MESHPROOF FORGE

Device Batch Pilot Scope

Fixed-scope security assessment for one device model, one firmware release, and one representative batch

Document status	Buyer-facing pilot scope
Fixed pilot fee	$15,000 USD
Designed for	Manufacturers, assemblers, resellers, and deployment integrators
Assessment basis	MeshProof Meshtastic Security Baseline v0.1
Pilot page	https://meshproofforge.redasgard.com/#pilot-intake
Contact	meshproofforge@redasgard.com

Prepared by MeshProof Forge, a Red Asgard initiative

Pilot objective

> **Outcome:** Produce a reproducible security record that binds the submitted device sample to its model, hardware revision, firmware release, identity-key results, assessed configuration, applicable advisories, and retest state.

The pilot is deliberately narrow. It tests one defined release path before a broader assurance program is designed. It does not certify Meshtastic, guarantee fleet security, or make statistical claims about units that were not included in the agreed sampling plan.

1. Fixed assessment boundary

Scope element	Included boundary
Device	One commercial device model and one hardware revision.
Release	One firmware release, build identity, and regional radio configuration.
Batch	One production or pre-deployment batch with the physical sample and batch population recorded in the SOW.
Provisioning	One documented flashing, first-boot, enrollment, and configuration workflow.
Administration	One primary local or remote administration path used for the submitted release.
Gateway	One MQTT or internet-gateway boundary when it is part of the submitted product or deployment package.
Retest	One focused retest of agreed remediations within the retest window stated in the SOW.

> **Sampling decision:** The physical sample count is confirmed during intake from batch size, hardware access, provisioning method, and the claims the customer wants to make. The signed SOW records both the assessed sample and the larger batch population, if any.

2. Included assessment activities

- Bind every submitted unit to an assessment ID, device model, hardware revision, firmware build, and declared batch.
- Compare public-key fingerprints across the submitted sample and flag duplicate, missing, replaced, or known-compromised identities without collecting private keys.
- Review the flashing and first-boot process to determine when device-unique identity material is created and whether configured images can clone it.
- Evaluate security-relevant radio, channel, administration, Bluetooth, network, serial, debug, and gateway settings against the agreed baseline controls.
- Map applicable published Meshtastic security advisories to the exact submitted release and observed conditions.

- Record observed, verified, inferred, assumed, unknown, and not-tested boundaries separately so unsupported claims cannot become a pass.
- Review agreed remediation with engineering and repeat the affected checks once during the retest window.

3. Deliverables

Deliverable	What it contains
Device-batch manifest	Submitted-unit identifiers, model and hardware revision, firmware build, public-key fingerprint classification, and evidence references.
Security findings report	Evidence-led findings, affected units and versions, impact, uncertainty, prioritized remediation, and closure tests.
Configuration results	Control-by-control pass, fail, not applicable, or not tested results for the agreed configuration boundary.
Advisory mapping	Applicable published advisories mapped to the submitted release and the conditions actually inspected.
Remediation workshop	One working session with engineering and product owners to resolve findings and bind retest scope.
Focused retest record	Verified disposition of the agreed corrected findings, with remaining limitations stated.

4. Customer prerequisites

- Written authorization identifying the device model, submitted units, firmware release, interfaces, test boundary, and owner.
- Representative devices shipped or made available through an agreed controlled-access method.
- Firmware release files or authoritative release identifiers, build procedure, and relevant configuration profile.
- Provisioning procedure from flashing through first boot and customer-ready configuration.
- An engineering contact able to explain expected behavior and approve controlled validation steps.
- For gateway review, a consenting test environment with non-production credentials and an agreed broker boundary.

> **Do not send:** Do not email private keys, channel PSKs, broker passwords, WiFi credentials, recoverable configuration QR codes, customer data, or production secrets during intake. Secret-bearing evidence is handled only through the method agreed in the executed SOW.

5. Indicative engagement sequence

1. **Intake and scope confirmation.** Confirm the model, release, batch, sample, interfaces, prerequisites, exclusions, schedule, and authorized test boundary.
2. **Evidence and device receipt.** Verify that the submitted sample and required records are complete before the assessment clock starts.
3. **Assessment.** Inspect the evidence chain, reproduce safe checks, and issue questions through the named engineering contact.
4. **Findings workshop.** Review evidence, disposition factual corrections, agree remediation owners, and bind the focused retest.
5. **Retest and final package.** Repeat affected checks once and issue the final evidence package with unresolved limitations retained.

The calendar schedule begins only after the SOW is executed and all required devices, evidence, access, and customer contacts are available. Dates are confirmed in the SOW rather than promised by this overview.

6. Exclusions and separate authorization

- Certification, regulatory compliance attestation, product endorsement, or a guarantee that the product is vulnerability-free.
- Destructive hardware analysis, component decapsulation, invasive fault injection, RF geolocation, or testing outside the agreed radio environment.
- Exploit development, denial-of-service activity, third-party infrastructure testing, production broker access, or testing against customer fleets outside the submitted boundary.
- Source-code review, mobile-application review, cloud-platform review, penetration testing, or additional firmware releases unless separately scoped.
- Continuous monitoring, ongoing release certification, statistical lot acceptance, or additional remediation cycles.
- Shipping, customs, taxes, replacement hardware, and third-party laboratory costs unless the SOW explicitly includes them.

7. Commercial and completion terms

Term	Pilot position
Fixed fee	$15,000 USD for the boundary described here and finalized in the executed SOW.
Payment	Payment schedule, applicable taxes, shipping, and approved external costs are stated in the SOW.
Scope changes	A second model, hardware revision, firmware release, gateway boundary, or remediation cycle requires written scope adjustment.
Completion	The final package is issued after the included workshop and focused retest, or after the retest window expires or is declined.
Customer claims	Only the exact assessed model, release, sample, and evidence state may be represented. MeshProof does not authorize broader certification claims.

Start the intake

> **Next step:** Complete the structured pilot intake at https://meshproofforge.redasgard.com/#pilot-intake or email meshproofforge@redasgard.com. Final scope is created only after MeshProof confirms the submitted boundary and prerequisites.