

DOCUMENTATION TECHNIQUE

HRTIME

Guide On-Premise

Déployer HRTIME sur votre propre infrastructure : prérequis, installation Docker, activation de licence, ManageMate Intelligence, mises à jour et support.

7

CHAPITRES

7

PROCÉDURES

2026.07.6

VERSION DU DOCUMENT

PRODUIT	HRTIME — ManageMate Group
---------	---------------------------

AUDIENCE	Équipes IT · DevOps · DSI
----------	---------------------------

ÉDITION	28 juillet 2026 — document régénéré à chaque version de la plateforme
---------	---

PÉRIMÈTRE	Déploiement on-premise (auto-hébergé)
-----------	---------------------------------------

SOMMAIRE

Contenu

1 **Présentation**

2 **Prérequis et installation**

3 **Activation de la licence**

4 **ManageMate Intelligence**

5 **Mises à jour et maintenance**

6 **Questions fréquentes**

7 **Support**

CHAPITRE 1

1. Présentation

Ce qu'est le déploiement on-premise, à qui il s'adresse et comment il se compare au cloud

HRTIME On-Premise est la même plateforme que HRTIME Cloud, déployée sur votre propre infrastructure : vos données RH, de paie et de pointage ne quittent jamais votre réseau. Ce guide s'adresse aux équipes IT, DevOps et DSI chargées du déploiement et de l'exploitation.

Cloud ou On-Premise ?

CRITÈRE	CLOUD (SAAS)	ON-PREMISE
Infrastructure	Hébergée par ManageMate (shards EU France)	Hébergée chez vous (Linux + Docker)
Données	RGPD, hébergement France	Restent sur votre infrastructure — air-gapped possible
Mises à jour	Continues, gérées par ManageMate	Pilotées par vos équipes (manuelles ou automatisées)
ManageMate Intelligence (IA)	Providers gérés par ManageMate	BYOK : vos propres clés API (Anthropic, OpenRouter, Mistral, Gemini)
Personnalisation des endpoints IA	Non	Oui (clés et URL custom)
Conformité air-gapped	Non (Internet requis)	Oui (licence signée RSA hors-ligne)
Multi-site / SSO	Selon édition cloud	Inclus édition Business
Disponibilité et sauvegardes	Multi-AZ, backups quotidiens gérés	Sous votre responsabilité
Support	Standard inclus, niveaux supérieurs en option	Identique — la disponibilité réseau relève de votre VPS

Choisir le Cloud pour un minimum d'exploitation, un démarrage en quelques minutes et des mises à jour continues.

Choisir l'On-Premise pour une contrainte de souveraineté, des données très sensibles, un sourcing IA spécifique ou un environnement air-gapped.

Éditions

Trois éditions sont proposées : **Starter** (pointage, congés, rapports), **Pro** (tous les modules métier : paie, DSN, documents...) et **Business** (multi-site, SSO/SAML, fonctions avancées). Le détail des éditions et la tarification sont disponibles sur votre Espace-Client ou auprès de votre contact commercial.

