

Guida agli assistenti AI

La versione sempre aggiornata, con la ricerca dentro il testo, è sul sito.

IN QUESTA GUIDA

- | | |
|------------------------------|-----------------------------|
| 01 Cos'è | 09 Claude sul web |
| 02 Cosa può fare | 10 Cambiare idea |
| 03 Primo collegamento | 11 «Visibile a» |
| 04 Claude Code | 12 L'amministratore |
| 05 Cursor | 13 Sicurezza |
| 06 Claude Desktop | 14 Domande frequenti |
| 07 Codex | 15 Se non va |
| 08 ChatGPT | |

01 Cos'è un assistente collegato

Per far leggere un documento a un assistente AI (Claude, ChatGPT, Cursor, Codex), di solito lo si scarica e lo si ricarica nella chat: una copia in più che gira per conto suo, senza versioni, senza permessi, senza che resti traccia di chi ha letto cosa.

Con **Assistenti AI** colleghi l'assistente a Flow una volta sola, e da lì in poi lavora sui documenti dove sono già. Tre cose reggono tutto il resto:

1. **Scegli tu le cartelle.** Un collegamento apre solo le cartelle che elenchi. Fuori da quelle, per l'assistente non esiste niente: non può aprirle, cercarle, nemmeno sapere che ci sono.
2. **L'azienda decide cosa è apribile.** Negli spazi di team è l'amministratore a stabilire, cartella per cartella, cosa si può aprire e se in lettura o anche in scrittura. Tu scegli dentro quell'elenco: puoi restringerlo, mai allargarlo.
3. **Di partenza legge e basta.** Un collegamento nuovo è in **Sola lettura**. Può modificare solo se lo scegli tu e solo dove l'amministratore l'ha permesso, e niente è definitivo: restano il cestino e le versioni.

Nel tuo **spazio personale** decidi da solo, senza passare dall'amministratore.

I collegamenti si creano e si gestiscono in **Account → Assistenti Ai**.

Assistenti Ai dipende dal piano e oggi si attiva su richiesta: se nel tuo Account non trovi la voce, scrivici. Serve anche che il piano legga il testo dei documenti (la stessa lettura che alimenta la ricerca nei contenuti), altrimenti l'assistente troverebbe i nomi dei file e non quello che c'è dentro. Dove il piano non arriva, l'assistente lo dice: non inventa.

02 Cosa può fare, e cosa no

Dentro le cartelle che gli hai aperto, un assistente collegato **legge sempre**:

- elenca il contenuto di una cartella e le proprietà di un file: dimensione, date, versione, tag;
- **legge il testo** di PDF, documenti Office e immagini con testo. È il testo che Flow ha già estratto per la ricerca, quindi non ci sono conversioni da fare né limiti di dimensione del file;
- **cerca** per nome e dentro il contenuto, con filtri per cartella, tipo e data;
- vede le versioni di un file e cosa è stato aggiunto, modificato o cancellato di recente;
- vede lo spazio usato e la quota dell'azienda;
- ottiene un collegamento temporaneo, valido un'ora, per scaricare un file così com'è;
- vede i link di condivisione e di deposito che **tu** hai creato su quelle cartelle, non quelli dei colleghi.

Se il collegamento è «Può modificare», e solo nelle cartelle che l'amministratore ha messo in Scrittura (o nel tuo spazio personale), fa anche: creare cartelle, creare file di testo fino a 5 MB, copiare, spostare, rinominare, mandare nel cestino (chiedendoti conferma) e riportare un file a una versione precedente. Se un nome esiste già non lo sovrascrive: lo fa solo se glielo chiedi, e la versione vecchia resta comunque nelle versioni.

Quello che non fa, nemmeno se glielo chiedi:

- uscire dalle cartelle che gli hai aperto: questo non succederà mai, in nessun caso;

- creare link di condivisione o di deposito: è l'unico gesto con cui un errore farebbe uscire documenti dall'azienda, e per adesso resta fuori;
- cancellare in modo definitivo: tutto passa dal cestino;
- spostare, rinominare o cestinare le cartelle stesse che gli hai aperto;
- toccare un file che un collega ha in modifica esclusiva;
- vedere Dati protetti, firme, task e repository Git: vede file e cartelle, e basta.

