
Leitfaden zu den KI-Assistenten

Die stets aktuelle Fassung, mit Suche im Text, steht auf der Website.

IN DIESER ANLEITUNG

- | | |
|----------------------------|--------------------------------------|
| 01 Was es ist | 09 Claude im Web |
| 02 Was er kann | 10 Es sich anders überlegen |
| 03 Erste Verbindung | 11 „Sichtbar für“ |
| 04 Claude Code | 12 Der Administrator |
| 05 Cursor | 13 Sicherheit |
| 06 Claude Desktop | 14 Häufige Fragen |
| 07 Codex | 15 Wenn es nicht funktioniert |
| 08 ChatGPT | |

01 Was ein verbundener Assistent ist

Um einen KI-Assistenten ein Dokument lesen zu lassen (Claude, ChatGPT, Cursor, Codex), lädt man es normalerweise herunter und im Chat wieder hoch: eine weitere Kopie, die ihre eigenen Wege geht, ohne Versionen, ohne Berechtigungen und ohne Spur davon, wer was gelesen hat.

Mit **KI-Assistenten** verbindest du den Assistenten ein einziges Mal mit Flow, und von da an arbeitet er mit den Dokumenten dort, wo sie schon liegen. Drei Grundsätze tragen alles Weitere:

1. **Du wählst die Ordner.** Eine Verbindung öffnet nur die Ordner, die du angibst. Außerhalb davon existiert für den Assistenten nichts: Er kann sie weder öffnen noch durchsuchen, er weiß nicht einmal, dass es sie gibt.
2. **Das Unternehmen entscheidet, was sich öffnen lässt.** In den Team-Bereichen legt der Administrator Ordner für Ordner fest, was sich öffnen lässt und ob nur zum Lesen oder auch zum Schreiben. Du wählst innerhalb dieser Liste: Du kannst sie einschränken, nie erweitern.
3. **Anfangs liest er nur.** Eine neue Verbindung steht auf **Nur lesen**. Ändern darf er nur, wenn du das wählst, und nur dort, wo der Administrator es erlaubt hat.

Und nichts ist endgültig: Papierkorb und Versionen bleiben.

In deinem **persönlichen Bereich** entscheidest du selbst, ohne den Administrator.

Verbindungen erstellst und verwaltest du unter **Konto → KI-Assistenten**.

KI-Assistenten hängt vom Tarif ab und wird derzeit auf Anfrage aktiviert: Wenn du in deinem Konto den Eintrag nicht findest, schreib uns. Außerdem muss der Tarif den Text der Dokumente lesen (dieselbe Erfassung, die auch die Suche in den Inhalten speist), sonst fände der Assistent nur die Dateinamen und nicht, was darin steht. Wo der Tarif nicht reicht, sagt der Assistent das: Er erfindet nichts.

02 Was er kann und was nicht

In den Ordnern, die du ihm geöffnet hast, kann ein verbundener Assistent **immer lesen**:

- er listet den Inhalt eines Ordners und die Eigenschaften einer Datei auf: Größe, Datumsangaben, Version, Tags;
- er **liest den Text** von PDFs, Office-Dokumenten und Bildern mit Text. Es ist der Text, den Flow bereits für die Suche erfasst hat, deshalb braucht es keine Umwandlung und es gibt keine Grenze für die Dateigröße;
- er **sucht** nach Namen und im Inhalt, mit Filtern nach Ordner, Typ und Datum;
- er sieht die Versionen einer Datei und was zuletzt hinzugefügt, geändert oder gelöscht wurde;
- er sieht den belegten Speicher und das Kontingent des Unternehmens;
- er erhält einen befristeten Link, eine Stunde gültig, um eine Datei unverändert herunterzuladen;
- er sieht die Freigabe- und Upload-Links, die **du** für diese Ordner erstellt hast, nicht die der Kollegen.