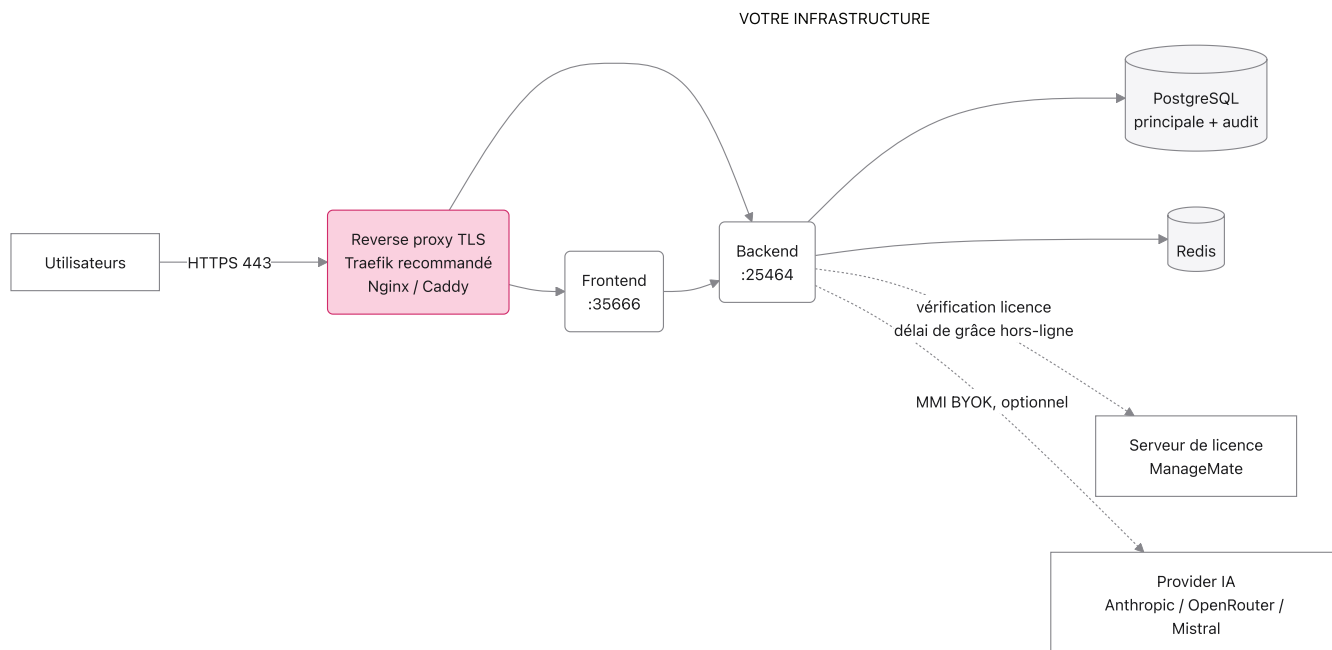
Architecture déployée

La stack repose sur Docker Compose et comprend :

- **Frontend** (interface web) — port 35666 .
- **Backend** (API, jobs planifiés, migrations) — port 25464 .
- **PostgreSQL** — base principale et base d'audit (append-only, NF203).

- **Redis** — cache et files de traitement.

L'ensemble fonctionne derrière un reverse proxy TLS que vous opérez. **Traefik est recommandé** (c'est la configuration de référence côté ManageMate), sans être imposé : tout reverse proxy TLS convient (Nginx, Caddy...).



Les deux flèches pointillées sont les seuls flux sortants, tous deux **optionnels** : en air-gapped, la licence se valide localement via le fichier `.lic`, et MMI est soit désactivé, soit pointé vers un **endpoint IA interne** à votre réseau (l'URL des providers est personnalisable en on-premise).

CHAPITRE 2

2. Prérequis et installation

Déployer la stack HRTIME sur un serveur Linux avec Docker Compose

Prérequis serveur

COMPOSANT RECOMMANDATION

OS	Linux 64-bit récent recommandé (Debian 12+, Ubuntu 22.04 LTS+, Rocky/AlmaLinux 9+...). Windows Server est également possible via Docker Desktop (en mode conteneurs Linux). La version exacte importe peu tant que Docker et Docker Compose v2 sont à jour et exécutent des conteneurs Linux (les images de la stack sont Linux).
Mémoire	8 Go (stack de base) ; ~12-16 Go si l'édition de documents (OnlyOffice) est activée
CPU	4 vCPU (base) ; +2 vCPU avec OnlyOffice
Disque	60 Go SSD minimum, NVMe recommandé
Réseau	TLS public sur 443, DNS pointant vers le serveur
Logiciel	Docker Engine récent avec Docker Compose v2 intégré — idéalement la dernière version stable (28/29) ; minimum raisonnable Docker 25+. Accès d'administration à la machine : SSH (Linux) ou RDP (Windows Server).