Se un file non ha testo leggibile (un archivio compresso, un formato che non conosce), te lo dice. Non inventa.

03 Il primo collegamento

Account → Assistenti AI → «Nuovo collegamento». Quattro scelte:

1. **Nome:** serve a te, per riconoscerlo fra sei mesi. «Claude sul progetto Dainese» dice più di «Claude».
2. **Cosa può fare:** **Sola lettura**, già selezionato, oppure **Può modificare**. Nel dubbio lascia la prima: si cambia quando vuoi, senza rifare niente.
3. **Scadenza:** mai, 30 giorni, 90 giorni, 1 anno. Per una consulenza che finisce, una scadenza è più comoda di un promemoria.
4. **Cartelle aperte:** l'albero a colonne, lo stesso della sincronizzazione selettiva. Spunti una o più cartelle, anche in spazi diversi.

Sulle cartelle vale una regola sola, e conviene tenerla a mente: **spuntare una cartella apre tutto ciò che contiene**. Non si toglie un pezzo da dentro: se una sottocartella non deve vedersi, spunti le sorelle e non la madre.

Negli spazi di team quello che l'amministratore non ha aperto ha un **lucchetto** («Non apribile agli assistenti: deciso dall'amministratore») e le cartelle in cui un assistente potrà anche scrivere hanno una **matita**. Nel tuo spazio personale spunti quello che vuoi.

Sopra le cartelle resta scritto, sempre: *«I documenti che l'assistente legge vengono inviati al fornitore di quell'assistente (Anthropic, OpenAI...). Apri solo le cartelle che servono.»* È il motivo per cui conviene aprire poco.

Alla conferma compaiono la **chiave di accesso**, l'**indirizzo del server** e un blocco pronto da copiare per ciascun assistente.

La chiave si vede una volta sola. Copiala adesso: dopo non è più recuperabile da nessuno, nemmeno da noi. Se la perdi non è un dramma: revochi il collegamento e ne crei un altro in un minuto.

04 Collegare Claude Code

Claude Code si collega dal **terminale**. Nella pagina del collegamento, sotto «Come collegarlo», il primo blocco è già pronto con la tua chiave dentro: si copia e si incolla nel terminale così com'è.

Poi, dentro Claude Code, il comando `/mcp` elenca i server collegati: fra questi deve comparire **flow**. Da quel momento puoi chiedere «cosa vedi su Flow?» e l'assistente risponde con le cartelle che gli hai aperto.

MCP è lo standard con cui gli assistenti si collegano a una fonte di dati. Lo nominiamo perché è la parola che troverai scritta nelle impostazioni degli assistenti.

Copia il blocco che ti dà Flow, non un esempio letto altrove: quello di Flow contiene già la chiave vera. Un blocco con il segnaposto al posto della chiave si installa lo stesso, e l'assistente poi risponde che di Flow non sa niente.

05 Collegare Cursor

In Cursor il blocco pronto va in uno di questi due posti, a scelta:

- **Impostazioni → MCP → aggiungi server;**
- oppure il file `.cursor/mcp.json` del progetto, se preferisci che il collegamento resti insieme al progetto.

Il blocco da incollare è il secondo di quelli che la pagina del collegamento ti mostra. Contiene già la chiave. Dopo averlo salvato, Cursor mostra **flow** fra i server disponibili.

Vale l'avvertenza di sempre: copia il blocco che ti dà Flow, non un esempio trovato altrove: un segnaposto al posto della chiave passa inosservato e poi l'assistente non trova niente.

06 Collegare Claude Desktop

Claude Desktop tiene i collegamenti in un file di configurazione. Ci si arriva dall'app: **Impostazioni** → **Sviluppatore** → **Modifica configurazione**, che apre `claude_desktop_config.json`.

