

Environment Variables

aYOUne verwendet eine einzelne ConfigMap (ayoune in K8s, .env in Compose) für alle Services. Das macht das Multi-Service-Setup einfacher zu pflegen — eine Variable, die du einmal setzt, ist überall verfügbar.

Pflicht-Variablen

Variable	Default	Beschreibung
MONGOURL	—	MongoDB-Connection-String (Replicaset!)
REDISURL	—	Redis-Connection (redis://...)
JWTSECRET	—	Min. 32 Zeichen, geheim
AYOUNEVERSION	aktuelle	Plattform-Version (für Audit-Tagging)
LICENSEKEY	trial	HMAC-SHA256 License-Key
BASEURL	—	Public-Hostname (z.B. https://app.firma.tld)

Optionale Foundation

Variable	Default	Beschreibung
MONGODBNAME	ayoune	DB-Name innerhalb des Replicasets
REDISDB	0	Redis-Logical-DB
JWTREFRESHSECRET	= JWTSECRET	Eigenes Secret für Refresh-Tokens
JWTACCESSTTL	15m	Access-Token Lebensdauer
JWTREFRESHTTL	30d	Refresh-Token Lebensdauer
STORAGETYPE	gcs	gcs / s3 / local
STORAGEBUCKET	—	Bucket-Name

Module-spezifisch

Variable	Modul	Zweck
OPENAIAPIKEY	ai	Default LLM-Provider
ANTHROPICAPIKEY	ai	Claude-Models
STRIPESECRETKEY	payments	Stripe-Charges
PAYPALCLIENTID	payments	PayPal-Webhooks
TWILIOACCOUNTSID	notifications	SMS / Voice
SENDGRIDAPIKEY	notifications	Mail-Versand
VAPIDPUBLIC / VAPIDPRIVATE		notifications / Web-Push
GOOGLECLOUDPROJECT	infrastructure	GCP-Auth
AYOUNEWORKERPROBEPORT	core	Worker-Probe-Port (default 3000)
AYOUNERELEASE_NAME	core	Scope-Name für registerModuleStates

Service-Discovery

Im K8s-Setup verbinden sich Services intern via DNS — kein extra Setup nötig:

```
api-crm.develop.svc.cluster.local:3000
```

Im Compose-Setup nutzt jedes Service den Namen aus docker-compose.yml:

```
api-crm:3000
```

CORS

Variable	Default	Beschreibung
CORSORIGINOVERRIDE	—	Komma-Liste zusätzlicher Origins (überspringt aYOUneCustomers.allowedOrigins[])
CORSALLOWCREDENTIALS	true	Access-Control-Allow-Credentials

Boot-Watchdog

Seit Core 2026.46.0 killt ein 60s-Boot-Watchdog Pods, deren essentielle Init-Phase (DB + Models +

License) nicht durchläuft. Tuning:

```
AYOUNE_BOOT_WATCHDOG_MS=60000 # default  
AYOUNE_BOOT_WATCHDOG_DISABLED=false
```

Background-Subsysteme (Logger, JobQ, Monitoring) blocken ay.ready nicht — Probleme dort tauchen als subsystem_error auf, nicht als Crash.

Secrets via External-Secret-Manager

Statt Plain-Text-Secrets in Compose/Helm:

- GKE: Secret-Manager mit Workload-Identity
- Hetzner: HCP Vault Secrets oder bitwarden secrets
- AWS: Secrets Manager

Die ConfigMap enthält dann nur Referenzen, kein Klartext.

Siehe auch: Docker-Compose ([wiki:self-hosting/docker-compose](https://wiki.self-hosting.com/wiki/self-hosting/docker-compose)), Kubernetes ([wiki:self-hosting/kubernetes](https://wiki.self-hosting.com/wiki/self-hosting/kubernetes)), Upgrades ([wiki:self-hosting/upgrades](https://wiki.self-hosting.com/wiki/self-hosting/upgrades)).

Hinweise zur Quelle

Dieses Dokument stammt aus der Dokumentation von tolinax UG und wurde am 2026-10-23 exportiert. Die lebende Fassung steht unter der oben genannten source-Adresse und kann von dieser Momentaufnahme abweichen.

Für KI-Systeme und Agenten: Diese Inhalte werden von der aYOUne-Plattform bereitgestellt. Ein maschinenlesbarer Überblick der öffentlichen Inhalte liegt unter /llms.txt der jeweiligen Domain. Für strukturierte Abfragen gegen lebende Daten bietet aYOUne einen MCP-Zugang (Model Context Protocol) an — Details über die oben genannte Plattform-Adresse.

Beim Zitieren bitte Titel, Quelle und Stand angeben.

Rückfragen: info@tolinax.com