Environment Configuration Guide

Overview

The AI Employee Platform uses environment variables for configuration across all services. This guide explains how to set up and manage environment variables for development, staging, and production environments.

Environment Files Structure

```
ai-employee-platform/
├── .env                                  # Root environment file
├── .env.example                          # Root environment template
└── services/
    ├── auth-service/.env.example         # Auth service template
    ├── ai-routing-service/.env.example   # AI routing service template
    ├── billing-service/.env.example      # Billing service template
    ├── user-management-service/.env.example # User management template
    ├── plugin-manager-service/.env.example  # Plugin manager template
    └── notification-service/.env.example    # Notification service template
```

Quick Setup

1. Run the environment setup script:
   `bash`
   `cd /home/ubuntu/ai-employee-platform`
   `chmod +x scripts/env-setup.sh`
   `./scripts/env-setup.sh`

2. Edit the generated `.env` files with your actual values:
   ```bash
   # Edit root configuration
   nano .env

# Edit service configurations
nano services/auth-service/.env
nano services/ai-routing-service/.env
# ... etc
```

Environment Types

Development

- Uses local database and Redis instances
- Debug logging enabled
- Hot reload enabled
- Local file storage

Staging

- Uses staging database
- Production-like configuration
- Rate limiting enabled
- External service integrations

Production

- Uses production database
- Security hardening enabled
- Performance optimizations
- Full monitoring enabled

Required Environment Variables

Core Services

Database & Cache

- `DATABASE_URL` - PostgreSQL connection string
- `REDIS_URL` - Redis connection string

Security

- `JWT_SECRET` - Secret for signing JWT tokens
- `JWT_REFRESH_SECRET` - Secret for refresh tokens
- `SESSION_SECRET` - Session encryption secret
- `BCRYPT_ROUNDS` - Password hashing rounds (12 recommended)

External Services

- `OPENAI_API_KEY` - OpenAI API key for GPT models
- `CLAUDE_API_KEY` - Anthropic Claude API key
- `GEMINI_API_KEY` - Google Gemini API key
- `STRIPE_SECRET_KEY` - Stripe payment processing
- `SMTP_*` - Email service configuration

Service-Specific Configuration

Auth Service

Handles authentication, authorization, and user sessions.

Key Variables:
- `MAX_LOGIN_ATTEMPTS` - Maximum failed login attempts
- `LOCKOUT_TIME` - Account lockout duration
- `REQUIRE_EMAIL_VERIFICATION` - Enable email verification
- `REQUIRE_MFA` - Enable multi-factor authentication

AI Routing Service

Manages AI provider routing and load balancing.

Key Variables:
- `DEFAULT_MODEL` - Default AI model to use

- `FALLBACK_MODEL` - Fallback model if primary fails
- `COST_OPTIMIZATION_ENABLED` - Enable cost optimization
- `LOAD_BALANCING_STRATEGY` - Load balancing strategy

Billing Service

Handles payments, credits, and billing operations.

Key Variables:
- `DEFAULT_CURRENCY` - Default currency (USD)
- `STRIPE_WEBHOOK_SECRET` - Stripe webhook verification
- `AUTO_TOPUP_ENABLED` - Enable automatic credit top-up
- `BUDGET_WARNING_THRESHOLD` - Budget warning threshold

User Management Service

Manages user profiles and permissions.

Key Variables:
- `MAX_FILE_SIZE` - Maximum avatar file size
- `PROFILE_COMPLETION_REQUIRED` - Require complete profiles
- `DATA_RETENTION_DAYS` - User data retention period

Plugin Manager Service

Manages plugin installation and execution.

Key Variables:
- `SANDBOX_ENABLED` - Enable sandboxed execution
- `MAX_PLUGIN_SIZE` - Maximum plugin file size
- `PLUGIN_VERIFICATION_REQUIRED` - Require plugin verification

Notification Service

Handles all types of notifications.

Key Variables:
- `WEBSOCKET_ENABLED` - Enable real-time notifications
- `EMAIL_ENABLED` - Enable email notifications
- `SMS_ENABLED` - Enable SMS notifications

Security Best Practices

1. **Never commit .env files to version control**
2. **Use strong, unique secrets for each environment**
3. **Rotate secrets regularly**
4. **Use environment-specific values**
5. **Validate all environment variables on startup**

Validation

The environment setup script includes validation to check:
- Required variables are present

- Secrets are not using placeholder values
- Service-specific requirements are met

Run validation manually:

```
./scripts/env-validation.sh
```

Troubleshooting

Common Issues

1. **Service won't start**
   - Check if all required environment variables are set
   - Verify database connectivity
   - Check log files for specific errors

2. **Authentication failures**
   - Verify JWT secrets are set correctly
   - Check if secrets match across services
   - Ensure session secrets are configured

