
Guide des assistants IA

La version toujours à jour, avec la recherche dans le texte, est sur le site.

DANS CE GUIDE

- | | |
|--|--|
| 01 Qu'est-ce que c'est | 09 Claude sur le web |
| 02 Ce qu'il peut faire | 10 Changer d'avis |
| 03 Première connexion | 11 « Visible par » |
| 04 Claude Code | 12 L'administrateur |
| 05 Cursor | 13 Sécurité |
| 06 Claude Desktop | 14 Questions fréquentes |
| 07 Codex | 15 Si ça ne fonctionne pas |
| 08 ChatGPT | |

01 Qu'est-ce qu'un assistant connecté

Pour faire lire un document à un assistant IA (Claude, ChatGPT, Cursor, Codex), on le télécharge d'habitude pour le recharger dans la conversation : une copie de plus qui circule de son côté, sans versions, sans permissions, sans trace de qui a lu quoi.

Avec **Assistants IA**, tu connectes l'assistant à Flow une seule fois, et à partir de là il travaille sur les documents là où ils se trouvent déjà. Trois principes portent tout le reste :

1. **C'est toi qui choisis les dossiers.** Une connexion n'ouvre que les dossiers que tu indiques. En dehors de ceux-là, rien n'existe pour l'assistant : il ne peut ni les ouvrir, ni les chercher, ni même savoir qu'ils existent.
2. **L'entreprise décide de ce qui peut être ouvert.** Dans les espaces d'équipe, c'est l'administrateur qui établit, dossier par dossier, ce qui peut être ouvert et si c'est en lecture ou aussi en écriture. Tu choisis à l'intérieur de cette liste : tu peux la restreindre, jamais l'élargir.

3. **Au départ, il lit, et c'est tout.** Une nouvelle connexion est en **Lecture seule**.

Elle ne peut modifier que si tu le choisis, et seulement là où l'administrateur l'a permis. Et rien n'est définitif : la corbeille et les versions restent là.

Dans ton **espace personnel**, tu décides seul, sans passer par l'administrateur.

Les connexions se créent et se gèrent dans **Compte → Assistants IA**.

Assistants IA dépend de l'offre, et s'active aujourd'hui sur demande : si tu ne trouves pas l'entrée dans ton Compte, écris-nous. Il faut aussi que l'offre lise le texte des documents (la même lecture qui alimente la recherche dans le contenu), sinon l'assistant trouverait le nom des fichiers et non ce qu'ils contiennent. Là où l'offre ne va pas, l'assistant le dit : il n'invente pas.

02 Ce qu'il peut faire, et ce qu'il ne fait pas

Dans les dossiers que tu lui as ouverts, un assistant connecté **lit toujours** :

- il liste le contenu d'un dossier et les propriétés d'un fichier : taille, dates, version, tags ;
- il **lit le texte** des PDF, des documents Office et des images contenant du texte. C'est le texte que Flow a déjà extrait pour la recherche : il n'y a donc aucune conversion à faire ni de limite de taille de fichier ;
- il **cherche** par nom et dans le contenu, avec des filtres par dossier, type et date ;
- il voit les versions d'un fichier et ce qui a été ajouté, modifié ou supprimé récemment ;
- il voit l'espace utilisé et le quota de l'entreprise ;
- il obtient un lien temporaire, valable une heure, pour télécharger un fichier tel quel ;
- il voit les liens de partage et de dépôt que **toi** tu as créés sur ces dossiers, pas ceux de tes collègues.

Si la connexion est en « Peut modifier », et seulement dans les dossiers que l'administrateur a mis en Écriture (ou dans ton espace personnel), il peut aussi : créer des dossiers, créer des fichiers texte jusqu'à 5 Mo, copier, déplacer, renommer, mettre à la corbeille (en te demandant confirmation) et ramener un fichier à une version précédente. Si un nom existe déjà, il ne l'écrase pas : il le fait

seulement si tu le lui demandes, et l'ancienne version reste de toute façon dans les versions.

