BLUEDOT

QUANTUMBNG · OPERATOR REFERENCE

# QuantumBNG Operator Guide

## Day-to-day operation, tasks, and console reference

*The complete operator reference for QuantumBNG: architecture, every console panel, common operator tasks, backup and restore, key rotation, and troubleshooting.*

| | |
|---|---|
| **Document Type** | BlueDot Operator Reference |
| **Audience** | Operators running QuantumBNG day-to-day |
| **Product** | QuantumBNG — Quantum IPoE BNG |
| **Version** | v1.2.0-09 |
| **Classification** | **BlueDot Proprietary** |
| **Date** | July 2026 |

# Contents

# QuantumBNG Operator Guide

**Audience:** the operator running QuantumBNG day-to-day. **Complements:** `quick-start.md` for first-time install; this document is the reference for everything after.

## What QuantumBNG is

A self-contained Broadband Network Gateway for small and mid-size ISPs. One box takes DHCP requests from subscriber CPEs, provisions IPs from your pool, enforces per-plan rate limits at line rate via a 3-color policer, and forwards subscriber traffic to your upstream router.

One tarball, one `sudo ./install.sh`, one web UI at `https://<box>:8443`. No separate controller box, no separate database, no separate telemetry stack — everything lives on the appliance and starts on boot.

## Architecture at a glance

| Plane | Component | What it does | Where it lives |
|---|---|---|---|
| **Management** | QuantumTouch (bng-deploy) | The web UI + REST API operators use. Flask + gunicorn. | Port 8443 (HTTPS) |
| **Control** | Quantum Controller | Source of truth for subscribers, sessions, DHCP leases, AAA state. | Docker container, port 3000 (HTTPS, `127.0.0.1` only) |
| **Data** | VPP + tuned DPDK | Line-rate packet forwarding with a per-subscriber 3-color policer (trTCM). | Kernel-adjacent, one main core + N workers pinned to isolcpus |
| **Bridge** | vpp-bridge | Go daemon that translates controller decisions into VPP CLI operations and vice versa. | `systemd` unit |

Traffic path for a subscriber packet:

```
CPE  →  Access NIC (VPP)  →  BNG plugin (policer + session lookup)  →  Uplink NIC (VPP)  →  Core router
                                  ↑
                                  Controller (via vpp-bridge) — session install, plan lookup
```

DHCP path:

```
CPE DHCP DISCOVER → Access NIC (VPP) → BNG plugin punts → vpp-bridge → Controller
                                                                          ↓
                                                                  AAA lookup (Local or RADIUS)
                                                                          ↓
Controller crafts OFFER → back down the stack → CPE
```

The Community Edition license caps concurrent sessions at 1000. That's shown in the header pill and in the Sessions "over time" chart.

For a deeper theory-of-operation (packet path, state ownership, DHCP/AAA state machines), see `../theory-of-operation.md` — that document is for engineers integrating against QuantumBNG; this one is for operators running it.

---

# The console

You reach it at `https://<box-ip>:8443`. First-run brings you to the setup wizard (see the Quick Start). After that, you land on **Dashboard**.

The left nav is grouped into four sections:

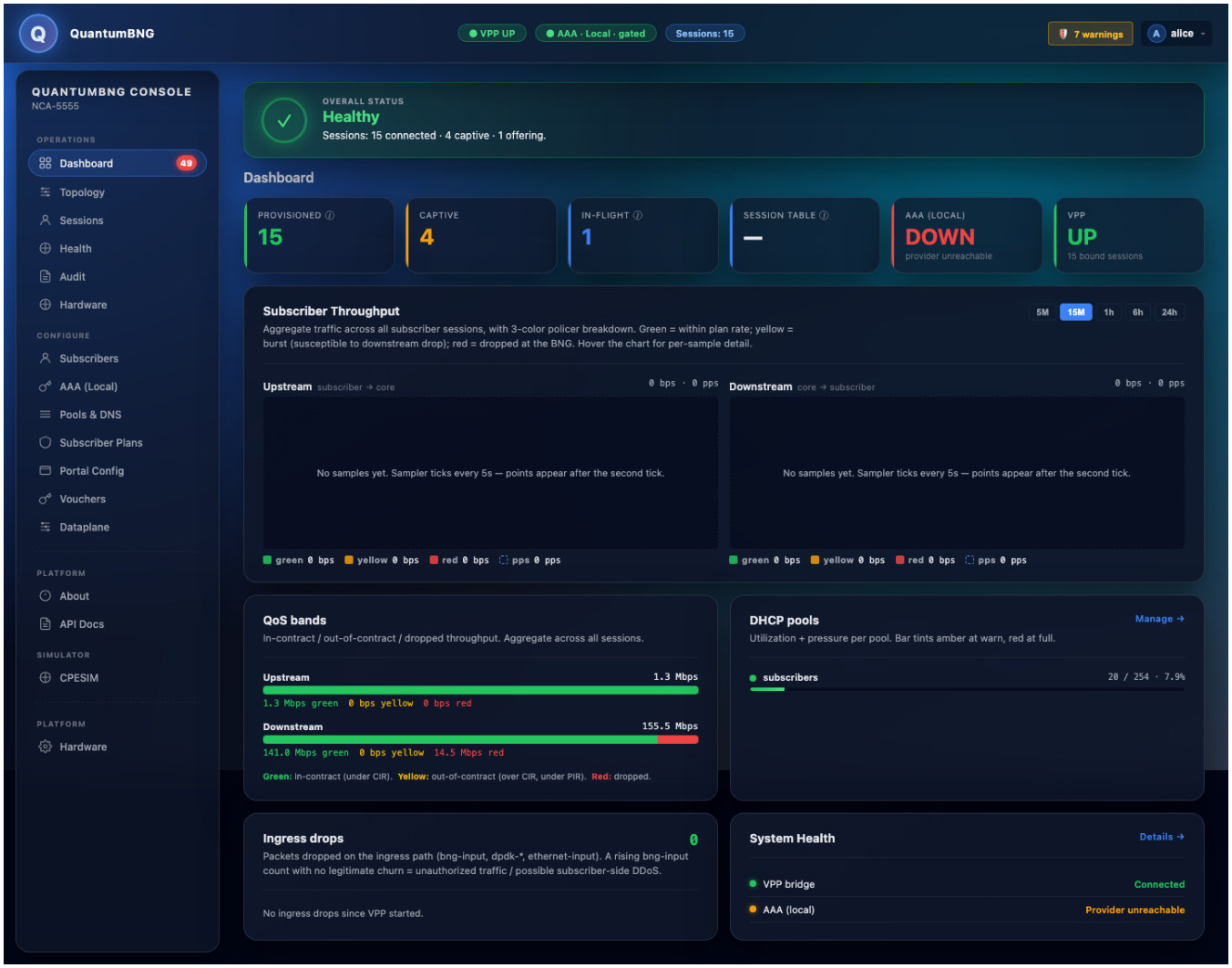
| Group | Purpose |
|---|---|
| **OPERATIONS** | What's happening right now — live counters, sessions, health, audit trail |
| **CONFIGURE** | The knobs — pools, plans, subscribers, portal, dataplane |
| **PLATFORM** | About page, hardware inventory |
| **SIMULATOR** | CPESIM (only visible if the CPESIM plugin is installed) |

Header pills are the always-on status snapshot. Green = OK, amber = warning, red = action needed:

- **VPP** — dataplane up? If `?` for more than 10s, the controller can't reach vpp-bridge (see Troubleshooting).
- **AAA · Local · gated** (or `open`) — provider health + mode. `Local · unreachable` means the local AAA store isn't loading.
- **Sessions: N** — current onboarded subscriber count.
- **N warnings** (amber shield) — click to see open events (unread events also show as a badge next to Dashboard in the nav).

## Dashboard

The operator's home screen. Six top-line KPIs plus two live throughput charts and three panels.




**KPIs (top row, left to right):**

| KPI | What it means | When to look |
|---|---|---|
| **Provisioned** | Subscribers currently CONNECTED (have an IP, on their plan) | Baseline health |
| **Captive** | Subscribers redirected to portal (unprovisioned or awaiting login) | Rising during business hours = provisioning workflow lag |
| **In-flight** | Sessions mid-DORA (OFFERING or REQUESTING) | > 10 for more than 30s = reply-path stall |
| **Session Table** | VPP-side session-slot occupancy | Approaches 1000 = at Community Edition cap |
| **AAA (Local)** | Local AAA provider health | `DOWN` = users can't authenticate (see AAA (Local)) |
| **VPP** | Dataplane status + bound-session count | `UP N bound sessions` — should match Provisioned KPI |

**Subscriber Throughput** — two stacked-area charts, upstream and downstream. Each shows the 3-color QoS breakdown: green = within CIR (in-contract), yellow = between CIR and PIR (burst), red = dropped by the policer. Time-range picker top-right (5M / 15M / 1H / 6H / 24H).

**QoS bands** — same three colors as the throughput chart but as a rolling-average bar per direction. Use the throughput chart to see when a spike happened; use the bands to see the current split.

