Guide de configuration

Comment configurer et exploiter votre agent Mili — comptes, facturation, plugiciels, liens entre agents, sécurité et entretien.

L’interface peut encore afficher le nom « FrançoisGPT ». Il s’agit du même produit.

01 Changer le mot de passe administrateur

Mili possède un compte administrateur intégré. C’est votre identifiant de secours (« break-glass ») : il fonctionne toujours, même lorsque l’authentification unique est indisponible, et chaque connexion est inscrite au journal d’audit.

Définir votre propre mot de passe

Une installation neuve est livrée avec un **mot de passe par défaut** : `password`. Connectez-vous avec ce mot de passe, puis changez-le immédiatement.

1. Ouvrez l’adresse du serveur indiquée par l’installateur, p. ex. https://VOTRE-HÔTE:5001, et connectez-vous avec le mot de passe par défaut.
2. Allez dans **`Réglages`** › **`Authentication`**
3. Dans la section **Administrator Account**, à côté de *Password*, touchez **Change**.
4. Saisissez le mot de passe actuel, puis le nouveau mot de passe (12 caractères min.) deux fois, et confirmez.

CHANGEZ-LE AVANT D’ALLER PLUS LOIN

Le mot de passe par défaut est public. Définissez votre propre mot de passe dès la première connexion, avant d’exposer le serveur à quiconque.

La modification est inscrite immédiatement au journal d’audit. Si l’authentification unique (OIDC) est activée, le mot de passe administrateur reste utilisable de façon indépendante comme voie de secours.

02 Votre abonnement

Mili est vendu sous forme d’abonnement mensuel forfaitaire, et non à l’usage.

Prix

600 $ / mois

Ce qui est couvert

L’accès au logiciel et le soutien continu.

Crédit inclus

600 $ de crédit d’usage LLM géré, inclus chaque période.

Report

Aucun. Le crédit inutilisé est **perdu à la fin de chaque période** — il n’est pas reporté.

En clair : le forfait mensuel paie l’accès à la plateforme et le soutien qui l’accompagne, et inclut 600 $ de crédit d’usage de modèles à dépenser durant la période. Le crédit que vous n’utilisez pas est perdu lors de la réinitialisation du cycle — il n’y a pas d’accumulation.

CONSEIL

Pour toute modification de facturation, question sur le forfait ou ajustement de votre crédit inclus, contactez le soutien de Québec Agentique.

03 Plugiciels — ajout et connexion

Les plugiciels donnent de nouvelles capacités à votre agent en le reliant à des services externes — courriel, agendas, messagerie, dépôts de code, et bien d'autres. Un plugiciel doit *s'authentifier* auprès du service auquel il s'adresse, et il y a deux façons de le faire.

Méthode A — OAuth (se connecter via le fournisseur)

Pour les services qui le prennent en charge (Google, Microsoft, etc.), vous vous connectez via l'écran de consentement du fournisseur. Vous approuvez l'accès une seule fois, et la plateforme conserve et renouvelle automatiquement les jetons obtenus — vous ne collez jamais de secret à la main.

1. Activez le plugiciel souhaité.
2. Choisissez **Connecter / Se connecter**. Vous êtes redirigé vers la page d'autorisation du fournisseur.
3. Vérifiez les permissions demandées et approuvez. Vous revenez à Mili, et le plugiciel est connecté.

Méthode B — Coffre-fort d'identifiants (clé API ou jeton)

Pour les services qui émettent une clé API, un jeton ou un mot de passe, vous stockez ce secret dans le **coffre-fort** (voir la section 6) et le plugiciel l'y lit. Le secret reste chiffré au repos et n'est que référencé — jamais dupliqué — par le plugiciel.

1. Créez le secret dans le coffre-fort, en lui donnant une clé telle que `github_token` ou `smtp_password`.
2. Dans les réglages du plugiciel, pointez le champ d'identifiant vers cette clé du coffre (écrite `github_token`).
3. Saisissez les réglages non secrets dont le plugiciel a besoin — hôte, port, nom d'utilisateur — directement dans ses champs habituels.

GARDEZ LES SECRETS DANS LE COFFRE-FORT

Seuls les véritables secrets (mots de passe, clés API, jetons) vont dans le coffre. Les réglages non secrets comme les noms d'hôtes, ports et noms d'utilisateur vont dans les champs de configuration ordinaires du plugiciel.