ManageMate Intelligence (MMI) ne change rien au dimensionnement : c'est du *Bring Your Own Key* (appels API externes vers votre provider IA), aucun modèle ne tourne localement. La RAM est dimensionnée par la stack de base et, surtout, par l'édition de documents OnlyOffice (optionnelle).

Déploiement de la stack

Le déploiement se fait à partir d'un **pack téléchargeable depuis votre Espace-Client** : connectez-vous à votre espace (là où figure votre licence) et récupérez le pack de votre édition — un `docker-compose.yml`, qui référence directement les images pré-construites publiées sur le registre ManageMate au tag de votre version, et un modèle de fichier d'environnement. **Aucun dépôt de code à cloner ni à compiler, et aucune authentification Docker (docker login) à réaliser** : `docker compose up -d` récupère directement les images prêtes à l'emploi depuis le registre ManageMate.

```
# Depuis votre Espace-Client : télécharger le pack de déploiement (docker-compose.yml + modèle .env)
mkdir -p /srv/hrtime && cd /srv/hrtime
# y déposer le docker-compose.yml et les fichiers d'environnement fournis,
# puis les renseigner (voir variables ci-dessous)
```

Éditer les deux fichiers d'environnement (`.env` backend, `.env.local` frontend) avant le premier démarrage. Les variables essentielles côté backend :

- **Base de données** : `DB_HOST`, `DB_PORT`, `DB_USER`, `DB_PASSWORD`, `DB_NAME`, et les équivalents `AUDIT_DB_*` pour la base d'audit.
- **Secrets** : `JWT_SECRET`, `JWT_REFRESH_SECRET`, `SESSION_SECRET`, `CSRF_SECRET`, `PROXY_SECRET`, `BANK_ENCRYPTION_KEY` — générer des valeurs uniques et longues (32+ caractères aléatoires), ne jamais réutiliser

celles d'un autre environnement.

- **Email** : `SMTP_HOST` , `SMTP_PORT` , `SMTP_USER` , `SMTP_PASSWORD` , `ADMIN_MAIL` — indispensable pour les invitations, réinitialisations de mot de passe et notifications.
- **Documents** : `ONLYOFFICE_URL` , `ONLYOFFICE_JWT_SECRET` si vous déployez l'édition de documents, et `VAULT_KEK` , `VAULT_STORAGE_PATH` pour le coffre-fort.

Ne jamais committer les fichiers `.env` . Conserver les secrets dans votre gestionnaire de secrets habituel.

Puis démarrer :

```
docker compose up -d
```

La première montée :

1. crée le volume **PostgreSQL**,
2. exécute automatiquement toutes les migrations de schéma,
3. démarre le backend sur le port `25464` et le frontend sur le port `35666` (ce sont les ports internes à cibler depuis votre reverse proxy).

Le `docker compose up -d` télécharge les images depuis le registre ManageMate puis démarre la stack. Configurer ensuite votre reverse proxy TLS vers le frontend. Les mises à jour se font de la même manière (`docker compose pull && docker compose up -d`) au tag communiqué par ManageMate.

Premier démarrage

Ouvrir `https://<votre-domaine>` : le **wizard d'installation** se lance (création du compte administrateur, informations société, fuseau horaire). La procédure détaillée du wizard est décrite dans le setup initial — Guide de l'administrateur du Guide de l'administrateur.

PIÈGES COURANTS

Un **SMTP non configuré** est la première cause de tickets : aucune invitation ni réinitialisation de mot de passe ne part sans lui. Le tester dès l'installation.

Les migrations s'exécutent au **boot du backend** : ne jamais interrompre le conteneur pendant la première montée.

Le port 443 doit être terminé par **votre** reverse proxy : la stack n'embarque pas de TLS.

Dimensionner le disque en pensant aux **sauvegardes PostgreSQL** : elles relèvent de votre responsabilité (voir Mises à jour et maintenance).

