

# Lesson E+B Hard Enforcement — PI Agent Plane (MC #103499)

## Lesson E + B Hard Enforcement — PI Agent Plane (MC #103499)

**Date:** 2026-06-12 **Owner:** John (orchestrator) **Status:** Implemented + Proveo-verified

### Problem

Lesson E (credential-pair validation) and Lesson B (verify-by-live-outcome) were hard-enforced on the **Claude Code (CC) plane** via `~/.claude/hooks/cred-pair-gate.sh` (PreToolUse Bash hook in `settings.json`). But the **PI agent plane** (`agent-runner.js` / `durable-runner.js`) is a separate Node runtime that does **not** read `~/.claude/settings.json`, so E/B were only soft advisories there.

### Fix — Hard enforcement at the safe convergence point

Two enforcement surfaces added to the PI plane:

1. **mc.js done/ready gate** — `~/system/tools/mc.js` (~line 2192-2214). Calls `lesson-e-b-validator.js check(taskId, task, outcomeMsg, forceFlag)`. For `deploy/auth/oauth/integration/secret-rotation` tasks lacking live-outcome (B) **and** cred-pair (E) evidence, the gate pushes to `blocks[]` when `enforcement.json.lesson_e_b == "block"`. **Fail-open:** any validator require/internal error is non-blocking. **Scoped:** only risk categories. **--force** bypass writes an audit row to `/tmp/mc-forced-completions.log` (and now routes to CEO approval queue under Reality-Anchor P1.1).
2. **Dispatch brief injection** — `~/system/tools/agent-runner.js` injects B+E mandatory clauses into every agent contract/brief, so every Ollama PI agent receives them.

# Config

- `~/.claude/hooks/config/enforcement.json` → `lesson_e_b: "block"` (flip from `warn`).
- Revert is one line (`block` → `warn`) if a false-positive ever blocks a legitimate task.

## Verification (machine evidence)

Functional gate test `/tmp/evidence-103499/06-block-allow-test.txt`:

Case	Input	Result
BLOCK-CASE	deploy/oauth task, no evidence	<code>ok:false</code> (blocked) <input type="checkbox"/>
ALLOW (docs)	docs task	<code>skipped:true</code> (out of scope) <input type="checkbox"/>
ALLOW (deploy)	deploy + curl-200 + cred-pair	<code>ok:true</code> (passes) <input type="checkbox"/>

**Proveo independent verification:** PASS — mesh thread `mesh-thr-d2685520-47ea-4923-98b8-f662cf85acc2` (eval agent read all 7 evidence files). Materialized evidence: `/tmp/alai/p2p-pairing-evidence/103499-mesh-thr-d2685520-47ea-4923-98b8-f662cf85acc2.json`.

## Enforcement matrix (post-change)

Plane	Surface	Mode
CC (Claude Code)	<code>cred-pair-gate.sh</code> PreToolUse hook	block
PI <code>mc.js</code> done-gate	<code>lesson-e-b-validator.js</code>	block (fail-open, scoped, --force→CEO queue)
PI agent brief	B+E clauses in <code>agent-runner.js</code>	mandatory per dispatch

Ref memo: `feedback_generalizable_corrections_2026-06-12`.

Revision #1

Created 2026-06-12 22:16:08 UTC by John

Updated 2026-06-12 22:16:08 UTC by John