Wenn die Verbindung auf „Darf ändern“ steht, und nur in den Ordnern, die der Administrator auf Schreiben gesetzt hat (oder in deinem persönlichen Bereich), kann er außerdem: Ordner anlegen, Textdateien bis 5 MB erstellen, kopieren, verschieben, umbenennen, in den Papierkorb legen (nach deiner Bestätigung) und eine Datei auf eine frühere Version zurücksetzen. Wenn ein Name schon existiert, überschreibt er ihn nicht: Das tut er nur, wenn du ihn darum bittest, und die alte Version bleibt ohnehin in den Versionen.

Was er nicht tut, auch nicht auf deine Bitte:

- die Ordner verlassen, die du ihm geöffnet hast: Das passiert nie, in keinem Fall;
- Freigabe- oder Upload-Links erstellen: Das ist der einzige Schritt, mit dem ein Fehler Dokumente aus dem Unternehmen hinausbringen würde, und er bleibt vorerst ausgeschlossen;
- endgültig löschen: Alles geht über den Papierkorb;
- die Ordner selbst verschieben, umbenennen oder in den Papierkorb legen, die du ihm geöffnet hast;
- eine Datei anfassen, die ein Kollege in exklusiver Bearbeitung hat;
- geschützte Daten, Signaturen, Tasks und Git-Repositories sehen: Er sieht Dateien und Ordner, sonst nichts.

Wenn eine Datei keinen lesbaren Text hat (ein komprimiertes Archiv, ein Format, das er nicht kennt), sagt er dir das. Er erfindet nichts.

03 Die erste Verbindung

Konto → KI-Assistenten → „Neue Verbindung“. Vier Entscheidungen:

1. **Name:** Er ist für dich, damit du die Verbindung in sechs Monaten wiedererkennt: „Claude im Projekt Dainese“ sagt mehr als „Claude“.
2. **Was er darf:** **Nur lesen**, bereits ausgewählt, oder **Darf ändern**. Im Zweifel lass die erste Option: Du kannst sie jederzeit ändern, ohne etwas neu einzurichten.
3. **Ablauf:** nie, 30 Tage, 90 Tage, 1 Jahr. Für eine Beratung, die endet, ist ein Ablaufdatum bequemer als eine Erinnerung.
4. **Geöffnete Ordner:** der Spaltenbaum, derselbe wie bei der selektiven Synchronisierung. Du hakst einen oder mehrere Ordner ab, auch in verschiedenen Bereichen.

Für die Ordner gilt eine einzige Regel, die du dir merken solltest: **Einen Ordner abzuheben öffnet alles, was er enthält**. Einzelne Teile darin lassen sich nicht ausheben: Wenn ein Unterordner nicht sichtbar sein soll, hakst du die Geschwisterordner ab und nicht den übergeordneten.

In den Team-Bereichen trägt, was der Administrator nicht geöffnet hat, ein **Schloss** („Für Assistenten nicht freigebbar: vom Administrator festgelegt“), und

die Ordner, in die ein Assistent auch schreiben darf, tragen einen **Stift**. In deinem persönlichen Bereich hakst du ab, was du willst.

Über den Ordnern steht immer: „*Dokumente, die der Assistent liest, werden an den Anbieter dieses Assistenten gesendet (Anthropic, OpenAI...). Öffne nur die Ordner, die nötig sind.*“ Das ist der Grund, warum es sich lohnt, wenig zu öffnen.

Nach der Bestätigung erscheinen der **Zugangsschlüssel**, die **Serveradresse** und ein fertiger Block zum Kopieren für jeden Assistenten.

Den Schlüssel siehst du nur einmal. Kopiere ihn jetzt: Danach kann ihn niemand mehr abrufen, auch wir nicht. Wenn du ihn verlierst, ist das kein Drama: Du widerrufst die Verbindung und erstellst in einer Minute eine neue.

04 Claude Code verbinden

Claude Code wird über das **Terminal** verbunden. Auf der Seite der Verbindung, unter „So wird verbunden“, ist der erste Block schon fertig, mit deinem Schlüssel darin: Du kopierst ihn und fügst ihn unverändert im Terminal ein.

