MESHPROOF FORGE

Meshtastic® Security Baseline v0.1

An evidence-led control standard for privately operated fleets

Document status	Public review draft
Release date	August 20, 2026
Applies to	Meshtastic nodes, clients, gateways, MQTT brokers, and fleet operations
Canonical URL	https://meshproofforge.redasgard.com/meshtastic-security-baseline
Contact	meshproofforge@redasgard.com

Prepared by MeshProof Forge, a Red Asgard initiative

Executive purpose

> **Outcome:** This baseline defines what an assessor must inspect, what evidence is acceptable, and which conditions prevent a Meshtastic fleet from being represented as conformant.

Meshtastic is designed for useful, low-bandwidth, off-grid communication. It is not equivalent to modern authenticated enterprise messaging. Upstream documentation explicitly identifies limits in forward secrecy, group-message integrity, and sender authentication. This baseline turns those known properties, current configuration options, and published advisories into auditable fleet controls. [S1-S13]

The baseline is intentionally independent. It is not a Meshtastic certification, does not promise that a conformant fleet is breach-proof, and does not replace spectrum, privacy, safety, or sector-specific compliance obligations.

How to use this document

- Fleet owners use it to establish a defensible minimum configuration and evidence set.
- Assessors use it to plan read-only review, controlled validation, findings, and retesting.
- Hardware vendors use it to prove per-device identity generation and batch provisioning hygiene.
- Integrators use it to define the MQTT, client, network, and administration trust boundaries.

Public review process

The v0.1 review window closes October 1, 2026. Send comments to meshproofforge@redasgard.com with the subject `Baseline v0.1 feedback: CONTROL-ID`.

- Identify the affected control ID, disputed behavior, and deployment context.
- Provide reproducible evidence or an authoritative source when challenging a technical statement.
- Propose corrected language when possible. Material dispositions will be recorded in the next revision history as accepted, revised, held, or rejected with rationale.

Evidence language

Label	Meaning	Allowed use
Observed	Directly present in inspected configuration, documentation, logs, or records.	May support a finding when scope and timestamp are stated.
Verified	Independently reproduced or corroborated beyond the originating assertion.	May support a conclusion within the tested scope.
Inferred	Reasoned from observations, with the reasoning and limits stated.	Must not be presented as direct test evidence.
Assumed	A working premise that has not been established.	Must be resolved or retained as a limitation.
Unknown	Evidence was unavailable, inaccessible, or outside scope.	Cannot be converted into a pass.

1. Scope and threat model

The assessment boundary includes the complete path from radio node to operator and internet integration. A narrow radio-only review is insufficient when phones, workstations, MQTT brokers, automation, or remote-administration keys can alter fleet behavior.

Boundary	Included assets	Primary concerns
RF mesh	Nodes, channels, roles, routing behavior	Public headers, group identity, replay/injection limits, availability
Device	Hardware, firmware, identity keys, local interfaces	Provenance, duplicate keys, physical access, configuration writes
Operator	Mobile apps, CLI hosts, administrator nodes	Credential exposure, authorization, stale access, backup handling
Gateway	WiFi/Ethernet nodes and MQTT bridge	External input, plaintext publication, TLS, credentials, ACLs
Operations	Inventory, change control, monitoring, incident response	Drift, recovery, revocation, evidence retention

Threat actors considered

- A nearby radio participant or observer without a private channel key.
- A current or former channel member who knows a shared PSK.
- An internet actor who can reach a misconfigured MQTT boundary.
- A person with physical possession of a field node or operator device.
- A provisioning, maintenance, or integration error that creates duplicate identity, stale access, or unsafe defaults.

Explicit limitations

- Conformance does not add forward secrecy to captured channel traffic. [S1]
- Conformance does not make group-channel sender fields cryptographically trustworthy. [S1]
- Conformance does not prove hardware has no undisclosed vulnerabilities.
- RF localization, destructive testing, exploit development, and third-party infrastructure testing require separate written authorization and scope.
- A sample or self-attested evidence package is not independent verification.

2. Conformance model

Controls are classified as Core or Enhanced. Core is the minimum claimable baseline. Enhanced adds stronger lifecycle, provenance, monitoring, and physical controls for higher-impact fleets.

Result	Definition
Pass	Requirement is satisfied and supported by current, scoped evidence.
Fail	Evidence contradicts the requirement or a required safeguard is absent.
Not applicable	Requirement does not apply; rationale and boundary are documented.
Not tested	Evidence was unavailable or testing was outside scope. For Core controls this blocks conformance.

