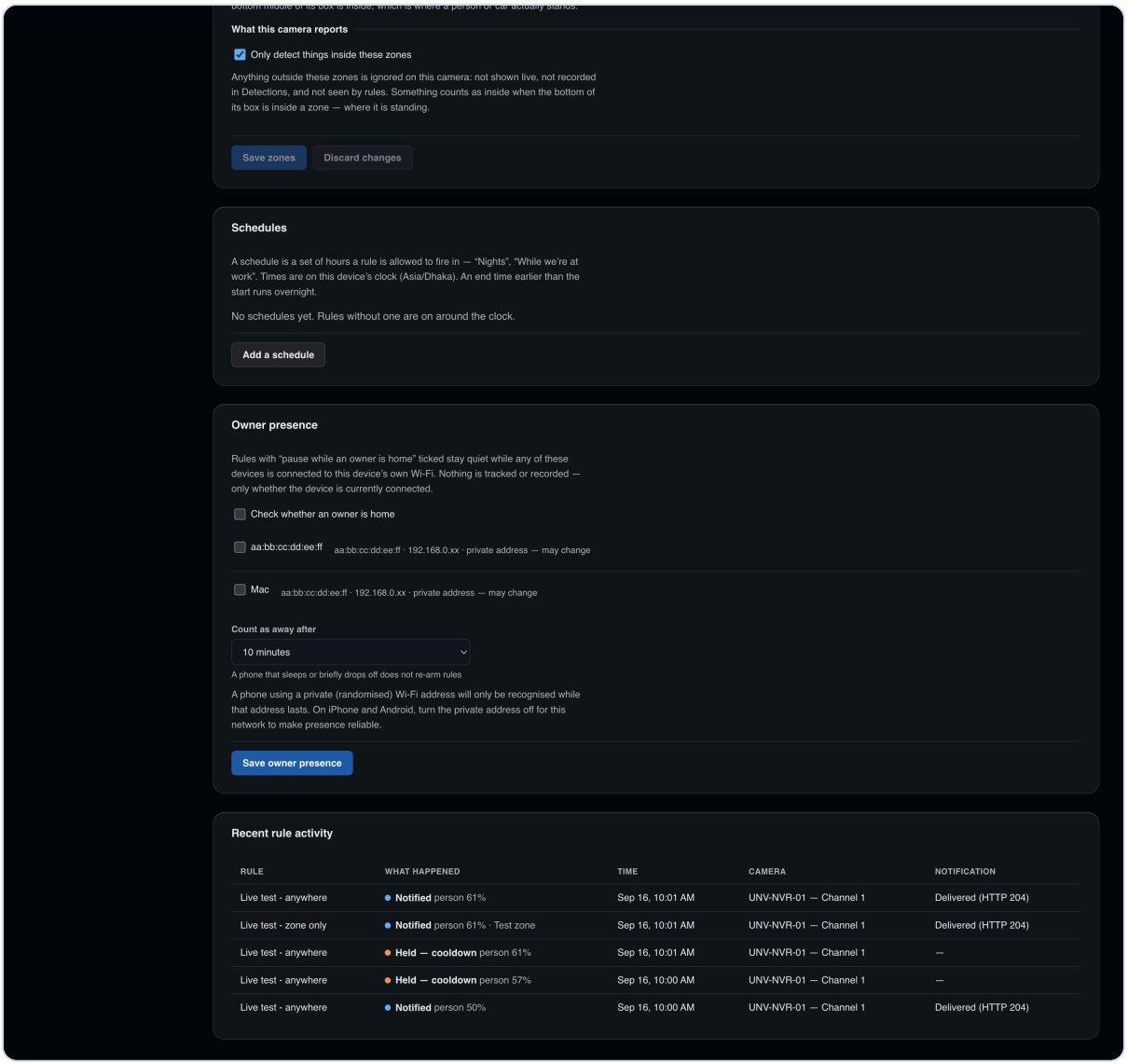
A schedule is a set of hours a rule may fire in — "Nights", "While we're at work". Up to 16 schedules, each with up to 14 windows of days plus a start and end time, on the device's own clock.

An end earlier than the start runs **overnight** and belongs to the day it started on: *Mon 22:00–06:00* covers Monday night into Tuesday morning. Start and end equal means the whole day. A rule with no schedule is active around the clock.

17 Rules and notifications



Surveillance → Rules, upper half. Everything that turns a detection into an action: the rules themselves, and the zones they watch.



Surveillance → Rules, lower half. Schedules, the presence check that pauses rules while you are home, and recent activity.

A rule is a sentence the device checks: *on these cameras, when a person is seen in this zone, during these hours, for at least so long — send a notification, then stay quiet.*

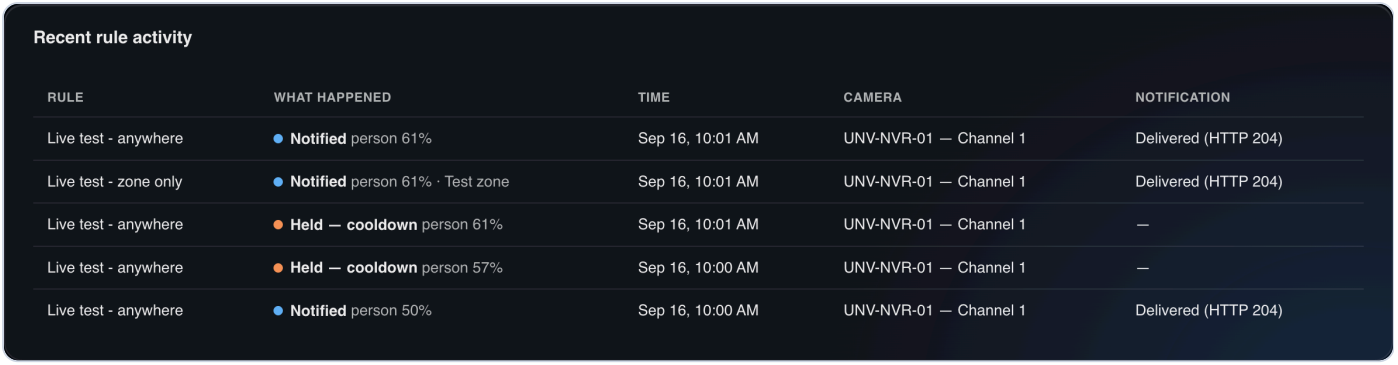
FIELD	MEANING
Cameras	Which to watch. None ticked means every camera with detection on.
What to look for	People, vehicles, animals.
Minimum confidence	For this rule, on top of the global setting.
Seen for	Ignores someone walking straight past.
How many at once	Requires several objects together.
Where in the picture	Which zones; empty means anywhere.
Only while	A schedule, or any time.
Send a notification to	A web address accepting JSON.
Signing secret	Optional; sent as a signature header so the receiver can verify the message.
Then stay quiet for	The cooldown, 0 seconds to 24 hours.
Pause while an owner is home	See the next section.

Would it have fired? replays the last 24 hours against the rule as written — an estimate, since cooldown and presence are not applied. **Send a test notification** delivers one message immediately, signed with the saved secret if there is one.

```
POST to your web address, Content-Type: application/json
{
  "source": "firefly-cap100",
  "type": "surveillance.rule_fired",
  "device": "Firefly-CAP100-W",
  "rule":   { "id": "rule_someone_at_the_gate", "name": "Someone at the gate" },
  "camera": { "id": "unv_nvr_01_channel_1", "name": "UNV-NVR-01 — Channel 1" },
  "detection": { "class": "human", "confidence": 0.61, "zones": ["Baggage zone"] },
  "time": "2026-09-16T10:01:30+06:00"
}
```