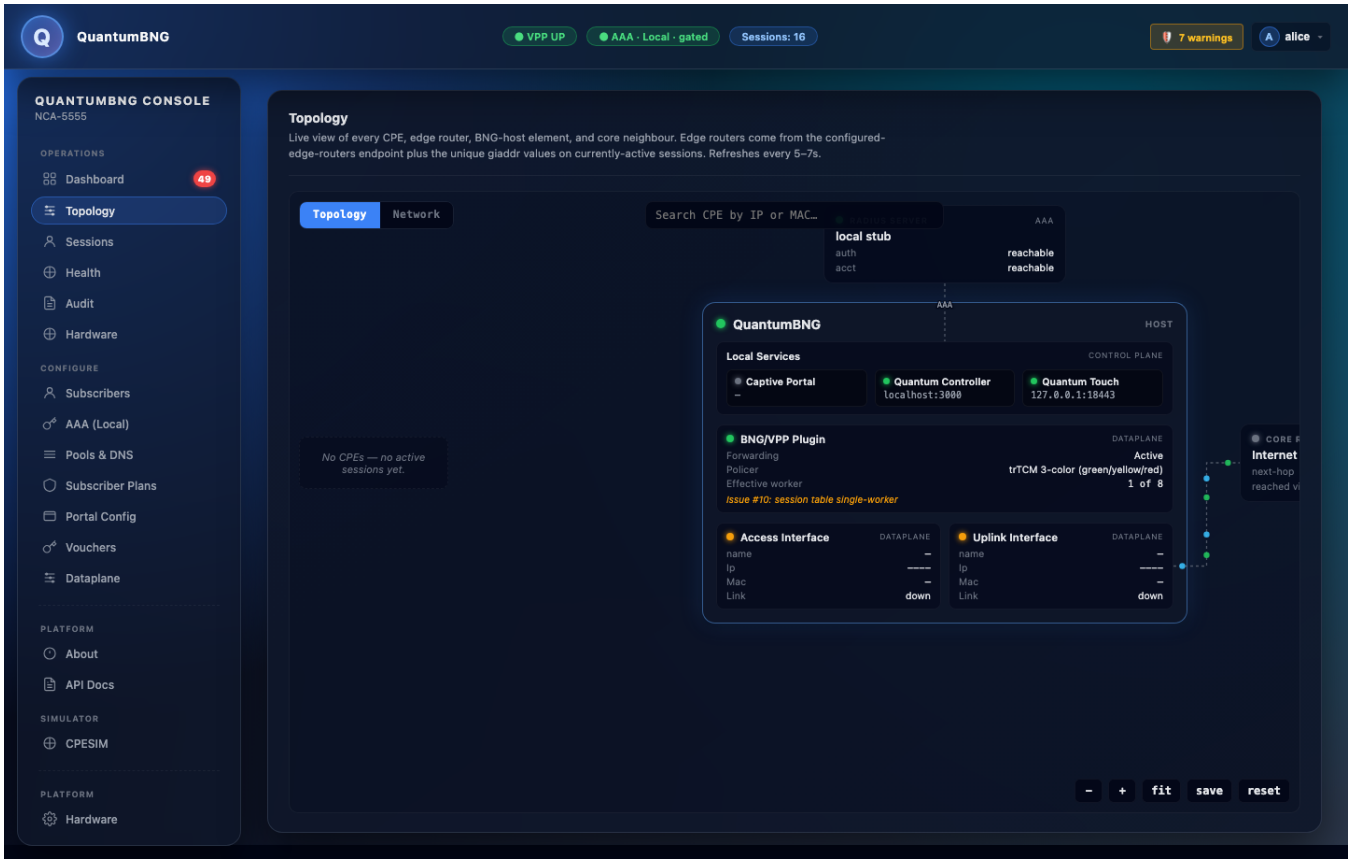
**DHCP pools** — per-pool utilization bar. Tints amber at warn threshold, red at full. Click **Manage** to jump to Pools & DNS.

**Ingress drops** — a counter of packets dropped on the ingress path ( `bng-input` , `dpdk-*` , `ethernet-input` ). A rising count with no legitimate churn typically means unauthorized traffic or subscriber-side DDoS.

**System Health** — one-liner status of each subsystem. Click **Details** for the full Health page.

## Topology

Live map of every element in the packet path — from CPEs on the left to the core router on the right.

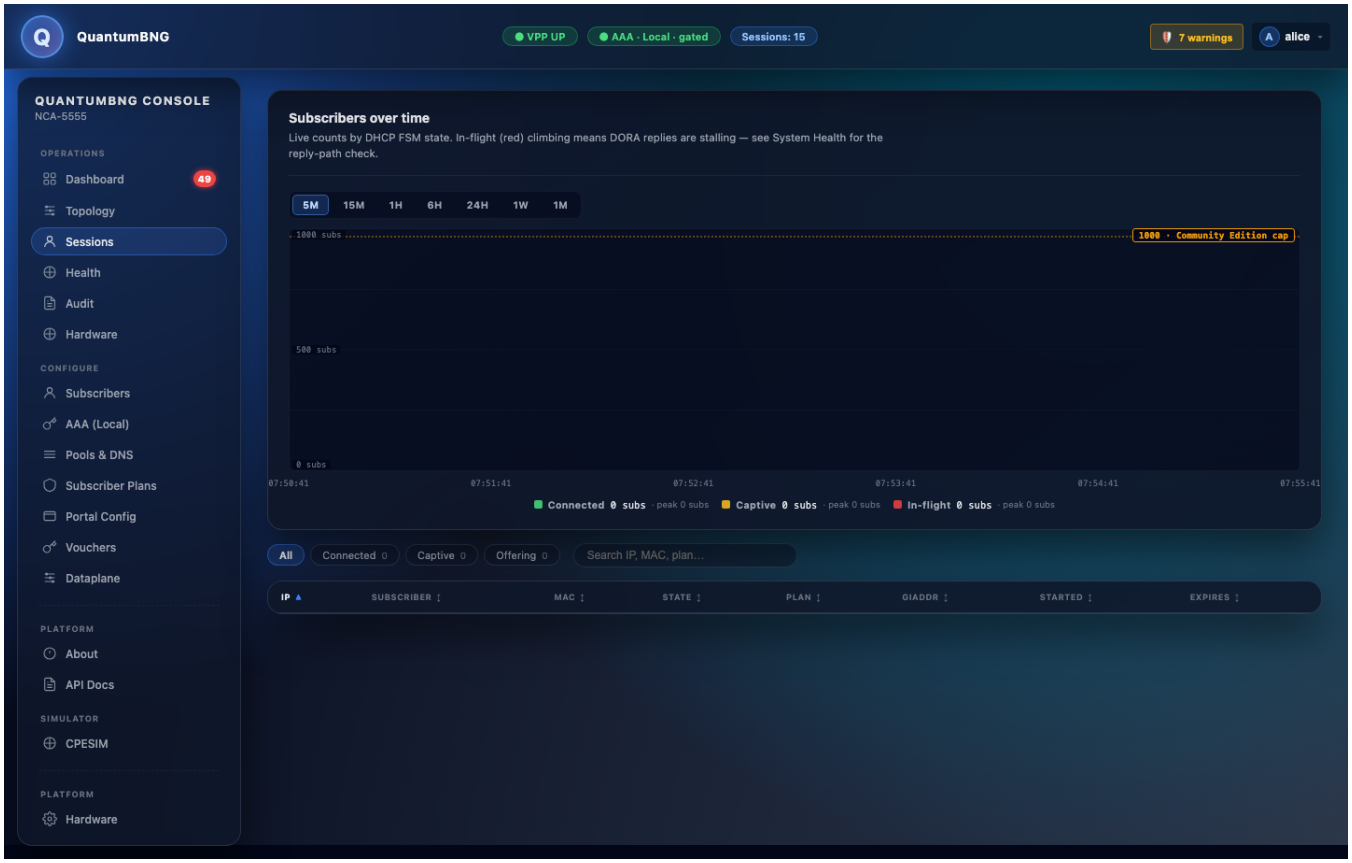



Green dots = healthy. Amber = warning (e.g., access interface `down` because no cable). Red = broken. Hovers on each element give you IP, MAC, driver, throughput.

Two tabs: **Topology** — network connectivity + per-element status (the view above) — and **Network** — bandwidth measurements at key points in the system (edge, uplink, per-interface throughput).

## Sessions

Every current subscriber session. Filter by state (Connected / Captive / Offering / All), search by IP / MAC / plan / giaddr.

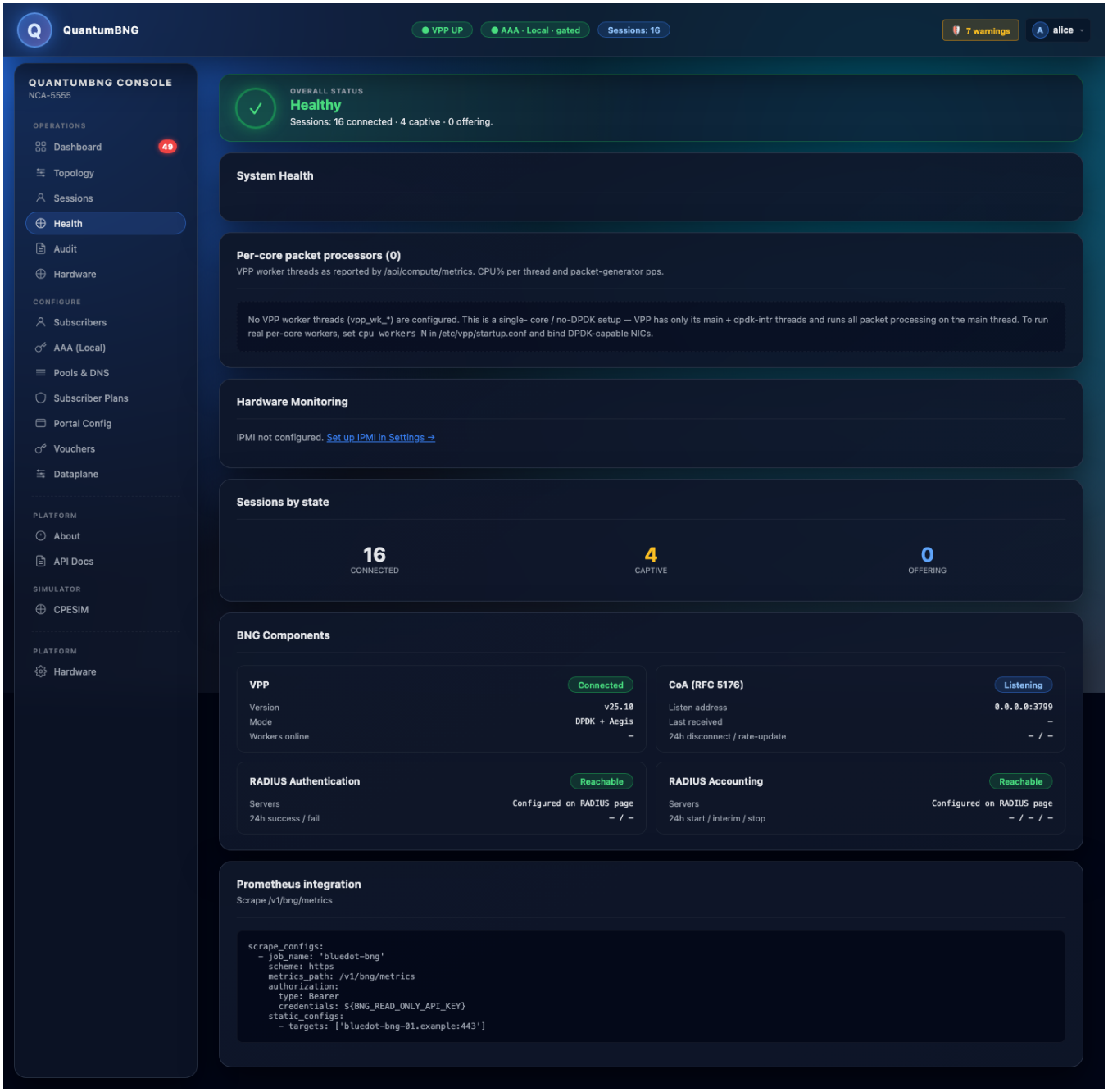



The "Subscribers over time" chart at the top shows connected + captive + in-flight over your chosen range. Persistent in-flight (red) with low connected typically means the DHCP reply path is stalled — see the Health page's reply-path check.