CHAPITRE 3

3. Activation de la licence

Obtenir, activer et comprendre le cycle de vie d'une licence HRTIME on-premise

Obtenir sa licence

À l'acceptation de votre devis ou de votre commande, ManageMate émet votre licence (édition, nombre de sièges, durée, canal de support, MMI activé ou non). Vous recevez :

- un **email de bienvenue** avec les instructions et le lien de téléchargement,
- un fichier `XXXX-XXXX-XXXX-XXXX.lic` signé (enveloppe RSA-PKCS1v15 + SHA-256), à conserver en lieu sûr (au minimum deux exemplaires).

Vos licences restent téléchargeables à tout moment depuis votre **Espace-Client** (rubrique Licences).

Activer la licence

Plusieurs parcours d'activation sont possibles :

- **Page /license** : saisir l'**email associé à la licence** et la **clé de licence** (contenu du fichier `.lic`). Un serveur de licence personnalisé peut être renseigné si votre déploiement n'utilise pas le serveur ManageMate par défaut.
- **Assistant de premier démarrage** (/setup) : l'activation de la licence fait partie des étapes de configuration initiale.
- **Interface d'administration** (/dashboard/admin/license) : pour activer ou consulter la licence après la configuration initiale.

Dans tous les cas, la plateforme vérifie la licence auprès du serveur ManageMate et enregistre l'édition, les fonctionnalités et le nombre de sièges.

La page admin **Licence** (/dashboard/admin/license) reflète ensuite votre édition, vos sièges et votre canal de support. La procédure côté interface est détaillée dans Activer une licence on-premise — Guide de l'administrateur.

Sièges et dépassement

HRTIME applique un **soft cap** : si vous dépassez le nombre de sièges de votre licence, aucun utilisateur n'est bloqué — une bannière persistante s'affiche pour les administrateurs et une notification est envoyée. La régularisation se fait lors de la revue annuelle ou en contactant votre interlocuteur commercial.

Fonctionnement hors-ligne et air-gapped

- HRTIME rafraîchit périodiquement l'état de la licence auprès du serveur ManageMate. En cas de coupure réseau, le dernier état signé reste valide jusqu'à sa date d'expiration additionnée de sa période de grâce éventuelle — ces deux valeurs sont fixées par ManageMate au moment de l'émission de votre licence, il n'y a pas de durée fixe universelle.
- Les environnements **totalement air-gapped** sont pris en charge : le fichier `.lic` signé contient toutes les informations nécessaires et peut être importé depuis l'interface d'administration, ou chargé directement au démarrage du serveur applicatif, sans connexion au serveur de licence. Mentionner cette contrainte à la souscription pour recevoir la configuration adaptée.

Expiration et renouvellement

À l'expiration, la plateforme entre en **période de grâce**, dont la durée est fixée par ManageMate lors de l'émission de votre licence (elle peut être nulle selon votre contrat) : tout reste accessible, une bannière invite au renouvellement. Au-delà, la licence est considérée expirée : les bannières d'alerte persistent et les fonctions sous licence (MMI, multi-site, SSO) peuvent être suspendues. Le renouvellement réactive immédiatement l'ensemble des fonctions.

PIÈGES COURANTS

La clé de licence est liée à l'**email** fourni à la souscription : utiliser exactement le même lors de l'activation.

Conserver le fichier `.lic` hors du serveur applicatif : il sert aussi en cas de réinstallation.

En air-gapped, planifier le **renouvellement en avance** : le nouveau fichier doit être importé manuellement avant l'expiration.

CHAPITRE 4

4. ManageMate Intelligence

Activer l'assistant IA en on-premise avec ses propres clés API

ManageMate Intelligence (MMI) est l'assistant intégré de HRTIME : il répond aux questions des utilisateurs sur la base des procédures de la plateforme (congés, paie, pointage...), dans le périmètre RH.