Ce qu'il ne fait pas, même si tu le lui demandes :

- sortir des dossiers que tu lui as ouverts : cela n'arrivera jamais, en aucun cas ;
- créer des liens de partage ou de dépôt : c'est le seul geste par lequel une erreur ferait sortir des documents de l'entreprise, et pour l'instant il reste exclu ;
- supprimer définitivement : tout passe par la corbeille ;
- déplacer, renommer ou mettre à la corbeille les dossiers mêmes que tu lui as ouverts ;
- toucher un fichier qu'un collègue est en train de modifier en exclusivité ;
- voir les Données protégées, les signatures, les tasks et les dépôts Git : il voit les fichiers et les dossiers, et c'est tout.

Si un fichier n'a pas de texte lisible (une archive compressée, un format qu'il ne connaît pas), il te le dit. Il n'invente pas.

03 La première connexion

Compte → Assistants IA → « Nouvelle connexion ». Quatre choix :

1. **Nom** : il te sert à toi, pour la reconnaître dans six mois : « Claude sur le projet Dainese » en dit plus que « Claude ».
2. **Ce qu'il peut faire** : **Lecture seule**, déjà sélectionné, ou **Peut modifier**. Dans le doute, laisse le premier : cela se change quand tu veux, sans rien refaire.
3. **Expiration** : jamais, 30 jours, 90 jours, 1 an. Pour une mission de conseil qui se termine, une date d'expiration est plus pratique qu'un rappel.
4. **Dossiers ouverts** : l'arborescence en colonnes, la même que celle de la synchronisation sélective. Tu coches un ou plusieurs dossiers, même dans des espaces différents.

Pour les dossiers, une seule règle s'applique, et il vaut mieux la garder en tête : **cocher un dossier ouvre tout ce qu'il contient**. On ne retire pas une partie de l'intérieur : si un sous-dossier ne doit pas être visible, tu coches ses dossiers voisins et non le dossier parent.

Dans les espaces d'équipe, ce que l'administrateur n'a pas ouvert porte un **cadenas** (« Non ouvrable aux assistants : décidé par l'administrateur ») et les dossiers dans lesquels un assistant pourra aussi écrire portent un **crayon**. Dans ton espace personnel, tu coches ce que tu veux.

Au-dessus des dossiers, il reste toujours écrit : « *Les documents lus par l'assistant sont envoyés au fournisseur de cet assistant (Anthropic, OpenAI...).* N'ouvre que les dossiers nécessaires. » C'est la raison pour laquelle il vaut mieux ouvrir peu.

À la confirmation apparaissent la **clé d'accès**, l'**adresse du serveur** et un bloc prêt à copier pour chaque assistant.

La clé ne s'affiche qu'une seule fois. Copie-la maintenant : ensuite, personne ne peut plus la récupérer, pas même nous. Si tu la perds, ce n'est pas grave : tu révoques la connexion et tu en crées une autre en une minute.

04 Connecter Claude Code

Claude Code se connecte depuis le **terminal**. Sur la page de la connexion, sous « Comment le connecter », le premier bloc est déjà prêt avec ta clé dedans : on le copie et on le colle dans le terminal tel quel.

Ensuite, dans Claude Code, la commande `/mcp` liste les serveurs connectés : **flow** doit y apparaître. À partir de là, tu peux demander « que vois-tu sur Flow ? » et l'assistant répond avec les dossiers que tu lui as ouverts.

MCP est le standard par lequel les assistants se connectent à une source de données. Nous le nommons parce que c'est le mot que tu trouveras écrit dans les réglages des assistants.

Copie le bloc que te donne Flow, plutôt qu'un exemple lu ailleurs : celui de Flow contient déjà la vraie clé. Un bloc avec l'espace réservé à la place de la clé s'installe quand même, et l'assistant répond ensuite qu'il ne sait rien de Flow.

05 Connecter Cursor

Dans Cursor, le bloc prêt à l'emploi va à l'un de ces deux endroits, au choix :

- **Settings → MCP → Add server ;**

- ou bien le fichier `.cursor/mcp.json` du projet, si tu préfères que la connexion reste avec le projet.

Le bloc à coller est le deuxième de ceux que la page de la connexion te montre, et il contient déjà la clé. Une fois enregistré, Cursor affiche **flow** parmi les serveurs disponibles.

L'avertissement habituel s'applique : copie le bloc que te donne Flow, plutôt qu'un exemple trouvé ailleurs : un espace réservé à la place de la clé passe inaperçu, et ensuite l'assistant ne trouve rien.