Click any session row to open the **Session Drawer** (right-side panel): live per-session traffic sparkline, session events (DORA, plan changes, disconnects), operator actions (disconnect, re-rate, move to captive).

## Health

Subsystem-by-subsystem diagnostic page. Every check has a green/amber/red pill, a description of what the check verifies, and a "why this matters" note.

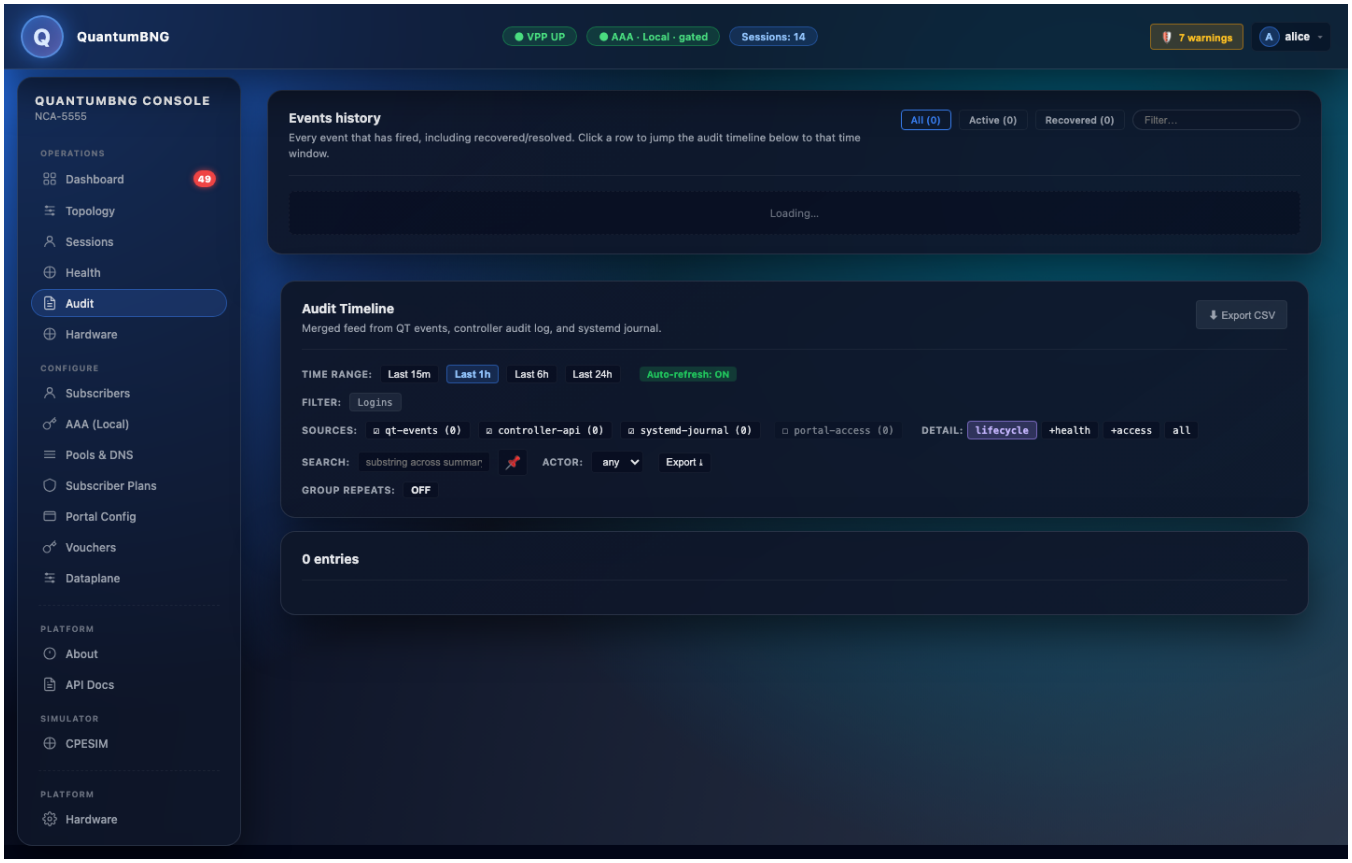



Checks include: TLS cert expiry, controller ↔ vpp-bridge connection, punt socket health, reply-path stall detector (see the memory note about `tx_pps < rx_pps × 0.5` under load), snapshot store size, audit shipper backlog, AAA provider reachability.

Two sub-tabs: **Health** (checks) and **Workers** (VPP worker CPU utilization + per-worker packet counts — helpful to see if your `corelist-workers` sizing matches your traffic load).

## Audit

Every operator action and every controller-observed event, correlated across three sources: QT audit log, controller API log, systemd journal.



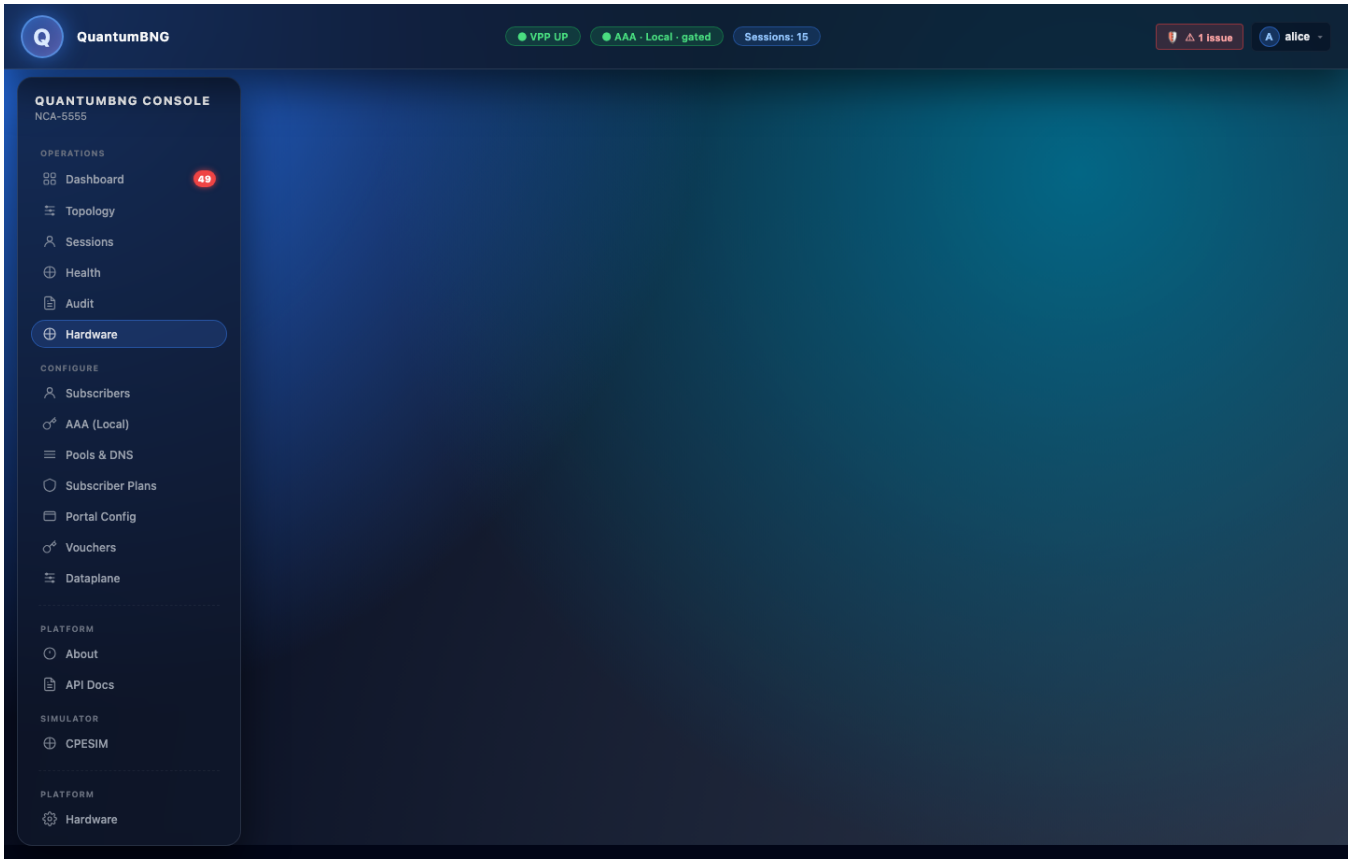

The timeline defaults to "live tail" — click **Return to live** if you scroll back. Each row includes:

- Timestamp + source (QT / Controller / Journal)
- Actor (username, API key ID, or `system`)
- Event kind + one-line description
- Rev-ID chip (linkable back to the source log line)

Use the date+time filters top-right to scope. Click **Verbose journal** to include noisy systemd events (default off).