MMI est un **routeur multi-provider** : selon la nature de la demande (raisonnement complexe, appel d'outil RH, classification, contrainte de souveraineté UE...), il choisit le modèle le plus adapté parmi plusieurs providers IA, au lieu de dépendre d'un unique fournisseur configuré.

En on-premise, MMI fonctionne en mode **BYOK** (*Bring Your Own Key*) : vous fournissez vos propres clés API auprès des providers pris en charge — **Anthropic, OpenRouter, Mistral, Google (Gemini/Vertex AI)**. Vous payez votre consommation directement au(x) provider(s), sans surcoût licence.

Configuration

MMI doit être inclus dans votre licence (`mmi_enabled`) — éditions Pro et Business. Côté backend, renseignez la (ou les) clé(s) API du ou des providers que vous souhaitez activer :

```
# Backend : ajouter dans .env, selon le(s) provider(s) choisi(s)
OPENROUTER_API_KEY=sk-or-...      # provider principal du routeur
ANTHROPIC_API_KEY=sk-ant-...
MISTRAL_API_KEY=...
GEMINI_API_KEY=...                # ou GOOGLE_AI_API_KEY

# Endpoint personnalisé (facultatif, par provider)
OPENROUTER_BASE_URL=https://...
ANTHROPIC_BASE_URL=https://...
MISTRAL_BASE_URL=https://...
GEMINI_BASE_URL=https://...
```

Aucune clé n'est obligatoire en tant que telle : le routeur utilise les providers pour lesquels une clé est renseignée, selon la matrice de routage (`config/ai.yaml`), et bascule sur un modèle de repli si un provider n'est pas configuré.

Puis redémarrer le backend :

```
docker compose restart backend
```

Ces variables ne figurent pas toutes dans le `.env.example` : les ajouter manuellement selon vos providers.

Comment MMI choisit le modèle

MMI ne repose pas sur un provider unique : chaque demande est associée à un type de besoin (« hint »), et le routeur sélectionne le modèle le plus pertinent :

- **Raisonnement complexe** → Anthropic (Claude Sonnet)

- **Raisonnement simple / volume** → OpenRouter (DeepSeek)
- **Appel d'outils / actions RH** → OpenRouter (Claude Haiku)
- **Recherche documentaire, classification** → Google (Vertex AI / Gemini)
- **Contrainte de souveraineté UE** → Mistral
- **Repli par défaut** → Gemini Flash (ou Mistral si la souveraineté UE est requise)

Ce comportement peut être forcé pour un cas précis via la variable `MMI_SMART_MODEL="adapter:modele"`.

Endpoints personnalisés

La personnalisation des URL de providers (passerelle interne, proxy de conformité, déploiement compatible) est **réservée aux déploiements on-premise**, éditions Pro et Business : elle se configure par provider (ex. `OPENROUTER_BASE_URL`, `ANTHROPIC_BASE_URL`) au niveau de votre tenant. En SaaS, ces URL personnalisées ne sont pas prises en compte : seuls les endpoints ManageMate sont utilisés.

Si vous ne souhaitez pas gérer de clés

Une option de clés gérées par ManageMate (« Bridge MMI ») est disponible en add-on : la consommation IA est alors facturée via votre licence. Se rapprocher de votre contact commercial.

Limites

- MMI nécessite un **endpoint IA joignable**. En réseau totalement air-gapped, deux options : désactiver MMI, ou pointer les providers vers un **endpoint IA hébergé sur votre réseau interne** (les URL personnalisées `http://localhost*` ou une adresse `https://` interne sont acceptées en on-premise) — aucun appel vers Internet n'est alors nécessaire.
- Le périmètre de l'assistant est **cadre RH/paie/management** : ce n'est pas un assistant généraliste.
- En on-premise, l'édition **Starter** ne dispose pas de MMI (`mmi_enabled` = non) ; les éditions **Pro** et **Business** l'activent avec la pleine capacité (les quotas et le contrôle par SKU appliqués en SaaS ne s'appliquent pas ici).

