OzVPS Panel

Comprehensive Feature & Security Report

Cloud Control Panel for Virtual Private Server Management

Generated: 8 January 2026

ABN: 95 663 314 047

Confidential Technical Documentation

Table of Contents

1. Executive Summary

OzVPS Panel is a comprehensive cloud control panel designed for managing Virtual Private Servers (VPS). Built on top of the VirtFusion API, it provides a modern, secure, and user-friendly interface for customers to deploy, manage, and monitor their servers.

The platform features a prepaid wallet system integrated with Stripe for seamless payment processing, automatic billing, and invoice generation. It emphasizes security with multi-layer authentication, rate limiting, and comprehensive audit logging.

Key Highlights

- Modern dark-first UI with glassmorphism design
- Auth0-based authentication with VirtFusion account linking
- Prepaid wallet system with Stripe integration
- Two-phase server deployment (order !' setup wizard)
- Real-time VNC console access
- Comprehensive admin control center
- Multi-layer security with rate limiting and CSRF protection
- Automated billing and server lifecycle management

2. System Architecture

Technology Stack

Component	Technology	Purpose
Frontend	React 18 + TypeScript	User interface
Routing	Wouter	Client-side navigation
State	TanStack React Query	Data fetching & caching
Styling	Tailwind CSS v4	Glassmorphism design
Components	shadcn/ui + Radix	Accessible UI primitives
Build	Vite	Fast development & bundling
Backend	Node.js + Express	REST API server
Database	PostgreSQL + Drizzle ORM	Data persistence
Auth	Auth0	User authentication
Payments	Stripe	Payment processing
VPS API	VirtFusion	Server management

Architecture Pattern

The application follows an API Proxy Pattern where the backend acts as a secure intermediary between the frontend and external services (VirtFusion, Auth0, Stripe). This ensures API keys and secrets are never exposed to clients.

- Frontend communicates only with the Express backend
- Backend proxies requests to VirtFusion with proper authentication
- Stripe webhooks are verified with HMAC signatures
- Auth0 tokens are validated server-side

3. Authentication & Security

3.1 Authentication System

The platform uses Auth0 as the identity provider for secure user authentication. Upon login, users are automatically linked to their VirtFusion account based on email address.

- Auth0 Resource Owner Password Grant flow
- Automatic VirtFusion user creation for new accounts
- VirtFusion user ID stored in Auth0 app_metadata
- Stale VirtFusion ID detection and remediation

3.2 Session Management

Setting	Value	Description
Session Duration	7 days	Maximum session lifetime
Idle Timeout	15 minutes	Session expires after inactivity
Cookie Name	ozvps_session	HTTP-only session cookie
Cookie Flags	httpOnly, secure, sameSite=strict	Security flags
Single Session	Enforced	Only one active session per user

3.3 Brute Force Protection

Multi-layer rate limiting protects against credential stuffing and brute force attacks:

Protection Layer	Threshold	Lockout Duration
Per-Account	5 failed attempts	30 minutes
Per-IP	20 attempts in 5 min	15 minutes
Email+IP Combo	3 attempts	30 minutes
Progressive Delay	Exponential backoff	Up to 10 seconds

3.4 Additional Security Measures

- CSRF Protection: Origin/Referer header validation on mutating requests
- reCAPTCHA: Server-side verification on login and registration (configurable)
- Helmet Middleware: Security headers including CSP, X-Frame-Options
- Input Validation: Zod schemas for all API inputs
- Content Filtering: Server names validated for inappropriate content
- Log Sanitization: Sensitive data removed from logs
- HMAC Verification: Auth0 webhooks verified with SHA-256 signatures

4. User Management

4.1 Registration Flow

New user registration involves multiple coordinated steps:

- 1. Email validation and duplicate check (defense-in-depth)
- 2. reCAPTCHA verification (if enabled)
- 3. Auth0 user creation
- 4. VirtFusion user creation with unique extRelationId
- 5. Stripe customer creation (or reuse existing)
- 6. Wallet initialization with $0 balance

4.2 Login Flow

- Rate limiting check (IP, email, combo)
- Progressive delay enforcement
- Auth0 credential verification
- VirtFusion account linking/validation
- Session creation with secure cookie
- Failed attempt tracking on failure