## Hardware / Compute

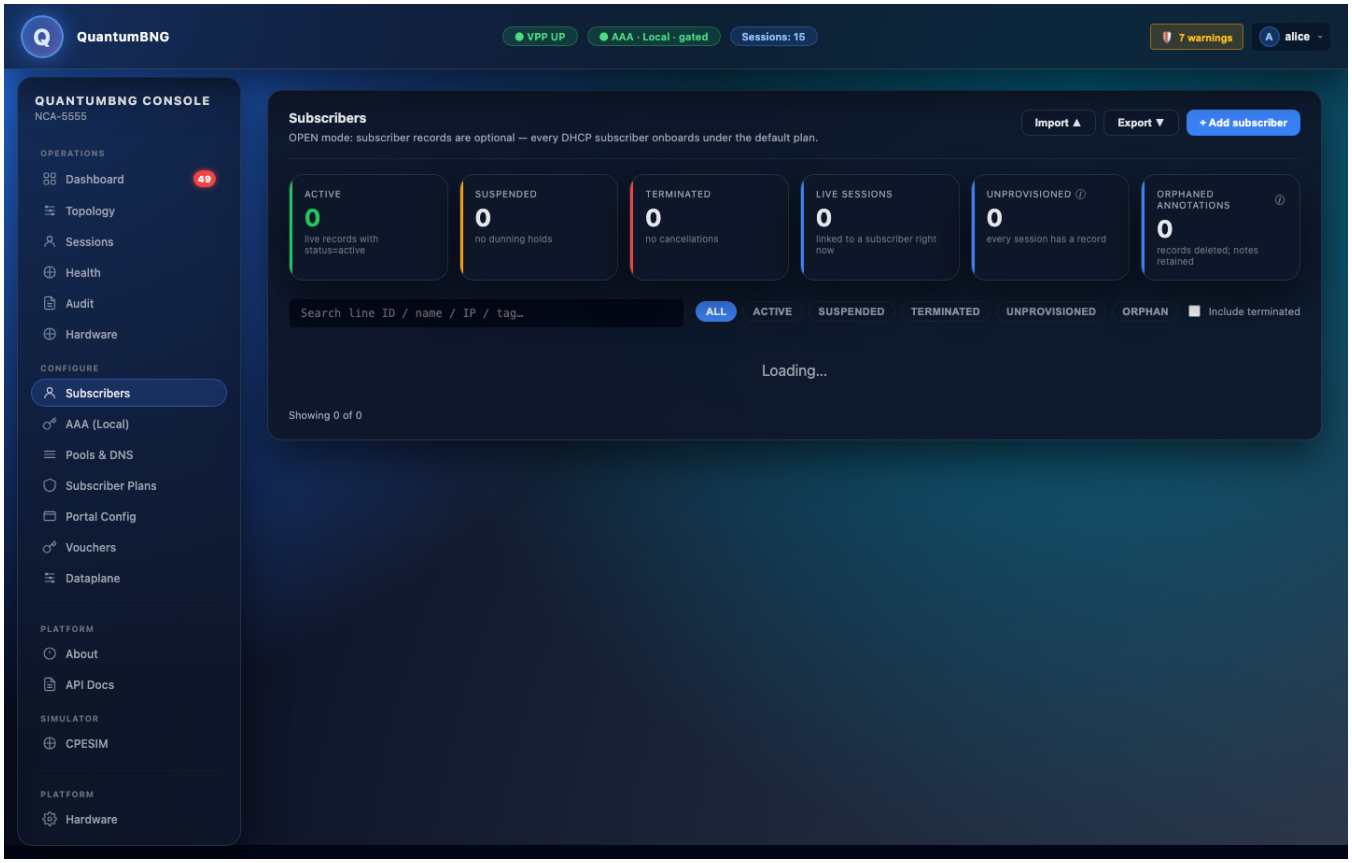
Hardware inventory (NICs, CPU, mem, disk) plus VPP CPU/worker mapping.




Use this page to sanity-check your box config before opening a support ticket: it shows exactly what VPP thinks it has ( `corelist-workers` , hugepages, buffer allocations, per-worker queue placements) alongside what the kernel thinks it has (isolcpus, NUMA topology, IOMMU groups).

## Subscribers

The provisioned-subscriber list (AAA source of truth). This is the roster of who's allowed to onboard; **it's not the same as the Sessions list** (which is who's currently online).



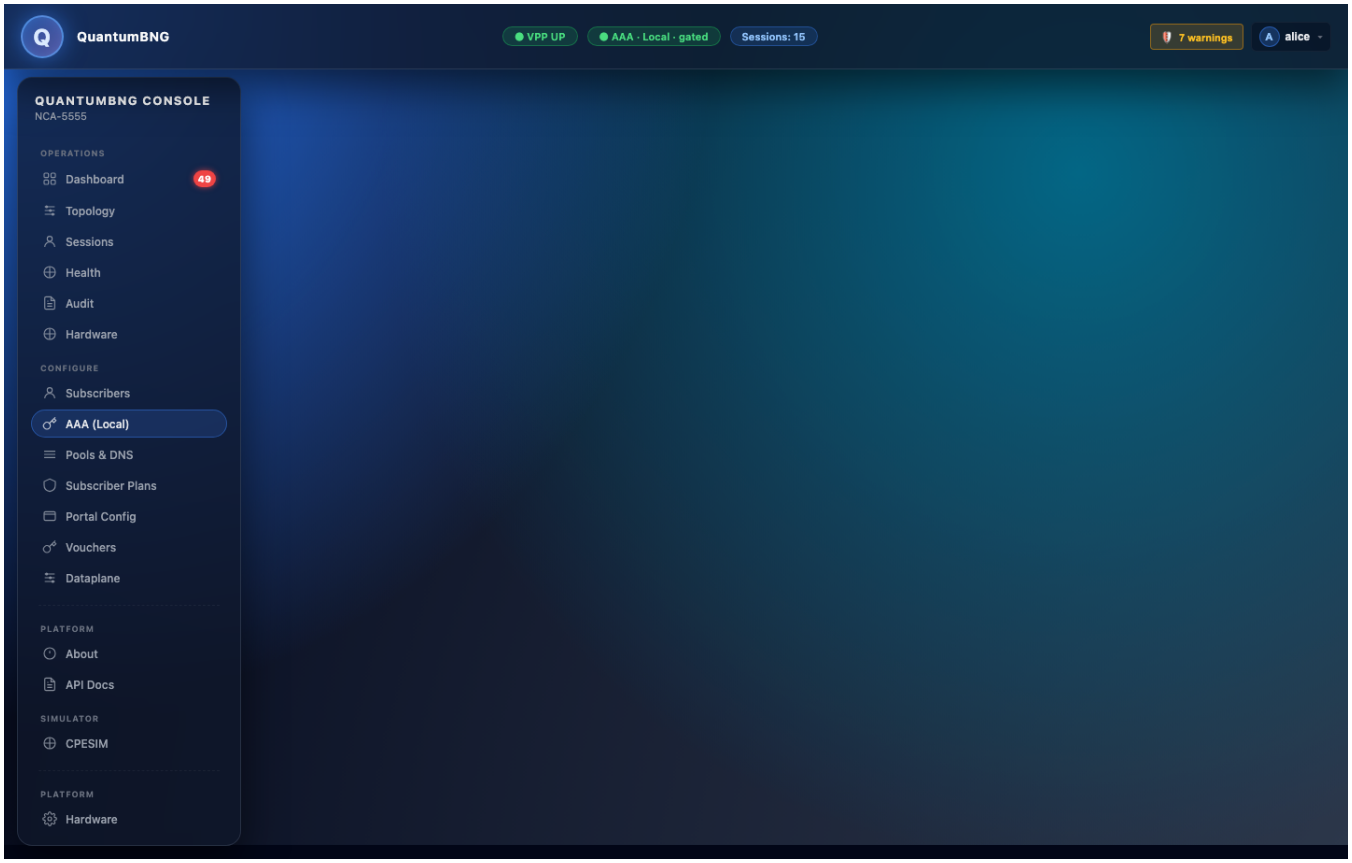

Columns: line identity (DHCP Option 82 circuit-id in hex), plan, status (active / suspended / terminated), lease-time overrides.

**Add subscriber** button top-right → single-form editor. For bulk import, use the Upload button and a CSV.

## AAA (Local)

The local-AAA provider config. Two modes:

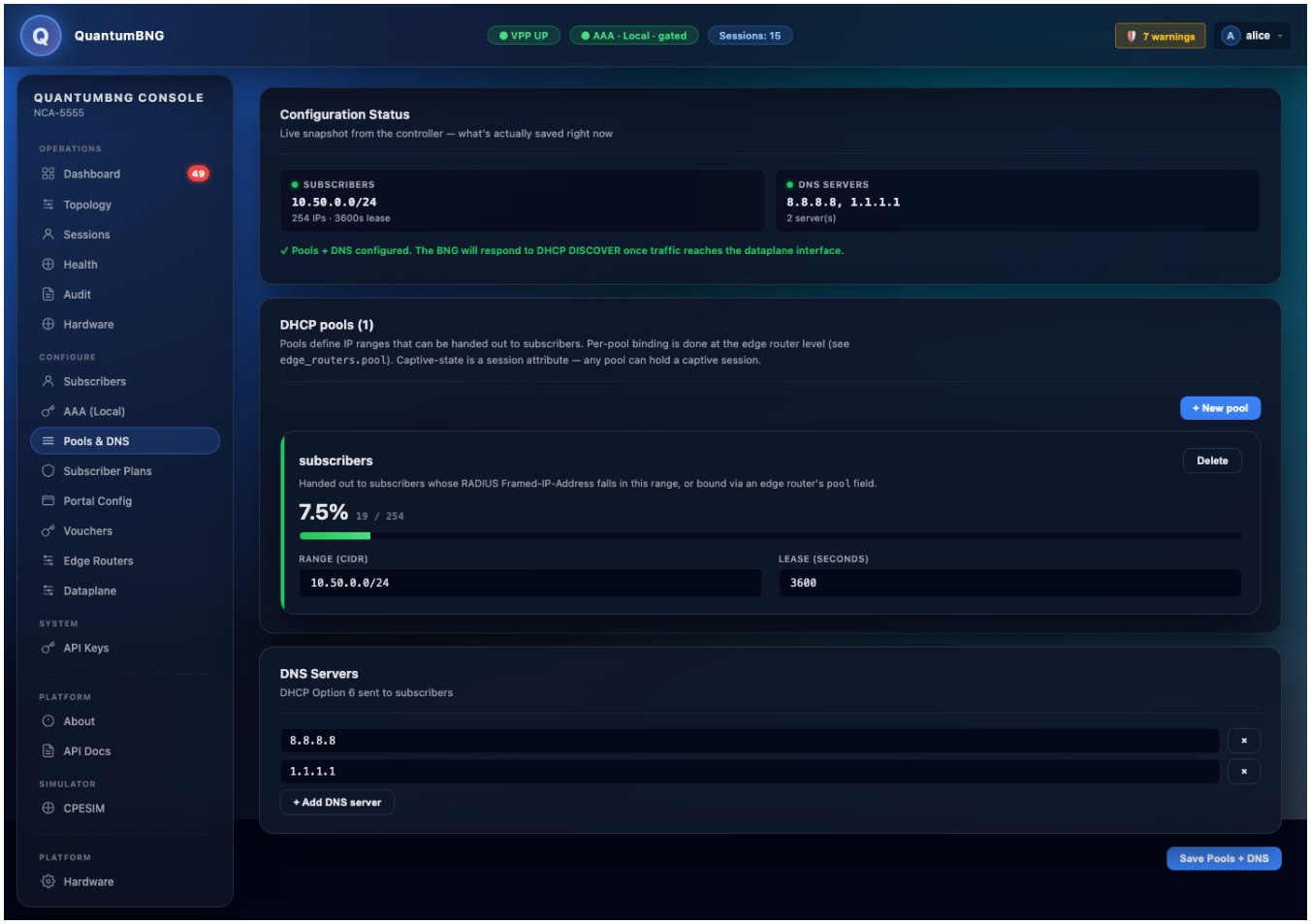
- **Open** — every DHCP DISCOVER is accepted, default plan assigned. Fine for lab / demo / small deployments where every connected device is trusted.
- **Gated** — only provisioned lines (see Subscribers) are accepted at plan. Unlisted lines get the `unknown` disposition (currently `captive` → portal, or `reject` → NAK).




