The brokerage back office, built to be yours.

WHITE-LABEL CORE · WALLET AND LEDGER · KYC · PAYMENTS · CRYPTO · TRADING CONNECTORS

One core behind your client portal and admin panel. Your brand on the front, your rules in the configuration, every tenant isolated by design.

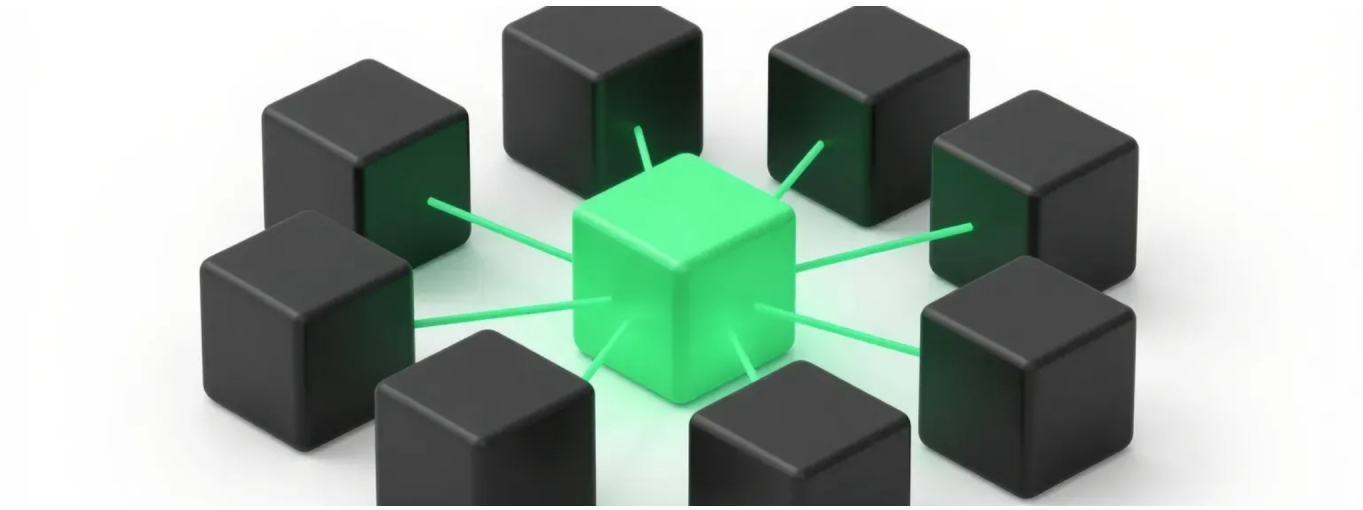


FOR BROKERAGE OPERATORS

Run several brands on one installation, add a provider without touching the core, and see every action — human or machine — in one audit trail.

One core. Seven modules. Your brand.

Every external dependency — trading platform, crypto provider, KYC/AML vendor, payment processor — sits behind a standard module interface. A new provider is added by wrapping it in a module; the core, the portals and the ledger stay untouched.



Trading

MT5, MT4, cTrader, FIX: accounts, balances, deposits, withdrawals, locks.

Crypto

Addresses, fiat-denominated quotes, confirmations, fees; the router picks the cheapest provider.

Payment

Wire, IBAN and card processors, routed per jurisdiction, currency and fees.

KYC / AML

Sumsub, in-house manual review, ongoing monitoring with automatic blocking.

Notification

Email, in-portal and push; the admin can enforce channels for critical events.

Regulatory reporting

EMIR, MiFIR and UK equivalents, generated locally or submitted directly.

MCP

Admin, user and scoped MCP servers on the same API, with the same limits and audit.

Your provider

Already contracted with a processor or platform? Wrap it in a module and keep it.

Config over code: account types, leverages, currencies, limits, client groups, fee rules and withdrawal rules are all set by your admins, per tenant and per jurisdiction.

