HAMR-FORGE

FORGE OS · PUBLIC TECHNICAL WHITEPAPER

Fleet Operations & Enterprise Integration

A customer-controlled operating model for NOC monitoring, site lifecycle, identity, logging, and recovery

PUBLIC RELEASE

VALIDATED BASELINE V0.9.239 · SUPERSEDES V0.9.173 EDITION

PUBLISHED BY HAMR-FORGE, LLC · AUGUST 2026

Executive Abstract

FORGE OS presents a unified HUB and SPOKE operating model without imposing a vendor cloud. The HUB is the fleet authority; every SPOKE remains locally operable when management or external services are interrupted.

This paper describes the operational surface of the v0.9.239 baseline: site lifecycle, truthful health, fleet monitoring with the geographic Fleet Map, routing and traffic visibility, centralized policy, enterprise DNS/NTP/authentication, TLS syslog, SNMPv3, diagnostic audit collection, signed firmware, backup, and recovery.

Intended audience. NOC managers, network operations engineers, systems integrators, security operations teams, and service owners.

> **Publication boundary: v0.9.239 capability is stated as current. Future work is labeled ROADMAP — NOT INCLUDED IN v0.9.239.**

1. Operating Model

The HUB is the fleet authority for registration, trust, routing context, centrally distributed service policy, audit collection, and recovery escrow — the HUB's encrypted custody of each site's recovery credentials. Each SPOKE remains locally operable and continues path health, routing, LAN services, containment, and reconnect behavior when the management plane or external services are temporarily unavailable.

This paper describes the publicly releasable behavior of FORGE OS v0.9.239, the current validated pre-release baseline. Validation evidence cited here comes from the project's automated release gates, virtual-appliance exercises, physical hardware testing, and a completed 72-hour firmware-lock endurance soak under continuous load. The term validated does not imply a third-party certification, government approval, product-level FIPS validation, or general-availability designation.

FIGURE PLACEHOLDER

operating model — HUB fleet authority, autonomous spokes, enterprise services, monitoring and recovery relationships

Persona	Primary interface	Expected decisions
NOC administrator	HUB	Register sites, approve enrollment, configure integrations, monitor fleet, manage recovery and firmware

Persona	Primary interface	Expected decisions
Site administrator	SPOKE	Assign WAN/LAN interfaces, confirm tunnel and routes, inspect local health, coordinate maintenance
Viewer/kiosk	HUB or SPOKE	Read-only monitoring without configuration or recovery access
Security operations	SIEM/NMS plus HUB	Correlate audit, syslog, traps, identity, and recovery actions

2. Site Lifecycle

- Create the expected site name and BGP/OSPF role at the HUB, with the site's AS number where BGP is used. An unset AS is supported: a deployment running no BGP is a normal configuration, not an incomplete one.
- Assign a standby HUB if the region has one.
- Provision the SPOKE with HUB address and out-of-band CA fingerprint.
- Review the pending identity and approve it at the HUB.
- Confirm tunnel, routing adjacency, received prefixes, advertised prefixes, and intended WAN subflows.
- Confirm recovery escrow availability and run a diagnostic/audit pull.
- For retirement, revoke the tunnel identity, remove the site record, preserve required logs, and sanitize storage under customer policy.

> **A tunnel being up is not the completion criterion. Routing, path contribution, service health, escrow, and monitoring must also be verified.**

3. Truthful Health Model

The UI favors explicit status over optimistic configuration echoes. DNS performs a live lookup; NTP reports synchronization; syslog distinguishes connected, retrying, queued, and caught-up states; routing reports protocol state; firmware reports active and standby slots; audit reports chain verification.

Label	Evidence required
Configured	A valid saved configuration exists
Reachable	A live network check succeeds
Connected	An authenticated session exists

Label	Evidence required
Established / Full	The selected dynamic-routing protocol converged
Synchronized	A live protocol-specific synchronization check succeeds
Forwarding	The system observed or installed the intended forwarding state
Degraded	Service remains available but a required path or dependency is impaired
Unavailable	The live function cannot currently be used
Checking	No live result has been received yet. The interface will not report a state it cannot evidence, and does not fall back to a default.