Change with care — flipping from Open to Gated on a running system silently kicks unprovisioned CPEs to captive.

## Pools & DNS

The DHCP pools. Each pool has a name, a CIDR range, a lease time, and one or more DNS resolvers.

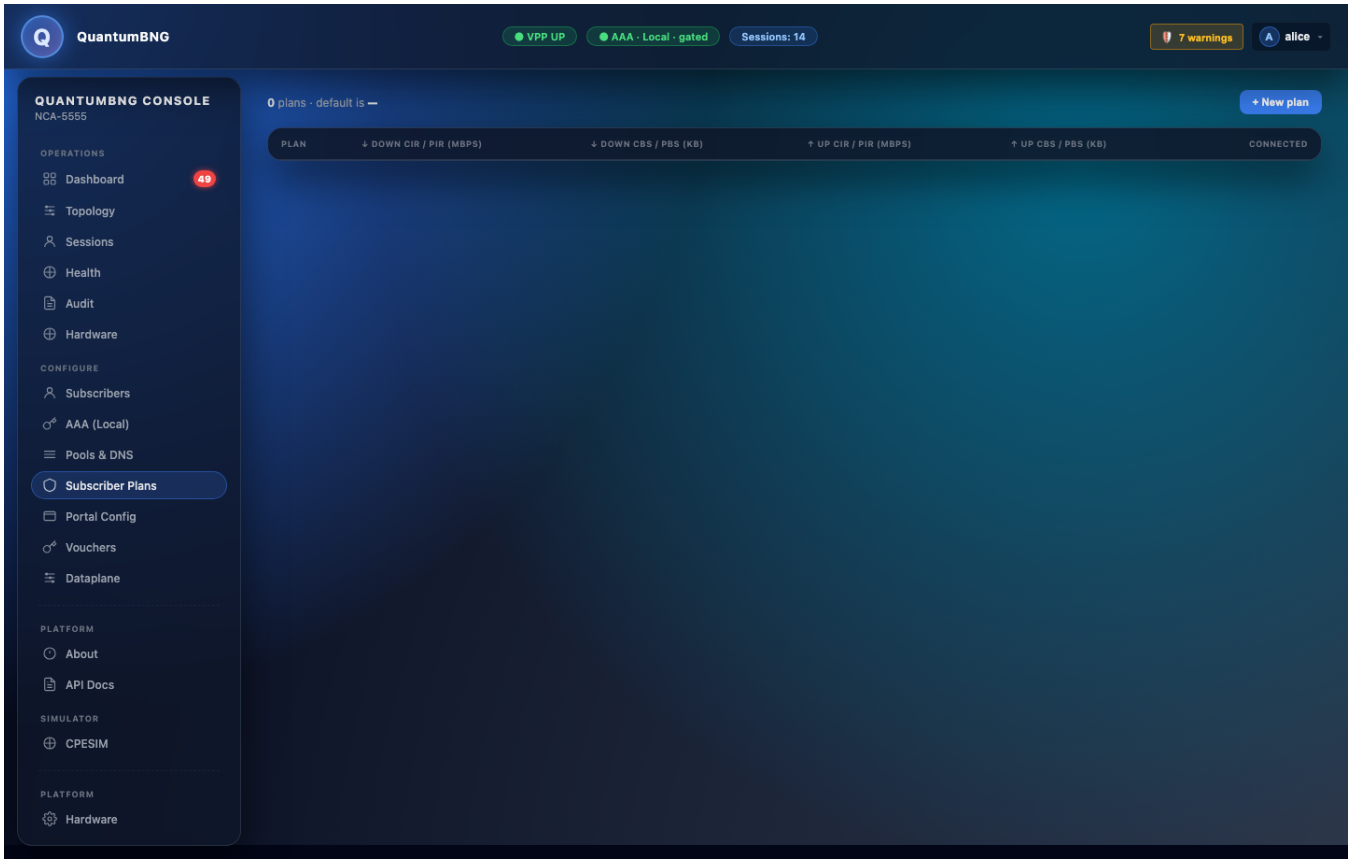



**Default pool** must exist — the setup wizard creates it. Add more pools if you need per-plan or per-geography allocation.

Pool utilization is shown as a horizontal bar with color-coded thresholds (amber at 80%, red at 95%). Alloc-failure counter shows how many DISCOVERs got NAK'd because the pool was exhausted.

## Subscriber Plans

Rate plans — each defines up_cir_kbps, up_pir_kbps, dn_cir_kbps, dn_pir_kbps plus optional session/idle/interim timers.



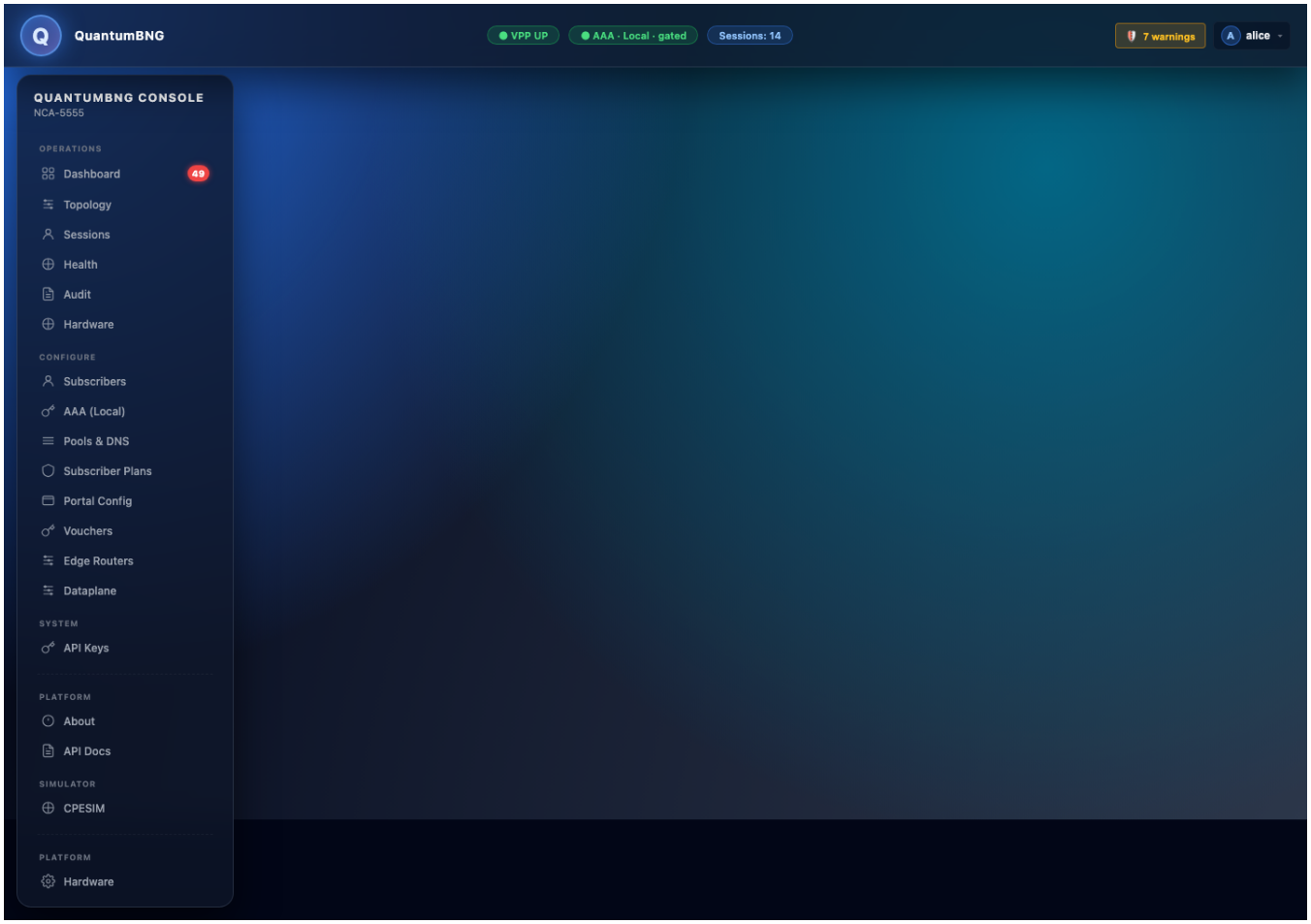

**CIR** = Committed Information Rate (guaranteed minimum, packets colored green). **PIR** = Peak Information Rate (burst ceiling, packets between CIR and PIR colored yellow). Packets above PIR are dropped (red).

`*_bps` fields in the API are BYTES per second. Multiply by 8 for bits/s (the webui shows Mbps).

Changes to a plan take effect on the next subscriber onboard OR when you click **Re-rate active sessions** to push the change immediately.