04 Clients MCP — appeler d’autres agents

Mili peut dialoguer avec d’autres agents Mili (ou tout agent compatible MCP) afin qu’ils utilisent mutuellement leurs outils. Chaque pair que vous souhaitez joindre est enregistré comme un **Contact**. C’est le côté « sortant » : *votre* agent qui appelle *le leur*.

Ouvrez `Contacts` depuis l’écran principal, puis ajoutez un contact et remplissez :

Display Name

Un libellé convivial, p. ex. « Agent d’Alice ».

Contact ID

L’identifiant de l’agent pair.

Endpoint URL

L’adresse MCP du pair, p. ex. `https://agent.local:5001/mcp`

Transport

HTTP SSE (par le réseau) ou STDIO (processus local).

Verify SSL

Laissez activé pour de vrais certificats ; désactivez seulement pour des pairs auto-signés.

Outbound Token

Le secret **que vous envoyez** à chaque appel vers ce pair (utilisez une longue chaîne aléatoire, 32 caractères ou plus).

Délais (timeouts)

Le temps d’attente pour les appels sortants (et entrants).

Une fois enregistré, votre agent peut invoquer les outils permis de ce pair dans le cadre de son travail.

05 Serveur MCP — exposer vos outils

Votre agent est aussi un **serveur** MCP : d'autres agents peuvent appeler *vos* outils, mais uniquement ceux que vous autorisez explicitement, et seulement pour les contacts que vous avez approuvés. C'est le côté « entrant », configuré par contact.

Ouvrez un contact dans `Contacts` et réglez ses options **entrantes** :

Allowed Tools

La liste blanche de *vos* outils que ce contact peut invoquer. **Une liste vide n'autorise rien.**

Inbound Token

Le secret que ce contact **doit vous envoyer** à chaque appel entrant.

IP Validation

Off (toute IP), IP (doit correspondre à l'adresse du endpoint) ou DNS (résolution du nom d'hôte du endpoint).

Inbound Guard Rails

Des consignes ajoutées au prompt système pour chaque requête de ce contact, p. ex. « Ne répondre qu'aux questions sur X. Ne jamais divulguer d'identifiants. »

Inbound Mode

Single Message — chaque appel obtient une session neuve. **Conversation** — tous les appels de ce contact partagent une même session continue avec historique.

N'AUTORISEZ QUE CE QUE VOUS VOULEZ PARTAGER

La liste Allowed Tools est la barrière. Ajoutez les outils délibérément ; une liste vide bloque entièrement le contact, ce qui est la valeur sûre par défaut.

06 Le coffre-fort d’identifiants

Le coffre-fort est un magasin chiffré pour les secrets dont vos plugiciels et outils ont besoin — clés API, mots de passe, jetons. Les secrets sont chiffrés au repos avec AES-256-GCM et ne sont déchiffrés qu’en mémoire au moment de leur utilisation.

Ouvrez `Réglages › Credential Vault` (votre mot de passe administrateur vous sera demandé pour entrer).

Ajouter un identifiant

1. Touchez **+ Add**.
2. Saisissez une **clé** — un identifiant court tel que `smtp_password`. Vous le référencez ailleurs sous la forme `{{vault:smtp_password}}`.
3. Saisissez un **libellé** lisible et collez la **valeur** secrète. Enregistrez.

Source de la clé maîtresse

Le contenu du coffre est protégé par une clé maîtresse, et vous pouvez choisir sa provenance :

Fichier *(défaut)*

Un fichier de clé généré automatiquement, conservé avec des permissions strictes sur l’hôte.

Variable d’environnement

Vous fournissez la clé via une variable d’environnement — pour configurations avancées.

AWS / GCP / Azure KMS

Un service de gestion de clés infonuagique déverrouille la clé au démarrage.

YubiKey

Une clé matérielle déverrouille la clé maîtresse.

Changer la source **rechiffre** l’ensemble du coffre avec la nouvelle clé — vos secrets stockés sont préservés. Chaque lecture, écriture et changement de source est consigné au journal d’audit du coffre.

07 Exposition réseau et durcissement

Par défaut, Mili écoute sur `0.0.0.0:5001` — ce qui signifie qu'il est joignable depuis **tout appareil du réseau** capable d'atteindre l'hôte. Pratique pour un déploiement partagé, mais plus ouvert que nécessaire dans bien des cas.

Restreindre à la machine locale

Pour rendre l'agent joignable uniquement depuis l'hôte sur lequel il s'exécute, réglez le **Server IP / Host** à `127.0.0.1` au lieu de `0.0.0.0`.

