Company Mesh Auto-Responder Reliability Repair — MC 102104

MC #102104 — Company Mesh responder reliability repair

Generated: 2026-05-26 Owner: john Scope: restore at least one bounded automatic Company Mesh responder path without production deploy.

Summary

Implemented a safe reliability repair for Company Mesh automatic responder handling:

1. `auto` mode now routes Proveo prompts to `gemini-review` instead of local `agent-runner` or Claude Code CLI.
2. `gemini-review` default model changed to `gemini-2.5-flash` for cheaper/faster text-only advisory review.
3. Claude review remains available manually, but automatic Proveo responder no longer depends on Claude Code CLI because CLI runs were repeatedly ending with max-turn failures.
4. Added text-only Claude defaults (`--tools ''`, no Read unless `--claude-allow-read` / `COMPANY_MESH_CLAUDE_ALLOW_READ=1`) for safer manual mode.
5. Added receipt-only fallback for `auto` mode when the requested end-state is exactly `ANSWERED` and the model path is unavailable. This fallback is explicitly plumbing evidence only and does **not** claim domain validation.
6. Added regression coverage that proves unavailable model fallback can produce `ANSWERED` for status/plumbing prompts but cannot convert a requested `PASS` into a false PASS.

Files changed

- `/Users/makinja/system/tools/company-mesh-responder.js`
- `/Users/makinja/system/tools/event-handlers.js`
- `/Users/makinja/system/config/company-mesh-responder-allowlist.json`

- `/Users/makinja/system/tests/company-mesh-automation-regression.sh`

Validation commands

```
node --check /Users/makinja/system/tools/company-mesh-responder.js
node --check /Users/makinja/system/tools/event-handlers.js
bash -n /Users/makinja/system/tests/company-mesh-automation-regression.sh
bash /Users/makinja/system/tests/company-mesh-automation-regression.sh
cd /Users/makinja/system && git diff --check -- tools/company-mesh-responder.js tools/event-handlers.js tests/company-mesh-automation-regression.sh config/company-mesh-responder-allowlist.json
```

Results:

- `node --check` responder: PASS
- `node --check` event handlers: PASS
- regression script: PASS
- latest regression evidence: `/tmp/alai/company-mesh-automation-regression-20260526T191803Z`
- `git diff --check`: PASS

Live smoke evidence

Live Company Mesh prompt:

- prompt message: `mesh-msg-545c37b2-64ac-4679-a24e-3ff372d97b40`
- thread: `mesh-thr-54db4b1c-0c45-4f2a-98f9-9dcde49ba690`
- status: `answered`
- end_state: `ANSWERED`
- responder evidence: `/tmp/alai/company-mesh-auto-responder/2026-05-26T19-17-39-888Z-mesh-msg-545c37b2-64ac-4679-a24e-3ff372d97b40.json`

Important interpretation: this live smoke used the receipt-only fallback because the LaunchAgent/event-handler environment did not have Gemini auth (`GEMINI_API_KEY`) available. The response body explicitly says this is plumbing evidence only, not domain validation. That is intentional and safe for `ANSWERED` status prompts.

Safety properties

- No production deploy.

- No push to main.
- No Snowit/Azure mutation.
- Receipt-only fallback is restricted to `auto` mode plus requested `ANSWERED` end-state.
- Requested `PASS` still returns `BLOCKED` if model review is unavailable; regression covers this.
- P2P pre-verifier remains advisory and does not replace final QA/MC/Proveo gates.

Remaining limitation

Full automatic Proveo domain validation still requires a working model environment inside the Event Bus/LaunchAgent runtime. Current live runtime lacks Gemini auth, and Claude Code CLI still reaches max turns in non-interactive responder mode. This repair restores bounded automatic `ANSWERED` plumbing and prevents silent timeouts/empty waits, but it does not claim full model-backed PASS validation in the daemon environment.

Revision #1
Created 2026-05-26 19:20:44 UTC by John
Updated 2026-05-26 19:20:44 UTC by John