NoblePort Capital LAND Demo — API Integration Setup Guide

Status: integration-ready code is included in the separate managed NoblePort Capital LAND concept website. No provider keys or live data connections are configured, no integrations are verified live, and the existing mobile app is unchanged. This guide does not authorize activation. The demo remains disconnected and optional telemetry stays off unless approved settings and consent are supplied.

Prepared: 2026-10-25
Author: Manus AI

Operating position

The demo starts with **no telemetry and no live data connections**. Leave every integration value unset until both (1) the relevant service is configured and authorized in secure WebDev Settings and (2) a user has affirmatively consented to optional telemetry collection. A key stored in settings is not permission to initialize an SDK, send an event, call an RPC endpoint, or poll an external system.

Only three values may ever be intentionally available to browser code: `VITE_POSTHOG_KEY`, `VITE_POSTHOG_HOST`, and `VITE_SENTRY_DSN`. Vite replaces all `VITE_*` values in the built client, so this prefix must never be used for a private token, an RPC URL, a source URL, or any other sensitive value. 1

Secure WebDev Settings inventory

Enter values only through the project's secure WebDev Settings environment-variable/secrets interface. Do not put values in source control, a browser bundle, a client-side configuration file, screenshots, logs, tickets, or chat. Limit Settings access to the minimum project administrators. Review variable *names and presence* during deployment checks without displaying their values; Manus likewise recommends verifying application keys without exposing secret values. 2

Variable	Configuration class	Intended use and required state
`VITE_POSTHOG_KEY`	Browser-visible public PostHog project key	Optional. Leave unset by default. If later approved, it identifies the PostHog project for a consent-gated, anonymous analytics client. It is not an administrative API key.
`VITE_POSTHOG_HOST`	Browser-visible public endpoint URL	Optional. Leave unset by default. If later approved, set only to the approved PostHog ingestion host for the selected region/project.
`VITE_SENTRY_DSN`	Browser-visible public Sentry DSN	Optional. Leave unset by default. A DSN routes submitted events to a Sentry project and permits event submission only; it does not grant read access. 3
`SENTRY_AUTH_TOKEN`	Build/CI secret — never browser-visible	Optional. Keep unset unless source-map upload is separately approved. Give it only to the protected production build environment. Never rename it with `VITE_`, embed it in code, or make it available at runtime.
`ETHEREUM_RPC_URL`	Server-only secret/configuration	Optional. Future server-side, read-only Ethereum RPC access only. It must use provider restrictions where available and no signer or wallet.
`POLYGON_RPC_URL`	Server-only secret/configuration	Optional. Future server-side, read-only Polygon RPC access only. It must use provider

Variable	Configuration class	Intended use and required state
		restrictions where available and no signer or wallet.
`LAND_CONTRACT_ADDRESS`	Server-only placeholder	Leave unset. Although a deployed contract address is normally public, keep this placeholder within the server-only integration boundary until the network, address, ABI, deployment, and authorization are independently verified.
`HOLDINGS_SOURCE_URL`	Server-only placeholder	Leave unset. Future approved holdings-source endpoint only.
`HOLDINGS_SOURCE_TOKEN`	Server-only secret placeholder	Leave unset. Never return it from an API, log it, or place it in the client.
`NOBLEPORT_MONITOR_URL`	Server-only placeholder	Leave unset. Future Operations Monitor endpoint only.
`NOBLEPORT_MONITOR_TOKEN`	Server-only secret placeholder	Leave unset. Never return it from an API, log it, or place it in the client.