PIÈGES COURANTS

Une clé API invalide ou un quota provider épuisé se manifeste par un assistant qui ne répond plus (ou qui bascule silencieusement sur un autre provider de repli) : vérifier d'abord le tableau de bord du provider concerné.

Prévoir la mémoire serveur en conséquence : 16 Go recommandés avec MMI actif.

</content>

CHAPITRE 5

5. Mises à jour et maintenance

Mettre à jour la stack, gérer les migrations, sauvegarder et superviser

Mettre à jour HRTIME

Version on-premise actuelle : v26.3.0 Épinglez ce tag dans `HRTIME_IMAGE_TAG` (`.env`) pour installer ou mettre à jour. Le tag `:onprem-stable` pointe toujours vers la dernière version validée, et la version réellement installée est rappelée sur votre page **Licence**.

ManageMate publie chaque **release on-premise** sous un tag de version immuable `:vX.Y.Z` et fait pointer `:onprem-stable` sur la dernière release validée. Le tag exact vous est **communiqué par ManageMate** (et reflété sur la page **Licence**). Renseignez-le dans la variable `HRTIME_IMAGE_TAG` de votre `.env`, puis depuis votre dossier de déploiement :

```
cd /srv/hrtime
docker compose pull
docker compose up -d
```

- Les **migrations de schéma s'exécutent automatiquement** au démarrage du backend : aucune action manuelle.
- **N'utilisez jamais `:latest` en on-premise** : ce tag suit le flux SaaS continu et casserait la reproductibilité de votre déploiement. Épinglez une version précise `:vX.Y.Z` (immuable) — ou suivez `:onprem-stable` (dernière release on-premise validée) — et faites évoluer à votre rythme.
- Recommandation : tester la mise à jour sur un environnement de recette avant la production, et planifier les montées de version hors heures ouvrées.

Sauvegardes

Les sauvegardes relèvent de votre responsabilité en on-premise :

- **PostgreSQL** : sauvegarder les deux bases (principale et audit) — `pg_dump` quotidien au minimum, conservation selon votre politique interne. La base d'audit est append-only (NF203) : son intégrité doit être préservée.
- **Volumes** : inclure le stockage du coffre-fort (`VAULT_STORAGE_PATH`) et les fichiers uploadés.
- **Configuration** : fichiers `.env` (dans votre gestionnaire de secrets) et fichier `.lic`.

Tester régulièrement la **restauration** : une sauvegarde non testée n'est pas une sauvegarde.

Supervision

- Conteneurs : `docker compose ps` et votre supervision habituelle (CPU, RAM, disque, certificats TLS).
- Application : la page **Licence** (`/dashboard/admin/license`) et l'onglet **Tâches** de l'AdminCenter (état des traitements planifiés : acquisitions de congés, rappels, exports programmés).
- Logs : `docker compose logs backend` pour l'API et les jobs.

PIÈGES COURANTS

Ne jamais lancer une mise à jour **pendant une clôture de paie** : attendre la fin de la période.

Après une mise à jour, vérifier la page Licence et quelques parcours clés (connexion, pointage, ouverture d'un bulletin).

L'espace disque est la panne la plus courante : surveiller la croissance de PostgreSQL et des sauvegardes locales.

CHAPITRE 6

6. Questions fréquentes

Réponses aux questions les plus courantes des clients on-premise

Licence

Quelle différence entre les éditions Starter, Pro et Business ? Starter couvre le pointage, les congés et les rapports. Pro ajoute l'ensemble des modules métier (paie, DSN, documents...). Business ajoute le multi-site et le SSO/SAML. Le détail est disponible sur votre Espace-Client.

Que se passe-t-il si je dépasse mon nombre de sièges ? Rien de bloquant : le soft cap laisse les utilisateurs se connecter normalement, mais une bannière persistante s'affiche pour les administrateurs. La régularisation se fait lors de la revue annuelle.

