

Bilko CSP Cleanup — MC #10440 (next.config.js basicconsulting.no to alai.no migration)

Bilko CSP Cleanup — MC #10440 (next.config.js basicconsulting.no ? alai.no migration)

Documentation for **MC #10440** — follow-up to MC #10428 (Gemini code-review) to clean up stale/misleading CSP entries and `allowedDevOrigins` in `apps/web/next.config.js` after the basicconsulting.no → alai.no domain migration.

Context

During a Gemini-driven code review of Bilko's Next.js configuration (MC #10428), several stale domain entries were flagged in the development CSP (Content Security Policy) and `allowedDevOrigins` array. These entries pointed to the old `basicconsulting.no` domain, which has been retired in favor of `alai.no`.

Changes Applied

File: `apps/web/next.config.js`

Removed Dead Hosts (basicconsulting.no)

- `bilko-demo.basicconsulting.no` — curl verification: TLS handshake completes, no HTTP response (CNAMEs to the same dead GCP Cloud Run family MC #104221 already confirmed dead)
- `bilko-demo-api.basicconsulting.no` — curl verification: HTTP 502 (Cloudflare proxy up, origin dead)
- `*.basicconsulting.no` wildcard — removed from both `connect-src` and `allowedDevOrigins`

Scoped Wildcard to Explicit Host

The `allowedDevOrigins` array contained a broad `*.alai.no` wildcard. Narrowed to the single explicit host actually used:

- Before: `*.alai.no`
- After: `bilko-demo-api.alai.no`

Corrected Misleading Comment

A comment incorrectly described the `alai.no` hosts as "dev tunnels" when they actually point to a remote Cloud Run demo environment. Corrected for accuracy.

Production CSP Untouched

The production CSP branch was left unchanged. All modifications were scoped to the development environment only.

Audited (Not Modified)

Additional vestigial CSP entries were identified but **not removed** — outside this task's scope:

- `script-src` / `style-src` — Google Fonts CDN entries (app self-hosts fonts via `next/font/google`, per MC #100227)
- `script-src` — Sentry CDN entry (app uses the npm SDK, not the CDN loader)
- `img-src` — `r2.bilko.io` confirmed as a near-term placeholder for an OG image (`app/page.tsx` comment)

Flagged as future cleanup candidates.

Validation

- curl verification: all dead hosts independently confirmed (basicconsulting.no timeout/502; bilko-demo-api.alai.no SSL error — see below)
- grep verification: no other live `alai.no` subdomain needed by the dev server
- Build sanity: `npx turbo run lint --filter=@bilko/web` and `npx turbo run build --filter=@bilko/web` both green
- Independent re-validation: Proveo independently re-ran all checks (curl, grep, build) — **PASS** on all 5 acceptance criteria

Known Open Issue — MC #104570

Important: during this work, `bilko-demo-api.alai.no` itself was found **dead** (SSL_ERROR_SYSCALL; DNS resolves to an orphaned Google-hosted IP, `142.251.38.115`).

This contradicts MC #104221 (2026-06-28, 3 days prior), which reported this host as "LIVE 200". MC #104570 (H priority, opened 2026-07-01) tracks investigating whether the Bilko live demo is currently broken.

The CSP entry referencing `bilko-demo-api.alai.no` was **correctly left in place** (CodeCraft/Proveo decision) — removing a currently-referenced entry without confirming permanent death risks breaking an expected path. Do not treat this host as confirmed-live until MC #104570 resolves.

Related Tasks

- MC #10428 — Gemini code-review that flagged these concerns
- MC #104221 — Prior CSP work (2026-06-28), reported `bilko-demo-api.alai.no` as "LIVE"
- MC #104570 — Follow-up investigation into `bilko-demo-api.alai.no` death (H priority, opened 2026-07-01)

Deployment

No separate deployment required — config-only change, lands via normal PR merge to `azdo/main`.

Documented: 2026-07-01

Revision #1

Created 2026-07-01 07:28:45 UTC by John

Updated 2026-07-01 07:28:45 UTC by John