Dentro quel file si incolla il blocco che la pagina del collegamento indica per Claude Desktop, e poi **si riavvia Claude Desktop**: i collegamenti li legge all'avvio.

Non devi installare niente su Flow. Claude Desktop, per parlare con la chiave, usa un piccolo ponte che si scarica da sé la prima volta: se la prima risposta tarda qualche secondo è quello.

07 Collegare Codex

In Codex il blocco va nel file `~/codex/config.toml`. Dall'app ci arrivi con **Impostazioni** → **Configurazione**; da terminale c'è anche il comando `codex mcp add`.

Salvato il file, **riavvia Codex**. In chat, `/mcp` elenca i server collegati: fra questi **flow**.

Due avvertenze, tutte e due imparate sbagliando:

- la voce **«Connessioni»** delle impostazioni di Codex è un'altra cosa (il controllo remoto del computer) e non c'entra con gli assistenti collegati a Flow;
- se incolli un blocco d'esempio lasciando il segnaposto al posto della chiave, Codex scrive comunque **«Autenticato»**, ma poi l'assistente risponde che non ha strumenti di Flow. Il blocco giusto è quello che ti dà la pagina del collegamento, con la chiave già dentro.

08 Collegare ChatGPT

ChatGPT prende un'altra strada: **niente chiave da copiare**. Gli dai solo l'indirizzo del tuo Flow e ChatGPT apre una pagina di Flow dove entri, scegli le cartelle e confermi. Il collegamento compare da solo in Account → Assistenti AI, col nome dell'assistente, e da lì si gestisce come tutti gli altri.

Il percorso, dentro ChatGPT:

1. **Impostazioni → Sicurezza e accesso**, in fondo, **Modalità sviluppatore**: accendila. ChatGPT la segnala come «rischio elevato»: è l'avviso che mette a chiunque aggiunga un server proprio, e serve per questo.
2. **Impostazioni → Plugin → Sfoglia plugin**.
3. In alto a destra il tasto **+**, che apre il modulo «Nuovo plugin».
4. Nome **Flow**; nel collegamento, l'indirizzo del tuo Flow seguito da `/mcp`, per esempio `https://flow.kaigrid.ai/mcp`; autenticazione **OAuth**; spunta «Ho capito e voglio continuare»; **Crea**.
5. **Accedi con Flow**: si apre la pagina di Flow «... chiede di accedere a Flow», dove scegli fra Sola lettura e Può modificare, spunti le cartelle e leggi l'avviso sui dati. **Consenti** (o **Non consentire**, e non succede niente).
6. In una chat nuova scegli Flow fra i plugin e prova: «cosa vedi su Flow?».

Nella pagina di consenso, negli spazi di team vedi **solo** le cartelle che l'amministratore ha aperto: niente lucchetti, niente elenco da decifrare.

ChatGPT cambia spesso i nomi delle sue voci: fino a poco fa i plugin si chiamavano connettori. Se una voce non si chiama più così, cercala per quello che fa.

09 Collegare Claude sul web

Claude sul web prende la stessa strada di ChatGPT: **niente chiave da copiare**. Gli dai l'indirizzo del tuo Flow e Claude apre una pagina di Flow dove entri, scegli le cartelle e confermi.

In Claude: **Impostazioni → Connettori → «Aggiungi connettore personalizzato»**, e come indirizzo l'indirizzo del tuo Flow seguito da `/mcp`, per esempio `https://flow.kaigrid.ai/mcp`.

Da lì in poi è identico: si apre la pagina «... chiede di accedere a Flow», dove scegli fra Sola lettura e Può modificare, spunti le cartelle e leggi l'avviso sui dati. Alla conferma il collegamento compare da solo in **Account → Assistenti Ai**, col nome dell'assistente, e si gestisce come tutti gli altri: cambi le cartelle, cambi cosa può fare, revochi.