1. Ouvrez les réglages du serveur à /server/settings.
2. Remplacez **Host** : `0.0.0.0` → `127.0.0.1`.
3. Enregistrez, puis redémarrez le serveur pour appliquer le changement.

DÉPLOIEMENTS CONTENEURISÉS

Quand Mili tourne dans Docker, le port publié gouverne aussi l'exposition. Pour le lier à la seule machine locale, mappez le port en `127.0.0.1:5001:5001` dans `docker-compose.yml` en plus du réglage de l'hôte. Pour tout ce qui est joignable depuis le réseau, associez toujours l'exposition à TLS (section 11) et à l'authentification.

08 URL publique — transferts de fichiers entre agents

Le champ **Public URL** (sous les réglages du serveur) est l’adresse de base de cet agent, joignable depuis l’extérieur. Il sert au partage de fichiers entre agents.

Lorsque votre agent partage un fichier avec un pair, il construit un lien de téléchargement à partir de sa propre URL publique — car lui seul connaît sa propre adresse joignable de l’extérieur. Le pair récupère ensuite le fichier depuis ce lien. Les destinataires ne devinent jamais l’adresse ; c’est l’expéditeur qui la fournit.

Où

Server settings › Public URL

Exemple

`https://172.31.124.220:5001`

Pourquoi c’est important

Si elle n’est pas définie, le partage de fichiers entre agents ne peut pas produire de lien de téléchargement utilisable.

INDIQUEZ L’ADRESSE RÉELLEMENT JOIGNABLE PAR LES PAIRS

Utilisez l’adresse réseau réelle de l’hôte (et le port), joignable par les agents avec qui vous échangez des fichiers — et non `127.0.0.1`, valide uniquement sur la machine locale.

09 Mises à jour logicielles

Les mises à jour sont livrées sous forme d’un nouveau paquet de version. Vous en appliquez une en relançant l’installateur sur chaque machine.

1. Procurez-vous la nouvelle version et lancez l’installateur de votre plateforme sur la machine cible.
2. L’installateur charge la nouvelle image applicative (remplaçant la version précédente) et redémarre le conteneur.
3. Vos réglages et votre historique sont conservés : l’installateur **n’écrase pas** votre configuration, vos certificats ni vos conversations s’ils existent déjà.

CONSERVÉ D’UNE MISE À JOUR À L’AUTRE

La configuration, les certificats TLS et tout l’historique des conversations sont repris automatiquement. Aucune exportation préalable n’est requise pour une mise à jour normale.

Certaines opérations — rechargement de configuration, mise à jour de politique, ou redémarrage — peuvent aussi être appliquées de façon centralisée par le serveur de gestion, sans réinstallation complète.

10 Sauvegarde et restauration

Ouvrez `Réglages › Backup & Restore` .

Créer une sauvegarde

Touchez **Download Backup** pour enregistrer un unique fichier `.zip`. Il contient votre configuration, votre persona, la mémoire, les tâches, les conversations et les identifiants stockés. Conservez ce fichier en lieu sûr — il contient des secrets.

Restaurer

1. Glissez un fichier de sauvegarde `.zip` sur la zone de restauration, ou touchez pour en choisir un.
2. Confirmez. Le serveur remplace toutes les données actuelles par le contenu de la sauvegarde et redémarre.

LA RESTAURATION EST DESTRUCTIVE

Restaurer **remplace toutes les données existantes** et est irréversible. Faites d’abord une sauvegarde de l’état actuel si vous pourriez en avoir besoin.

11 Certificats TLS

Mili est servi en HTTPS. Au premier démarrage, il génère un certificat auto-signé afin que la connexion soit chiffrée immédiatement ; en production, vous le remplacerez généralement par votre propre certificat de confiance.

Ouvrez `Réglages › SSL / TLS` .

SSL Enabled

Active ou désactive le HTTPS.

Status

Indique si le certificat et la clé privée sont présents.

Téléverser votre propre certificat

1. Sous **Upload Certificate & Key**, téléversez votre certificat (`.crt` / `.pem`).
2. Téléversez la clé privée correspondante (`.key` / `.pem`).
3. Redémarrez le serveur. Les fichiers téléversés remplacent le certificat et la clé précédents.

AUTO-SIGNÉ OU DE CONFIANCE

Le certificat auto-signé du premier démarrage chiffre le trafic, mais les navigateurs avertiront qu'il n'est pas de confiance. Téléversez un certificat émis par une autorité de confiance (ou votre AC interne) pour supprimer l'avertissement.