4. Fleet Monitoring

The HUB dashboard is attention-oriented: fleet health with an explicit needs-attention count, per-WAN and tunnel throughput, recent operator-impacting activity, and system vitals. Compact health bars and an attention list replace decoration — the fastest read of the fleet is the list of sites that need a human.

The **Fleet Map** places the fleet on an offline geographic map: link lines from the HUB to each placed site, status-colored pins with per-site traffic detail, and Connected/Degraded filters that narrow a large fleet to what matters now. Map data is served entirely from signed, customer-installed offline map packs — address and place lookup work without any external mapping service, and nothing about the fleet ever leaves the appliance. Packs install per appliance, survive A/B firmware updates, and report their coverage, vintage, and content hash for provenance tracking.

The **Sites** page remains the scalable authoritative list, with per-site detail including routing state, top talkers, on-demand speed tests, and recovery access according to role.

- Use the attention count and health states to triage; use the detail pages to diagnose.
- Keep a viewer-only account for wallboard or kiosk use.
- Use SIEM/NMS as the durable cross-system history and correlation layer.
- Treat a green SPOKE as healthy whether it is attached to its home HUB or to an assigned alternate — but read which HUB is serving it before drawing conclusions about the region. A site healthy on its alternate still means its home HUB needs attention.

5. Traffic, QoS, and Multicast

Top-talkers views expose high-volume sources and destinations. QoS classes are ordered, centrally distributed, and mapped to DSCP. SPOKE shaping can use a measured or manual

bandwidth cap. This is especially important where unexpected multicast or discovery traffic can consume constrained backhaul.

- Multicast forwarding to the HUB is disabled by default.
- Enable it only where the operational application requires it.
- Use plan bandwidth as display context, then validate with measured service behavior.
- Document the business meaning of custom QoS classes; do not rely only on DSCP names.

6. Enterprise DNS and NTP

The HUB uses customer-selected upstream DNS and NTP sources and serves or distributes the resulting policy downstream. DNS health is based on live resolution. Internal zones can be exempted from public DNSSEC validation when they are outside the public signed tree. SPOKEs verify local service state and synchronization to the HUB.

> **Each HUB in a multi-HUB region requires its own customer continuity plan for DNS and NTP. A SPOKE that fails over reaches its alternate HUB for these services, so an alternate without working upstream DNS and NTP yields a site that is connected and routed but cannot resolve or synchronize. FORGE OS can carry configuration and connectivity; it cannot invent authoritative customer services during a NOC outage.**

7. Identity Integration

The HUB supports local users plus RADIUS, verified LDAP/Active Directory, and TACACS+. Directory configuration includes a server identity, trusted CA, search filter, and optional admin-group mapping. SPOKE external login is relayed through the authenticated HUB control channel while local accounts remain available for continuity.

- Use verified TLS for directory connections.
- Maintain at least one protected local administrative path.
- Map external groups to the minimum required role.
- Audit both successful and denied sensitive actions.

8. Syslog, SNMP, and Audit Collection

TLS syslog forwarding supports server-name verification, a trusted collector CA, and optional mutual TLS. The HUB distributes per-SPOKE severity policy. Disk-assisted queues retain a bounded backlog when the collector is unavailable and flush on recovery.

SNMPv3 supplies authenticated, private polling and optional traps. Scheduled diagnostic audit pulls collect secret-free support bundles per SPOKE on a configurable cadence and retention window.

Channel	Best use	Security boundary
TLS syslog	Event history, security correlation, audit durability	Customer SIEM and retention policy
SNMPv3	NMS polling and critical traps	Customer NMS credentials and availability
Diagnostic audit bundle	Point-in-time troubleshooting evidence	Secret-free archive; not a configuration or DR backup
Local logs	Immediate appliance diagnosis	Bounded local retention; root-administered host

9. Backup and Recovery Artifacts

These artifacts are intentionally separate. Operators should not send a recovery bundle where a diagnostic bundle is requested, and should not assume a configuration export alone can replace the HUB's cryptographic identity.

