Crypta Labs

QRNG Appliance Gen 2 User Manual

1U quantum random number generator appliance for data centre and enterprise use



Product	Crypta Labs QRNG Appliance Gen 2
SKU	QRNG-APPLIANCE-2
Document	Customer User Manual
Revision	October 2026 (software 0.6.5)
Software	See appliance `/status` page (Code Ver)
Support	support@cryptalabs.com
Website	https://cryptalabs.com

© Crypta Labs Limited. All rights reserved.

Contents

1. Important notices, warranty & intellectual property
2. Package contents
3. Physical description & specifications
4. Rack mounting & cabling
5. First power-on & console login
6. Initial configuration (required)
7. Verify the appliance
8. Using quantum entropy (use cases)
9. Sample client scripts
10. API reference
11. TLS certificates
12. Day-to-day operations
13. Troubleshooting
14. Support

> **Audience**
> This manual is for customers and system integrators receiving a factory-built appliance. It does *not* describe factory manufacturing procedures.

1. Important notices, warranty & intellectual property

1.1 Copyright

© Crypta Labs Limited. All rights reserved. This document and the software, firmware, configuration, and design of the QRNG Appliance Gen 2 (SKU **QRNG-APPLIANCE-2**) are the intellectual property of Crypta Labs Limited ("Crypta Labs").

1.2 Intellectual property & reverse engineering

The appliance software, configuration scripts, factory tooling, and related materials are licensed for use solely as delivered on the Crypta Labs QRNG Appliance Gen 2. Any attempt to:

- duplicate, copy, reverse engineer, decompile, or redistribute the appliance software or configuration;
- open, modify, or tamper with the chassis or internal assemblies except under explicit written instruction from Crypta Labs;
- extract and reuse Crypta Labs software with third-party or substitute hardware without a valid Crypta Labs licence;

is strictly prohibited and **voids the product warranty**. Unauthorised use may also constitute infringement of Crypta Labs' intellectual property rights.

1.3 Warranty disclaimer

Except as expressly stated in a separate written warranty agreement between you and Crypta Labs, the appliance and software are provided "as is". To the maximum extent permitted by applicable law, Crypta Labs disclaims all warranties, express or implied, including merchantability, fitness for a particular purpose, and non-infringement.

1.4 Limitation of liability

Crypta Labs shall not be liable for any indirect, incidental, special, consequential, or punitive damages, or for any loss of profits, revenue, data, goodwill, or business opportunity, arising from use of (or inability to use) the appliance, even if advised of the possibility of such damages. Crypta Labs' total liability shall not exceed the amount paid for the specific unit giving rise to the claim, except where liability cannot be limited by law.

1.5 Safety

- Install only in a suitable 19-inch rack with adequate ventilation.
- Use the supplied power cable (or an equivalent rated cable for your region).
- Do not open the chassis unless instructed in writing by Crypta Labs support.

- Disconnect power before attaching or removing rack ears if the unit is already powered.

2. Package contents

Your shipment should include:

- Crypta Labs QRNG Appliance Gen 2 (1U chassis)
- EU power cable
- Rack mount ears (pair)
- Screws to attach the ears to the chassis

> **Not included**
>
> Rack screws (cage nuts / rail screws) for your rack are *not* supplied. Use hardware appropriate to your rack manufacturer.

If any item is missing or damaged, contact **support@cryptalabs.com** before installation.

3. Physical description & specifications



Figure 1 — Crypta Labs QRNG Appliance Gen 2

SKU	QRNG-APPLIANCE-2
Form factor	1U rackmount appliance
Chassis (W × H × D)	440 mm × 48 mm × 257 mm
Width with ears	480 mm
Entropy source	Crypta Labs Dragonfly PCIe QRNG
Raw entropy rate	Up to 280 Mb/s
Entropy pool	32 MiB base (dynamic scaling up to 64 MiB)
Max API request	10 MiB per request
Network	Multiple Gigabit Ethernet ports (customer configures eth0)
Management	Physical console + `doas qrng-config` (optional SSH via menu)
Data plane	HTTPS (TLS) for web UI and API only
OS	Hardened Alpine Linux
Compliance notes	Hardware designed to NIST SP 800-90B criteria; hybrid PQC TLS aligned with FIPS 203 (ML-KEM)

4. Rack mounting & cabling

4.1 Attach the rack ears

1. Place the appliance on a clean, stable surface.
2. Align each rack ear with the front side mounting holes on the chassis.
3. Secure using the supplied ear-mounting screws. Do not overtighten.

4.2 Install in the rack

1. Select a 1U location with free airflow front-to-back.
2. Support the unit while aligning the ears with your rack posts.
3. Fasten the ears to the rack with **your own rack screws** (not supplied).
4. Ensure the chassis is level and fully seated.