06 Connecter Claude Desktop

Claude Desktop garde les connexions dans un fichier de configuration. On y accède depuis l'app : **Settings** → **Developer** → **Edit Config**, qui ouvre `claude_desktop_config.json`.

Dans ce fichier, on colle le bloc que la page de la connexion indique pour Claude Desktop, puis **on redémarre Claude Desktop** : il lit les connexions au démarrage.

Tu n'as rien à installer sur Flow. Pour dialoguer avec la clé, Claude Desktop utilise un petit pont qui se télécharge tout seul la première fois : si la première réponse met quelques secondes à arriver, c'est pour cela.

07 Connecter Codex

Dans Codex, le bloc va dans le fichier `~/codex/config.toml`. Depuis l'app, tu y accèdes par **Settings** → **Configuration** ; depuis le terminal, il y a aussi la commande `codex mcp add`.

Une fois le fichier enregistré, **redémarre Codex**. Dans la conversation, `/mcp` liste les serveurs connectés : **flow** doit en faire partie.

Deux avertissements, appris tous les deux à nos dépens :

- l'entrée « **Connections** » des réglages de Codex est autre chose (le contrôle à distance de l'ordinateur) et n'a rien à voir avec les assistants connectés à Flow ;
- si tu colles un bloc d'exemple en laissant l'espace réservé à la place de la clé, Codex affiche quand même « **Authenticated** », mais l'assistant répond ensuite

qu'il n'a pas d'outils Flow. Le bon bloc est celui que te donne la page de la connexion, avec la clé déjà dedans.

08 Connecter ChatGPT

ChatGPT suit un autre chemin : **aucune clé à copier**. Tu lui donnes seulement l'adresse de ton Flow, il ouvre une page de Flow où tu te connectes, choisis les dossiers et confirmes. La connexion apparaît toute seule dans Compte → Assistants IA, avec le nom de l'assistant, et se gère ensuite comme toutes les autres.

Le parcours, dans ChatGPT :

1. **Settings → Security and access**, tout en bas, **Developer mode** : active-le. ChatGPT le signale comme « risque élevé » : c'est l'avertissement qu'il affiche pour quiconque ajoute son propre serveur, et il sert à cela.
2. **Settings → Plugins → Browse plugins**.
3. En haut à droite, le bouton **+**, qui ouvre le formulaire « New plugin ».
4. Nom **Flow** ; dans le lien, l'adresse de ton Flow suivie de `/mcp`, par exemple `https://flow.kaigrid.ai/mcp` ; authentification **OAuth** ; coche « I understand and want to continue » ; **Create**.
5. **Se connecter à Flow** : la page de Flow « ... demande l'accès à Flow » s'ouvre, où tu choisis entre Lecture seule et Peut modifier, coches les dossiers et lis l'avertissement sur les données. **Autoriser**, ou **Ne pas autoriser**, et il ne se passe rien.
6. Dans une nouvelle conversation, choisis Flow parmi les plugins et essaie : « que vois-tu sur Flow ? ».

Sur la page de consentement, dans les espaces d'équipe, tu vois **seulement** les dossiers que l'administrateur a ouverts : pas de cadenas, pas de liste à déchiffrer.

ChatGPT change souvent le nom de ses menus : il y a peu, les plugins s'appelaient encore connecteurs. Si une entrée ne porte plus ce nom, cherche-la d'après ce qu'elle fait.

09 Connecter Claude sur le web

Claude sur le web suit le même chemin que ChatGPT : **aucune clé à copier**. Tu lui donnes l'adresse de ton Flow, il ouvre une page de Flow où tu te connectes, choisis les dossiers et confirmes.

Dans Claude : **Settings → Connectors → « Add custom connector »**, et comme adresse, l'adresse de ton Flow suivie de `/mcp`, par exemple

`https://flow.kaigrid.ai/mcp`.

À partir de là, c'est identique : la page « ... demande l'accès à Flow » s'ouvre, où tu choisis entre Lecture seule et Peut modifier, coches les dossiers et lis l'avertissement sur les données. À la confirmation, la connexion apparaît toute seule dans **Compte → Assistants IA**, avec le nom de l'assistant, et se gère comme toutes les autres : tu changes les dossiers, tu changes ce qu'il peut faire, tu révoques.

Ici aussi, ce qui vaut pour ChatGPT s'applique : dans les espaces d'équipe, sur la page de consentement, tu vois **seulement** les dossiers que l'administrateur a ouverts.

