MESHPROOF FORGE

Sample Meshtastic® Fleet Security Assessment

Illustrative assessment for a representative 24-node event-communications fleet

SAMPLE REPORT - ILLUSTRATIVE DATA - NOT A CLIENT AUDIT

Document status	Sample only - not a client audit
Assessment date	August 20, 2026 (illustrative)
Baseline	MeshProof Meshtastic Security Baseline v0.1
Canonical baseline	https://meshproofforge.redasgard.com/meshtastic-security-baseline
Contact	meshproofforge@redasgard.com

Prepared by MeshProof Forge, a Red Asgard initiative

Executive summary

> **Assessment result:** NOT CONFORMANT in this illustrative sample. Duplicate identity keys, a public default channel key on operational traffic, unsupported firmware, and an uncontrolled MQTT boundary trigger Core stop conditions.

This report uses a representative 24-node event-communications environment to demonstrate MeshProof reporting. All organization details, assets, configurations, evidence, and findings are illustrative. This document does not describe a real client or completed field test.

The sample shows how configuration evidence, key fingerprints, broker policy, and recovery readiness are translated into actionable findings. It deliberately avoids exploit instructions and excludes all usable secrets.

Critical	High	Medium	Low	Informational
1	3	3	0	0

Priority actions

- Quarantine the four nodes with duplicate identity fingerprints; wipe, reprovision, and verify unique keys before redeployment.
- Replace the public default operational channel key and redistribute a unique random 256-bit PSK through a controlled process.
- Upgrade or remove unsupported firmware and revalidate all identity keys after upgrade.
- Disable MQTT downlink until TLS, unique credentials, least-privilege ACLs, encrypted payload policy, and monitoring are verified.

1. Scope and limitations

In scope	Illustrative quantity	Review method
Portable radio nodes	20	Configuration export, firmware inventory, public-key fingerprint comparison
Fixed routers	2	Configuration and physical-role review
MQTT gateways	2	Module configuration, TLS behavior, credential and ACL review
Operator clients	3 Android, 1 CLI host	Access path and configuration-backup review
Private MQTT broker	1	Broker policy and synthetic log review

Illustrative methods included read-only configuration review, offline public-key fingerprint comparison, firmware support checks, broker policy review, and safe validation in a consenting lab mesh. RF

geolocation, destructive hardware testing, password recovery, exploit development, and third-party infrastructure testing were excluded.

> **Evidence limitation:** The values and records in this sample are illustrative. They demonstrate how the report structure represents evidence and decisions; they do not prove the existence or prevalence of any condition in a real fleet.

2. Environment snapshot

Asset group	Role	Firmware	Administrative path	Notable sample state
SMP-ND-01 to SMP-ND-18	Portable client	v2.7.26.54e0d8d	Bluetooth	Six use default fixed PIN
SMP-ND-19 to SMP-ND-20	Portable client	v2.6.10	Bluetooth	Unsupported firmware
SMP-RT-01 to SMP-RT-02	Fixed router	v2.6.10	USB / remote	Duplicate identity fingerprint set
SMP-GW-01 to SMP-GW-02	MQTT gateway	v2.6.10	Ethernet / remote	Broad broker ACL; downlink enabled

The current upstream security policy lists 2.7.x as supported. The example therefore treats every 2.6.10 node as unsupported on the assessment date. [S7]

3. Conformance decision

Decision component	Sample result	Basis
Core controls	Fail	Seven open findings affect one or more Core controls.
Stop conditions	Present	Duplicate identity keys, public default operational PSK, unsupported firmware, and uncontrolled internet downlink.
Unknown / not tested	None retained	All sample Core areas were assigned an illustrative result.
Overall	Not conformant	A percentage score cannot override a stop condition.