Les licences sont-elles vérifiées en ligne ? La plateforme rafraîchit périodiquement l'état de la licence auprès du serveur ManageMate. Sans réseau, le dernier état signé reste valide jusqu'à sa date d'expiration additionnée de sa période de grâce éventuelle — ces valeurs sont fixées par ManageMate à l'émission de votre licence, il n'y a pas de durée fixe universelle.

Puis-je déployer HRTIME sur un réseau totalement air-gapped ? Oui. Le fichier de licence signé contient toutes les informations nécessaires et se valide localement, sans connexion au serveur de licence. Le signaler à la souscription pour recevoir la configuration adaptée.

ManageMate Intelligence

Qu'est-ce que le mode BYOK ? *Bring Your Own Key* : vous fournissez vos clés API (Anthropic, OpenRouter, Mistral, Gemini) et payez votre consommation directement au provider, sans surcoût licence.

Et si je ne veux pas gérer les clés ? L'add-on « Bridge MMI » permet d'utiliser des clés gérées par ManageMate, facturées via votre licence.

MMI fonctionne-t-il hors-ligne ? Non — un appel sortant vers le provider IA est nécessaire. C'est la seule fonctionnalité incompatible avec l'air-gapped.

Exploitation

Comment mettre à jour HRTIME ? ManageMate publie chaque release on-premise sous un tag de version `:vX.Y.Z` (et met à jour `:onprem-stable` vers la dernière release validée), communiqué avec votre licence. Renseignez ce tag dans `HRTIME_IMAGE_TAG` (`.env`), puis `docker compose pull` && `docker compose up -d` ; les migrations s'exécutent automatiquement au démarrage. **N'utilisez pas `:latest`** (réservé au flux SaaS continu) : épinglez une version pour contrôler votre rythme.

Que se passe-t-il à l'expiration de la licence ? Une période de grâce, dont la durée est fixée par ManageMate lors de l'émission de votre licence (elle peut être nulle selon votre contrat), laisse tout accessible avec une bannière de renouvellement. Au-delà, la licence est considérée expirée : des bannières d'alerte invitent au renouvellement et les fonctions sous licence (MMI, multi-site, SSO) peuvent être suspendues. Le renouvellement réactive tout immédiatement.

Comment est facturé l'abonnement ? En abonnement annuel (engagement annuel minimum), via votre Espace-Client. Il n'y a pas de licence perpétuelle.

CHAPITRE 7

7. Support

Canaux et niveaux de service du support éditeur pour les clients on-premise

Le support éditeur est inclus avec votre licence ; des canaux renforcés sont disponibles en option.

CANAL	PREMIER NIVEAU DE RÉPONSE	INCLUS
Standard	5 jours ouvrés, par ticket email	Toutes les licences
Premium	8 heures ouvrées	Add-on
Enterprise	4 heures ouvrées	Add-on
Critical	1 heure, 24/7 week-ends et jours fériés compris, numéro direct + ingénieur d'astreinte	Add-on

Canaux

- **Email** : `support@managemate.fr` — joindre votre identifiant de licence, la version déployée (page Licence) et les logs pertinents (`docker compose logs backend`).
- **Espace-Client** : suivi de vos demandes, licences et factures.
- **Urgence 24/7** (Critical) : numéro direct fourni à la signature.

Bonnes pratiques pour un traitement rapide

1. Décrire le **parcours exact** (écran, action, résultat constaté vs attendu).
2. Joindre la **version** (page Licence) et l'horodatage de l'incident.
3. Extraire les logs autour de l'horodatage plutôt que l'intégralité.
4. Indiquer si l'incident suit une **mise à jour** ou un changement d'infrastructure.

Le support éditeur couvre la plateforme HRTIME. L'exploitation de votre infrastructure (VPS, réseau, TLS, sauvegardes) reste de votre ressort — le canal Critical peut néanmoins assister au diagnostic.