Danach listet in Claude Code der Befehl `/mcp` die verbundenen Server auf: Darunter muss **flow** erscheinen. Ab dann kannst du fragen „Was siehst du auf Flow?“, und der Assistent antwortet mit den Ordnern, die du ihm geöffnet hast.

MCP ist der Standard, mit dem sich Assistenten mit einer Datenquelle verbinden. Wir nennen ihn, weil du dieses Wort in den Einstellungen der Assistenten finden wirst.

Kopiere den Block, den Flow dir gibt, kein Beispiel von anderswo: Der Block von Flow enthält bereits den echten Schlüssel. Ein Block mit dem Platzhalter statt des Schlüssels lässt sich trotzdem installieren, und der Assistent antwortet dann, dass er von Flow nichts weiß.

05 Cursor verbinden

In Cursor kommt der fertige Block an eine dieser beiden Stellen, nach Wahl:

- **Settings → MCP → Add server;**
- oder die Datei `.cursor/mcp.json` des Projekts, wenn die Verbindung beim Projekt bleiben soll.

Der Block zum Einfügen ist der zweite von denen, die dir die Seite der Verbindung zeigt, und er enthält bereits den Schlüssel. Nach dem Speichern zeigt Cursor **flow** unter den verfügbaren Servern.

Es gilt der übliche Hinweis: Kopiere den Block, den Flow dir gibt, kein Beispiel von anderswo. Ein Platzhalter statt des Schlüssels fällt nicht auf, und dann findet der Assistent nichts.

06 Claude Desktop verbinden

Claude Desktop speichert die Verbindungen in einer Konfigurationsdatei. Du erreichst sie in der App über **Settings → Developer → Edit Config**; das öffnet `claude_desktop_config.json`.

In diese Datei fügst du den Block ein, den die Seite der Verbindung für Claude Desktop angibt, und dann **startest du Claude Desktop neu**: Die Verbindungen liest es beim Start.

Auf Flow musst du nichts installieren. Claude Desktop nutzt für die Kommunikation mit dem Schlüssel eine kleine Brücke, die sich beim ersten Mal selbst herunterlädt: Wenn die erste Antwort ein paar Sekunden dauert, liegt es daran.

07 Codex verbinden

In Codex kommt der Block in die Datei `~/.codex/config.toml`. In der App erreichst du sie über **Settings → Configuration**; im Terminal gibt es auch den Befehl `codex mcp add`.

Nach dem Speichern der Datei **starte Codex neu**. Im Chat listet `/mcp` die verbundenen Server auf: darunter **flow**.

Zwei Hinweise, beide aus Fehlern gelernt:

- der Eintrag „**Connections**“ in den Einstellungen von Codex ist etwas anderes (die Fernsteuerung des Computers) und hat nichts mit den mit Flow verbundenen Assistenten zu tun;
- wenn du einen Beispielblock einfügst und den Platzhalter statt des Schlüssels stehen lässt, zeigt Codex trotzdem „**Authenticated**“ an, aber der Assistent

antwortet dann, dass er keine Flow-Werkzeuge hat. Der richtige Block ist der, den dir die Seite der Verbindung gibt, mit dem Schlüssel schon darin.

08 ChatGPT verbinden

ChatGPT geht einen anderen Weg: **kein Schlüssel zum Kopieren**. Du gibst ihm nur die Adresse deines Flow, und es öffnet eine Flow-Seite, auf der du dich anmeldest, die Ordner wählst und bestätigst. Die Verbindung erscheint von selbst unter Konto → KI-Assistenten, mit dem Namen des Assistenten, und wird dort wie alle anderen verwaltet.