4.3 Cabling

1. **Power** — connect the supplied EU power cable to the IEC inlet and a suitable mains outlet or PDU.
2. **Network** — connect a network cable to the primary management port you will configure as `eth0` (or the interface name shown by the OS).
3. **Console** — attach a display and USB keyboard (or use the platform's console/IPMI/iKVM if present) for first-time configuration.

> **Important**
> The appliance does *not* ship with a customer network pre-configured. You must set addressing for eth0 (or your chosen interface) using the console configuration tool after first login.



Figure 2 — Appliance overview

5. First power-on & console login

1. Power on the appliance.
2. Wait for the OS to complete boot (typically under a minute).
3. Log in at the physical console as:

Username	`admin`
Default password	`ApplianceUser`

> **Change the default password immediately**
> On first login, change the `admin` password (for example with `passwd`). Do not leave the factory default password on a production network. Crypta Labs may enforce a password change on first configuration in a future software update.

5.1 Privileged commands

All privileged operations are performed with `doas` (not `sudo`). When prompted for a password, enter the **admin** user password.

```
doas qrng-config
```

5.2 Access model after factory lockdown

- **Configuration** — physical console + `doas qrng-config` (recommended for first setup).
- **SSH** — **off by default**. Enable or disable from the qrng-config menu; the firewall (port 22) is updated at the same time.
- **Entropy API and status web UI** — HTTPS on port 443.

6. Initial configuration (required)

Network addressing is not pre-set. Until you configure an interface, the appliance may be unreachable from the LAN. Use the interactive tool:

```
doas qrng-config
```

6.1 Menu overview

1	Show current config
2	Set hostname
3	Configure network interface (e.g. eth0)
4	Set DNS
5	Set entropy pool size (bytes)
6	SSH access — enable/disable (firewall updated in lockstep)
7	Timezone / locale (e.g. America/New_York)
8	Apply & restart QRNG service
9	Reboot (graceful)
10	Power off (graceful) — prefer before cutting mains power
11	Update appliance (signed USB / optional HTTPS download)
12	Exit

Before removing power at the switch or PDU, use option **10 (Power off)** from the console (`doas qrng-config`). A chassis sticker may remind operators of this.

6.2 Recommended first-run sequence

1. **Set hostname** (option 2) to your site naming convention.
2. **Configure network** (option 3):
   - Select the interface (commonly `eth0`).
   - Enter IPv4 address (e.g. `192.168.10.50`) and netmask (e.g. `255.255.255.0` or prefix `24`). Optional gateway.
   - You may still type `192.168.10.50/24` in the IP field; the tool splits it. Persistent config uses classic `address` + `netmask` (BusyBox 1.37-friendly).
   - To **remove** an address from a NIC (e.g. clear eth3): select that interface and enter `none`, `clear`, `remove`, or `0.0.0.0`.
3. **Set DNS** (option 4) if you require name resolution (e.g. `1.1.1.1` and `8.8.8.8`).
4. **Set timezone** (option 7) for local log timestamps (e.g. `America/Argentina/Buenos_Aires`, `America/New_York`, or the Canada Pacific preset for Vancouver).
5. **SSH** (option 6) only if you need remote admin — default is off; enabling opens port 22 at the same time.
6. **Apply & restart** (option 8) after changes that affect the service.
7. Optionally **Set pool size** (option 5) if you need a non-default base pool (default is 32 MiB = 33554432 bytes).

> **Network change caution**
> Changing the management IP can interrupt remote sessions. Prefer console access for the first network configuration. Ensure gateway/routes are correct before leaving the site.

6.3 Multi-NIC appliances

Units with multiple Ethernet ports may list several interfaces. Configure only the port you have cabled for management/API access first. Additional interfaces can be configured later using the same tool.

6.4 Reboot after first config

```
doas reboot
```

After reboot, confirm the unit returns on the configured address and services start automatically.

7. Verify the appliance

7.1 From the console

```
# Service status
doas rc-service caddy status
doas rc-service qrng-server status

# Local HTTPS health (self-signed — use -k with curl)
curl -k https://127.0.0.1/
curl -k https://127.0.0.1/health
curl -k https://127.0.0.1/status
curl -k "https://127.0.0.1/api/v1/random?bytes=64" | xxd | head
```

7.2 From a client on the network

Replace `APPLIANCE-IP` with the address you configured:

```
curl -k https://APPLIANCE-IP/
curl -k https://APPLIANCE-IP/health
curl -k https://APPLIANCE-IP/status
curl -k "https://APPLIANCE-IP/api/v1/random?bytes=1024" --output sample.bin
ls -l sample.bin
```

> **Self-signed certificate**
>
> Factory units present a self-signed TLS certificate. Browsers will warn; `curl` requires `-k` (or equivalent) unless you install a trusted certificate later.