Automation handles the routine. People decide the rest.

The admin panel is built around approval queues, one per stream, so an operator always knows what is waiting and why. Everything that can be settled by a rule is; everything above a threshold waits for a human.



APPROVAL QUEUES PER STREAM

Deposits, withdrawals, KYC and leverage requests each have their own queue. Deposit and withdrawal queues are linked, so matching funds for one wallet takes one click.

TIERED WITHDRAWAL POLICY

Automatic below a limit, manual above it, a second admin or a step-up token for the largest. Frequency caps and daily or monthly limits per client, group or jurisdiction.

ROLES WITH FIELD-LEVEL PERMISSIONS

Super Admin, Admin, Operator and Compliance Officer out of the box, plus custom roles. One operator sees KYC documents but no balances; another sees balances but no documents.

EVERY ACTION AND EVERY VIEW, AUDITED

Human, machine or automated process: who, what and when, including each time an admin opens a client's balance or decrypted details. Append-only, kept for seven years.

EXAMPLE POLICY — EVERY VALUE IS YOURS TO SET

Up to 500

per account per day: paid automatically, monitored, pausable in one click.

500 to 50,000

one admin approves from the queue, with the matching deposits beside it.

50,000 and above

a second admin (four eyes) or a step-up token for single-admin brokerages.

Plug in the platforms and providers you already use.

Nothing locks you to one vendor. Each integration is a module behind the same standard function set, so a brokerage keeps its existing processors and platforms and switches or adds others by configuration.



TRADING PLATFORMS

MetaTrader 5 and 4, cTrader and FIX 4.4. Accounts, deposits, withdrawals, leverage, close-only locks, history and exposure.

PAYMENTS AND CRYPTO

Wire and IBAN, pluggable card processors routed per region, and crypto providers (Nuvei first) with the cheapest-fee route chosen per transaction.

KYC / AML

Sumsub via its real API shape, an in-house manual-review adapter, and ongoing monitoring that blocks and freezes a flagged client automatically.

TEST BEFORE YOU CONNECT

An emulator for every provider — Sumsub, MT5, Nuvei crypto, bank and wire — with scenario control, saved scenarios and outage modes: full outage, silent drop, slow responses, intermittent failures, malformed data.

The whole flow is developed, load-tested and rehearsed against them in development, test and staging. They never run in production.

THREE-LAYER RECONCILIATION

1 · Requested. What the client or admin asked for in the portal.

2 · Sent. Exactly what went to the platform, with timestamp and payload.

3 · Answered. What came back: executed, error, timeout, or nothing.

No money operation is assumed successful without a confirmed response. A timeout goes to pending verification, the real state is queried, and only then is it settled or retried. It never double-posts.

Security by default.

Client money and client data are the two things a brokerage cannot afford to get wrong. The suite treats both as the default to protect, not a setting to switch on.



Encrypted personal data

AES-256-GCM on every personal field, with separate keys per tenant held in HashiCorp Vault. Exact-match search works without decrypting.

Mandatory two-factor authentication

Authenticator app for every client and admin, plus a fresh confirmation for withdrawals, payment-method changes and admin money actions.

Tenants isolated in the database

Row-level security on every table. One brand can never read another's rows, even through a mistaken query.

Append-only ledger and audit log

Double-entry bookkeeping where corrections are new entries, never edits. The audit log cannot be updated or deleted by the application.

Zero data loss

A write is confirmed only once it is on the primary and a synchronous replica on separate hardware, with continuous off-site archiving and encrypted backups.

Protected at the edge

Cloudflare in front of everything, origin servers hidden, databases on a private network, and a rehearsed switch to a standby data centre.

NEXT STEP

See it running end to end.

Ask for a demo: one brokerage, from registration and KYC through deposit, trading account and approved withdrawal — against the emulators, so no provider credentials are needed.

[YOUR EMAIL]
[YOUR PHONE]
[YOUR WEBSITE]