Vale anche qui quello che vale per ChatGPT: negli spazi di team, nella pagina di consenso, vedi **solo** le cartelle che l'amministratore ha aperto.

10 Cambiare idea

Niente di quello che hai scelto è per sempre, e **non si rifà mai la chiave**.

- **Le cartelle:** da Account → Assistenti AI apri il collegamento e cambi le spunte. Le nuove cartelle valgono dalla richiesta successiva dell'assistente, e nell'assistente non devi toccare niente.
- **Cosa può fare:** si passa da Sola lettura a «Può modificare» e viceversa allo stesso modo.
- **Revoca:** l'assistente smette **subito** di vedere Flow. Si usa quando un progetto finisce, quando un computer si perde, o semplicemente quando hai finito.

La pagina dice, per ogni collegamento, quando l'hai creato, **l'ultimo uso** e la scadenza: se uno non lo usa nessuno da mesi, si vede.

Se l'assistente prova a fare qualcosa che il collegamento non permette (una modifica con un collegamento in sola lettura, o in una cartella dove l'amministratore non ha messo Scrittura), riceve un rifiuto che spiega cosa manca. Te lo riferisce invece di fallire in silenzio.

11 Chi lavora nella cartella lo sa

Una cartella aperta a un assistente non è una cosa privata di chi ha creato il collegamento: chi ci lavora deve poterlo sapere.

Per questo, accanto al nome delle cartelle e dei file che un assistente vede, c'è una **piccola icona**; passandoci sopra dice a quale collegamento. Nel pannello informazioni del file la stessa cosa è scritta per esteso: **«Visibile a: Claude sul progetto Dainese»**. La vedono tutti quelli che lavorano lì, non solo tu.

Nel **registro attività** resta traccia di tutto: quando un collegamento viene creato, quando cambiano le sue cartelle, quando viene revocato, **ogni lettura di contenuto** (quale collegamento, quale file, quando), ogni link di scaricamento e ogni modifica. Il registro degli assistenti è sempre acceso.

Quello che il registro **non** contiene è la conversazione: l'amministratore vede quali file l'assistente ha letto, non cosa gli hai chiesto.

12 Cosa decide l'amministratore

Negli spazi di team è l'azienda a stabilire cosa si può aprire a un assistente. L'amministratore lo fa in **Console amministratore** → **Assistenti AI**, con «Modifica l'elenco»: lo stesso albero a colonne, dove ogni spazio e ogni cartella ha una casella con **tre stati**, che si scorrono con un clic.

- **No** (casella vuota): gli assistenti non la vedono. È lo stato di partenza di tutto: un'azienda che non apre niente non espone niente.
- **Lettura** (l'occhio): gli assistenti possono leggerla.
- **Scrittura** (la matita): possono anche modificarla, se il collegamento è «Può modificare».

Lo stato vale per tutto ciò che la cartella contiene, e una sottocartella può averne uno **diverso**: vince sempre il più vicino. Lo spazio «Clienti» in Lettura può avere dentro «Bozze» in Scrittura; una cartella in Scrittura può avere dentro «Contratti» in sola Lettura. Le sottocartelle mostrano smorzato il livello che ereditano: un clic lo cambia solo lì, un altro lo riporta com'era.

Una cosa non si può fare: **rimettere «No» dentro una cartella aperta**. Niente buchi invisibili: se una sottocartella non deve vedersi, si aprono le sorelle e non la madre.

Gli **spazi personali** non sono in quell'elenco: li decide ogni utente per sé.

Togliere o abbassare una voce **vale subito**, anche per i collegamenti che esistono già. Perché non sia una sorpresa, accanto a ogni voce la pagina dice quanti collegamenti la stanno usando. Nella stessa pagina c'è l'elenco dei **collegamenti dell'azienda**: di chi sono, su quali cartelle, l'ultimo uso.