## Portal Config

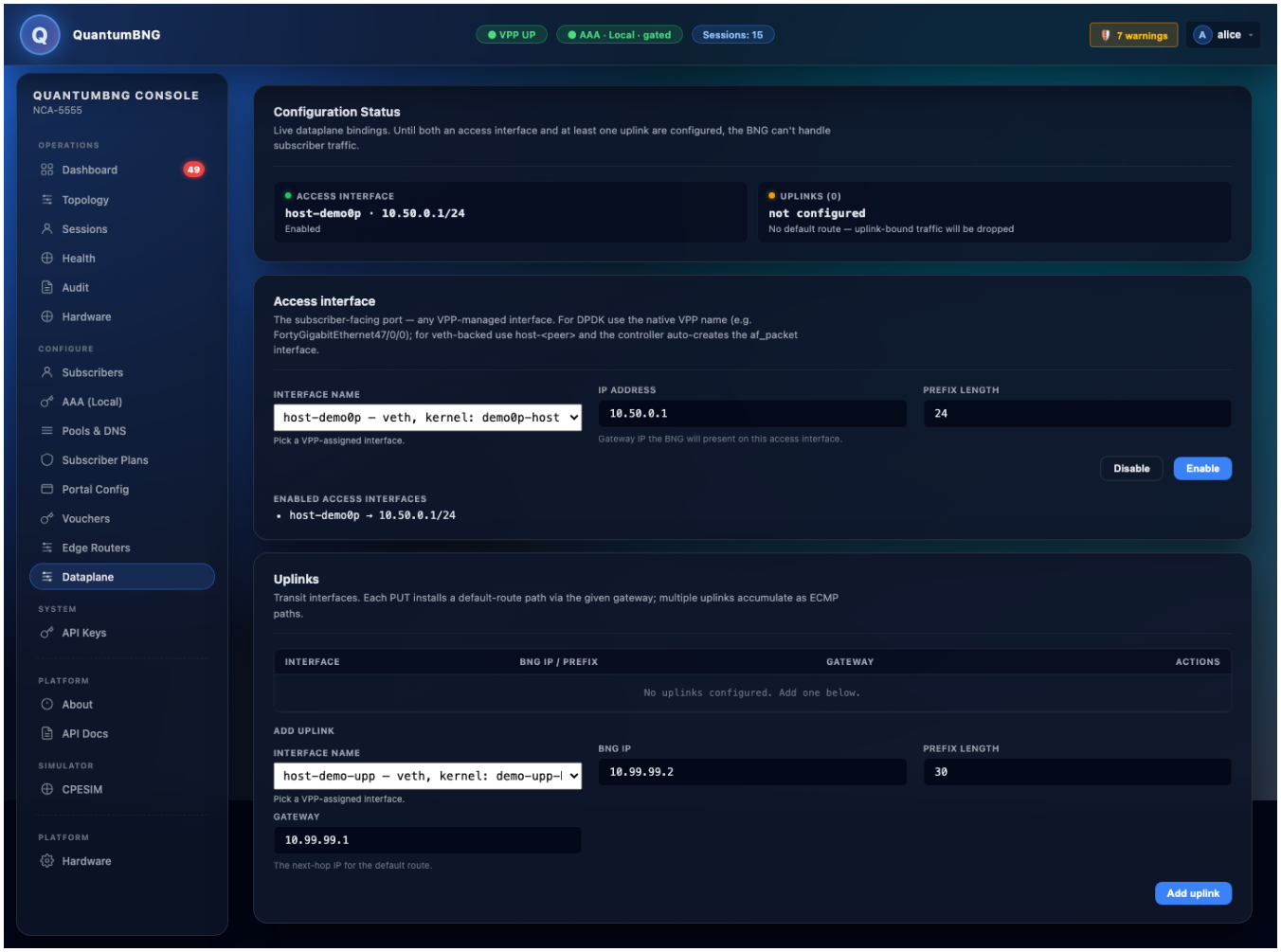
Captive portal setup — the portal_ip that the BNG hands to unprovisioned subscribers, the portal page's branding, and the vouchers page (if you use voucher-based auth instead of pure username/password).




If `portal_ip` is unset, unprovisioned DHCP DISCOVERs get silently dropped in gated mode. You'll see this in the controller log as `captive required but no captive portal IP configured, dropping`.

## Dataplane

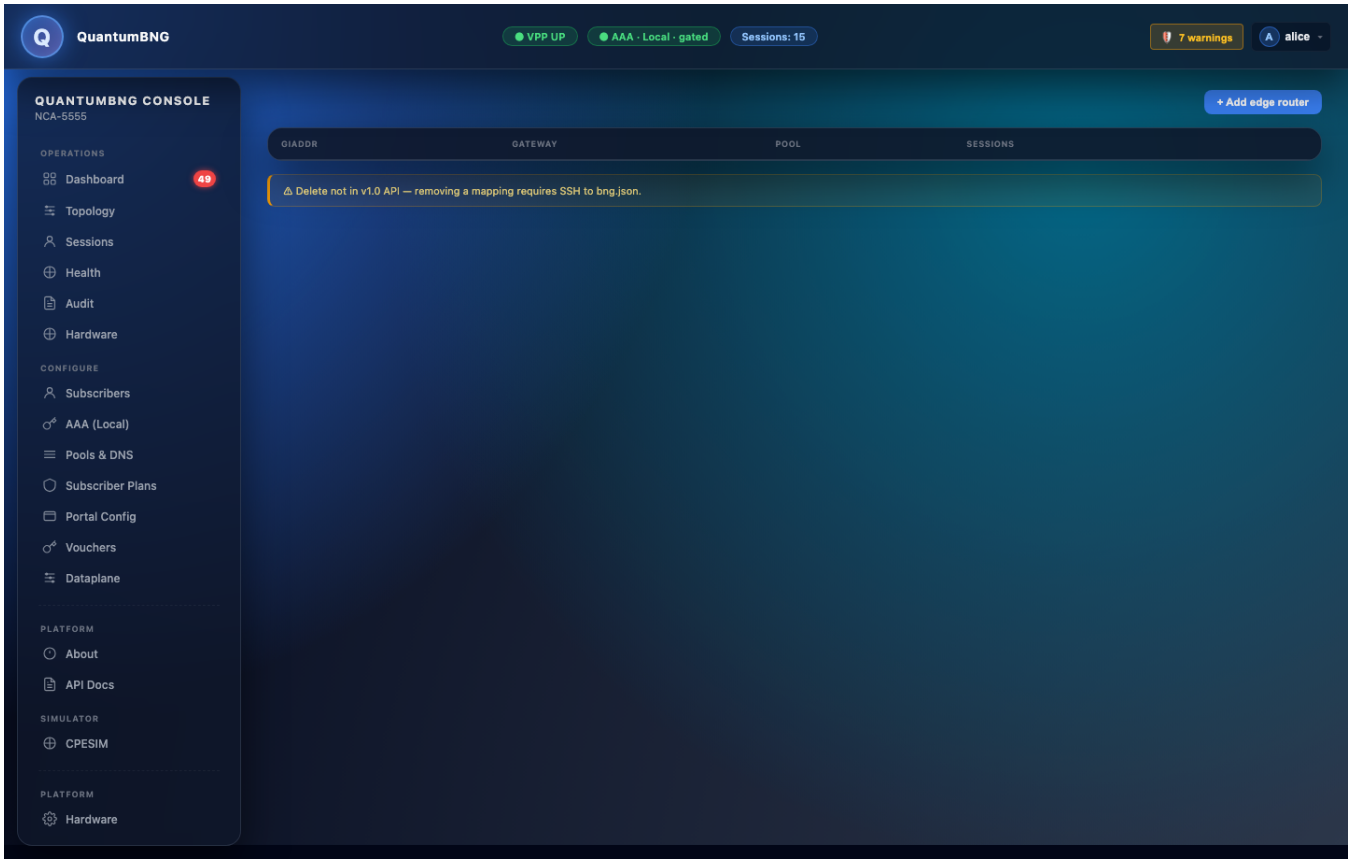
VPP-level knobs — interface state, RX/TX queue counts, RSS, worker placement, hugepage size, IOMMU groups.




Most operators never touch this page — the wizard's defaults are correct for most single-NIC boxes. Edit if you're doing custom NUMA pinning, split-NIC access/uplink topologies, or dpdk driver overrides (e.g. `vlan-strip`).

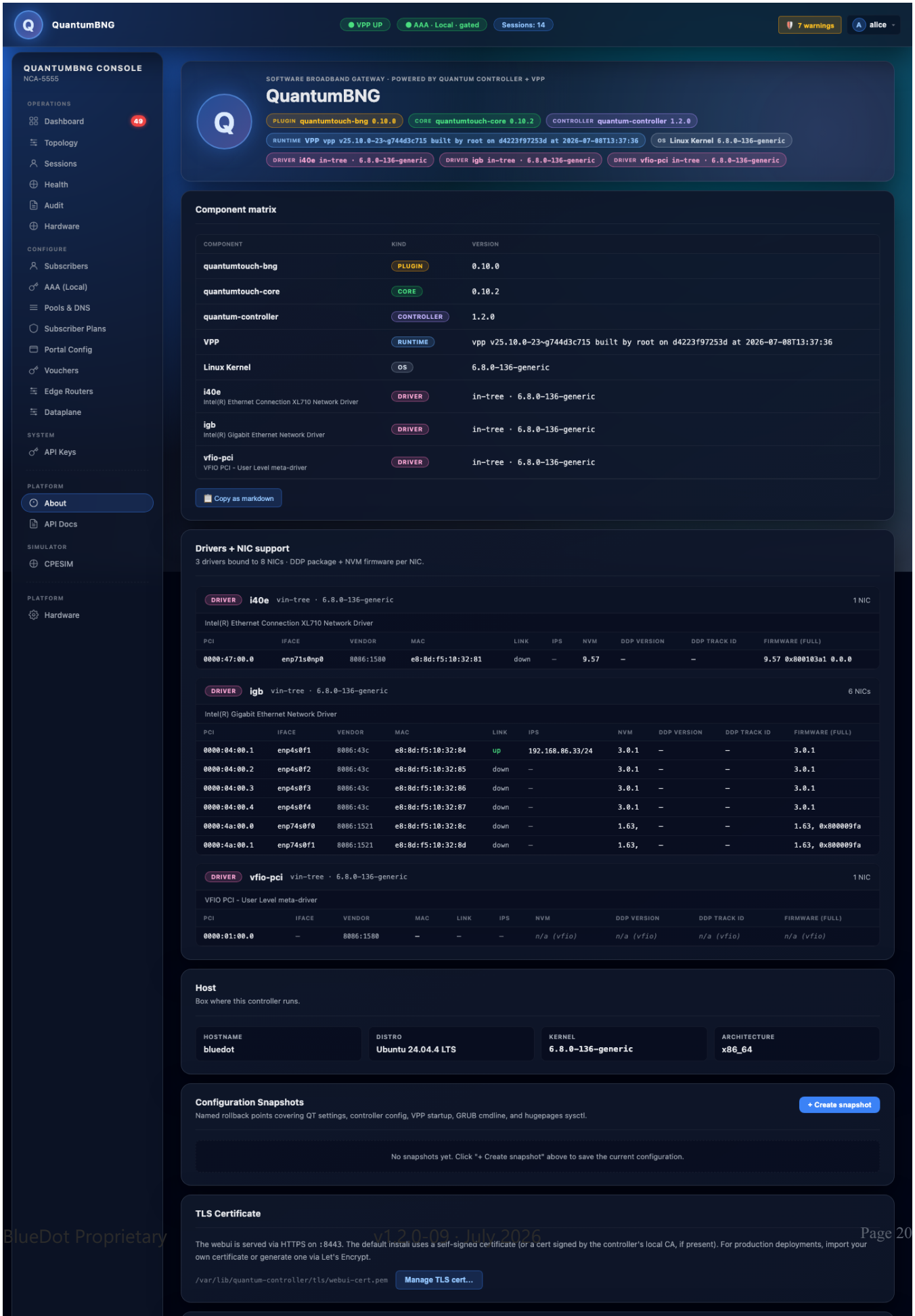
## Edge Routers

For deployments where the BNG faces multiple edge routers (e.g., separate business/residential upstream), list them here with their public IPs and next-hop configs. The topology page uses this list to draw the WAN-side of the map.