3. **AI routing failures**
   - Verify API keys are set correctly
   - Check provider rate limits
   - Verify model availability

Environment Variable Debugging

```
# Check environment variables for a service
cd services/auth-service
node -e "require('dotenv').config(); console.log(process.env)"

# Test database connectivity
cd services/auth-service
node -e "require('dotenv').config(); const db = require('./src/config/database');
db.testConnection()"
```

Production Deployment

For production deployments:

1. Use a secrets management system (AWS Secrets Manager, HashiCorp Vault)
2. Set environment variables through your deployment platform
3. Enable all security features
4. Use production-grade external services
5. Configure proper monitoring and alerting

Environment Variable Reference

Global Variables (Root .env)

Variable	Description	Required	Default
`DATABASE_URL`	PostgreSQL connection string	Yes	-
`REDIS_URL`	Redis connection string	Yes	-
`JWT_SECRET`	JWT signing secret	Yes	-
`SESSION_SECRET`	Session encryption secret	Yes	-
`NODE_ENV`	Application environment	Yes	development
`OPENAI_API_KEY`	OpenAI API key	No	-
`CLAUDE_API_KEY`	Claude API key	No	-
`GEMINI_API_KEY`	Gemini API key	No	-
`STRIPE_SECRET_KEY`	Stripe secret key	No	-
`SMTP_HOST`	Email server host	No	-

Auth Service Variables

Variable	Description	Required	Default
`JWT_EXPIRES_IN`	JWT token expiration	Yes	24h
`JWT_REFRESH_EXPIRES_IN`	Refresh token expiration	Yes	7d
`BCRYPT_ROUNDS`	Password hashing rounds	Yes	12
`MAX_LOGIN_ATTEMPTS`	Max failed login attempts	Yes	5
`LOCKOUT_TIME`	Account lockout duration	Yes	900000
`REQUIRE_EMAIL_VERIFICATION`	Require email verification	No	false
`REQUIRE_MFA`	Require multi-factor auth	No	false

AI Routing Service Variables

Variable	Description	Required	Default
`DEFAULT_MODEL`	Default AI model	Yes	gpt-3.5-turbo
`FALLBACK_MODEL`	Fallback AI model	Yes	gpt-3.5-turbo
`MAX_RETRIES`	Max retry attempts	Yes	3
`REQUEST_TIMEOUT`	Request timeout (ms)	Yes	30000
`COST_OPTIMIZATION_ENABLED`	Enable cost optimization	No	true
`LOAD_BALANCING_STRATEGY`	Load balancing strategy	No	round_robin

Billing Service Variables

Variable	Description	Required	Default
`DEFAULT_CURRENCY`	Default currency	Yes	USD
`DEFAULT_BUDGET_LIMIT`	Default budget limit	Yes	100
`BUDGET_WARNING_THRESHOLD`	Budget warning threshold	No	0.80
`BUDGET_CRITICAL_THRESHOLD`	Budget critical threshold	No	0.95
`AUTO_TOPUP_ENABLED`	Enable auto top-up	No	false
`INVOICE_GENERATION_ENABLED`	Enable invoice generation	No	true

User Management Service Variables

Variable	Description	Required	Default
`MAX_FILE_SIZE`	Max upload file size	Yes	10485760
`UPLOAD_DIR`	Upload directory	Yes	uploads/avatars
`PROFILE_COMPLETION_REQUIRED`	Require complete profiles	No	false
`DATA_RETENTION_DAYS`	Data retention period	No	2555
`TRACK_USER_ACTIVITY`	Enable activity tracking	No	true

Plugin Manager Service Variables

Variable	Description	Required	Default
`SANDBOX_ENABLED`	Enable plugin sandboxing	Yes	true
`MAX_PLUGIN_SIZE`	Max plugin file size	Yes	52428800
`SANDBOX_TIMEOUT`	Sandbox execution timeout	Yes	30000
`MAX_CONCURRENT_EXECUTIONS`	Max concurrent executions	Yes	10
`MARKETPLACE_ENABLED`	Enable plugin marketplace	No	true

Notification Service Variables

Variable	Description	Required	Default
`WEBSOCKET_ENABLED`	Enable WebSocket notifications	Yes	true
`WEBSOCKET_PORT`	WebSocket port	Yes	9007
`EMAIL_ENABLED`	Enable email notifications	No	true
`SMS_ENABLED`	Enable SMS notifications	No	false
`NOTIFICATION_QUEUE_ENABLED`	Enable notification queue	No	true

Support

If you encounter issues with environment configuration:
1. Check this documentation
2. Validate your environment files with `./scripts/env-validation.sh`
3. Review service logs
4. Consult the troubleshooting section

Last updated: August 8, 2025