7.3 Status dashboard

Open `https://APPLIANCE-IP/` in a browser (accept the certificate warning if self-signed). That landing menu links to Status, Health, Metrics, and the on-box manual. Open **Status** (`/status`) and confirm Dragonfly PCIe shows **Connected**, FPGA version, pool fill, and uptime.

8. Using quantum entropy (use cases)

The appliance continuously fills an in-memory entropy pool from the Dragonfly PCIe QRNG. Clients request bytes over HTTPS; there is no rate limiting on the entropy endpoint.

8.1 Typical use cases

- **Key generation** — seed HSMs, TLS key generation, or application-level keys with high-quality entropy.
- **Cryptographic libraries** — feed OS or application CSPRNG seed material.
- **Simulations & Monte Carlo** — large random batches for scientific or financial workloads.
- **Security appliances** — central entropy source for clusters (via your network controls).

8.2 Entropy pool behaviour

- **Base size:** 32 MiB by default (minimum retained).
- **Dynamic growth:** under load the pool may grow up to 64 MiB to reduce latency.
- **Freshness:** new quantum data is continuously appended; oldest data is discarded when over size.
- **Fast start:** a short high-speed burst refills the pool after service restart.

8.3 Network security note

The entropy API does not require application-level authentication. Protect access with network controls (VLAN, firewall, private management network). Only port **443** is intended for remote access on production-sealed units.

9. Sample client scripts

The following examples are provided with the product documentation and test suite. Run them from a client workstation (not necessarily from the appliance).

9.1 Simple Python client

Fetch quantum random bytes and optionally save to a file:

```
#!/usr/bin/env python3
import argparse
import requests
from urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

# IMPORTANT: Use the real appliance IP or a hostname that resolves.
# Unresolvable names (e.g. some .local names) can add multi-second delays per
request.

def get_random(server, bytes=4096, output=None):
    url = f"https://{server}/api/v1/random"
    r = requests.get(url, params={"bytes": bytes}, timeout=30, verify=False)
    r.raise_for_status()
    data = r.content
    print(f"Received {len(data)} quantum random bytes")
    if output:
        with open(output, "wb") as f:
            f.write(data)
        print(f"Saved to {output}")
    else:
        print("First 32 bytes:", data[:32].hex())
    return data

if __name__ == "__main__":
    p = argparse.ArgumentParser()
    p.add_argument("--server", required=True, help="Appliance IP or hostname")
    p.add_argument("--bytes", type=int, default=4096)
    p.add_argument("-o", "--output")
    args = p.parse_args()
    get_random(args.server, args.bytes, args.output)
```

Example:

```
python3 qrng-client.py --server 192.168.10.50 --bytes 65536 -o entropy.bin
```

9.2 Curl one-liners

```
# 8 KiB to a file
curl -k -s "https://APPLIANCE-IP/api/v1/random?bytes=8192" -o random.bin

# 1 MiB
curl -k -s "https://APPLIANCE-IP/api/v1/random?bytes=1048576" -o entropy-1m.bin

# Health check (JSON)
curl -k -s https://APPLIANCE-IP/health
```

9.3 Soak / repeatability tester

For validation, latency statistics, and CSV logging across multiple sizes and repeats, use the advanced tester (`qrng-test.py`):

```
python3 qrng-test.py --server APPLIANCE-IP --repeats 50 --csv soak.csv

# Custom sizes (bytes)
python3 qrng-test.py --server APPLIANCE-IP --repeats 20 \
  --sizes 64,1024,4096,1048576 --csv soak.csv
```

- `--server` is required (no hard-coded IP).
- Self-signed TLS is accepted by default for testing.
- Summary output includes overall and per-size latency statistics (including high percentiles where enabled).

10. API reference

10.1 GET /api/v1/random

Method / path	`GET /api/v1/random`
Query parameter	`bytes=N` — number of random bytes to return
Valid range	1 ≤ N ≤ 10 485 760 (10 MiB). Default if omitted: 4096
Success response	`200 OK`, `Content-Type: application/octet-stream`, body = exactly N bytes
Invalid N	`400` with a clear error message (no silent clamping)
Rate limiting	None
Authentication	None (protect with network policy)

10.2 Operational endpoints (root path)

`/`	Landing menu (Status, Health, Metrics, Manual, sample entropy)
`/status`	HTML dashboard: software version, pool fill, Dragonfly status, network, top clients
`/health`	JSON health (for load balancers / monitoring)
`/metrics`	Prometheus metrics (pool fill, reads, bytes served)
`/docs/manual.html`	On-box HTML reference (if enabled on your unit)

11. TLS certificates

Production units terminate HTTPS on port 443 (Caddy) and reverse-proxy to the local entropy service. Factory default is a **self-signed ECDSA P-256** certificate.