> **Core conformance:** Every applicable Core control must pass, no Core control may remain Not Tested, and no stop condition may be present. A percentage score cannot override a stop condition.

> **Enhanced conformance:** Core conformance plus every applicable Enhanced control. Exceptions must be documented but cannot waive a Core stop condition.

Stop conditions

- Duplicate device identity keys in the assessed fleet.
- A public, default, simple, or unencrypted key used for confidential or operational channel traffic.
- Unsupported firmware without a documented, time-bounded exception and compensating controls.
- Legacy admin-channel control enabled on current nodes outside an approved migration.
- Internet-reachable MQTT downlink without required TLS, authentication, least-privilege ACLs, and explicit approval.
- Known exposure of private device keys, channel PSKs, broker credentials, or administrator keys without completed containment and rotation.

3. Assessment workflow

1. **Authorize and bind scope.** Identify owners, assets, interfaces, test methods, excluded systems, and safe stop conditions.
2. **Collect evidence.** Export configuration through an authorized local path; immediately protect and redact secret-bearing files.
3. **Normalize inventory.** Bind asset IDs to hardware, role, firmware, Node ID, and public-key fingerprints.

4. **Review configuration.** Evaluate channels, security, Bluetooth, network, MQTT, position, and role settings against the control catalog.
5. **Validate safely.** Perform non-destructive checks for key uniqueness, administration paths, broker policy, recovery, and expected alerting.
6. **Report and remediate.** State evidence, affected assets, impact, uncertainty, ordered repair, owner, and verification method.
7. **Retest.** Recollect evidence after repair and close only findings whose corrected state is independently verified.

> **Evidence handling:** Never place full private keys, channel PSKs, broker passwords, WiFi credentials, or recoverable configuration QR codes in the report. Record classifications, truncated fingerprints, hashes, and controlled evidence references instead.

4. Control catalog

The Requirement column is normative for MeshProof conformance. The Source column distinguishes upstream behavior from independent MeshProof controls. Source IDs resolve in the source register.

1. Governance and scope

ID	Tier	Requirement	Minimum evidence	Basis
GOV-01	Core	Maintain an approved fleet boundary: nodes, gateways, clients, brokers, channels, operators, and data classifications.	Current inventory and architecture record	MeshProof
GOV-02	Core	Assign named owners for firmware, keys, broker administration, configuration changes, and incident response.	RACI or owner register	MeshProof
GOV-03	Enhanced	Record exceptions with owner, justification, compensating controls, and expiry date.	Exception register	MeshProof

2. Asset and firmware integrity

ID	Tier	Requirement	Minimum evidence	Basis
AST-01	Core	Inventory every node with a stable asset ID, hardware model, role, owner, firmware version, Node ID, and public-key fingerprint.	Export plus normalized fleet inventory	MeshProof
FW-01	Core	Run an upstream-supported firmware line and a current stable release unless a documented compatibility exception is approved.	Version export; S7 and current release check	S7, S8
FW-02	Core	Stage firmware updates on representative hardware and preserve a tested recovery path before fleet rollout.	Test record, rollback procedure, maintenance approval	MeshProof
FW-03	Enhanced	Record firmware provenance and integrity evidence for each approved image.	Release URL, hash, signer or provenance record	MeshProof

3. Device identity and key lifecycle

ID	Tier	Requirement	Minimum evidence	Basis
KEY-01	Core	Verify that every deployed node has a unique public key. Treat duplicate fingerprints as a stop condition until devices are wiped, reprovisioned, and rechecked.	Fleet-wide fingerprint comparison	S3, S9
KEY-02	Core	Provision devices so private keys are generated per device after the platform has usable entropy. Do not clone an image after identity generation.	Provisioning SOP and batch evidence	S9
KEY-03	Core	Keep private keys and full configuration exports confidential. Exclude private keys, channel PSKs, broker passwords, and WiFi credentials from assessment reports.	Storage ACLs, redacted evidence package	S3
KEY-04	Core	Verify public keys out of band before relying on direct messages or remote administration for sensitive operations.	Approved key fingerprints and verification record	S1, S3, S6, S10
KEY-05	Core	Maintain a documented response for lost, stolen, duplicated, or exposed node keys, including dependent channel and admin-key changes.	Key incident runbook and exercise evidence	S1, S3, S9
KEY-06	Enhanced	Use a controlled enrollment record that binds asset identity, approved firmware, public-key fingerprint, owner, and provisioning time.	Signed or access-controlled enrollment record	MeshProof