13 Sicurezza e riservatezza

I documenti letti escono verso il fornitore dell'assistente. Quando l'assistente legge un file, quel testo arriva a chi fornisce l'assistente (Anthropic, OpenAI o chi per loro) con il contratto che tu o la tua azienda avete con quel fornitore. Flow non manda niente di sua iniziativa: manda quello che l'assistente chiede, dentro le cartelle che gli hai aperto. È il motivo per cui conviene aprire poche cartelle e sceglierle bene.

Un documento può contenere istruzioni rivolte all'assistente: righe scritte apposta perché le legga e le esegua. Vale per qualunque assistente, e Flow ci mette quattro difese: di partenza il collegamento legge e basta; il testo arriva all'assistente marcato come contenuto di un documento, non come un ordine; l'assistente non può creare link verso l'esterno. Infine, tutto ciò che modifica si disfa dal cestino e dalle versioni.

Una chiave persa si revoca in un clic, e il collegamento può avere una scadenza fin dall'inizio. La pagina mostra l'ultimo uso di ciascuno.

Un assistente non vede mai più di te. Il collegamento vive dentro i tuoi permessi: se ti tolgono uno spazio, i tuoi collegamenti lo perdono nello stesso istante. E vale solo per gli assistenti: con quella chiave non si entra nel resto di Flow.

14 Domande frequenti

L'assistente vede tutti i miei file? No: solo le cartelle che hai spuntato nel collegamento.

Un collega può aprire a un assistente una cartella riservata? Solo se quella cartella la vede già lui, e solo se l'amministratore l'ha resa apribile.

Posso cambiare idea dopo? Sì: cambi le cartelle o revochi quando vuoi, e vale subito. La chiave resta quella.

L'assistente può cancellare i miei file? Solo se hai scelto «Può modificare» e solo dove l'amministratore ha messo Scrittura. E anche allora finiscono nel cestino, da cui si ripristinano.

Come faccio a sapere se una cartella è aperta a un assistente? Ha una piccola icona accanto al nome, e il pannello informazioni del file dice «Visibile a», col nome del collegamento.

Ho perso la chiave. Non è recuperabile: revoca il collegamento e creane uno nuovo.

Funziona con ChatGPT? Sì, dal web. E con Claude Code, Claude Desktop, Cursor e Codex.

Serve installare qualcosa? Su Flow no, niente. Claude Desktop usa un piccolo ponte che si scarica da sé al primo avvio.

L'amministratore vede cosa chiedo all'assistente? No. Vede quali file l'assistente ha letto o modificato, non la conversazione.

15 Se qualcosa non va

L'assistente dice che non ha strumenti di Flow, o non sa cosa sia. Quasi sempre è il blocco incollato a mano, con il segnaposto rimasto al posto della chiave. Alcuni assistenti in quel caso scrivono comunque «Autenticato». Ricopia il blocco dalla pagina del collegamento, che contiene già la chiave, e riavvia l'assistente.

L'assistente non vede una cartella che avevo spuntato. Controlla il collegamento in Account → Assistenti AI: se quella cartella ha un **lucchetto**, l'amministratore l'ha chiusa agli assistenti, e la chiusura vale subito, anche sui collegamenti già fatti.

Dice di non poter modificare. O il collegamento è in **Sola lettura**, e lo cambi dalla sua scheda, o quella cartella non ha la **matita**: negli spazi di team è l'amministratore a metterla.

Il collegamento è scaduto. Le scadenze sono quelle che hai scelto tu alla creazione. Un collegamento scaduto non si prolunga: se ne crea un altro.

ChatGPT non vede le funzioni nuove. ChatGPT tiene in memoria l'elenco delle operazioni di quando hai creato il plugin. Non lo rilegge da sé. Apri la scheda del plugin Flow e premi **Aggiorna**; se non c'è, elimina il plugin e ricrealo. Poi apri una **chat nuova**. I permessi invece valgono sempre subito, qualunque cosa ChatGPT abbia in memoria.

Ho revocato per sbaglio. Non si ripristina: si crea un collegamento nuovo e si rifà il giro nell'assistente. Ci vuole un minuto.