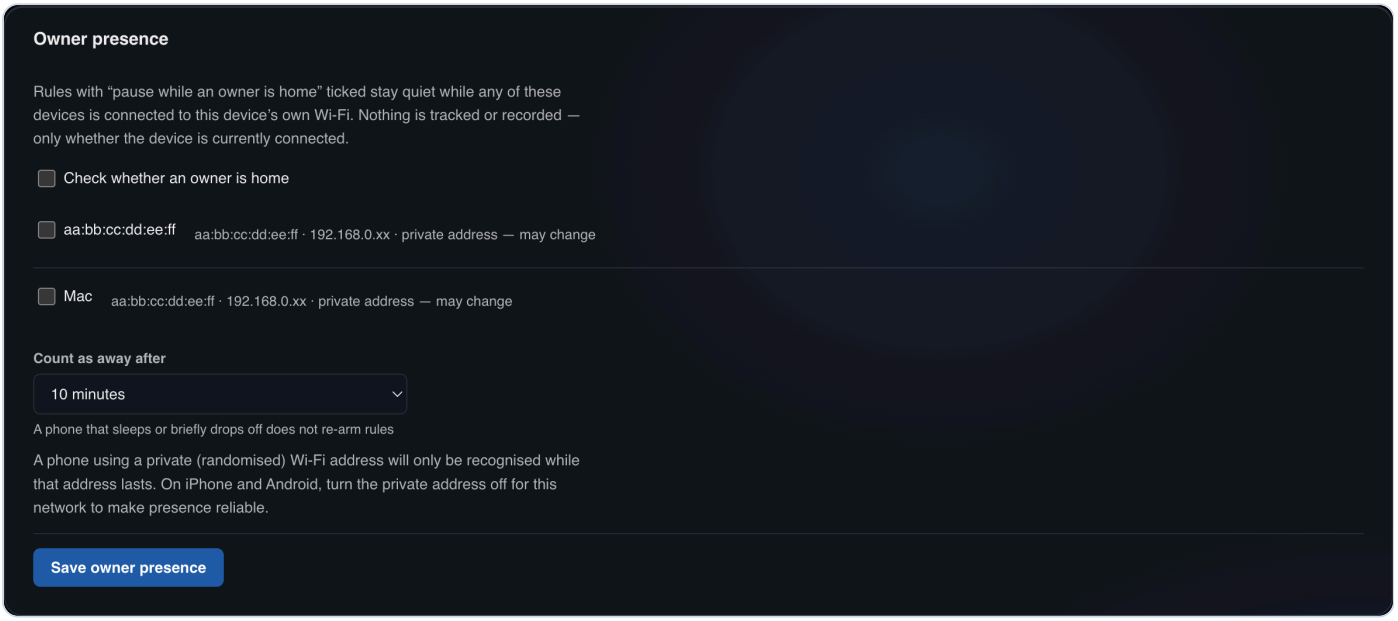
With a secret set, the request also carries `X-Firefly-Signature: sha256=…`, an HMAC of the exact body.

> **Notifications cannot be aimed at this device.** Addresses resolving to it are refused when saving and again before sending, and redirects are not followed — so a rule cannot be used to reach services meant to stay local.



Recent rule activity. Notified fired and sent; **Held — cooldown** matched while staying quiet; **Held — owner home** matched while somebody was in.

18 Owner presence



Surveillance → Rules → Owner presence. Addresses redacted here.

Rules with **pause while an owner is home** stay quiet while any listed device is on this device's own Wi-Fi. **Count as away after** sets how long a device must be absent before rules re-arm, so a sleeping phone does not trigger an alarm.

> **Private Wi-Fi addresses break this.** Phones randomise their address per network by default and it can change. Turn the private address **off** for this network on any phone you rely on. Nothing is tracked or recorded — only whether the device is connected now — and if the check fails, rules stay **armed** rather than silently paused.

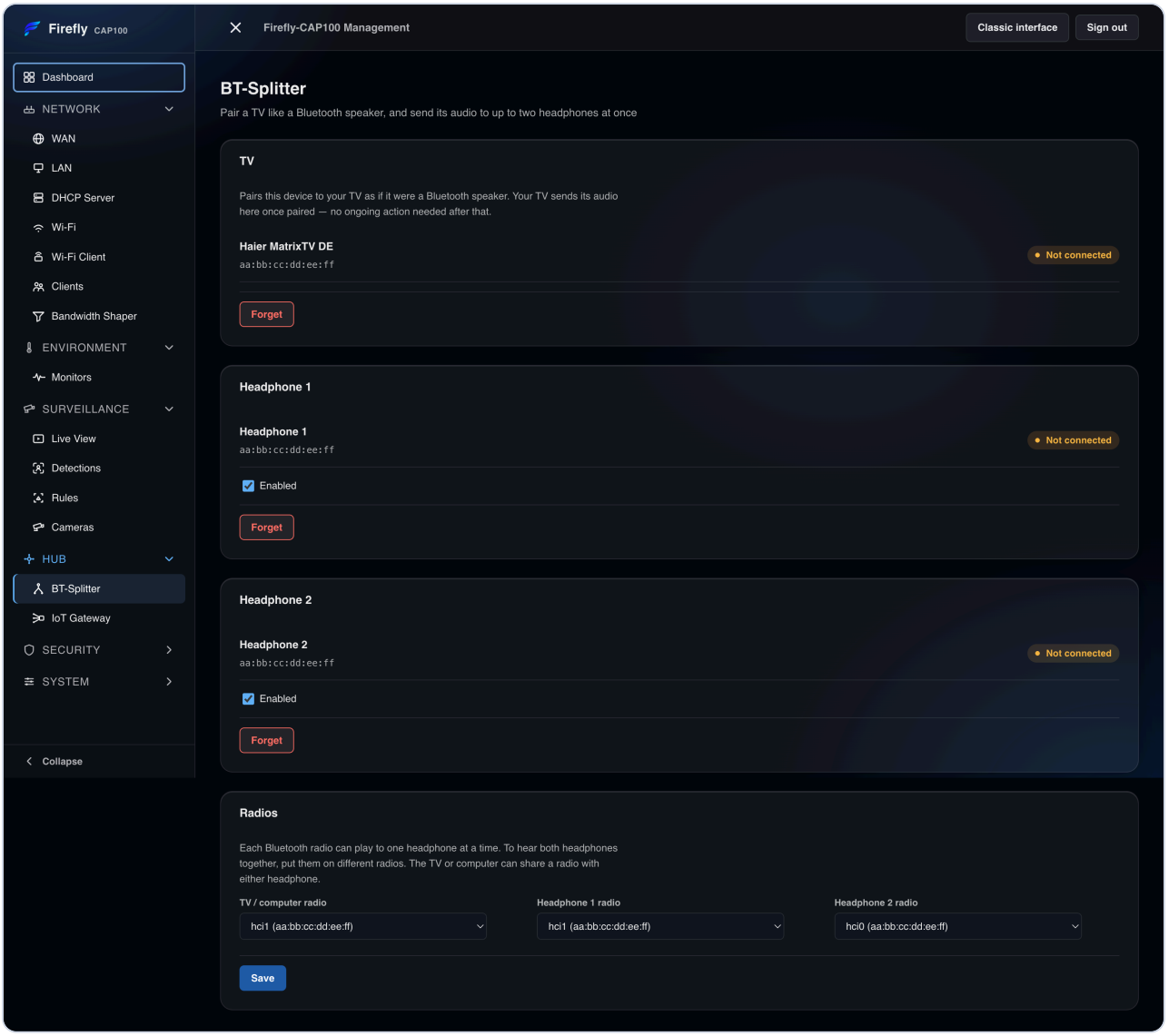
19 How detection works

1. **Motion is watched continuously** on a small greyscale copy — an idle scene costs almost nothing.
2. **While something moves**, the AI is asked what it is, roughly every two seconds, on the frame with the most movement.
3. **Findings are filtered** by kind, confidence and — if enabled — zone.
4. **Events are merged**, so one visit is one entry.
5. **Rules are evaluated** and notifications queued.

A check takes roughly **1.0–1.4 seconds** on CAP100-W hardware. Detections are stamped with the moment motion began, so the times line up with what happened even though the AI finished slightly later. Notifications are delivered on a separate thread, so a slow receiver never delays detection.