4. Detailed findings

MPF-001 - Duplicate device identity keys in a provisioned batch

Severity	Status	Affected sample assets	Baseline controls
Critical	Open	SMP-RT-01, SMP-RT-02, SMP-GW-01, SMP-GW-02	KEY-01, KEY-02, KEY-05, FW-01

> **Sample evidence:** All evidence below is illustrative and demonstrates report structure only.

- Four redacted configuration exports produced the same synthetic public-key fingerprint: `SHA256:7f3a…9c11`.
- The provisioning note states that a configured image was copied after first boot.

- No private key was collected or printed in the report.
- This sample condition matches the class documented in CVE-2025-52464. [S9]

Impact. A party possessing the corresponding duplicated private key could, under the conditions described by the upstream advisory, decrypt captured direct messages for affected identities or impersonate an authorized administrative path. A duplicate identity also destroys the fleet's assumption that one public key represents one device.

Required remediation

- Remove affected nodes from operational service and preserve only redacted evidence needed for the incident record.
- Perform a complete device wipe, install a supported stable release, set the LoRa region, and generate a fresh per-device identity.
- Re-enroll every device with a new public-key fingerprint and verify fleet-wide uniqueness before restoring channel or admin access.
- Change dependent admin keys, channel keys, and broker credentials if exposure cannot be excluded.
- Change the provisioning process so images are captured before device-unique identity generation.

Verification. Repeat the fleet-wide fingerprint comparison and require one unique fingerprint per asset. Confirm the provisioning SOP and a new sample batch pass before closure.

MPF-002 - Public default channel key used for operational traffic

Severity	Status	Affected sample assets	Baseline controls
High	Open	All 24 nodes; primary channel `OPS`	CHN-01, CHN-02, CHN-03, CHN-04

> **Sample evidence:** All evidence below is illustrative and demonstrates report structure only.

- The redacted channel export classifies the primary PSK as the known Meshtastic default `AQ==`.
- The channel carries staff coordination and location messages in the sample operating model.
- Upstream documentation states that the default key is publicly known and must be changed for proper private encryption. [S1, S2]

Impact. Any party using the known default channel configuration can read channel payloads and inject traffic attributed to arbitrary sender fields. Operators could mistake a public interoperability channel for a private operational channel.

Required remediation

- Create a unique random 256-bit PSK for the operational channel through an approved key-generation process.
- Distribute the new channel only to authorized operators and maintain a membership record.
- Separate public discovery traffic from private operations.
- Define immediate and periodic rotation triggers.
- Do not use group-channel sender identity alone to authorize machine actions.

Verification. Re-export every node, confirm the operational channel no longer matches `none`, `default`, or `simple`, and perform an authorized join/deny test with one excluded lab node.

MPF-003 - Unsupported firmware remains in the operational fleet

Severity	Status	Affected sample assets	Baseline controls
High	Open	SMP-ND-19, SMP-ND-20, SMP-RT-01, SMP-RT-02, SMP-GW-01, SMP-GW-02	FW-01, FW-02, KEY-01

> **Sample evidence:** All evidence below is illustrative and demonstrates report structure only.

- Six sample nodes report firmware v2.6.10.
- The upstream security policy checked on the sample assessment date lists 2.7.x as supported and <=2.6.x as unsupported. [S7]
- The stable release used as the sample target is v2.7.26.54e0d8d. [S8]

Impact. Unsupported firmware does not receive the current upstream support posture and precedes fixes relevant to the sample fleet's trust assumptions. Version drift also makes behavior and recovery inconsistent across nodes.

Required remediation

- Upgrade through a representative hardware staging set before broad rollout.
- Use the current supported stable release verified on the implementation date, not a hard-coded version copied from this sample.
- After upgrade, repeat public-key uniqueness, direct-message, remote-admin, and MQTT boundary checks.
- Document any compatibility exception with owner, compensating controls, and expiry date.

Verification. Collect fresh version evidence from all assets, confirm the supported line against the current upstream policy, and rerun the affected control tests.

