

Pointing Grafana at the Box

Operations Note — Prometheus Datasource

How to add QuantumTouch BNG's metrics as a Prometheus datasource in Grafana: mint a metrics-only API key, add the datasource, authenticate, deal with the box's TLS certificate, and understand what the key can see and how long the box retains metrics.

Document Type	BlueDot Operations Note
Component	QuantumTouch BNG — Prometheus endpoint
Audience	Operators & Monitoring Engineers
See Also	<i>QuantumBNG Grafana Dashboard Pack</i>
Classification	BlueDot Proprietary
Date	October 2026

Contents

- 1. Mint a key 3
- 2. Add the datasource 3
- 3. Authenticate 3
- 4. TLS 3
- 5. What this key can and cannot see 4
- 6. Retention 4

How to add QuantumTouch BNG's metrics as a Prometheus datasource in Grafana.

1. Mint a key

In the BNG web UI, go to **System** → **API Keys** and create a new key using the "**Grafana / metrics only**" preset. Selecting it sets the role to `read_only` and restricts the key to `/api/bng/prometheus/*` — it cannot be widened by mistake.

Click **Create + reveal once** and copy the token immediately. It is shown exactly once; only its SHA-256 hash is stored, so if you lose it there is no recovery — you must rotate or create a new key.

By default the preset gives the key a 365-day expiry (editable or clearable before you create it); once it passes, the dashboards querying through it stop returning data until you rotate the key or mint a new one.

2. Add the datasource

In Grafana, add a **Prometheus** datasource with URL:

```
https://<box>:8443/api/bng/prometheus
```

Paste only this base path. Grafana appends its own suffixes (e.g. `/api/v1/query_range`) when it queries.

3. Authenticate

Under **Custom HTTP Headers**, add one header:

```
Authorization: Bearer <token>
```

using the token from step 1.

4. TLS

By default the box's HTTPS certificate is not signed by a public certificate authority — it's either self-signed or signed by the box's own private CA — so Grafana will refuse the connection until you address that. You have two options.

(If your box was installed with `QT_CUSTOMER_CERT` / `QT_CUSTOMER_KEY`, it is serving a certificate you supplied rather than the default one. Where that certificate already chains to a CA Grafana trusts, none of the guidance below applies — the connection just works, and you should not disable verification. Check with your installer if you are not sure which applies to your box.)

- **Install the box's certificate in Grafana's trust store.** This is the right choice whenever Grafana can reach the box over a routable network. With verification on, Grafana can detect a server other than the box answering on that address; without it, it cannot, and the Bearer token from step 1 is exactly what such an interposer would collect.
- **Enable "Skip TLS certificate validation."** Acceptable only on a link you trust end-to-end — for example Grafana and the box on the same isolated management network or a direct connection with no routing between them. Do not use this as the default setting on a shared or routable network.

5. What this key can and cannot see

Through this datasource, Grafana can query time-series metrics only — the same read endpoints a stock Prometheus datasource uses (instant and range queries, series/label browsing, metric metadata). It cannot see sessions, subscriber addresses, or configuration: the key's path scope confines every request to the proxy path, and anything outside the metrics read surface (including Prometheus's own config/admin endpoints) is rejected as not found.

6. Retention

The box retains 30 days of metrics or 5 GB of storage, whichever comes first. A dashboard panel that asks for a longer range (e.g. 90 days) will render a partial series for the time that's still retained, not an error.