PART FOUR · HUB

20 BT-Splitter



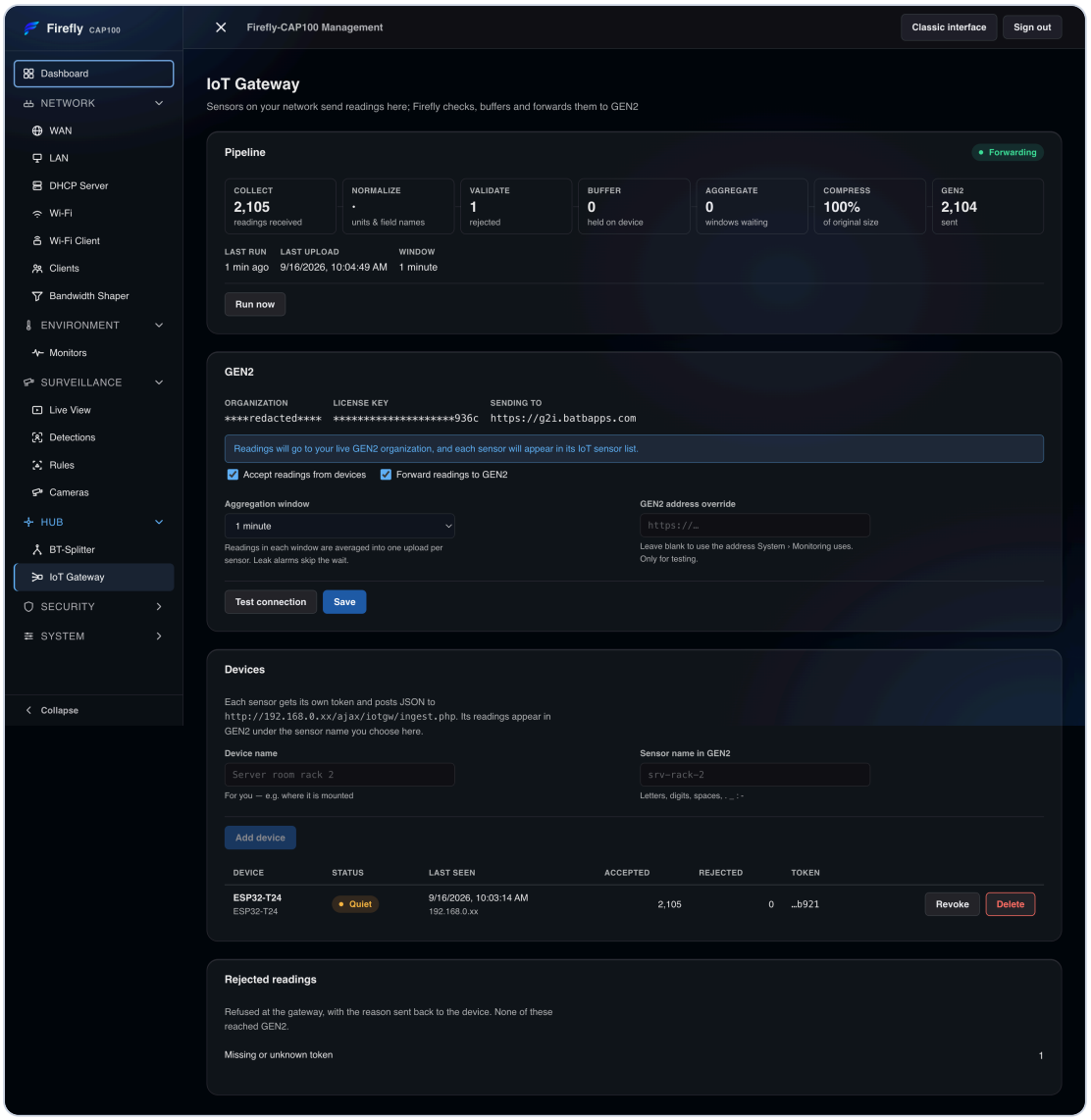
Hub → BT-Splitter. One source in, two headphones out.

BT-Splitter makes the device behave as a Bluetooth speaker for your TV or computer, then relays that audio out to two sets of headphones at once — useful for late-night television without disturbing anyone.

1. **TV** — start pairing here, then pair from the TV's own Bluetooth menu. Once paired the TV reconnects by itself; no ongoing action is needed.
2. **Headphone 1** and **Headphone 2** — scan and pick each set. Each has its own **Enabled** switch and **Forget**.
3. **Radios** — assign which Bluetooth radio each role uses.

> **Each radio plays to one headphone at a time.** To hear both headphones together, put them on **different** radios. The TV or computer may share a radio with a headphone. On a unit with a single radio you can pair both but only one will play.

21 IoT Gateway



Hub → IoT Gateway. Sensors post here; the device forwards to GEN2.

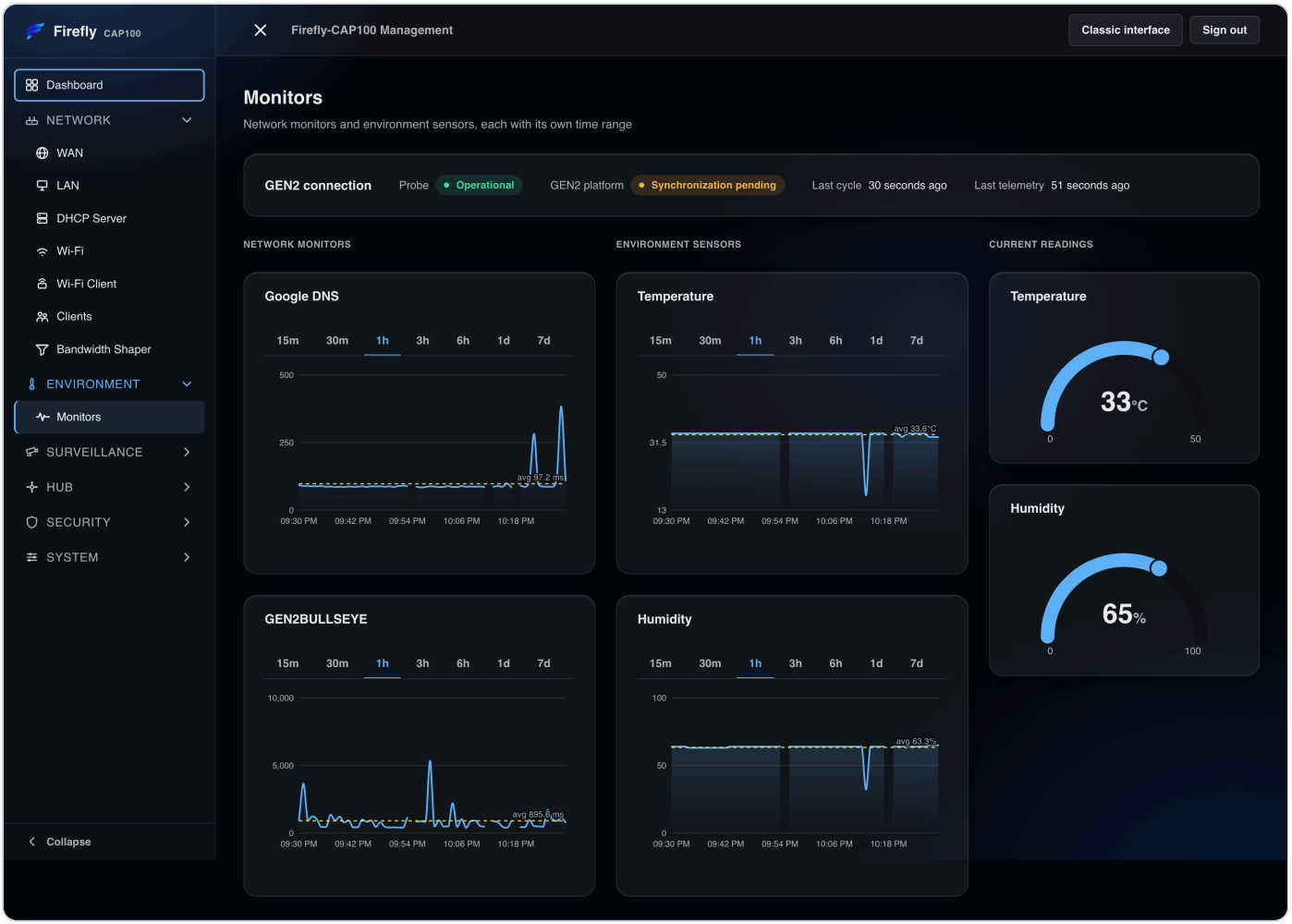
Sensors send readings to this device, which checks and combines them and forwards them to your GEN2 organisation. Readings are buffered, so a sensor keeps working through an internet outage.

CARD	WHAT IT DOES
Pipeline	Shows each stage — collect, validate, buffer, aggregate, forward. **Run now** forces a cycle instead of waiting.
GEN2	Whether readings are accepted at all, whether they are forwarded, the aggregation window (1–15 minutes), and an optional address override. **Test connection** checks the credentials.
Devices	Each sensor gets a name, a name to appear under in GEN2, and its own token. The table shows status, last seen, accepted and rejected counts. Tokens can be revoked.
Rejected readings	What was refused and why. None of these reached GEN2 — this is where to look when a sensor seems silent.

Forwarding sends data to your live GEN2 organisation, where each sensor appears in the IoT sensor list. It is off by default for that reason. Turn it on only when you mean to write real readings.