4. Channels and message trust

ID	Tier	Requirement	Minimum evidence	Basis
CHN-01	Core	Do not use `none`, `default`, or `simple` channel keys for confidential or operational traffic. Use a unique random 256-bit PSK.	Redacted channel classification and key-length check	S1, S2
CHN-02	Core	Separate public/discovery traffic from private operational channels, with deliberate channel membership and distribution.	Channel map and authorized-member list	S1, S2
CHN-03	Core	Treat group-channel sender identity as untrusted because channel encryption does not authenticate the sender and does not provide channel-message integrity.	Application design and operator guidance	S1
CHN-04	Core	Define a risk-based channel-key rotation interval and an immediate rotation trigger for lost nodes, staff changes, or suspected disclosure.	Rotation policy and last-rotation evidence	S1; MeshProof interval requirement
CHN-05	Enhanced	Add application-layer message authentication for high-impact machine actions carried over group channels.	Protocol design, test vectors, negative tests	S1; MeshProof implementation requirement

5. Administration and local interfaces

ID	Tier	Requirement	Minimum evidence	Basis
ADM-01	Core	Use PKC Remote Admin for current nodes and keep the insecure legacy admin channel disabled except during a time-bounded migration.	Security config and admin-key inventory	S3, S6
ADM-02	Core	Assign only required admin public keys, remove obsolete administrators, and verify control before enabling Managed Mode.	Admin-key register and recovery test	S3, S6
ADM-03	Enhanced	Enable Managed Mode on unattended or centrally governed nodes after a verified remote-administration and recovery test.	Managed-mode export and recovery test	S3, S6

ID	Tier	Requirement	Minimum evidence	Basis
ADM-04	Core	Disable unused serial, Bluetooth, WiFi, and Ethernet administration paths, or document why each remains enabled.	Interface inventory and configuration export	S3, S4
BLE-01	Core	Use RANDOM_PIN or a unique non-default FIXED_PIN. Do not use NO_PIN or the default fixed PIN `123456` on deployed nodes.	Bluetooth config and controlled pairing test	S4

6. MQTT and internet gateways

ID	Tier	Requirement	Minimum evidence	Basis
MQT-01	Core	Enable MQTT only on designated gateway nodes with an approved business purpose and named owner.	Gateway inventory and approval	S5; MeshProof governance requirement
MQT-02	Core	Require TLS for broker connections and reject broker endpoints that cannot be authenticated according to organizational policy.	MQTT config, certificate validation test	S5; MeshProof authentication requirement
MQT-03	Core	Use unique broker credentials per gateway and least-privilege topic ACLs. Do not reuse public/default credentials for private infrastructure.	Broker ACL export and credential inventory	S5; MeshProof least-privilege requirement
MQT-04	Core	Keep channel uplink and downlink disabled unless explicitly required. Treat downlink as an external input path into the RF mesh.	Per-channel gateway config and data-flow approval	S2, S5, S13
MQT-05	Core	Enable encrypted MQTT payloads unless the receiving system has an approved need for plaintext. Treat JSON and map reports as unencrypted data.	MQTT config and data-classification approval	S5
MQT-06	Core	Isolate broker roots and networks by environment, and monitor authentication failures, downlink activity, and unexpected topic use.	Network diagram, ACLs, logs, alert tests	MeshProof

7. Network, client, and physical protection

ID	Tier	Requirement	Minimum evidence	Basis
NET-01	Core	Do not perform local administration over an untrusted IP network. Place IP-enabled nodes on a controlled network segment.	Network path review and segmentation evidence	S15; MeshProof segmentation requirement
CLI-01	Core	Protect phones, workstations, and automation hosts that can read configuration or administer nodes using organizational endpoint controls.	Endpoint owner, access control, patch state	MeshProof
PHY-01	Core	Do not place private channel PSKs on unattended relay nodes unless decryption is operationally required and physical risk is accepted.	Role-to-key mapping and physical risk record	S1
PHY-02	Enhanced	Apply tamper evidence, controlled storage, and rapid loss reporting to high-impact gateway and administrator nodes.	Physical-control record and loss drill	MeshProof