10 Changer d'avis

Rien de ce que tu as choisi n'est définitif, et **on ne refait jamais la clé**.

- **Les dossiers** : depuis Compte → Assistants IA, ouvre la connexion et change les cases cochées. Les nouveaux dossiers s'appliquent dès la requête suivante de l'assistant, et tu n'as rien à toucher dans l'assistant.
- **Ce qu'il peut faire** : on passe de Lecture seule à « Peut modifier », et inversement, de la même façon.
- **Révoquer** : l'assistant cesse **immédiatement** de voir Flow. On s'en sert quand un projet se termine, quand un ordinateur est perdu, ou simplement quand tu as fini.

La page indique, pour chaque connexion, quand tu l'as créée, **la dernière utilisation** et l'expiration : si personne ne l'utilise depuis des mois, cela se voit.

Si l'assistant essaie de faire quelque chose que la connexion ne permet pas (une modification avec une connexion en lecture seule, ou dans un dossier où

l'administrateur n'a pas mis Écriture), il reçoit un refus qui explique ce qui manque, et il te le rapporte au lieu d'échouer en silence.

11 Qui travaille dans le dossier le sait

Un dossier ouvert à un assistant n'est pas l'affaire privée de la personne qui a créé la connexion : ceux qui y travaillent doivent pouvoir le savoir.

C'est pourquoi, à côté du nom des dossiers et des fichiers qu'un assistant voit, il y a une **petite icône** ; en la survolant, elle indique à quelle connexion. Dans le panneau d'informations du fichier, la même chose est écrite en toutes lettres : « **Visible par : Claude sur le projet Dainese** ». Tous ceux qui travaillent là la voient, pas seulement toi.

Le **journal d'activité** garde une trace de tout : quand une connexion est créée, quand ses dossiers changent, quand elle est révoquée, **chaque lecture de contenu** (quelle connexion, quel fichier, quand), chaque lien de téléchargement et chaque modification. Le journal des assistants est toujours actif.

Ce que le journal ne contient **pas**, c'est la conversation : l'administrateur voit quels fichiers l'assistant a lus, et non ce que tu lui as demandé.

12 Ce que décide l'administrateur

Dans les espaces d'équipe, c'est l'entreprise qui établit ce qui peut être ouvert à un assistant. L'administrateur le fait dans **Console administrateur → Assistants IA**, avec « Modifier la liste » : la même arborescence en colonnes, où chaque espace et chaque dossier a une case à **trois états**, que l'on fait défiler d'un clic.

- **Non** (case vide) : les assistants ne le voient pas. C'est l'état de départ de tout : une entreprise qui n'ouvre rien n'expose rien.
- **Lecture** (l'œil) : les assistants peuvent le lire.
- **Écriture** (le crayon) : ils peuvent aussi le modifier, si la connexion est en « Peut modifier ».

L'état vaut pour tout ce que le dossier contient, et un sous-dossier peut en avoir un **différent** : c'est toujours le plus proche qui l'emporte. L'espace « Clients » en Lecture peut contenir « Brouillons » en Écriture ; un dossier en Écriture peut contenir « Contrats » en Lecture seule. Les sous-dossiers affichent en grisé le

niveau dont ils héritent : un clic le change uniquement à cet endroit, un autre le remet comme avant.

Une chose n'est pas possible : **remettre « Non » à l'intérieur d'un dossier ouvert**.

Pas de trous invisibles : si un sous-dossier ne doit pas être visible, on ouvre ses dossiers voisins et non le dossier parent.

Les **espaces personnels** ne figurent pas dans cette liste : chaque utilisateur en décide pour lui-même.

Retirer ou abaisser une entrée **s'applique immédiatement**, y compris aux connexions qui existent déjà. Pour que ce ne soit pas une surprise, la page indique à côté de chaque entrée combien de connexions l'utilisent. Sur la même page se trouve la liste des **connexions de l'entreprise** : à qui elles appartiennent, sur quels dossiers, leur dernière utilisation.

13 Sécurité et confidentialité

Les documents lus partent vers le fournisseur de l'assistant. Quand l'assistant lit un fichier, ce texte arrive chez celui qui fournit l'assistant (Anthropic, OpenAI ou un autre), selon le contrat que toi ou ton entreprise avez avec ce fournisseur. Flow n'envoie rien de sa propre initiative : il envoie ce que l'assistant demande, dans les dossiers que tu lui as ouverts. C'est la raison pour laquelle il vaut mieux ouvrir peu de dossiers et bien les choisir.