PART FIVE · ENVIRONMENT

22 Monitors

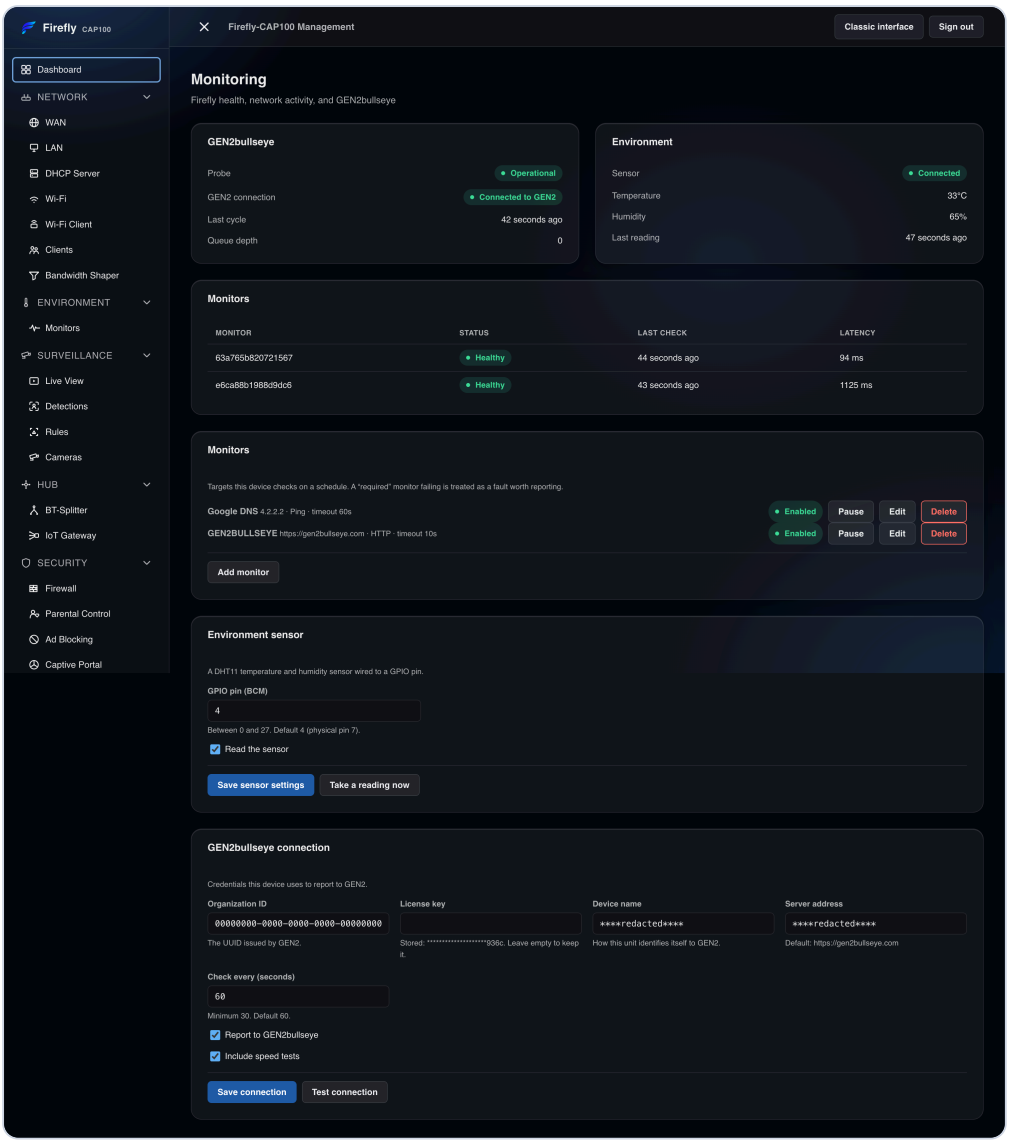


Environment → Monitors. Recorded history for each monitored target and sensor.

This is the **recorded data** — response times for each target being checked, plus temperature and humidity from the attached sensor. Each chart has its own range: 15 minutes, 30 minutes, 1, 3 or 6 hours, a day, or a week.

Configuration lives elsewhere: see Monitoring for adding targets and setting up the sensor.

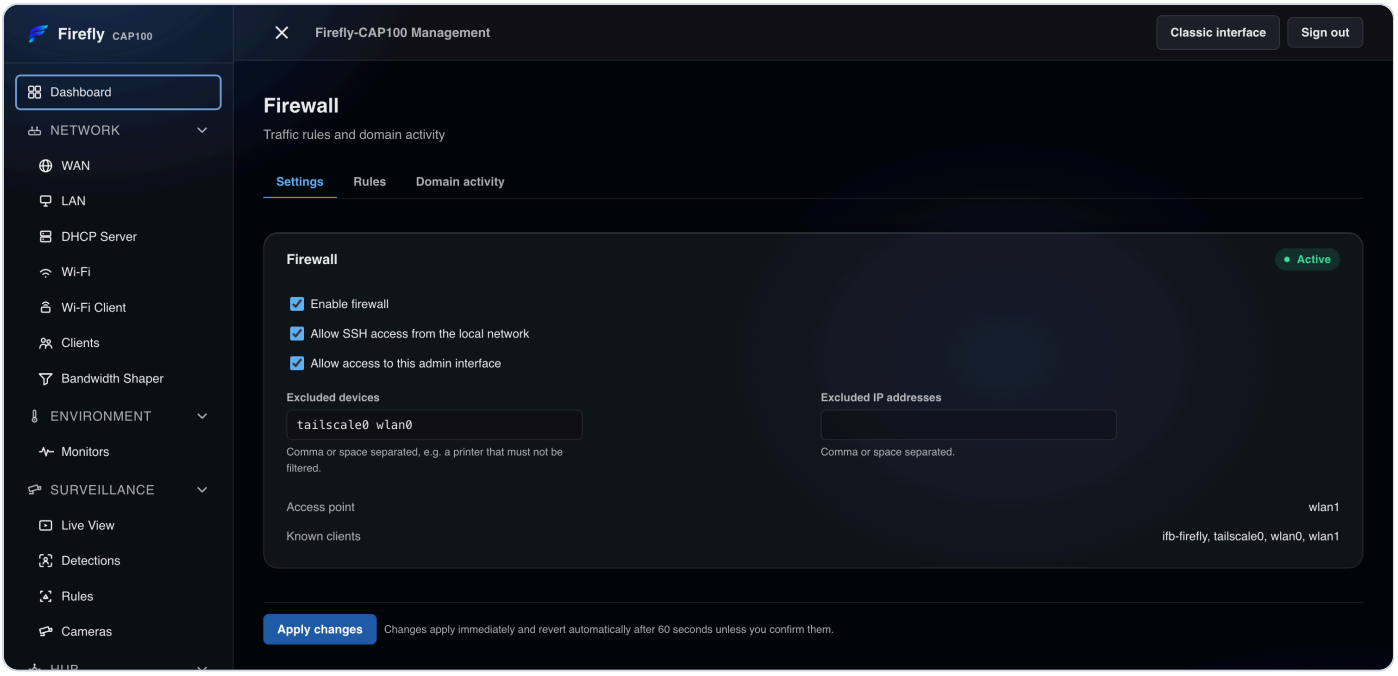
23 Monitoring and sensors



System → Monitoring. The configuration behind the Environment charts.

CARD	WHAT IT DOES
Monitors	Targets checked on a schedule, with status, last check and latency. Add, edit, pause or delete them. A **required** monitor failing is treated as a fault worth reporting.
Environment sensor	A DHT11 temperature and humidity sensor on a GPIO pin. Set the pin (BCM numbering), enable reading, and **Take a reading now** to test the wiring.
GEN2bullseye connection	Organisation ID, license key, device name, server address, how often to check, whether to report, and whether to include speed tests.