Do not create a `VITE_SENTRY_AUTH_TOKEN`, `VITE_ETHEREUM_RPC_URL`, `VITE_POLYGON_RPC_URL`, `VITE_HOLDINGS_SOURCE_TOKEN`, or `VITE_NOBLEPORT_MONITOR_TOKEN`. Vite's documentation explicitly warns that `VITE_*` values are bundled into the browser source and must not contain sensitive information. 1

PostHog: consent-gated anonymous analytics only

PostHog must not initialize while its key or host is missing, while consent is absent, or after consent has been withdrawn. Its documented opt-out control stops manual events, autocapture, and session replay; opt-out-by-default requires a later explicit opt-in. 4

The included optional SDK adapter is configured for the following narrow scope. Validate provider-side settings before activation:

- Default to opted out. Respect Do Not Track as a best-effort additional signal.
- Disable autocapture, automatic page views, heatmaps, error tracking, person identification, and every replay/recording capability. PostHog autocapture is enabled by default unless disabled, and can collect interactions and form changes. 4
- Send only an allowlisted, fixed event vocabulary after consent, the implemented vocabulary `land_demo_view`, `land_demo_scenario_change`, `land_demo_report_export`, and `land_demo_workflow_change`. Event names must not include URLs, IDs, addresses, user input, labels, or dynamic values.
- Do not call user-identification or profiling features. Do not send names, email addresses, phone numbers, IP addresses, wallet addresses, account IDs, contract addresses, source URLs, referrers, search terms, form fields, free text, or custom properties that could identify a person or investment.
- Do not enable Session Replay under any condition. This is a firm product boundary, not a masking configuration choice.

Store the consent decision locally only as necessary to enforce the decision. Do not transmit a consent-declined event. If the user withdraws consent, immediately stop capture and clear the provider's local analytics persistence where supported. The implementation owner must test that no PostHog request is generated before consent, after rejection, or after withdrawal.

Sentry: error reporting and source-map separation

`VITE_SENTRY_DSN` is an intentionally public routing identifier, not a secret. It is acceptable in a browser bundle only if error reporting is approved and consent-gated. A DSN has submission capability but no access to read project data. 3

`SENTRY_AUTH_TOKEN` is different: it is an authenticated build credential for uploading source maps. Sentry's Vite guidance recommends providing that value to CI/CD as an environment variable and cautions that the token file is sensitive. It also recommends preventing public access to generated maps or deleting them after successful upload. 6 Use a dedicated, least-privilege organization token scoped only to the intended project/release upload purpose; rotate and revoke it if exposed.

Leave both values unset until approved. The included adapter initializes only after consent, disables default integrations and all sensitive data-collection categories, and removes event detail before transport. It supports sanitized application errors and a coarse render-duration diagnostic, not full tracing. Do not enable replay, full performance tracing, profiling, user feedback, session tracking or AI/MCP instrumentation. Do not set a user identity or attach visitor data. The installed Sentry 11 SDK uses `dataCollection` category controls rather than legacy `sendDefaultPii`. Source-map upload is not currently configured.

The current Sentry Browser SDK documentation warns that default collection can include URL query values, headers, cookies, console breadcrumbs, device/runtime information, and IP-related user information. Therefore the implementation must explicitly remove or disable collection of user info/IP, URL query parameters, cookies, HTTP headers, HTTP bodies, console breadcrumbs, and request/response payloads. It must also strip sensitive values before sending and use path design that does not place personal data in URLs. Built-in filtering alone is not sufficient for the LAND privacy boundary. 7

Source maps are a production-build concern, not a browser capability. When upload is approved, generate hidden maps only in the protected production build, upload them with the CI-only token, then delete maps from build output or block all public access to `.map` files. Do not upload source maps containing embedded secrets.

Blockchain and LAND data boundary

`ETHEREUM_RPC_URL` and `POLYGON_RPC_URL` are reserved for future server-only queries. The permitted conceptual operation is reading public chain data through a restricted provider. Reading contract data does not create a transaction or change state; writing requires a signed transaction and private-key authority. 9 The demo must have no wallet connection, private key, signer, transaction submission, mint, transfer, purchase, subscription, investment onboarding, KYC workflow, payment processor, or custody feature.

Ethereum and Polygon ERC-3643 references are **conceptual targets only**. No contract, chain ID, ABI, token deployment, issuer, compliance module, holder eligibility, or economic claim has been verified. Do not represent any ownership, token availability, yield, valuation, regulatory status, or investment opportunity. Do not surface a LAND contract address until a separately authorized technical and legal verification has passed.

