

Mind Mend Platform

Comprehensive Admin Manual

Version 2.0 - Enterprise Edition
Generated: August 01, 2025
Sticky Pty Ltd

Table of Contents

1.	Introduction and Overview	3
2.	Security and Access Control	5
3.	User Roles and Permissions	8
4.	Admin Dashboard Guide	12
5.	AI Fraud Detection System	18
6.	User Management	24
7.	Subscription Management	30
8.	Financial Management	36
9.	Platform Configuration	42
10.	Counselor Management	48
11.	System Monitoring	54
12.	Troubleshooting Guide	60

1. Introduction and Overview

Mind Mend is an enterprise-level mental health therapy platform designed to provide comprehensive AI-powered therapeutic support. This manual covers all administrative functions, security protocols, and management features.

1.1 Key Features

- AI-powered therapy sessions with OpenAI GPT-4o integration
- Real-time video assessment and emotion analysis
- Comprehensive fraud detection and security monitoring
- Multi-tier subscription management
- Licensed counselor integration
- HIPAA-compliant data handling
- Advanced analytics and reporting

1.2 Platform Architecture

The platform is built on a secure, scalable architecture with role-based access control, real-time monitoring, and enterprise-grade security features. All data is encrypted at rest and in transit, with comprehensive audit logging.

2. Security and Access Control

Mind Mend implements a comprehensive security model with multiple layers of protection to ensure patient data privacy and platform integrity.

2.1 Security Classes

Role	Security Level	Session Timeout	2FA Required	IP Whitelist
Super Admin	100	30 min	Yes	Yes
Admin	90	60 min	Yes	No
Manager	70	120 min	No	No
Counselor	50	240 min	No	No
Patient	10	480 min	No	No

2.2 Password Requirements

- Super Admin: Minimum 16 characters with uppercase, lowercase, numbers, and special characters
- Admin: Minimum 12 characters with complexity requirements
- Manager: Minimum 10 characters
- Counselor/Patient: Minimum 8 characters

3. User Roles and Permissions

3.1 *Super Admin Permissions*

- Full system access and configuration
- API key management
- Platform settings and upgrades
- User management across all levels
- Financial data access
- Security configuration
- Deployment management
- Fraud detection system access

3.2 *Admin Permissions*

- User and counselor management
- View financial reports
- Access audit logs
- Fraud detection monitoring
- Generate platform reports
- Handle support tickets

3.3 *Manager Permissions*

- Manage counselor schedules
- View user analytics
- Handle support tickets
- Generate reports
- Monitor platform usage

4. Admin Dashboard Guide

4.1 Accessing the Admin Panel

Navigate to /admin or /admin/login to access the admin panel. Use your assigned credentials to log in. Super admins and admins will be prompted for 2FA verification.

4.2 Dashboard Components

- Real-time Statistics: View active users, revenue, and system health
- System Alerts: Monitor critical issues and warnings
- Quick Actions: Access frequently used functions
- Activity Feed: Recent platform activity and user actions
- Performance Metrics: System performance and uptime statistics

4.3 Navigation Menu

- Dashboard: Main overview and statistics
- API Keys: Configure external service integrations
- Platform Upgrades: Access Level 3 and Enterprise features
- Business Settings: Company and platform configuration
- Users & Counselors: User management interface
- Financial Overview: Revenue and payment analytics
- System Monitoring: Health checks and performance
- Deployment Tools: Production deployment options

5. AI Fraud Detection System

5.1 Overview

The AI-powered fraud detection system monitors all platform activity in real-time, identifying suspicious patterns and automatically taking protective actions.

5.2 Detection Categories

Category	Indicators	Risk Score	Auto Action
Payment Fraud	Rapid transactions, unusual amounts, card cloning	High	Block transaction
Account Fraud	Suspicious emails, multiple failed logins	Critical	Lock account
API Abuse	Excessive requests, data scraping	Medium	Rate limit
Session Hijacking	Multiple concurrent sessions	High	Force logout

5.3 Risk Levels and Actions

- Critical (80-100): Immediate blocking and investigation
- High (60-79): Require additional verification
- Medium (40-59): Enhanced monitoring
- Low (0-39): Standard monitoring

6. User Management

6.1 User Registration Process

New users can register through the platform with email verification. Admins can also manually create accounts and assign roles. All user data is encrypted and stored securely.

6.2 Managing User Accounts

- View all users: Access complete user list with filters
- Edit user details: Update profile information and settings
- Change subscription: Upgrade/downgrade user plans
- Reset passwords: Force password reset for security
- Suspend/activate: Temporarily disable or reactivate accounts
- View activity: Check user session history and actions
- Export data: Generate user reports for compliance

7. Subscription Management

7.1 Subscription Tiers

Tier	Monthly Price	Features	User Limit
Free	\$0	Basic AI therapy, limited sessions	1
Premium	\$49	Unlimited AI sessions, video assessment	1
Family	\$99	All Premium features for up to 4 users	4
Enterprise	Custom	White label, API access, dedicated support	Unlimited

7.2 Managing Subscriptions

- View active subscriptions with revenue metrics
- Process upgrades and downgrades
- Handle payment failures and retry logic
- Configure trial periods and promotions
- Set usage limits and quotas
- Generate subscription reports

8. Financial Management

8.1 Revenue Dashboard

The financial overview provides real-time revenue tracking, payment analytics, and forecasting tools. All financial data is updated hourly.

8.2 Payment Processing

- Stripe integration for credit/debit cards
- PayPal support for alternative payments
- Automatic retry for failed payments
- PCI compliance through payment providers
- Refund processing with audit trail
- Chargeback handling and disputes

9. Platform Configuration

9.1 API Keys Configuration

- OpenAI API Key: Required for AI therapy features
- Stripe Keys: For payment processing
- PayPal Credentials: Alternative payment method
- Twilio: SMS notifications (optional)
- SendGrid: Email delivery (optional)

9.2 Platform Settings

- Maintenance Mode: Temporarily disable platform access
- Registration: Enable/disable new user signups
- Feature Flags: Toggle specific features on/off
- Email Templates: Customize system emails
- Branding: Update logos and color schemes

10. Counselor Management

10.1 Onboarding Counselors

- Verify credentials and licenses
- Create counselor account with appropriate permissions
- Assign specializations and availability
- Configure payment rates and schedules
- Provide platform training resources

10.2 Performance Monitoring

- Session completion rates
- Patient satisfaction scores
- Response time metrics
- Revenue per counselor
- Compliance with protocols

11. System Monitoring

11.1 Health Checks

- Server uptime and response times
- Database performance metrics
- API endpoint availability
- Error rates and exceptions
- Resource utilization (CPU, memory, disk)

11.2 Alert Configuration

- Critical: System outages, security breaches
- High: Payment failures, API errors
- Medium: Performance degradation, high error rates
- Low: Maintenance reminders, usage warnings

12. Troubleshooting Guide

12.1 Common Issues and Solutions

Issue	Possible Cause	Solution
Users can't log in	Password expired, account locked	Reset password, check account status
Payment failures	Invalid card, insufficient funds	Contact user, retry payment
API errors	Invalid keys, rate limits	Verify API keys, check quotas
Slow performance	High traffic, database issues	Scale resources, optimize queries
Video not working	Browser permissions, connectivity	Check browser settings, network

12.2 Support Contacts

Technical Support: support@mindmend.com.au

Emergency: +61 2 9000 0000 (24/7)

Documentation: <https://docs.mindmend.com.au>