24 Firewall

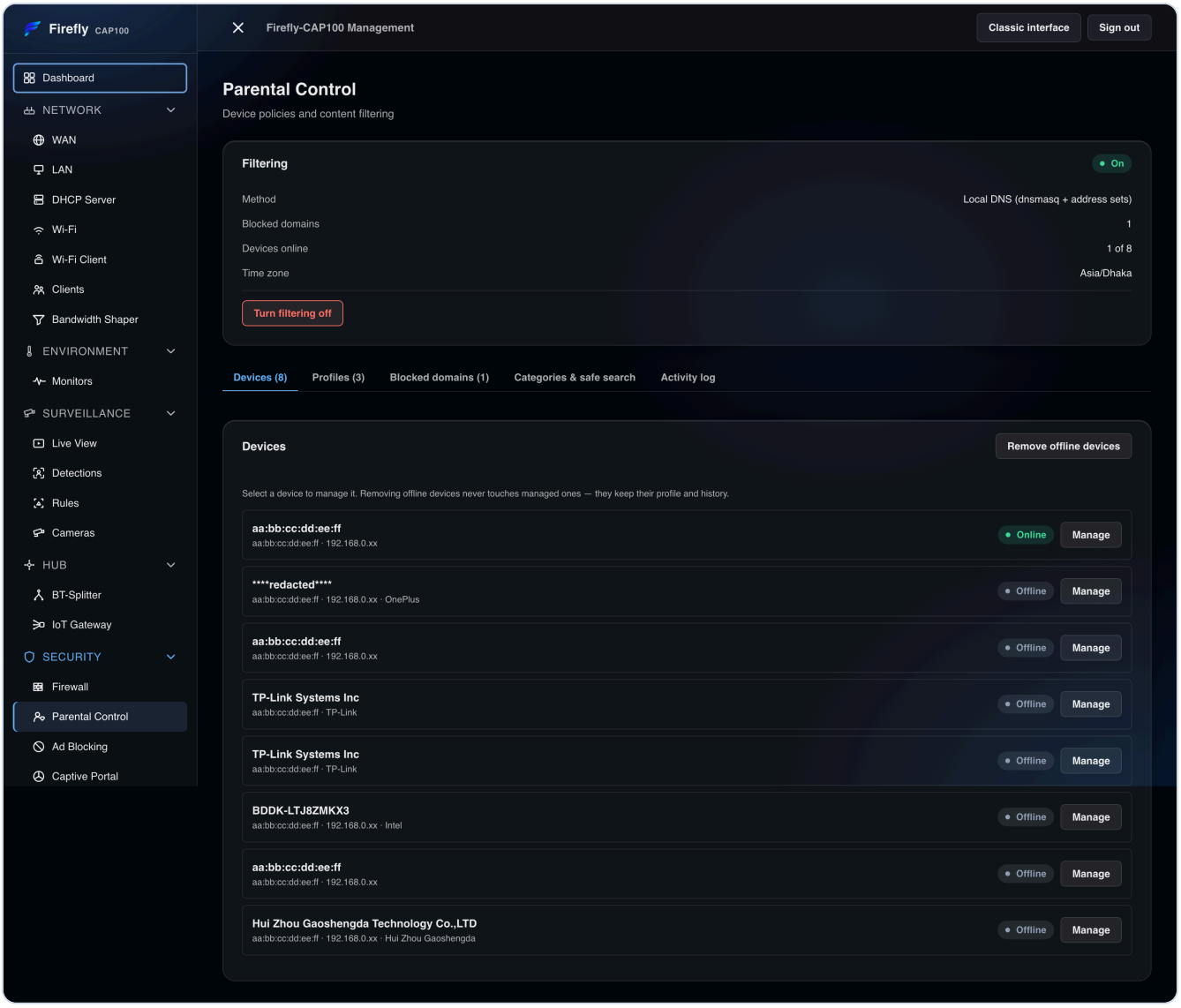


Security → Firewall.

SETTING	MEANING
Enable firewall	The master switch.
Allow SSH access from the local network	Command-line access from inside the network.
Allow access to this admin interface	Whether this web interface is reachable.
Excluded devices / IP addresses	Devices the rules do not apply to.

Do not switch off admin access unless you have another way in. Turning off both the admin interface and SSH can leave you needing physical access to recover the device.

25 Parental control

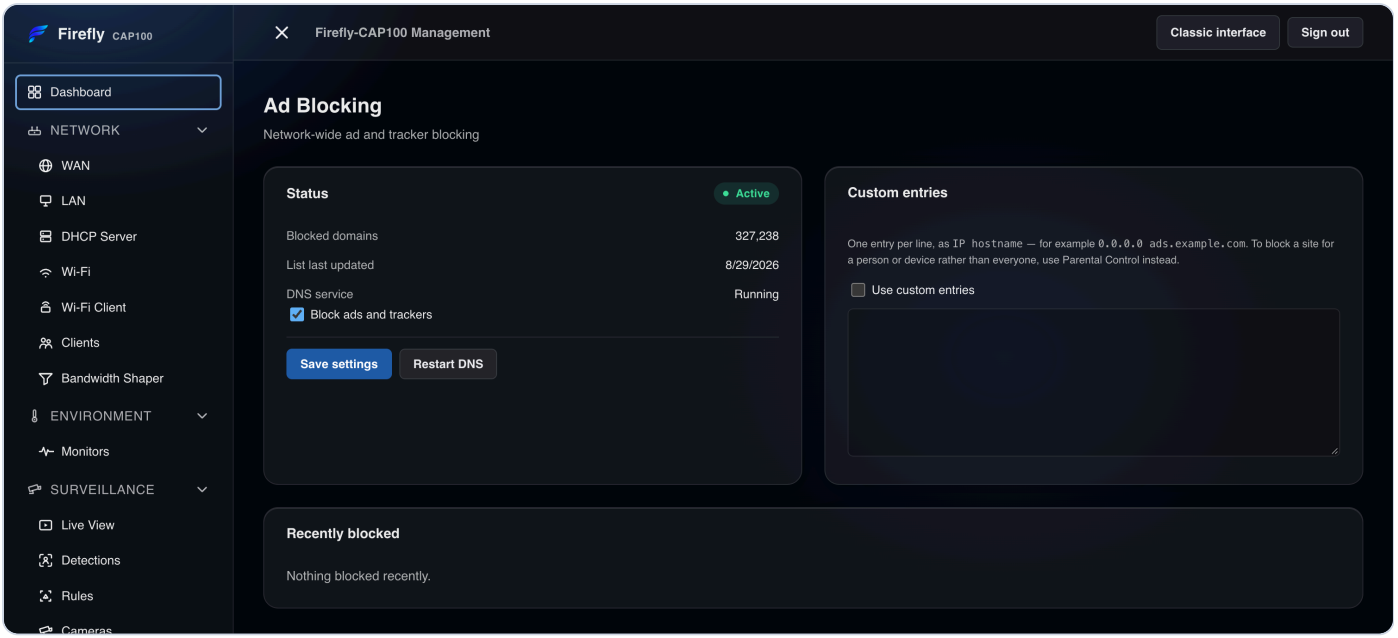


Security → Parental Control. Per-device rules rather than network-wide ones.

Turn filtering on, then **Manage** any device in the list to give it a profile. This is the right tool when a restriction should apply to one person or device — ad blocking, by contrast, applies to everyone.

> **Remove offline devices** tidies the list without touching managed devices; they keep their profile and history.

26 Ad blocking

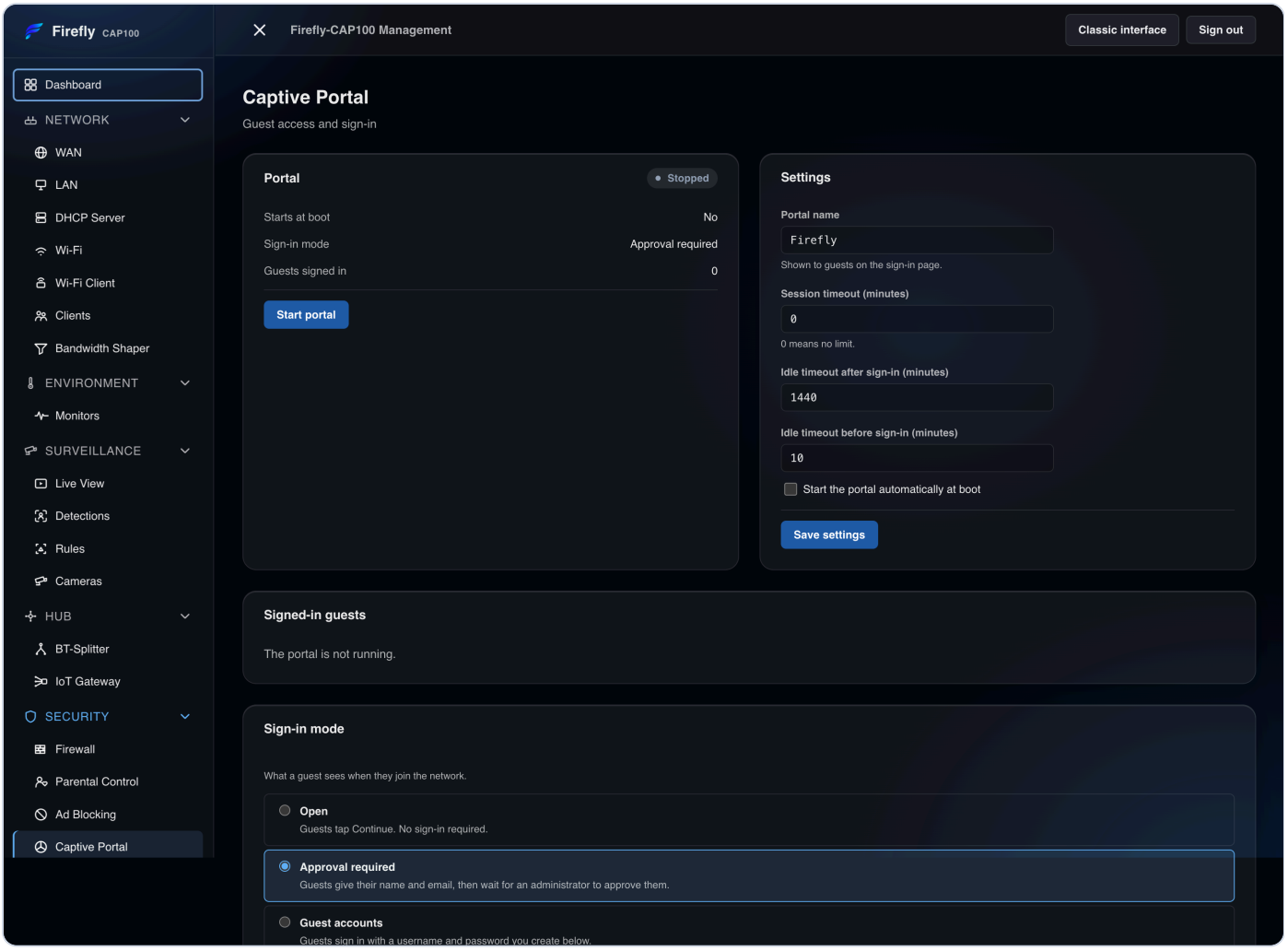


Security → Ad Blocking. Network-wide, for every device.