8. Privacy and data minimization

ID	Tier	Requirement	Minimum evidence	Basis
PRV-01	Core	Set position precision per channel according to the audience and disable location sharing where it is not required.	Per-channel position settings and data owner approval	S2
PRV-02	Core	Keep map reporting disabled unless publication of node identity, location, role, firmware, region, and channel metadata is approved.	MQTT map-report config and approval	S5
PRV-03	Enhanced	Document metadata that remains observable even when payload encryption is enabled and account for it in the threat model.	Threat model and operator notice	S1

9. Monitoring and incident response

ID	Tier	Requirement	Minimum evidence	Basis
MON-01	Core	Capture redacted configuration snapshots and alert on unexpected firmware, public-key, admin-key, channel, and gateway changes.	Baseline snapshot, diff output, alert test	S9, S10; MeshProof
MON-02	Enhanced	Monitor for duplicate identities, abrupt public-key changes, repeated malformed input, abnormal downlink volume, and unauthorized broker activity.	Detection logic, test events, retained logs	S9, S10, S12, S13
IR-01	Core	Maintain a mesh-specific incident procedure covering node isolation, key rotation, broker credential revocation, config restoration, and stakeholder notification.	Runbook and tabletop record	MeshProof
IR-02	Core	Test recovery from a wiped or replaced node without restoring compromised or duplicated keys.	Recovery exercise and post-restore uniqueness check	S3, S9

5. Severity model

Finding severity combines credible impact, required access, affected scope, and existing safeguards. CVE severity is not copied onto a fleet finding without evaluating whether the affected version and conditions are present.

Severity	Fleet interpretation	Expected action
Critical	Credible fleet-wide compromise, decryption, or unauthorized administration with low operational barriers.	Contain immediately; suspend conformance claim; executive owner.
High	Material confidentiality, integrity, or availability impact across important nodes or an exposed trust boundary.	Prioritize repair; time-bounded owner; verify before closure.
Medium	Meaningful weakness requiring additional access, proximity, configuration, or chaining.	Schedule repair and track compensating controls.
Low	Localized hygiene, visibility, or resilience weakness with limited direct impact.	Correct through normal maintenance.
Informational	Context, improvement opportunity, or evidence note without a demonstrated security defect.	Consider and document disposition.

6. Required evidence package

- Assessment authorization, scope, and test window.
- Normalized asset inventory with public-key fingerprints, not private keys.
- Firmware support and release verification captured on the assessment date.
- Redacted radio and module configuration snapshots.
- Channel classification and key-strength result without key disclosure.
- MQTT data-flow diagram, broker ACLs, TLS test, and uplink/downlink justification.
- Admin-key register, interface inventory, and controlled access tests.
- Finding evidence references, remediation owners, target dates, and retest results.
- Hash of each retained evidence artifact and access-controlled storage location.

7. Version and advisory anchors

> **Freshness requirement:** As of August 20, 2026, upstream lists 2.7.x as supported and the latest non-prerelease release is v2.7.26.54e0d8d. Recheck both facts before every assessment. [S7, S8]

Anchor	Affected / fixed information from advisory	Baseline use
CVE-2025-52464 [S9]	Affected >2.5.0; patched 2.6.11; duplicate and low-entropy identity keys.	Verify supported firmware and fleet-wide key uniqueness.
CVE-2025-55293 [S10]	Affected <2.6.3; patched 2.6.3; NodeInfo public-key overwrite.	Monitor key changes and verify sensitive peer keys out of band.
CVE-2025-53627 [S11]	Affected <2.7.15; patched 2.7.15; legacy DM downgrade/display ambiguity.	Do not accept legacy firmware for PKC-dependent communication.
CVE-2025-24797 [S12]	Affected <2.6; patched 2.6.2; malformed packet buffer overflow.	Use supported current firmware and record exceptions.
CVE-2024-45038 [S13]	Affected <=2.4.0; patched 2.4.1+; malformed MQTT packet crash.	Treat MQTT downlink as hostile input and keep current firmware.

These anchors explain selected baseline controls; they are not an exhaustive vulnerability inventory. Review the current upstream advisory list during every assessment.

Maintenance and freshness policy

MeshProof Forge owns the baseline review. While v0.1 is current, upstream firmware support, stable releases, security advisories, and trademark guidance will be rechecked at least monthly. The next scheduled review is September 20, 2026. A material upstream security or support change can trigger an earlier revision.