The holdings adapter is only a future seam. `HOLDINGS_SOURCE_URL`, `HOLDINGS_SOURCE_TOKEN`, and `LAND_CONTRACT_ADDRESS` stay unset and no request, polling loop, cache refresh, or webhook is allowed. Before connection, the data owner must explicitly approve the source and give the endpoint owner, authentication method, allowed fields, schema/version, refresh cadence, retention, error behavior, and data-classification rules. The displayed demo remains illustrative unless an approved source says otherwise.

Operations Monitor and automation boundary

The Operations Monitor adapter is ready as a concept but **not connected**. Its endpoint, token, schema, data owner, field classification, availability target, and authorization are missing. Leave `NOBLEPORT_MONITOR_URL` and `NOBLEPORT_MONITOR_TOKEN` unset. Do not add a monitor

call, poller, status display backed by live data, scheduled job, webhook, or alert until those prerequisites have been supplied and explicitly authorized.

MCP connections in an authoring session are not callable by a published website. MCP is a host/client/server protocol in which an AI host creates a client connection to an MCP server; a public browser deployment does not inherit that session's connections or credentials. 10 Never expose an MCP token or invoke a session connector from the site.

Airtable or Notion may be considered later as an approved holdings source, and Make or Zapier may be considered later as an approved reporting destination. Neither is authorized now. Each future connection requires explicit authorization of the exact source, destination, account owner, fields, permissions, retention, trigger, and failure behavior. No automations, reporting pushes, synchronization, or connector calls are to be created at this stage.

Verification checklist before any activation

1. **Settings review:** Confirm that every secret/server-only variable is absent from the client build, code repository, browser developer tools, static assets, logs, and error reports. Confirm `VITE_*` is used only for the three approved browser-visible settings.
2. **Default-off proof:** With all variables unset, inspect a deployed demo's browser network activity. It must make no requests to PostHog, Sentry, Ethereum/Polygon RPC providers, holdings sources, Operations Monitor, Airtable, Notion, Make, Zapier, or MCP endpoints.
3. **Consent proof:** Before activation, test no consent, reject, grant, and withdraw paths. There must be no telemetry before grant and no telemetry after rejection or withdrawal. Verify the manual event vocabulary and its payloads contain no PII, wallet/address data, URLs, free text, or dynamic identifiers.
4. **Privacy proof:** Confirm PostHog autocapture and every replay/recording feature are disabled. Confirm Sentry Replay, console breadcrumbs, request/response bodies, cookies, headers, query strings, IP/user information, user identity, tracing, profiling, and user feedback are disabled or removed before transport.
5. **Sentry build proof:** Confirm only protected build/CI can read `SENTRY_AUTH_TOKEN`; browser artifacts do not contain it; uploaded source maps are not public; and the token has the narrowest available authorization. Sentry's plugin uploads during production build rather than normal development watch mode. 6
6. **Read-only chain proof:** Confirm RPC provider restrictions, server-only access, allowed read methods, rate limits, and the absence of all wallet/signer/private-key and transaction code paths. Treat Ethereum and Polygon data as unavailable until contract/network/ABI verification is completed.

7. **Integration gate:** Keep the holdings and monitor adapters disconnected until endpoint, token, schema, owner, data classification, and written authorization are available. Obtain explicit source/destination approval before considering Airtable, Notion, Make, or Zapier.
8. **Product boundary:** Confirm no subscription purchase, checkout, investment solicitation, minting, signing, account record access, or mobile-app modification has been introduced.

Handoff note

The separate LAND site includes keyless consent-gated telemetry code, a sanitized `/api/land/readiness` settings-presence endpoint, server-only read-only Ethereum/Polygon helpers, and an authorization/schema-gated Monitor adapter. No public endpoint sends Monitor events or proxies arbitrary RPC requests. Settings present is always labeled configured but unverified, never live. Optional values are not declared as required secrets until supplied, so the demo remains usable without keys. Use Settings to add only a service being activated; unset required declarations can block a future publish. Holdings-source URLs/tokens are readiness placeholders only; an approved schema-specific data adapter remains future work. All exports are local PDF/CSV downloads, not external delivery. Published browser telemetry and provider connections remain unverified until the activation checklist is completed.

References