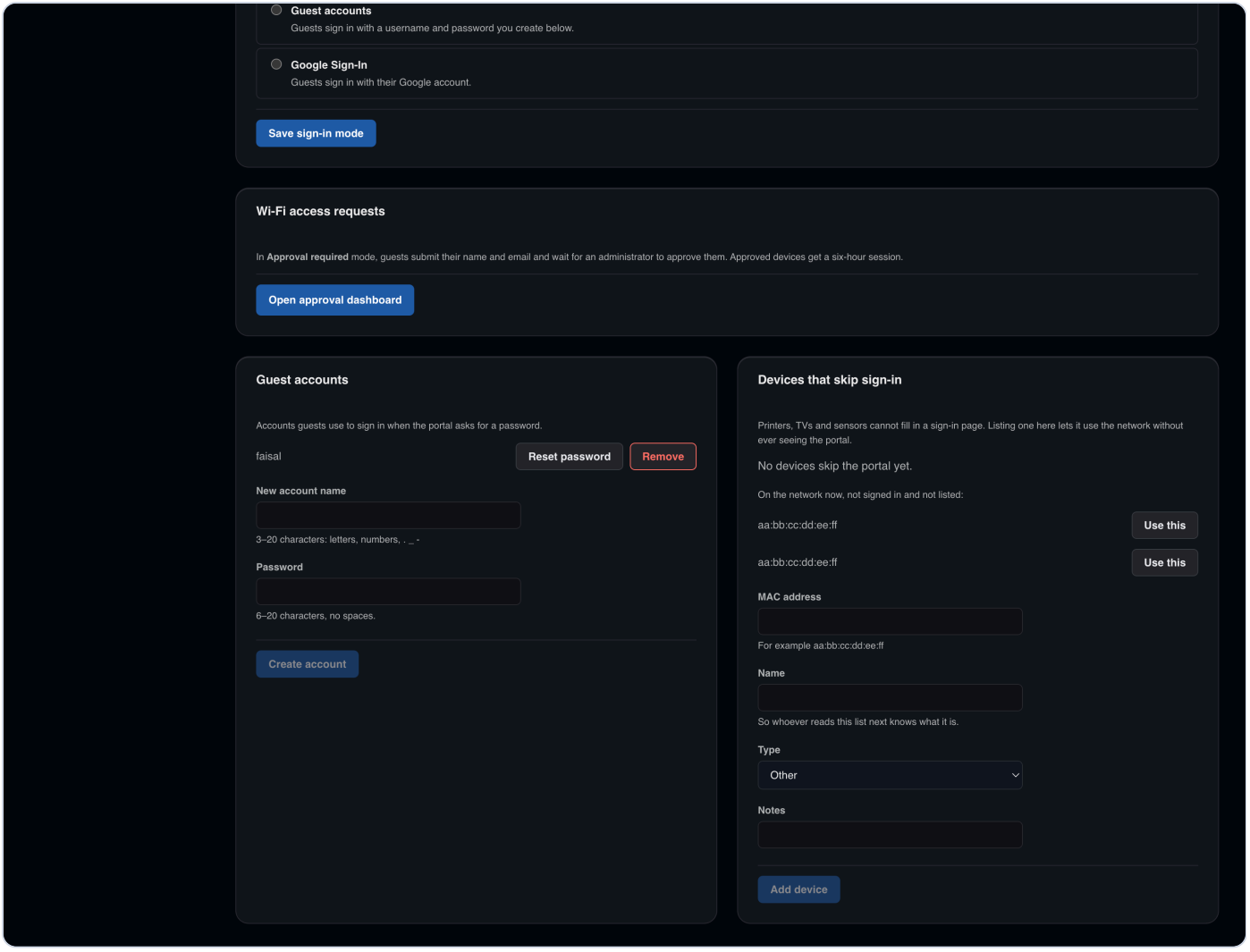
Block ads and trackers is the switch. **Custom entries** takes one entry per line in the form `0.0.0.0 ads.example.com`. **Recently blocked** shows what has been stopped lately, which is the quickest way to confirm it is working — or to spot a site broken by over-blocking.

Restart DNS applies changes that need the name server reloaded.

27 Captive portal



Security → Captive Portal, upper half. The sign-in page guests meet when they join, and how they are asked to sign in.

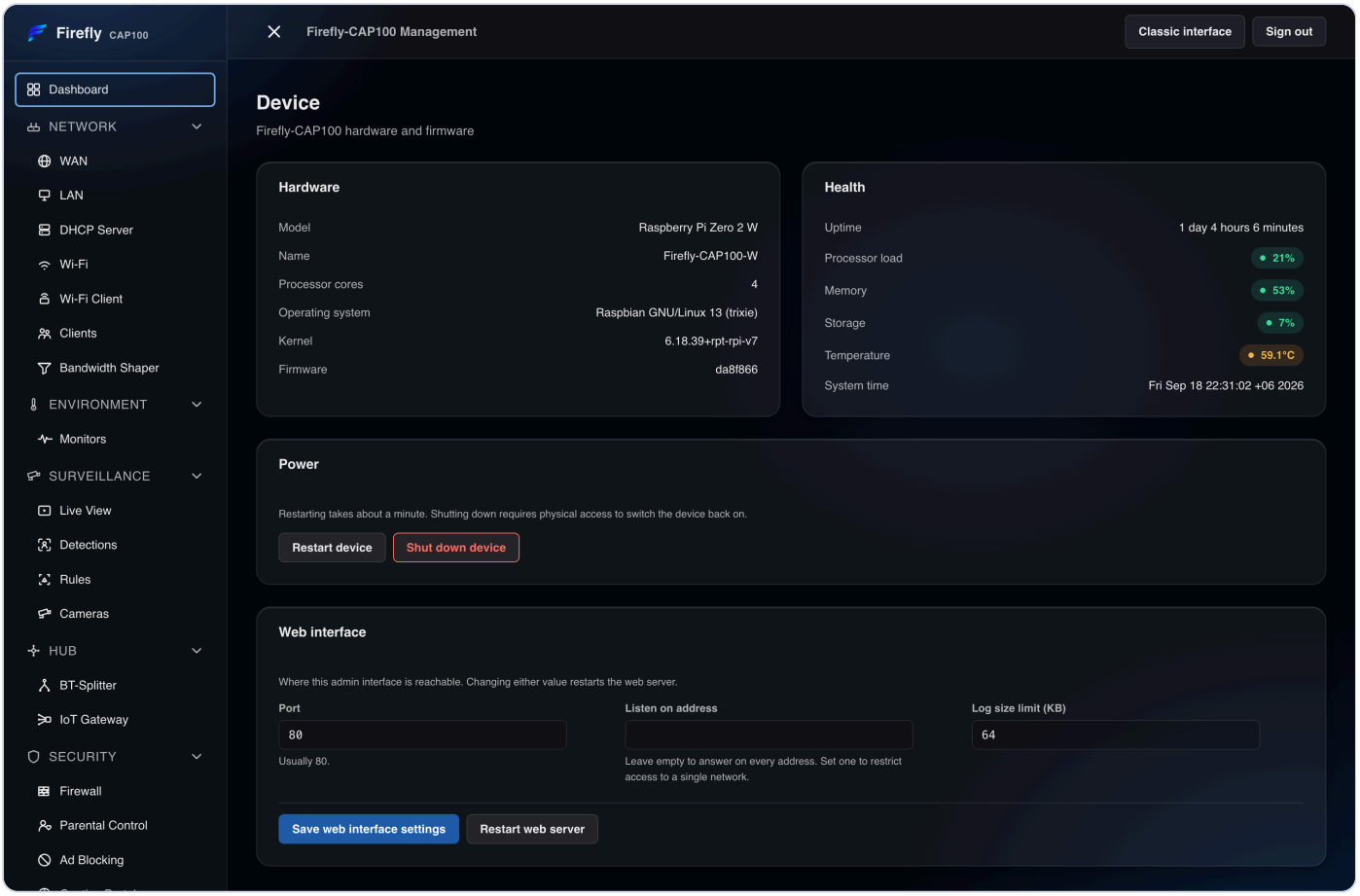


Security → Captive Portal, lower half. Guest accounts, and the devices exempt from signing in at all.