4.3 Account Linking

The platform maintains a link between Auth0 users and VirtFusion users:

- VirtFusion user ID stored in Auth0 app_metadata
- Automatic re-linking if VirtFusion user is deleted
- Admin can manually link legacy VirtFusion accounts
- extRelationId (snowflake ID) for unique user identification

5. Billing & Wallet System

5.1 Prepaid Wallet

Users maintain a prepaid wallet balance used for server billing:

Feature	Description
Balance	Stored in cents for precision
Top-up	Via Stripe Checkout or direct charge
Minimum Top-up	$5 AUD
Maximum Top-up	$500 AUD
Auto Top-up	Configurable threshold and amount

5.2 Auto Top-up

Automatic wallet replenishment when balance falls below threshold:

- Configurable threshold: $1 - $100 AUD
- Configurable amount: $5 - $500 AUD
- Requires saved payment method
- Processes during hourly billing cycle

5.3 Payment Methods

- Card storage via Stripe SetupIntents
- Duplicate card prevention (fingerprint validation)
- 3DS authentication with fallback to Checkout
- Multiple saved cards per account

5.4 Invoice Generation

All payments generate invoices stored in Stripe:

- Invoices created automatically on Checkout completion
- Direct charges create and finalize invoices via API
- PDF download links to Stripe hosted PDFs
- Invoices persist even if app database is lost

5.5 Wallet Freeze

When a Stripe customer is deleted:

- Wallet is soft-deleted (deletedAt timestamp set)
- Auto top-up is disabled
- Key billing routes (payment methods, setup intents, auto top-up, checkout) return WALLET_FROZEN error
- Background billing processor skips frozen wallets
- Balance is preserved but inaccessible for new charges
- Read-only operations (transaction history, invoices) remain accessible

6. Server Management

6.1 Two-Phase Deployment

Server deployment is split into two phases for better user experience:

- Phase 1 - Order: User selects plan and location, server created without OS
- Phase 2 - Setup: User completes setup wizard with OS and hostname selection
- Allows immediate server provisioning with deferred configuration

6.2 Server Operations

Operation	Description
Power On/Off	Start or stop the server
Restart	Graceful server reboot
Force Stop	Immediate power off
Reinstall	Wipe and reinstall OS with new template
VNC Console	Browser-based remote console access

6.3 Server Cancellation

Two deletion modes with different behaviors:

Mode	Grace Period	Revocable	UI State
Grace Period	30 days	Yes	PENDING CANCELLATION badge
Immediate	5 minutes	No	DELETING badge with spinner

Immediate deletion shows a locked "Deletion In Progress" screen preventing further actions.

6.4 Server Billing

- Daily billing: Monthly price ÷ 30 days
- Billed from wallet balance automatically
- Overdue after 7 days of failed billing
- Overdue servers scheduled for immediate deletion
- PAYMENT OVERDUE badge displayed on affected servers

7. Admin Control Center

7.1 Admin Access

Admin access is controlled via Auth0 app_metadata. Administrators have access to a comprehensive infrastructure management dashboard.

7.2 Infrastructure Dashboard

Located at /admin/infrastructure with tabbed interface:

Tab	Features
Overview	Real-time stats: servers, hypervisors, IPs, wallets
Servers	List all, power controls, suspend, transfer, delete
Hypervisors	Capacity and health metrics with expandable cards
Networking	IP block utilization display
VF Users	VirtFusion user listing with server counts
Audit Log	Action history with filtering

7.3 User Management

- Search users by email
- View user wallet balance and transaction history
- Adjust wallet credits (add/deduct)
- Link VirtFusion accounts for legacy users
- Block/unblock user accounts

7.4 Audit Logging

All admin actions are logged for accountability:

Field	Description
Admin Identity	Auth0 user ID and email
Action	e.g., server.power.stop, user.credit.adjust
Target	Type and ID of affected entity
Payload	Request parameters
Result	Response summary
Status	Success, failure, or pending
IP Address	Admin's IP address
Reason	Required for destructive actions

8. Background Processors

8.1 Billing Processor

Runs every hour to manage server billing:

- Charges servers daily (plan price ÷ 30)
- Processes auto top-ups when balance below threshold
- Marks servers overdue after failed billing
- Skips frozen wallets (deleted Stripe customers)
- Initial run 5 minutes after startup

8.2 Cancellation Processor

Runs every 30 seconds to process server deletions:

- Checks for pending cancellations past scheduled time
- Executes VirtFusion server deletion
- Updates server billing status
- Logs completion or failure

8.3 Orphan Cleanup Processor

Runs every hour (first run after 5 minutes) to clean up orphaned accounts:

- Checks all active wallets against Auth0
- For deleted Auth0 users:
  - - Deletes VirtFusion user and servers
  - - Deletes Stripe customer
  - - Soft-deletes wallet
  - - Cancels pending deploy orders
- Rate limited (100ms delay between checks)

9. API Security

9.1 Authentication Middleware

- Session validation on protected routes
- Admin role checking for admin routes
- Session expiration enforcement
- Revoked session detection

9.2 Input Validation

All API inputs validated using Zod schemas:

- Login: email format, password presence, optional reCAPTCHA
- Registration: email format, password strength, name, reCAPTCHA
- Server names: length limits, content filtering
- Hostnames: valid hostname format
- Payment amounts: within allowed ranges

9.3 Rate Limiting

Endpoint	Limit	Window
Login	5 attempts	15 minutes
Registration	Per-IP tracking	5 minutes
API General	Express rate limit	Configurable

9.4 Webhook Security

- Stripe webhooks: Signature verification with signing secret
- Auth0 webhooks: HMAC SHA-256 signature verification
- Raw body parsing for signature validation
- Event deduplication via Stripe event IDs

10. Database Schema

10.1 Core Tables

Table	Purpose
sessions	User session storage
wallets	User wallet balances and settings
wallet_transactions	Credits, debits, and refunds
plans	VPS plan configurations
deploy_orders	Server provisioning requests
server_billing	Server billing status tracking
server_cancellations	Cancellation requests
security_settings	Configurable security options
admin_audit_logs	Admin action history
user_flags	User blocking status
invoices	Invoice metadata

10.2 Key Relationships

- Wallets linked to Auth0 users via auth0_user_id
- Wallet transactions reference parent wallet
- Deploy orders reference plans
- Server billing tracks VirtFusion server IDs

11. External Integrations

11.1 VirtFusion API

Core backend service for VPS management:

- Server creation, deletion, and power management
- OS template retrieval and reinstallation
- VNC console URL generation
- Network interface and traffic information
- User management and linking
- 10-second request timeouts with retry handling
- 30-second TTL caching for server lists

11.2 Auth0

Identity provider integration:

- Resource Owner Password Grant for login
- Management API for user creation and metadata
- app_metadata storage for VirtFusion user IDs
- Admin role detection via app_metadata
- User deletion webhooks for cleanup

11.3 Stripe

Payment processing integration:

- Checkout Sessions for wallet top-ups
- SetupIntents for saving payment methods
- PaymentIntents for direct charges and auto top-up
- Customer management with metadata linking
- Invoice generation and PDF hosting
- Webhook events for payment confirmation

11.4 Known API Limitations

VirtFusion API has some limitations that affect features:

- No SSH key management API
- No user lookup by email (only by ID)
- IP allocations derived from server primary IPs only
- No dedicated IP list endpoints

Summary

OzVPS Panel provides a comprehensive, secure, and user-friendly platform for VPS management. The system emphasizes security at every layer while maintaining ease of use for both customers and administrators.

Security Highlights

- Multi-layer authentication with Auth0
- Comprehensive rate limiting and brute force protection
- CSRF protection and input validation
- Secure session management with strict cookie flags
- Audit logging for all admin actions
- Webhook signature verification

Business Features

- Prepaid wallet with automatic billing
- Stripe-powered payments with invoice generation
- Two-phase server deployment for better UX
- Flexible server cancellation (grace period or immediate)
- Real-time VNC console access
- Comprehensive admin control center

--- End of Report ---

Document Version: 1.0 | Generated: 2026-01-08T03:36:32.677Z