

TESLA FLEET API · APPLICATION APPROVED

UnyKorn Black Fleet — Tesla Developer Application Configuration

Onboarding request approved. Client ID and client secret exist. OAuth is bound to <https://black.unykorn.ai>. This note records the correct dashboard settings. The client secret is never written here, in Git, or in browser code.

1. Status

Tesla has approved the UnyKorn Black Fleet onboarding request. The application has a client ID, a client secret, authorization-code and client-credentials grant types, and a site origin. That is the correct grant mix: user-authorized vehicle connections plus server-side application workflows.

2. Dashboard settings — keep / fix

Field	Value	Action
Allowed Origin(s)	https://black.unykorn.ai	Keep. Canonical Tesla origin.
Allowed Redirect URI(s)	https://black.unykorn.ai/api/auth/tesla/callback	Keep. This is the only OAuth callback.
Allowed Returned URL(s)	https://black.unykorn.ai/tesla/connected	Use this as the post-connect page. Not a callback.
Redirect URI: /terms	https://black.unykorn.ai/terms	REMOVE. A terms page is not an OAuth callback.
Returned URL set to the callback	.../api/auth/tesla/callback as a “returned URL”	Change to /tesla/connected, or drop if unused.
Grant types	authorization-code + client-credentials	Keep.

Better final configuration (copy into Tesla Application Details):

Allowed Origin(s): <https://black.unykorn.ai>

Allowed Redirect URI(s): <https://black.unykorn.ai/api/auth/tesla/callback>

Allowed Returned URL(s): <https://black.unykorn.ai/tesla/connected>

3. Security

Treat the client secret as a production credential. Store it only in Cloudflare encrypted environment variables (TESLA_CLIENT_ID / TESLA_CLIENT_SECRET on the Pages Function). Never in browser JavaScript, GitHub, logs, screenshots, or PDFs. The public site talks only to /api/auth/tesla/start; the worker holds the secret and exchanges the code server-side.

black.unykorn.org is the public marketing host. Tesla OAuth is bound to black.unykorn.ai. Do not add .org as a redirect unless you also add it in the Tesla dashboard. Do not paste secrets into chat.

4. What we implemented on the site

GET /api/auth/tesla/start — 302 to Tesla authorize (state cookie). GET /api/auth/tesla/callback — server-side token exchange, then 302 to /tesla/connected. Tokens are not returned to the browser. Persist refresh tokens only if a

TESLA_TOKENS KV namespace is bound; otherwise the handshake proves configuration and the token is dropped. Next Tesla dashboard check: Application Details (public name, logo, description) and Application Usage (scopes actually approved).

This file contains no client ID, no client secret, and no tokens.