CARD	WHAT IT DOES
Portal	Start and stop the portal.
Settings	Portal name, session timeout, idle timeouts before and after sign-in, and whether it starts at boot.
Sign-in mode	What a guest sees on joining. In **approval required** mode they submit a name and email and wait for you; approved devices get a six-hour session.
Signed-in guests	Who is currently on.
Guest accounts	Named accounts with passwords, for when the portal asks for credentials.
Devices that skip sign-in	Printers, TVs and sensors cannot fill in a form. List one by address with a type and it uses the network without seeing the portal.

PART SEVEN · SYSTEM

28 Device



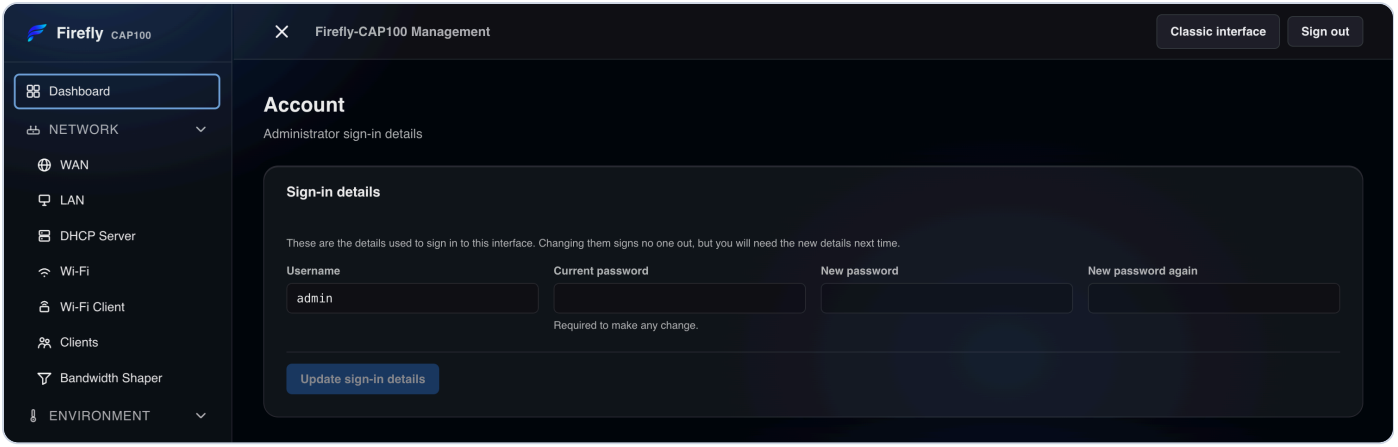
System → Device.

Hardware and **Health** report the model and its condition. **Power** restarts or shuts down the unit — a restart takes about a minute, and a shutdown needs physical access to switch it back on. **Web interface** sets the port, the address it listens on, and the log size limit.

> **Changing the port or listen address restarts the web server**, so this page will disappear briefly and may come back at a different address.

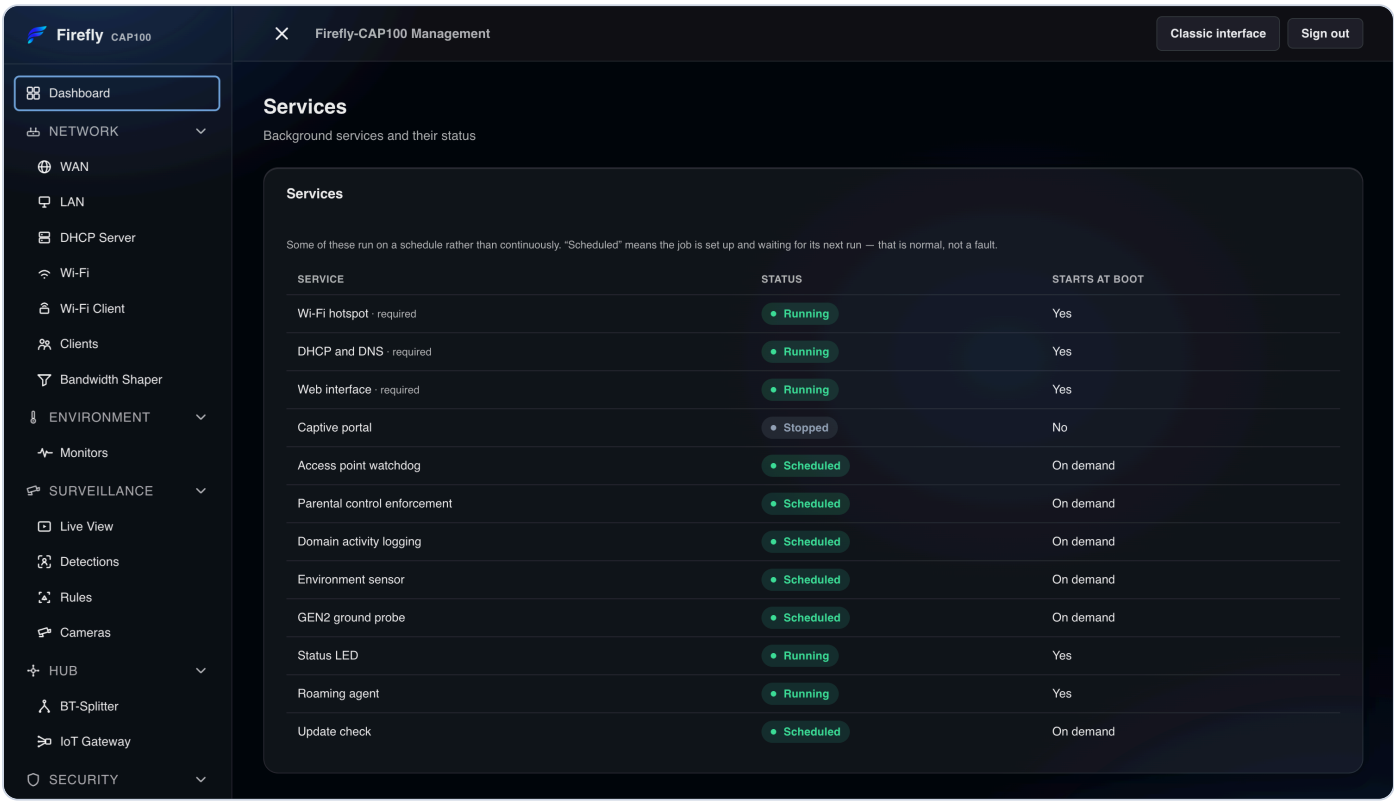
29 Account

The username and password for this interface. Changing them signs nobody out, but the new details are needed next time. Setting a password requires the current one.



System → Account. The sign-in details for this interface.