Der Weg in ChatGPT:

1. **Settings → Security and access**, ganz unten, **Developer mode**: Aktiviere ihn. ChatGPT kennzeichnet ihn als „hohes Risiko“: Das ist der Hinweis, den es allen zeigt, die einen eigenen Server hinzufügen, und er ist genau dafür da.
2. **Settings → Plugins → Browse plugins**.
3. Oben rechts die Schaltfläche **+**, die das Formular „New plugin“ öffnet.
4. Name **Flow**; als Link die Adresse deines Flow, gefolgt von `/mcp`, zum Beispiel `https://flow.kaigrid.ai/mcp`; Authentifizierung **OAuth**; hake „I understand and want to continue“ ab; **Create**.
5. **Sign in with Flow**: Es öffnet sich die Flow-Seite „... möchte auf Flow zugreifen“, auf der du zwischen Nur lesen und Darf ändern wählst, die Ordner abhakst und den Hinweis zu den Daten liest. **Erlauben** (oder **Nicht erlauben**, und es passiert nichts).
6. Wähle in einem neuen Chat Flow unter den Plugins und probiere es aus: „Was siehst du auf Flow?“.

Auf der Zustimmungssseite siehst du in den Team-Bereichen **nur** die Ordner, die der Administrator geöffnet hat: keine Schlösser, keine Liste zum Entschlüsseln.

ChatGPT ändert die Namen seiner Einträge häufig: Bis vor Kurzem hießen die Plugins Connectors. Wenn ein Eintrag nicht mehr so heißt, such ihn nach dem, was er tut.

09 Claude im Web verbinden

Claude im Web geht denselben Weg wie ChatGPT: **kein Schlüssel zum Kopieren**. Du gibst ihm die Adresse deines Flow, und es öffnet eine Flow-Seite, auf der du dich anmeldest, die Ordner wählst und bestätigst.

In Claude: **Settings** → **Connectors** → „**Add custom connector**“, und als Adresse die Adresse deines Flow, gefolgt von `/mcp`, zum Beispiel `https://flow.kaigrid.ai/mcp`.

Ab da ist alles gleich: Es öffnet sich die Seite „... möchte auf Flow zugreifen“, auf der du zwischen Nur lesen und Darf ändern wählst, die Ordner abhakst und den Hinweis zu den Daten liest. Nach der Bestätigung erscheint die Verbindung von selbst unter **Konto** → **KI-Assistenten**, mit dem Namen des Assistenten, und wird wie alle anderen verwaltet: Du änderst die Ordner, änderst, was er darf, oder widerrufst sie.

Auch hier gilt, was für ChatGPT gilt: In den Team-Bereichen siehst du auf der Zustimmungsseite **nur** die Ordner, die der Administrator geöffnet hat.

10 Es sich anders überlegen

Nichts von dem, was du gewählt hast, gilt für immer, und **der Schlüssel muss nie neu erstellt werden**.

- **Die Ordner:** Unter Konto → KI-Assistenten öffnest du die Verbindung und änderst die Häkchen. Die neuen Ordner gelten ab der nächsten Anfrage des Assistenten, und im Assistenten musst du nichts anfassen.
- **Was er darf:** Von Nur lesen zu „Darf ändern“ und zurück wechselst du auf dieselbe Weise.
- **Widerrufen:** Der Assistent sieht Flow **sofort** nicht mehr. Das nutzt du, wenn ein Projekt endet, wenn ein Computer verloren geht oder einfach, wenn du fertig bist.

Die Seite zeigt für jede Verbindung, wann du sie erstellt hast, **wann sie zuletzt benutzt wurde** und wann sie abläuft: Wenn eine seit Monaten niemand nutzt, sieht man das.

Wenn der Assistent etwas versucht, das die Verbindung nicht erlaubt (eine Änderung mit einer Verbindung auf Nur lesen oder in einem Ordner, in dem der

Administrator kein Schreiben gesetzt hat), erhält er eine Ablehnung, die erklärt, was fehlt, und teilt dir das mit, statt stillschweigend zu scheitern.

11 Wer im Ordner arbeitet, weiß es

Ein für einen Assistenten geöffneter Ordner ist keine Privatsache der Person, die die Verbindung erstellt hat: Wer darin arbeitet, muss es wissen können.

Deshalb steht neben dem Namen der Ordner und Dateien, die ein Assistent sieht, ein **kleines Symbol**; fährst du darüber, zeigt es, zu welcher Verbindung es gehört. Im Infobereich der Datei steht dasselbe ausgeschrieben: „**Sichtbar für: Claude im Projekt Dainese**“. Das sehen alle, die dort arbeiten, nicht nur du.