- **Air-gapped / high-security sites** often keep the self-signed certificate and pin the fingerprint in clients.
- **Public or enterprise PKI** deployments may replace certificates under Crypta Labs guidance (or using documented customer tooling where provided).

> **Certificate changes are high risk**
>
> Incorrect certificate replacement can lock out HTTPS access. Prefer console access and contact support@cryptalabs.com if you need assistance with corporate CA or ACME certificates.

Where supported, hybrid post-quantum TLS key exchange (X25519MLKEM768 with classical fallback) may be enabled on the appliance TLS stack for modern clients.

12. Day-to-day operations

12.1 Configuration changes

```
doas qrng-config
```

Use this for hostname, interfaces, DNS, pool size, SSH on/off (with firewall), timezone/locale, signed software update, and graceful reboot/power off. Configuration changes are audited.

12.2 Software update (signed pack)

Crypta Labs may supply a software update as two files on a USB stick (FAT32): `qrng-update-<version>.tar.gz` and `qrng-update-<version>.tar.gz.sig`. Plug the stick into the appliance, then from the console:

```
doas qrng-config
# 11) Update appliance → 1) From USB stick
# Type YES to apply after the signature checks out
```

The appliance verifies a Crypta Labs Ed25519 signature *before* any files are replaced. A USB stick or website copy that was altered, or that was not signed with the Crypta Labs factory key, is refused. Network, TLS certificates, firewall, and SSH settings are not changed by an update. A backup is kept under `/var/lib/qrng/backups/`.

If the unit has outbound internet, menu 11 also offers a download from Crypta Labs. HTTPS is used, but the signature is still required — a compromised website cannot install unsigned software.

> **Do not apply unsigned files**
>
> Never copy a tarball onto the appliance and extract it by hand. Only menu 11 (or Crypta Labs support with the matching `.sig`) is the supported path.

12.3 Graceful reboot and power off

Prefer a clean shutdown over switching the mains off while the OS is running. From the physical console (or SSH if enabled):

```
doas qrng-config
#  9) Reboot (graceful)
# 10) Power off (graceful) — type YES to confirm
```

OpenRC stops services in order, then reboots or powers off the chassis. Use the front/rear power switch or PDU only when the unit is already halted, or in an emergency.

12.4 Service control

```
doas rc-service caddy status
doas rc-service qrng-server status
doas rc-service caddy restart
doas rc-service qrng-server restart
doas reboot
doas poweroff
```

12.5 Logs

QRNG service	`/var/log/qrng-server.log`
Config audit	`/var/log/qrng-audit.log`
Caddy	`/var/log/caddy/` (access and service logs)

12.6 Access summary

Console	Primary path for configuration (`admin` + `doas`)
HTTPS :443	API, status, health, metrics
SSH	Off by default; enable via `doas qrng-config` (opens port 22 with firewall)

13. Troubleshooting

Cannot reach the appliance on the network	Use the physical console. Re-run `doas qrng-config` and verify interface, IP/CIDR, link lights, and cabling. Confirm you are on the correct NIC.
After power loss or hard power-off	Wait for a full boot (2–3 minutes). Check `https://APPLIANCE-IP/health`. The journaled filesystem normally recovers automatically; services start via OpenRC. If it does not come up: physical console → `doas rc-status default`, `doas rc-service qrng-server status`, `doas rc-service caddy status`, `curl -k https://127.0.0.1/health`, `dmesg | tail -40`. If the root filesystem is read-only or disk errors appear, contact support (recovery may need an install USB and offline filesystem check — do not force-write a failing disk). Prefer `doas qrng-config` → Power off before planned power removal. A UPS is recommended on unstable power.
Browser certificate warning	Expected with the factory self-signed certificate. Proceed only if you trust the network path, or install a trusted certificate with support guidance.
`curl` TLS errors	Add `-k` for self-signed testing, or configure proper trust store for production clients.
HTTP 400 on `/api/v1/random`	Check `bytes` is between 1 and 10 MiB.
Slow client requests	Use a real IP or properly resolving hostname. Avoid unresolvable names that cause DNS timeouts.
Services not running after reboot	`doas rc-service caddy status` and `doas rc-service qrng-server status`; review logs under `/var/log/`.
Status shows Dragonfly disconnected	Contact Crypta Labs support. Do not open the chassis unless instructed.

14. Support

For production support contact:

Email	support@cryptalabs.com
Web	https://cryptalabs.com

Please include:

- SKU / product: QRNG-APPLIANCE-2 (Gen 2)
- Appliance hostname and software version from `/status`
- Description of the issue and approximate time of occurrence
- Relevant log excerpts (redact sensitive network details if required)

© Crypta Labs Limited. All rights reserved.
Unauthorised duplication of software or opening of the chassis without Crypta Labs instruction voids warranty. Crypta Labs is not liable for losses arising from use of this product except as required by law.