30 Services

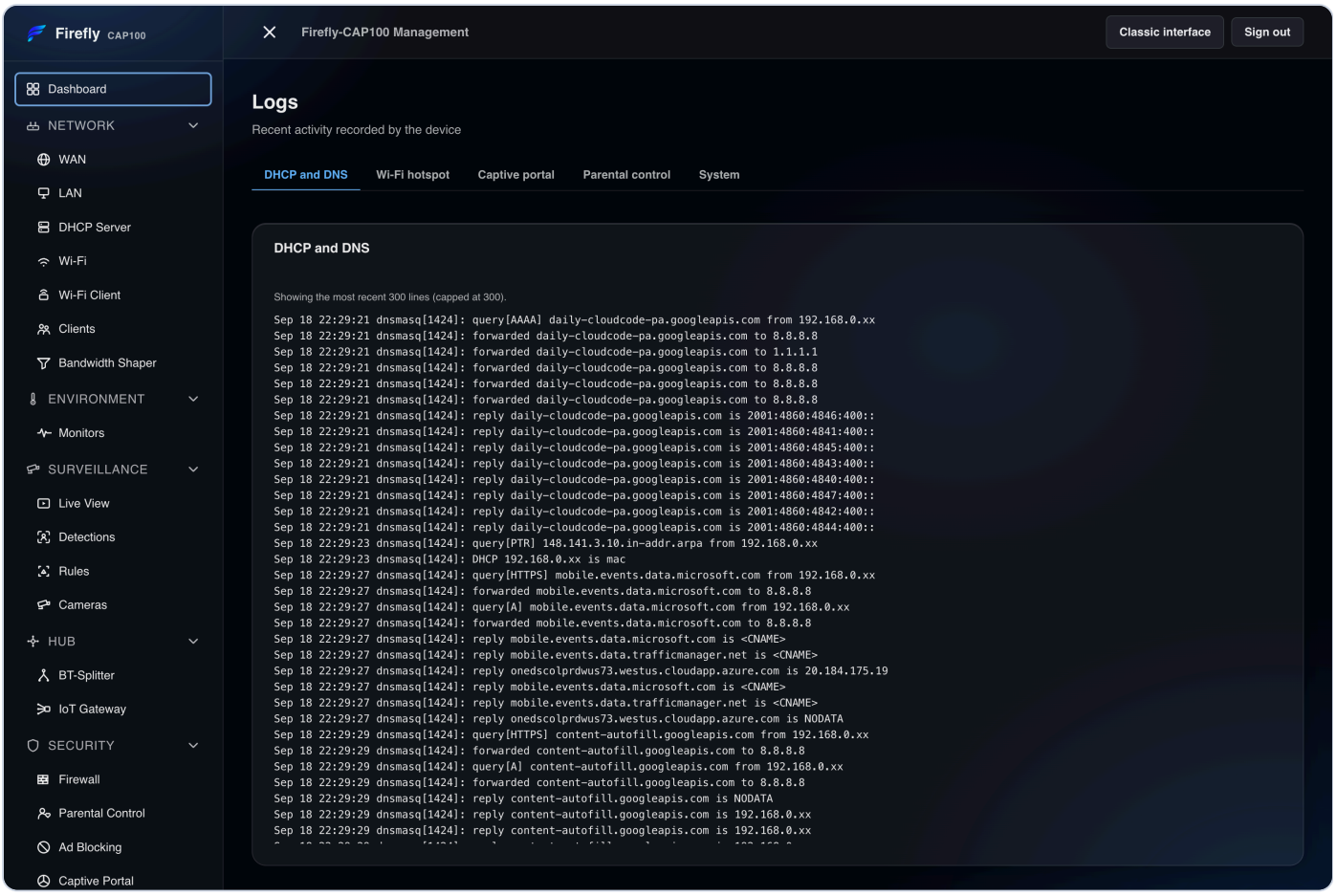


System → Services. What is running, and what starts at boot.

> **"Scheduled" is not a fault.** Some of these run on a timer rather than continuously; scheduled means the job is set up and waiting for its next run.

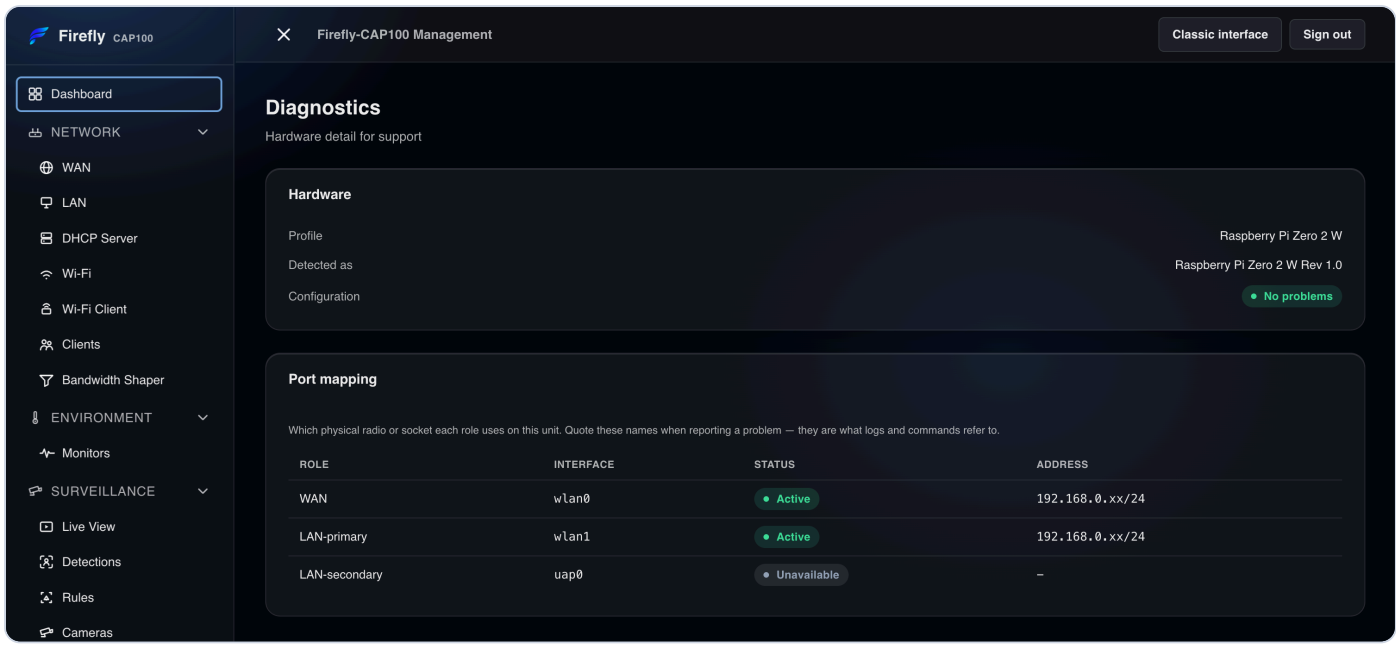
31 Logs

The most recent 300 lines of DHCP and DNS activity — address assignments and name lookups, if you enabled those under DHCP Server. This is where to confirm whether a device actually asked for an address.



System → Logs. Each tab is a separate log: DHCP and DNS, the Wi-Fi hotspot, the captive portal, parental control, and the system itself.

32 Diagnostics



System → Diagnostics. The port map names every radio and socket by role.

Port mapping shows which physical radio or socket each role uses on your unit, with its status and address.

> **Quote these names when reporting a problem.** They are what the logs and commands refer to, so they make a support conversation far shorter.

PART EIGHT · REFERENCE

33 Troubleshooting

WHAT YOU SEE	WHAT IT MEANS
The admin page is unreachable	Check you are on the right network. If the LAN address or web port was changed, the page moved. Firewall settings can also block it.
No internet for anyone	Start at **WAN**: is there a connection and an address? Then **Diagnostics** for the port map.
A device cannot get an address	**DHCP Server**: is it enabled, is the pool large enough, is the device in **Devices with an address now**? **Logs** shows whether it asked.
Wi-Fi is slow or drops	Check the channel against the dashboard's channel chart, and the country setting. Then look at **Bandwidth Shaper**.
"Detection is not running"	The detector is not reporting. Usually detection is off for every camera, which stops the service by design.
Zones show but no boxes	Same cause: zones come from settings, boxes only exist while the detector runs.
Live View frozen or blank	Usually the camera is sending **H.265**, which browsers handle poorly. Set that camera or channel to **H.264**.
Picture stalls every few minutes	Often the camera or NVR pausing; the relay reconnects. If several cameras stall in the same second, suspect the NVR.
A rule never fires	Work down the chain: detection on for that camera, the object kind enabled, confidence not too high, the object inside the zone at its feet, the schedule active, no owner home, not in cooldown. **Recent rule activity** separates "never matched" from "held back".
A sensor's readings never arrive	**IoT Gateway → Rejected readings** gives the reason. Check the token has not been revoked.
Only one headphone plays	Both are on the same Bluetooth radio. Put them on different radios.
Presence never sees a phone	The phone is using a private Wi-Fi address, or is not on this device's own network.

34 Privacy and stored data

WHAT	WHERE	HOW LONG
Camera video	Never recorded; passed from camera to viewer	—
Detections and snapshots	On the device	Your retention setting, 1–90 days
Rule matches	On the device, beside the detections	Same
Camera passwords and webhook secrets	On the device; never shown again	Until removed
Owner devices	The addresses you tick, plus whether they are connected now	No history kept
DHCP and DNS logs	On the device, if enabled	Last 300 lines shown
Sensor readings	Buffered on the device, forwarded to GEN2 if enabled	Until forwarded

35 Limits and specifications

Cameras	**8 per device**
Zones	**8 per camera, 3–24 corners each**
Schedules	**16, each up to 14 time windows**
Rules	**32**
Owner devices	**16**
Detection retention	**1–90 days; snapshots 100 MB – 20 GB**
Rule cooldown	**0 seconds – 24 hours**
Time present	**0 – 600 seconds**
IoT aggregation	**1 – 15 minutes**
Bluetooth	**Two headphones, one per radio**
Camera protocols	**RTSP, RTSPS, ONVIF — H.264 strongly preferred**
AI check time	**≈1.0–1.4 s on CAP100-W**