## About + Toybox

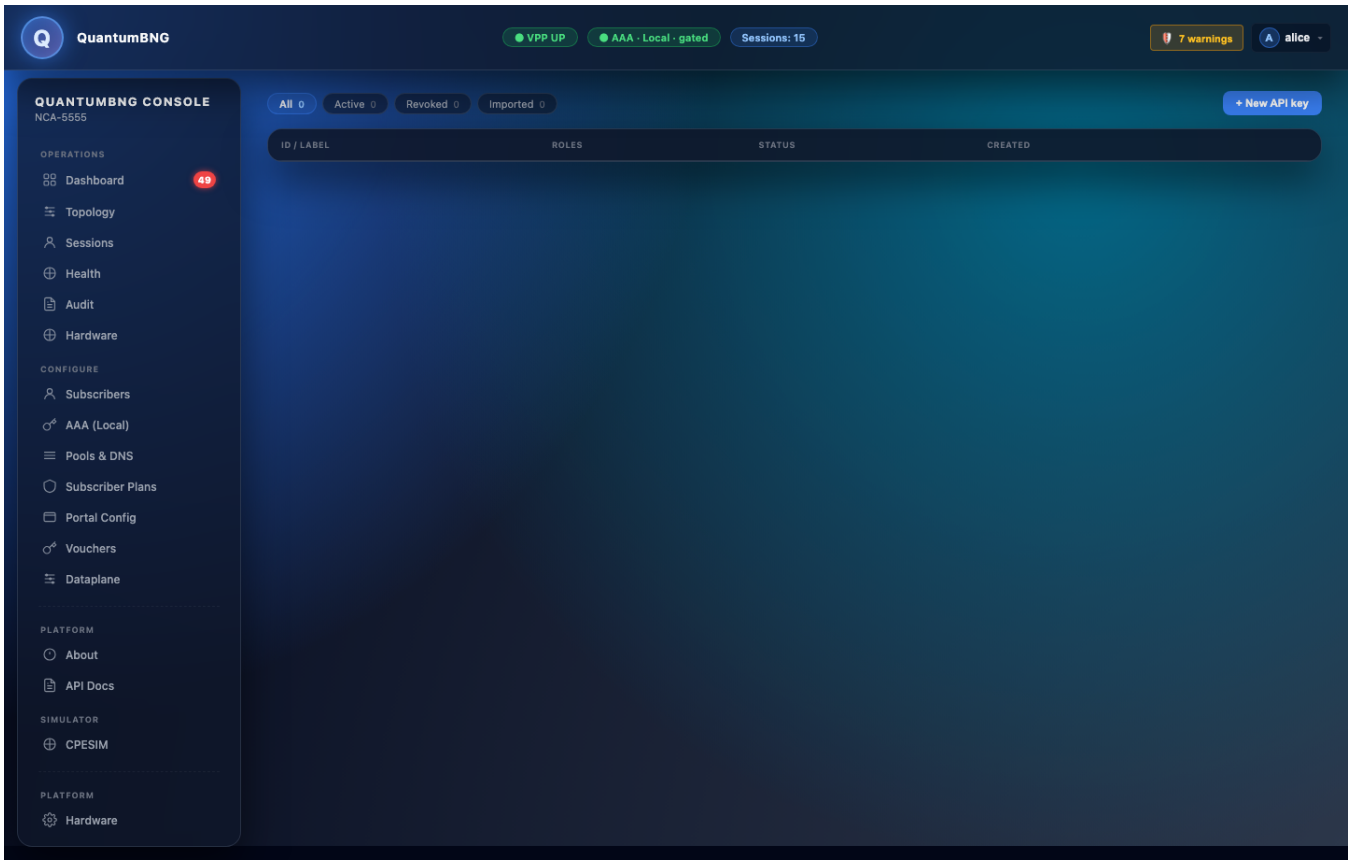
Version info + the Toybox plugin registry. Toybox is where operators install optional add-on modules — currently just CPESIM (the built-in subscriber simulator).


QuantumBNG
VPP UP
AAA · Local · gated
Sessions: 14
7 warnings
alice
QUANTUMBNG CONSOLE
NCA-5555
OPERATIONS
Dashboard
49
Topology
Sessions
Health
Audit
Hardware
CONFIGURE
Subscribers
AAA (Local)
Pools & DNS
Subscriber Plans
Portal Config
Vouchers
Edge Routers
Dataplane
SYSTEM
API Keys
PLATFORM
About
API Docs
SIMULATOR
CPESIM
PLATFORM
Hardware
SOFTWARE BROADBAND GATEWAY · POWERED BY QUANTUM CONTROLLER + VPP
QuantumBNG
PLUGIN quantumtouch-bng 0.10.0
CORE quantumtouch-core 0.10.2
CONTROLLER quantum-controller 1.2.0
RUNTIME VPP vpp v25.10.0-23~g744d3c715 built by root on d4223f97253d at 2026-07-08T13:37:36
OS Linux Kernel 6.8.0-136-generic
DRIVER i40e in-tree · 6.8.0-136-generic
DRIVER igb in-tree · 6.8.0-136-generic
DRIVER vfio-pci in-tree · 6.8.0-136-generic
Component matrix
COMPONENT KIND VERSION
quantumtouch-bng PLUGIN 0.10.0
quantumtouch-core CORE 0.10.2
quantum-controller CONTROLLER 1.2.0
VPP RUNTIME vpp v25.10.0-23~g744d3c715 built by root on d4223f97253d at 2026-07-08T13:37:36
Linux Kernel OS 6.8.0-136-generic
i40e DRIVER in-tree · 6.8.0-136-generic
Intel(R) Ethernet Connection XL710 Network Driver
igb DRIVER in-tree · 6.8.0-136-generic
Intel(R) Gigabit Ethernet Network Driver
vfio-pci DRIVER in-tree · 6.8.0-136-generic
VFIO PCI - User Level meta-driver
Copy as markdown
Drivers + NIC support
3 drivers bound to 8 NICs · DDP package + NVM firmware per NIC.
DRIVER i40e vin-tree · 6.8.0-136-generic 1 NIC
Intel(R) Ethernet Connection XL710 Network Driver
PCI IFACE VENDOR MAC LINK IPS NVM DDP VERSION DDP TRACK ID FIRMWARE (FULL)
0000:47:00.0 enp71s0np0 8086:1580 e8:8d:f5:10:32:81 down – 9.57 – – 9.57 0x800103a1 0.0.0
DRIVER igb vin-tree · 6.8.0-136-generic 6 NICs
Intel(R) Gigabit Ethernet Network Driver
PCI IFACE VENDOR MAC LINK IPS NVM DDP VERSION DDP TRACK ID FIRMWARE (FULL)
0000:04:00.1 enp4s0f1 8086:43c e8:8d:f5:10:32:84 up 192.168.86.33/24 3.0.1 – – 3.0.1
0000:04:00.2 enp4s0f2 8086:43c e8:8d:f5:10:32:85 down – 3.0.1 – – 3.0.1
0000:04:00.3 enp4s0f3 8086:43c e8:8d:f5:10:32:86 down – 3.0.1 – – 3.0.1
0000:04:00.4 enp4s0f4 8086:43c e8:8d:f5:10:32:87 down – 3.0.1 – – 3.0.1
0000:4a:00.0 enp74s0f0 8086:1521 e8:8d:f5:10:32:8c down – 1.63, – – 1.63, 0x800009fa
0000:4a:00.1 enp74s0f1 8086:1521 e8:8d:f5:10:32:8d down – 1.63, – – 1.63, 0x800009fa
DRIVER vfio-pci vin-tree · 6.8.0-136-generic 1 NIC
VFIO PCI - User Level meta-driver
PCI IFACE VENDOR MAC LINK IPS NVM DDP VERSION DDP TRACK ID FIRMWARE (FULL)
0000:01:00.0 – 8086:1580 – – – n/a (vfio) n/a (vfio) n/a (vfio) n/a (vfio)
Host
Box where this controller runs.
HOSTNAME bluedot
DISTRO Ubuntu 24.04.4 LTS
KERNEL 6.8.0-136-generic
ARCHITECTURE x86_64
Configuration Snapshots
Named rollback points covering QT settings, controller config, VPP startup, GRUB cmdline, and hugepages sysctl.
+ Create snapshot
No snapshots yet. Click "+ Create snapshot" above to save the current configuration.
TLS Certificate
The webui is served via HTTPS on :8443. The default install uses a self-signed certificate (or a cert signed by the controller's local CA, if present). For production deployments, import your own certificate or generate one via Let's Encrypt.
/var/lib/quantum-controller/tls/webui-cert.pem
Manage TLS cert...

Each plugin row shows: install status, installed version, install/remove button. **Install from URL** lets you install a beta/hotfix build without waiting for a full BNG release.