MPF-004 - MQTT gateway exposes an uncontrolled downlink boundary

Severity	Status	Affected sample assets	Baseline controls
High	Open	SMP-GW-01, SMP-GW-02	MQT-01 to MQT-06, CHN-01

Sample evidence: All evidence below is illustrative and demonstrates report structure only.

- Synthetic config: `tls_enabled=false`, `encryption_enabled=false`, `json_enabled=true`, and operational-channel downlink enabled.
- Illustrative broker: `broker.example.invalid`; both gateways share one credential and a wildcard ACL over `org/sample-fleet-a/#`.
- Upstream documentation states that unencrypted MQTT payloads, JSON packets, and map reports can expose plaintext and that downlink forwards internet-sourced messages to the local mesh. [S2, S5]

Impact. The broker becomes an external authority boundary into the RF mesh. A broker account compromise, topic-policy error, or reachable unauthenticated path could inject or expose traffic beyond the intended gateway scope.

Required remediation

- Disable operational-channel downlink until the boundary is rebuilt and tested.
- Enable TLS and validate the broker identity according to organizational policy.
- Issue unique credentials per gateway and restrict publish/subscribe ACLs to required roots and directions.
- Enable encrypted payloads unless plaintext integration has explicit data-owner approval.
- Separate environments and alert on authentication failures, unexpected topics, and downlink spikes.

Verification. Use a controlled broker test account to prove denied topics fail, required topics succeed over TLS, plaintext publication follows the approved classification, and alerts fire on synthetic abuse events.

MPF-005 - Default fixed Bluetooth PIN remains on headless nodes

Severity	Status	Affected sample assets	Baseline controls
Medium	Open	SMP-ND-03, SMP-ND-05, SMP-ND-08, SMP-ND-11, SMP-ND-14, SMP-ND-18	BLE-01, ADM-04

Sample evidence: All evidence below is illustrative and demonstrates report structure only.

- Six sample headless nodes report `FIXED_PIN` with value `123456`.

- Upstream documentation identifies `123456` as the default fixed PIN and strongly recommends changing it. [S4]

Impact. A nearby person who can reach the Bluetooth interface has a predictable pairing secret. Impact depends on client behavior, radio proximity, and what configuration actions the connected client can perform.

Required remediation

- Use a unique non-default fixed PIN for headless devices or disable Bluetooth where it is not operationally required.
- For screened devices, prefer random pairing and verify the operator procedure.
- Record the approved local-administration path for each role.

Verification. Attempt controlled pairing with the default PIN and require failure; then verify the approved administration path still works.

MPF-006 - Legacy admin channel enabled after migration

Severity	Status	Affected sample assets	Baseline controls
Medium	Open	SMP-RT-01, SMP-RT-02	ADM-01, ADM-02

> **Sample evidence:** All evidence below is illustrative and demonstrates report structure only.

- Synthetic configuration shows `security.admin_channel_enabled=true` on two routers.
- No pre-2.5 compatibility dependency is recorded.
- Upstream documentation describes the legacy admin channel as insecure and recommends PKC Remote Admin for current nodes. [S3, S6]

Impact. A shared legacy administration path expands the number of parties and secrets that can authorize device changes. It also undermines the fleet's move to per-administrator public keys.

Required remediation

- Configure approved PKC administrator public keys.
- Verify remote administration and a local recovery path.
- Disable the legacy admin channel and remove the shared admin-channel configuration.
- Review administrator access at staff and role changes.

Verification. Confirm the legacy setting is disabled, an authorized administrator succeeds through PKC Remote Admin, and an unlisted test key is rejected.

MPF-007 - No mesh-specific key and node incident procedure

Severity	Status	Affected sample assets	Baseline controls
Medium	Open	Fleet-wide operational process	KEY-05, CHN-04, IR-01, IR-02

Sample evidence: All evidence below is illustrative and demonstrates report structure only.

