Smart Home Energy Monitor - Security Recommendations

Generated: 2025-11-10 17:49:24.847 UTC

1. Lock down device/settings APIs and tenant data.
   Require auth for GET /api/devices and /api/settings and store per-user records.
   Add user_id ownership fields so one tenant cannot read another tenant’s devices.

2. Enforce strong secret and session management.
   Fail fast if JWT_SECRET is unset, rotate keys, and keep secrets out of source control.
   Always issue Secure SameSite=Strict cookies and shorten access token TTLs.

3. Enable CSRF protection and tighten security headers.
   Turn CSRF on by default, validate X-CSRF-Token, and drop ’unsafe-inline’/’eval’ in CSP.

4. Add adaptive login rate limiting and audit logging.
   Layer IP+account lockouts on /auth/login and track auth/audit events for forensics.

5. Require TLS plus authenticated MQTT transport.
   Move defaults to https/wss, enforce broker cert validation, and require per-device creds.

6. Protect data at rest and keep the SQLite DB out of the repo.
   Store smarthome.db outside source control, add encryption/backup, and secure .env files.