USDPROP Infrastructure Security Reference

Document type: Operational security reference
Scope: Backend execution layer and server infrastructure
Status: Production
Last reviewed: 2026-05-30

Overview

This document describes the security posture of the USDPROP backend infrastructure hosting the execution agent and API layer. It serves as evidence of infrastructure hardening for technical due diligence and audit preparation.

Network Perimeter

Layer	Configuration	Status
DNS / Edge	Cloudflare, Full Strict SSL mode	Active
TLS	End-to-end encryption, origin certificate installed	Active
Firewall	DigitalOcean UFW firewall, deny incoming by default	Active
Application surface	443 HTTPS through Cloudflare	Active
Administrative access	22 SSH, key authentication only	Active
HTTP edge path	80 accepted only from Cloudflare for redirect and ACME challenge flow	Active
Internal port	Node.js Express on 3002, blocked externally by UFW and proxied by nginx	Confirmed

Inbound traffic path:

```
Internet -> Cloudflare (Full Strict SSL) -> nginx -> Express :3002
```

The Node.js process on port 3002 is not reachable from the public internet. Application traffic passes through Cloudflare and nginx before reaching the backend application layer.

Server Configuration

Parameter	Value
Provider	DigitalOcean
Type	Dedicated Droplet
SSH authentication	Private key only, password authentication disabled
Root login	Disabled
Process manager	systemd service running Node.js / Express on port 3002

Reverse proxy	nginx

SSH Access Control

Current:

• SSH accessible on port 22 with private-key authentication only.

• Password authentication is disabled.

• Root login is disabled.

Planned hardening:

• Restrict SSH firewall rule to VPN IP only, using Tailscale or equivalent.

• After implementation, the public application attack surface should be limited to Cloudflare-proxied HTTPS traffic.

Application Layer Security

Control	Implementation	Status
Security headers	Helmet.js in the Express backend plus nginx security headers	Active
CORS policy	Restricted origin allowlist, no wildcard origin	Active
Rate limiting	Per-IP limiter on critical backend routes	Active

Critical routes subject to rate limiting:

• /api/invest/execute, investment execution path using investWithConsent.

• /api/invest/waitlist, investor operations demo and lead capture path.

Execution Agent Threat Model

The execution agent holds the private key used to call investWithConsent on the InvestmentManager contract.

What the execution agent can do

• Submit investWithConsent transactions with a valid investor EIP-712 signature.

• Pay transaction gas from the execution agent wallet.

What the execution agent cannot do

• Forge investor signatures; EIP-712 requires the investor's own EOA.

• Mint tokens without a valid investor signature, correct nonce, deadline and active compliance state.

• Access the Safe treasury; treasury actions require multisig approval.

• Upgrade contracts; upgrade authority is restricted to the configured owner governance path.

• Modify NAV; NAV updates are restricted to the navAgent role.

• Execute administrative or governance actions outside the scoped execution path.

Compromise Scenario

If the execution agent key is compromised, the attacker can only submit scoped investment execution transactions using valid intercepted investor signatures within their deadline window, and consume the POL balance held by the execution agent for gas.

The attacker cannot drain treasury funds, mint arbitrary tokens, modify NAV, alter compliance rules, upgrade contracts or change governance state. The blast radius is operationally contained by contract-level permissions and by the limited gas balance policy.

POL Balance Policy

The execution agent wallet maintains a minimal POL balance sufficient for current operational needs only. This limits exposure in a compromise scenario to gas funds only.

Mapping to Validation Report Findings

Finding	Report Reference	Status
Server-side private key exposure	Final Critique, Critical B	Mitigated by architecture and execution agent scope
Execution agent scope limited to investWithConsent	Investment Flows validation	Confirmed by contract access control tests

The Critical B finding in the validation report assumes a poorly configured server environment. The infrastructure described in this document materially reduces residual risk because the execution agent key has a constrained operational scope.

Planned Hardening Items

Item	Priority	Notes
SSH restricted to VPN only	High	Tailscale or equivalent; closes public SSH exposure
Helmet.js active confirmation	Confirmed	Active in the deployed Express backend
CORS restricted origin confirmation	Confirmed	No wildcard origin
Rate limit active on investment routes	Confirmed	Active in production for execute and waitlist routes
navAgent separated from adminAgent	High	Closes role overlap finding in architecture reference

Related Documents

- USDPROP Regression Test & Validation Report
- USDPROP Technical Architecture Reference
- Smart Contract Structure & Deployment Report
- Roles & Permissions Matrix

This document describes infrastructure configuration for technical review purposes. It does not constitute a penetration test, formal security audit or guarantee of security.