## API Keys

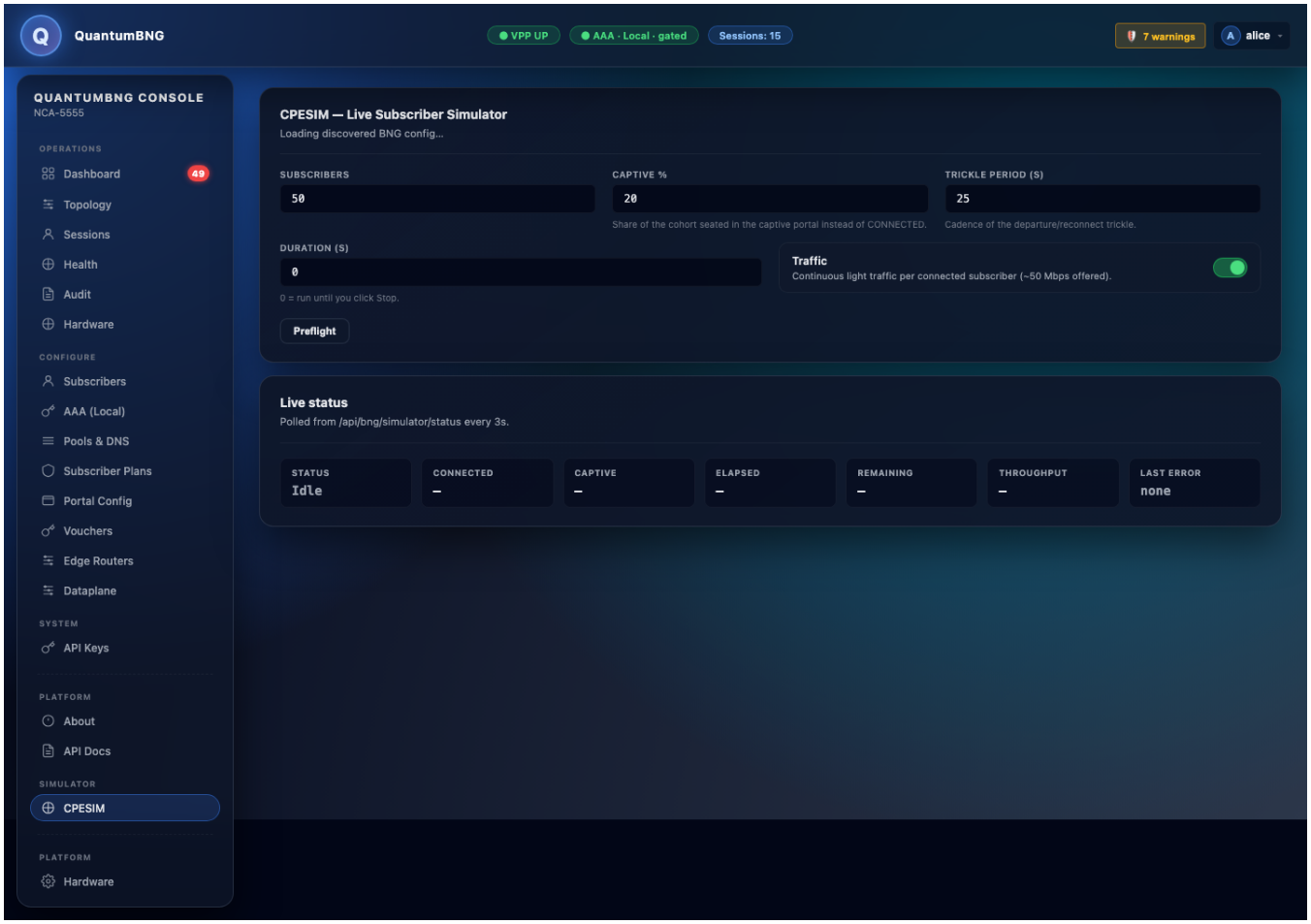
The webui's key store. Mint per-operator keys (recommended over sharing the bootstrap admin key), scope them to roles ( `read_only` , `read_write` , `admin_only` , `metrics_scraper` ), set expiry.




The `metrics_scraper` role is scoped to `/metrics` only and is what Prometheus uses. Rotate with `sudo /opt/bng-deploy/bin/qt-scrape-token-rotate` .

## CPESIM

The subscriber simulator plugin's control page. Only visible if you installed CPESIM via Toybox.




**Start** — spawn N simulated subscribers doing real DHCP + AAA + HTTP video traffic through your BNG. **Stop** — clean teardown. **Reset simulator** (admin-only) — recovery button that clears wedged state and restarts the whole CPESIM engine.

Configuration: subscribers count, captive fraction, duration. Sensible defaults are baked in — click Start and go.

---

# Common operator tasks

## Add a new rate plan

1. Subscriber Plans → **Add plan**
2. Name it, set the four `*_bps` fields (BYTES/s — multiply your Mbps target by 125000)
3. Save. New onboards will pick it up; existing sessions keep their current plan until you either change their individual subscriber record or re-rate.

## Move a subscriber to a different plan

1. Subscribers → find the row → click to edit

2. Change **Plan** dropdown → Save
3. In Sessions, find their active session → drawer → **Re-rate now** (avoids waiting until their next reconnect)

### Suspend a subscriber

1. Subscribers → find the row → set **Status** to `suspended`
2. In Sessions, find the active session → drawer → **Disconnect**. The next time they reconnect, gated AAA will send them to captive.

### Add a new DHCP pool

1. Pools & DNS → **Add pool**
2. Name, CIDR, lease time (default 3600s is fine), one or more DNS resolvers
3. Save. If you want subscribers to prefer this pool, edit the plan(s) to reference it.

### Rotate the metrics scrape token

```
sudo /opt/bng-deploy/bin/qt-scrape-token-rotate
```

Writes the new token to `/opt/quantumtouch/etc/scrape-token` and reloads the Prometheus container. Point your monitoring scrape at the new value.

### Enable HTTPS with a real cert (Let's Encrypt)

See `letsencrypt-on-bng.md` — walks through the ACME HTTP-01 challenge flow and cert renewal automation.

---

## Backup and restore

Backup — writes an encrypted bundle of the user store, API keys, session store, and system config to a file:

```
sudo /opt/bng-deploy/bin/qt-auth-backup.sh /path/to/backup.tar.gz.enc
```

You'll be prompted for a passphrase. Store both the file and the passphrase somewhere durable.

Restore on a fresh install:

```
sudo /opt/bng-deploy/bin/qt-auth-restore.sh /path/to/backup.tar.gz.enc
```

The restore replaces `/opt/bng-deploy/data/{users,api_keys,sessions}.json` and restarts bng-deploy. It does NOT restore subscribers/plans/pools — those live in the controller's `controller.db` and roll over from install to install; snapshot via **About** → **Snapshot** in the webui.

# Key rotation

| Key type | Command | When to rotate |
|---|---|---|
| Bootstrap admin API key | `sudo /opt/bng-deploy/bin/rotate-controller-key.sh` | Immediately after first-run wizard |
| Metrics scrape token | `sudo /opt/bng-deploy/bin/qt-scrape-token-rotate` | Quarterly, or after staff turnover |
| Per-operator API key | Delete + re-mint from **API Keys** page | Staff turnover; suspected leak |
| User password | `sudo /opt/bng-deploy/bin/reset-user-password.sh <username>` | User forgot / suspected compromise |

Full recovery from complete key loss is documented in `bootstrap-recovery.md`.

# Troubleshooting

## Header shows `VPP ?` for > 10s

The controller can't talk to vpp-bridge. Usually a punt-socket or vpp-bridge health issue:

```
sudo systemctl status vpp vpp-bridge quantum-controller
sudo vppctl show errors | grep -i punt      # if "Socket TX" errors, vpp-bridge lost the socket
```

Restart in the right order (vpp first, then vpp-bridge, then controller):

```
sudo systemctl restart vpp
sleep 3
sudo systemctl restart vpp-bridge
sleep 2
sudo systemctl restart quantum-controller
```

## DHCP DISCOVERs are being dropped

Controller journal will tell you why:

```
sudo journalctl -u quantum-controller --since '5 minutes ago' | grep onDiscover
```

Common causes:

| Message | Cause | Fix |
|---|---|---|
| `captive required but no captive portal IP configured, dropping` | Gated AAA + no `portal_ip` set | Portal Config → set portal_ip |
| `pool 'default' exhausted` | DHCP pool full | Pools & DNS → add capacity |
| `unknown line identity, unknown=reject` | Gated AAA, unlisted line, policy set to reject | Provision the line or flip `unknown` to `captive` |
| `session cap reached` | 1000-session Community Edition cap | Contact BlueDot for a larger license |

## Sessions header shows N but Sessions page table is empty

The header polls one endpoint; the page polls a different one. Usually a transient auth race just after login — hard-refresh the page (Cmd+Shift+R / Ctrl+Shift+R). If it persists across refreshes, check that the session cookie is still valid: **User menu (top-right)** → **Profile** → **Session info**.

## CPESIM demo won't start — `pool gateway 10.50.0.1/24 is already held by host-demo0p`

The controller has a stale `access_interfaces` binding from a previous CPESIM run that didn't teardown cleanly. Reset:

```
sudo /usr/local/bin/reset-cpesim
```

This clears the stale record + restarts the whole CPESIM engine in the right order (vpp → vpp-bridge → controller → bng-demo).

## `AAA (LOCAL) DOWN — provider unreachable` on the dashboard

The AAA local-provider file isn't readable. Usually a permissions issue after a manual API key mint:

```
sudo ls -la /var/lib/quantum-controller/api_keys.json
# should be owned by quantum-controller:quantum-controller, mode 0600
sudo chown quantum-controller:quantum-controller /var/lib/quantum-controller/api_keys.json
sudo systemctl restart quantum-controller
```

### Long-running API calls (e.g., snapshot restore) return HTTP 500

Gunicorn's per-worker timeout killed the request. The installer drops in a 180s override at `/etc/systemd/system/bng-deploy.service.d/10-timeout.conf` — check it's still there. If you're doing something that takes longer than 180s (e.g., importing 5000 subscribers), bump the override:

```
sudo sed -i 's/--timeout 180/--timeout 300/' /etc/systemd/system/bng-deploy.service.d/10-timeout.conf
sudo systemctl daemon-reload
sudo systemctl restart bng-deploy
```

---

## File locations + service commands

| Path | What lives there |
|---|---|
| `/opt/bng-deploy/` | The webui shim (Flask app, venv, static assets, /bin/ scripts) |
| `/opt/bng-deploy/data/` | User store, API keys, session store, settings, sqlite audit log |
| `/opt/bng-deploy/data/.controller_key` | The shim's own key for talking to the controller. Not for operator use. |
| `/opt/bng-deploy/data/.bootstrap_token` | The first-run setup wizard token (consumed on first use) |
| `/var/lib/quantum-controller/` | Controller state: `controller.db` (SQLite), `api_keys.json`, `audit.log`, `bng.json` |
| `/opt/quantumtouch/data/prometheus/` | Prometheus TSDB (14-day retention default) |
| `/opt/quantumtouch/etc/scrape-token` | The Prometheus scrape token |
| `/opt/bng-demo/` | CPESIM plugin install root (only if installed via Toybox) |
| `/etc/vpp/startup.conf` | VPP dataplane config — `cpu {}` block controls worker pinning |
| `/etc/systemd/system/bng-deploy.service.d/10-timeout.conf` | Gunicorn `--timeout` override installed by the wrapper |

Service commands:

```
sudo systemctl status vpp vpp-bridge quantum-controller bng-deploy quantumtouch-prometheus
sudo systemctl restart bng-deploy               # webui restart, no dataplane impact
sudo journalctl -u quantum-controller -f        # tail controller log
sudo journalctl -u bng-deploy -f                # tail webui log
sudo vppctl show interface                      # VPP interface state
sudo vppctl show errors                         # VPP node error counters
sudo vppctl show threads                        # VPP worker mapping
```