The website must display the current document version, last reviewed date, next scheduled review, SHA-256 file hash, and archived superseded editions. Assessors must still verify mutable facts on the date of each engagement.

8. Assessment worksheet

Copy this row for each control. Not Tested is never equivalent to Pass.

Field	Assessment record
Control ID	
Result	Pass / Fail / Not applicable / Not tested
Claim state	Observed / Verified / Inferred / Assumed / Unknown
Assets	
Evidence reference	
Finding / rationale	
Owner and due date	
Retest evidence	

Revision history

Version	Date	Status	Change
0.1	2026-08-20	Public review draft	Initial evidence-led controls, public review process, maintenance policy, and publication terms.

Publication and trademark notice

Meshtastic® is a registered trademark of Meshtastic LLC. This independent publication is not affiliated with or endorsed by the Meshtastic project. Use of the name identifies the assessed technology and does not imply certification, sponsorship, or approval. Before distribution, follow the current attribution and notification rules, including providing the publication URL or a copy to the Meshtastic Trademark Supervisor within the period stated by the policy. MeshProof Forge and Red Asgard provide this baseline without warranty; security depends on implementation, hardware, environment, operations, and evidence available at the assessment date. [S14]

Source register

Sources identify upstream facts separately from MeshProof recommendations. Web material can change; recheck the current upstream security policy and stable release before each assessment.

ID	Source	Location and freshness
S1	Meshtastic Encryption (Official documentation)	https://meshtastic.org/docs/overview/encryption/ Retrieved 2026-08-20
S2	Channel Configuration (Official documentation)	https://meshtastic.org/docs/configuration/radio/channels/ Retrieved 2026-08-20
S3	Security Configuration (Official documentation)	https://meshtastic.org/docs/configuration/radio/security/ Retrieved 2026-08-20
S4	Bluetooth Configuration (Official documentation)	https://meshtastic.org/docs/configuration/radio/bluetooth/ Retrieved 2026-08-20
S5	MQTT Module Configuration (Official documentation)	https://meshtastic.org/docs/configuration/module/mqtt/ Retrieved 2026-08-20
S6	Remote Administration (Official documentation)	https://meshtastic.org/docs/configuration/remote-admin/ Retrieved 2026-08-20
S7	Firmware Security Policy at commit 6d41e279f1f51bd59f687b9d441c1bf47b1594fc (Upstream repository)	https://github.com/meshtastic/firmware/blob/6d41e279f1f51bd59f687b9d441c1bf47b1594fc/SECURITY.md Checked 2026-08-20
S8	Firmware release v2.7.26.54e0d8d (Upstream release)	https://github.com/meshtastic/firmware/releases/tag/v2.7.26.54e0d8d Published 2026-06-24; checked 2026-08-20
S9	GHSA-gq7v-jr8c-mfr7 / CVE-2025-52464: repeated public/private keypairs (GitHub Security Advisory)	https://github.com/meshtastic/firmware/security/advisories/GHSA-gq7v-jr8c-mfr7 Published 2025-06-18
S10	GHSA-95pq-gj5v-4fg2 / CVE-2025-55293: NodeInfo public-key overwrite (GitHub Security Advisory)	https://github.com/meshtastic/firmware/security/advisories/GHSA-95pq-gj5v-4fg2 Published 2025-08-16
S11	GHSA-377p-prwp-4hwf / CVE-2025-53627: legacy DM downgrade path (GitHub Security Advisory)	https://github.com/meshtastic/firmware/security/advisories/GHSA-377p-prwp-4hwf Published 2025-12-29
S12	GHSA-33hw-xhfh-944r / CVE-2025-24797: malformed-packet buffer overflow (GitHub Security Advisory)	https://github.com/meshtastic/firmware/security/advisories/GHSA-33hw-xhfh-944r Published 2025-04-11
S13	GHSA-3x3r-vw9f-pxq5 / CVE-2024-45038: malformed MQTT packet crash (GitHub Security Advisory)	https://github.com/meshtastic/firmware/security/advisories/GHSA-3x3r-vw9f-pxq5 Published 2024-08-27
S14	Meshtastic Licensing and Trademark Policy (Official policy)	https://meshtastic.org/docs/legal/licensing-and-trademark/ Retrieved 2026-08-20
S15	Network Configuration (Official documentation)	https://meshtastic.org/docs/configuration/radio/network/ Retrieved 2026-08-20