Artifact	Contains	Use
Diagnostic bundle	System state and logs without passwords, keys, or certificates	Support and troubleshooting
Configuration export	Full JSON configuration including encrypted site escrow records	Routine configuration backup
HUB recovery bundle	Passphrase-sealed HUB CA and enrollment identity	First-run adoption by a replacement HUB
Per-site recovery reveal	Break-glass and LUKS recovery values, disclosed to an Admin after step-up authentication	Authorized site disaster recovery

10. Firmware Operations

- Verify the signed package and release version before upload.
- Apply first to a representative SPOKE canary, then test rollback and reapply.
- Promote to the HUB after SPOKE health, routing, data plane, audit, and recovery continuity pass.
- Confirm whether the data-plane binary was preserved or restarted according to its hash.
- Retain the previous signed package until fleet promotion and acceptance complete.
- Avoid routine fleet-wide rebooting merely to activate unchanged data-plane code.

11. Incident Workflow

Symptom	First evidence	Next action
Site down	Tunnel state, WAN leases, HUB reachability	Confirm underlay, route guard, and enrollment identity
Tunnel up, traffic down	BGP/OSPF state and route lists	Confirm advertised/received prefixes and forwarding allowlist
Poor application quality	Per-path contribution, top talkers, latency/loss	Isolate carrier impairment, congestion, or QoS mismatch
DNS failure	Live resolver check and SPOKE service page	Confirm HUB upstream resolver and local unbound state
Logs missing	Syslog forwarding state and queue	Confirm collector identity, route, TLS, and backlog recovery
Suspected tamper	Local chain verification plus off-box SIEM	Preserve external evidence and follow incident response
Site attached to an unexpected HUB	Serving-HUB indicator, standby assignment, home-HUB reachability	Confirm the home-HUB outage is real before scheduling failback; failback is a second interruption

12. Roadmap — Not Included in v0.9.239

Roadmap items are architectural direction, not v0.9.239 capability. They are visually labeled and must not be used as procurement or deployment claims.

- Additional guided remediation text and role-specific runbooks

The fleet-scale attention dashboard and the geographic Fleet Map, listed as roadmap in the v0.9.118 edition of this paper, shipped before v0.9.173 and are described in Section 4 as current capability. Multi-HUB reachability and replication, and per-SPOKE automatic failover with operator-controlled failback, were carried as roadmap in the v0.9.173 edition and have since shipped; they are described in Sections 2 and 4.

13. Operational Readiness Checklist

- HUB recovery export completed and stored offline.
- Configuration export scheduled under customer backup policy.
- SIEM and NMS receiving expected data.
- External identity tested, with local fallback verified.
- Every site shows intended WAN path count and converged routing.
- Multicast posture explicitly reviewed.

- Firmware canary, rollback, and reapply evidence retained.
- Approved hardware inventory and TPM/Secure Boot evidence recorded.
- NOC contacts, maintenance windows, and upstream-provider escalation paths documented.
- Standby HUB assignments recorded, and each alternate verified reachable from the sites assigned to it.
- A failover drill executed and its result recorded, per site or per representative site.
- DNS and NTP continuity confirmed at every HUB in the region, not only the home HUB.
- Failback windows agreed with site owners in advance, so the second interruption is scheduled rather than improvised.

14. Conclusion

The FORGE OS operating model concentrates fleet authority — trust, policy, monitoring, escrow — at a HUB the customer owns, while keeping every SPOKE independently viable through management interruptions. Enterprise integration is deliberately conventional: the customer's existing SIEM, NMS, directory, DNS, and NTP remain the systems of record, fed by standard protocols rather than replaced by a proprietary console. Operating the fleet well means verifying what the truthful health model reports, keeping recovery artifacts current and separate, and treating the readiness checklist above as the ongoing definition of done for every site.

Document Control

Field	Value
Publisher	HAMR-FORGE, LLC
Platform	FORGE OS
Validated baseline	v0.9.239
Classification	Public release
Release date	22 August 2026
Supersedes	v0.9.173 edition (August 2026)
Claims boundary	No third-party certification or general-availability claim