Im **Aktivitätsprotokoll** bleibt alles nachvollziehbar: wann eine Verbindung erstellt wird, wann sich ihre Ordner ändern, wann sie widerrufen wird, **jedes Lesen von Inhalten** (welche Verbindung, welche Datei, wann), jeder Download-Link und jede Änderung. Das Protokoll der Assistenten ist immer aktiv.

Was das Protokoll **nicht** enthält, ist die Unterhaltung: Der Administrator sieht, welche Dateien der Assistent gelesen hat, nicht, was du ihn gefragt hast.

12 Was der Administrator entscheidet

In den Team-Bereichen legt das Unternehmen fest, was sich für einen Assistenten öffnen lässt. Der Administrator tut das in **Admin-Konsole → KI-Assistenten**, mit „Liste bearbeiten“: derselbe Spaltenbaum, in dem jeder Bereich und jeder Ordner ein Kästchen mit **drei Zuständen** hat, die du per Klick durchläufst.

- **Nein**, leeres Kästchen: Die Assistenten sehen ihn nicht. Das ist der Ausgangszustand für alles: Ein Unternehmen, das nichts öffnet, gibt nichts preis.
- **Lesen**, das Auge: Die Assistenten dürfen ihn lesen.
- **Schreiben**, der Stift: Sie dürfen ihn auch ändern, wenn die Verbindung auf „Darf ändern“ steht.

Der Zustand gilt für alles, was der Ordner enthält, und ein Unterordner kann einen **anderen** haben: Es gilt immer der nächstgelegene. Der Bereich „Kunden“ auf Lesen kann darin „Entwürfe“ auf Schreiben haben; ein Ordner auf Schreiben kann

darin „Verträge“ nur auf Lesen haben. Die Unterordner zeigen die geerbte Stufe abgeschwächt an: Ein Klick ändert sie nur dort, ein weiterer setzt sie zurück.

Eines geht nicht: **innerhalb eines geöffneten Ordners wieder „Nein“ setzen.**

Keine unsichtbaren Lücken: Wenn ein Unterordner nicht sichtbar sein soll, öffnet man die Geschwisterordner und nicht den übergeordneten.

Die **persönlichen Bereiche** stehen nicht in dieser Liste: Über sie entscheidet jeder Nutzer selbst.

Einen Eintrag zu entfernen oder herabzustufen **gilt sofort**, auch für bestehende Verbindungen. Damit es keine Überraschung wird, zeigt die Seite neben jedem Eintrag, wie viele Verbindungen ihn nutzen. Auf derselben Seite steht die Liste der **Verbindungen des Unternehmens**: wem sie gehören, auf welchen Ordnern, wann sie zuletzt benutzt wurden.

13 Sicherheit und Vertraulichkeit

Gelesene Dokumente gehen an den Anbieter des Assistenten. Wenn der Assistent eine Datei liest, gelangt dieser Text zum Anbieter des Assistenten (Anthropic, OpenAI oder wer an ihrer Stelle), unter dem Vertrag, den du oder dein Unternehmen mit diesem Anbieter habt. Flow sendet nichts aus eigenem Antrieb: Es sendet das, was der Assistent anfragt, innerhalb der Ordner, die du ihm geöffnet hast. Das ist der Grund, warum es sich lohnt, wenige Ordner zu öffnen und sie gut auszuwählen.

Ein Dokument kann Anweisungen an den Assistenten enthalten: Zeilen, die eigens geschrieben wurden, damit er sie liest und ausführt. Das gilt für jeden Assistenten, und Flow setzt vier Schutzmaßnahmen dagegen: Anfangs liest die Verbindung nur; der Text erreicht den Assistenten als Inhalt eines Dokuments gekennzeichnet, nicht als Befehl; der Assistent kann keine Links nach außen erstellen; und alles, was er ändert, lässt sich über Papierkorb und Versionen rückgängig machen.

Ein verlorener Schlüssel wird mit einem Klick widerrufen, und die Verbindung kann von Anfang an ein Ablaufdatum haben. Die Seite zeigt für jede, wann sie zuletzt benutzt wurde.