Un document peut contenir des instructions adressées à l'assistant : des lignes écrites exprès pour qu'il les lise et les exécute. Cela vaut pour n'importe quel assistant, et Flow y oppose quatre défenses : au départ, la connexion ne fait que lire ; le texte arrive à l'assistant marqué comme contenu d'un document, et non comme un ordre ; l'assistant ne peut pas créer de liens vers l'extérieur ; et tout ce qu'il modifie s'annule depuis la corbeille et les versions.

Une clé perdue se révoque en un clic, et la connexion peut avoir une date d'expiration dès le départ. La page affiche la dernière utilisation de chacune.

Un assistant ne voit jamais plus que toi. La connexion vit à l'intérieur de tes permissions : si on te retire un espace, tes connexions le perdent au même instant. Et elle ne vaut que pour les assistants : avec cette clé, on n'entre pas dans le reste de Flow.

14 Questions fréquentes

L'assistant voit-il tous mes fichiers ? Non : seulement les dossiers que tu as cochés dans la connexion.

Un collègue peut-il ouvrir à un assistant un dossier réservé ? Seulement s'il voit déjà ce dossier lui-même, et seulement si l'administrateur l'a rendu ouvrable.

Puis-je changer d'avis ensuite ? Oui : tu changes les dossiers ou tu révoques quand tu veux, et cela s'applique immédiatement. La clé reste la même.

L'assistant peut-il supprimer mes fichiers ? Seulement si tu as choisi « Peut modifier » et seulement là où l'administrateur a mis Écriture. Et même dans ce cas, ils vont à la corbeille, d'où on les restaure.

Comment savoir si un dossier est ouvert à un assistant ? Il a une petite icône à côté de son nom, et le panneau d'informations du fichier indique « Visible par », avec le nom de la connexion.

J'ai perdu la clé. Elle ne se récupère pas : révoque la connexion et crées-en une nouvelle.

Cela fonctionne-t-il avec ChatGPT ? Oui, depuis le web. Et avec Claude Code, Claude Desktop, Cursor et Codex.

Faut-il installer quelque chose ? Sur Flow, non, rien. Claude Desktop utilise un petit pont qui se télécharge tout seul au premier lancement.

L'administrateur voit-il ce que je demande à l'assistant ? Non. Il voit quels fichiers l'assistant a lus ou modifiés, pas la conversation.

15 Si quelque chose ne fonctionne pas

L'assistant dit qu'il n'a pas d'outils Flow, ou ne sait pas ce que c'est. C'est presque toujours le bloc collé à la main, avec l'espace réservé resté à la place de la clé. Certains assistants affichent quand même « Authenticated » dans ce cas. Recopie le bloc depuis la page de la connexion, qui contient déjà la clé, et redémarre l'assistant.

L'assistant ne voit pas un dossier que j'avais coché. Vérifie la connexion dans Compte → Assistants IA : si ce dossier porte un **cadenas**, l'administrateur l'a fermé aux assistants, et la fermeture s'applique immédiatement, y compris aux connexions déjà créées.

Il dit ne pas pouvoir modifier. Soit la connexion est en **Lecture seule**, et tu la changes depuis sa fiche, soit ce dossier n'a pas le **crayon** : dans les espaces d'équipe, c'est l'administrateur qui le met.

La connexion a expiré. Les dates d'expiration sont celles que tu as choisies à la création. Une connexion expirée ne se prolonge pas : on en crée une autre.

ChatGPT ne voit pas les nouvelles fonctions. ChatGPT garde en mémoire la liste des opérations du moment où tu as créé le plugin, et ne la relit pas de lui-même. Ouvre la fiche du plugin Flow et appuie sur **Refresh** ; s'il n'existe pas, supprime le plugin et recrée-le. Ouvre ensuite une **nouvelle conversation**. Les permissions, elles, s'appliquent toujours immédiatement, quoi que ChatGPT ait en mémoire.

J'ai révoqué par erreur. Cela ne se restaure pas : on crée une nouvelle connexion et on refait le parcours dans l'assistant. Cela prend une minute.