- The sample operations binder has no response steps for a lost node, exposed channel key, duplicated identity, or broker credential compromise.
- No owner or maximum response time is assigned for key rotation and node replacement.
- The last configuration restore test is recorded as `not performed`.

Impact. Containment would depend on improvised action during a real loss or compromise. Delayed rotation can extend exposure, and an untested restore can accidentally reintroduce old or duplicated keys.

Required remediation

- Create an incident playbook covering isolation, evidence preservation, key and credential rotation, admin-key review, broker containment, node wipe, recovery, and notification.
- Assign owners and decision thresholds.
- Run a tabletop and a controlled node-replacement exercise.
- Verify restored nodes receive fresh identity when prior keys are suspect.

Verification. Complete the tabletop and recovery exercise, retain the redacted evidence, and verify the replacement node has a unique public-key fingerprint.

5. Controls that passed in the sample

A useful assessment records retained safeguards as well as failures. The following sample controls passed and should be preserved during remediation:

- Map reporting is disabled on both MQTT gateways.
- Position precision is reduced on the public discovery channel.
- Private keys and channel PSKs are absent from the report evidence package.
- Eighteen current-firmware portable nodes have unique public-key fingerprints in the sample inventory.
- Operator workstations use named accounts and full-disk encryption in the sample endpoint record.

6. Remediation roadmap

Order	Action	Owner	Target	Closure evidence
1	Quarantine and reprovision duplicate-key nodes	Fleet engineer	24 hours	Unique fingerprints and clean enrollment
2	Rotate operational channel key	Security owner	24 hours	Redacted config classification and denied-node test
3	Disable MQTT downlink pending rebuild	Broker owner	Immediate	Config export and broker policy
4	Upgrade unsupported firmware	Fleet engineer	7 days	Supported-version inventory and regression tests
5	Harden MQTT TLS, credentials, ACLs, and alerts	Broker owner	14 days	TLS/ACL tests and alert evidence
6	Replace Bluetooth defaults and legacy admin	Fleet engineer	14 days	Pairing and PKC admin negative tests
7	Exercise incident and recovery playbook	Security owner	30 days	Tabletop and recovery record

7. Retest requirements

- Recollect evidence from the same asset IDs and identify any replacement nodes.
- Recheck the current upstream support boundary and stable release on the retest date.
- Repeat fleet-wide public-key uniqueness checks after all wipe, upgrade, and restore actions.
- Verify channel key classification without storing the PSK in the report.
- Test allowed and denied PKC administrator keys.
- Test broker TLS, per-gateway credentials, topic ACLs, payload mode, and alerts.
- Close findings only when the corrected state is verified; management acceptance does not convert a failed Core control into a pass.

Appendix A - Sample evidence index

Evidence ID	Description	Claim state	Handling
EV-01	Redacted fleet inventory and version export	Observed (illustrative)	No private keys
EV-02	Public-key fingerprint comparison output	Verified (illustrative)	Truncated fingerprints
EV-03	Redacted channel configuration classification	Observed (illustrative)	No PSK value stored
EV-04	MQTT module configuration and data-flow record	Observed (illustrative)	Reserved `.invalid` broker name
EV-05	Broker ACL and TLS test record	Verified (illustrative)	No credential stored
EV-06	Bluetooth and remote-admin controlled test	Verified (illustrative)	No reusable access material
EV-07	Incident tabletop and recovery record	Unknown / absent	Drives MPF-007

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
S14	Meshtastic Licensing and Trademark Policy (Official policy)	https://meshtastic.org/docs/legal/licensing-and-trademark/ Retrieved 2026-08-20

Trademark and independence notice

Meshtastic® is a registered trademark of Meshtastic LLC. MeshProof Forge is independent and is not affiliated with or endorsed by the Meshtastic project. This sample report does not confer certification or describe a real customer assessment. [S14]

Before public distribution, apply the current attribution and notification requirements in the official trademark policy. [S14]