Ein Assistent sieht nie mehr als du. Die Verbindung lebt innerhalb deiner Berechtigungen: Wird dir ein Bereich entzogen, verlieren deine Verbindungen ihn

im selben Augenblick. Und sie gilt nur für die Assistenten: Mit diesem Schlüssel gelangt man nicht in den Rest von Flow.

14 Häufige Fragen

Sieht der Assistent alle meine Dateien? Nein: nur die Ordner, die du in der Verbindung abgehakt hast.

Kann ein Kollege einem Assistenten einen vertraulichen Ordner öffnen? Nur wenn er diesen Ordner selbst schon sieht, und nur wenn der Administrator ihn freigebbar gemacht hat.

Kann ich es mir später anders überlegen? Ja: Du änderst die Ordner oder widerrufst, wann du willst, und es gilt sofort. Der Schlüssel bleibt derselbe.

Kann der Assistent meine Dateien löschen? Nur wenn du „Darf ändern“ gewählt hast und nur dort, wo der Administrator Schreiben gesetzt hat. Und selbst dann landen sie im Papierkorb, aus dem sie sich wiederherstellen lassen.

Woran erkenne ich, ob ein Ordner für einen Assistenten geöffnet ist? Er hat ein kleines Symbol neben dem Namen, und der Infobereich der Datei zeigt „Sichtbar für“ mit dem Namen der Verbindung.

Ich habe den Schlüssel verloren. Er lässt sich nicht wiederherstellen: Widerrufe die Verbindung und erstelle eine neue.

Funktioniert es mit ChatGPT? Ja, im Web. Und mit Claude Code, Claude Desktop, Cursor und Codex.

Muss ich etwas installieren? Auf Flow nicht, gar nichts. Claude Desktop nutzt eine kleine Brücke, die sich beim ersten Start selbst herunterlädt.

Sieht der Administrator, was ich den Assistenten frage? Nein. Er sieht, welche Dateien der Assistent gelesen oder geändert hat, nicht die Unterhaltung.

15 Wenn etwas nicht funktioniert

Der Assistent sagt, er habe keine Flow-Werkzeuge oder wisse nicht, was das ist. Fast immer liegt es am von Hand eingefügten Block, in dem der Platzhalter statt des Schlüssels stehen geblieben ist. Manche Assistenten zeigen in diesem

Fall trotzdem „Authenticated“ an. Kopiere den Block erneut von der Seite der Verbindung, die den Schlüssel bereits enthält, und starte den Assistenten neu.

Der Assistent sieht einen Ordner nicht, den ich abgehakt hatte. Prüfe die Verbindung unter Konto → KI-Assistenten: Wenn dieser Ordner ein **Schloss** hat, hat der Administrator ihn für Assistenten geschlossen, und das gilt sofort, auch für bestehende Verbindungen.

Er sagt, er dürfe nichts ändern. Entweder steht die Verbindung auf **Nur lesen**, dann änderst du das in ihrer Karte, oder dieser Ordner hat keinen **Stift**: In den Team-Bereichen setzt ihn der Administrator.

Die Verbindung ist abgelaufen. Die Ablaufdaten hast du selbst beim Erstellen gewählt. Eine abgelaufene Verbindung lässt sich nicht verlängern: Du erstellst eine neue.

ChatGPT sieht die neuen Funktionen nicht. ChatGPT merkt sich die Liste der Operationen vom Zeitpunkt, als du das Plugin erstellt hast, und liest sie nicht von selbst neu ein. Öffne die Karte des Plugins Flow und klicke auf **Refresh**; wenn es das nicht gibt, lösche das Plugin und erstelle es neu. Öffne dann einen **neuen Chat**. Die Berechtigungen dagegen gelten immer sofort, egal, was ChatGPT gespeichert hat.

Ich habe versehentlich widerrufen. Das lässt sich nicht rückgängig machen: Du erstellst eine neue Verbindung und richtest sie im Assistenten erneut ein. Das dauert eine Minute.