
AI assistants guide

The always up-to-date version, with search inside the text, is on the website.

IN THIS GUIDE

- | | |
|-------------------------------------|---|
| 01 What it is | 09 Claude on the web |
| 02 What it can do | 10 Changing your mind |
| 03 First connection | 11 "Visible to" |
| 04 Claude Code | 12 The administrator |
| 05 Cursor | 13 Security |
| 06 Claude Desktop | 14 Frequently asked questions |
| 07 Codex | 15 If it goes wrong |
| 08 ChatGPT | |

01 What a connected assistant is

To have an AI assistant (Claude, ChatGPT, Cursor, Codex) read a document, you usually download it and upload it again into the chat: one more copy travelling on its own, with no versions, no permissions and no record of who read what.

With **AI assistants** you connect the assistant to Flow once, and from then on it works on documents where they already are. Three principles hold everything else up:

1. **You choose the folders.** A connection opens only the folders you list. Outside those, nothing exists for the assistant: it cannot open them, search them, or even know they are there.
2. **Your company decides what can be opened.** In team spaces, the administrator decides, folder by folder, what can be opened and whether for reading only or for writing too. You choose within that list: you can narrow it, never widen it.
3. **By default it only reads.** A new connection is **Read only**. It can make changes only if you choose so, and only where the administrator has allowed it, and

nothing is final: the trash and versions remain.

In your **personal space** you decide on your own, without going through the administrator.

Connections are created and managed in **Account → Ai assistants**.

Ai assistants depends on the plan, and for now it is turned on on request: if you cannot find the item in your Account, write to us. The plan also needs to read the text of documents (the same reading that powers content search), otherwise the assistant would find file names but not what is inside them. Where the plan does not cover it, the assistant says so: it does not make things up.

02 What it can do, and what it cannot

Inside the folders you have opened to it, a connected assistant **can always read**:

- it lists the contents of a folder and the properties of a file: size, dates, version, tags;
- it **reads the text** of PDFs, Office documents and images containing text. This is the text Flow has already extracted for search, so there are no conversions to run and no file size limits;
- it **searches** by name and within content, with filters for folder, type and date;
- it sees a file's versions and what has been added, changed or deleted recently;
- it sees the space used and the company's quota;
- it gets a temporary link, valid for one hour, to download a file as it is;
- it sees the sharing and upload links that **you** created on those folders, not your colleagues' links.

If the connection is "Can edit", and only in the folders the administrator has set to Write (or in your personal space), it can also: create folders, create text files up to 5 MB, copy, move, rename, send to the trash (asking you for confirmation) and restore a file to an earlier version. If a name already exists, it does not overwrite it: it does so only if you ask, and the old version stays in the versions anyway.

What it does not do, even if you ask:

- leave the folders you have opened to it: this will never happen, under any circumstances;
- create sharing or upload links: it is the only action through which a mistake could send documents outside the company, and for now it is left out;
- delete permanently: everything goes through the trash;
- move, rename or trash the very folders you have opened to it;
- touch a file a colleague is editing exclusively;
- see Protected data, signatures, tasks and Git repositories: it sees files and folders, nothing else.

If a file has no readable text (a compressed archive, a format it does not know), it tells you. It does not make things up.

03 Your first connection

Account → Ai assistants → "New connection". Four choices:

1. **Name:** it is for you, so you recognize it six months from now: "Claude on the Dainese project" says more than "Claude".
2. **What it can do:** **Read only**, already selected, or **Can edit**. If in doubt, keep the first: you can change it whenever you like, without redoing anything.
3. **Expiry:** never, 30 days, 90 days, 1 year. For a consultancy that comes to an end, an expiry date is more convenient than a reminder.
4. **Open folders:** the column tree, the same one used for selective sync. Tick one or more folders, even in different spaces.

One rule applies to folders, and it is worth keeping in mind: **ticking a folder opens everything it contains**. You cannot remove a part from inside: if a subfolder must stay hidden, tick its sibling folders and not the parent.

In team spaces, what the administrator has not opened has a **padlock** ("Cannot be opened to assistants: decided by the administrator") and folders where an assistant will also be able to write have a **pencil**. In your personal space you tick whatever you want.

Above the folders this notice is always shown: *"Documents the assistant reads are sent to that assistant's provider (Anthropic, OpenAI...). Open only the folders you need."* This is why it pays to open little.

When you confirm, you see the **access key**, the **server address** and a ready-to-copy block for each assistant.

The key is shown only once. Copy it now: afterwards nobody can recover it, not even us. If you lose it, it is no big deal: revoke the connection and create another one in a minute.

04 Connecting Claude Code

Claude Code connects from the **terminal**. On the connection page, under "How to connect it", the first block is ready with your key already inside: you copy it and paste it into the terminal as it is.

Then, inside Claude Code, the `/mcp` command lists the connected servers: **flow** must appear among them. From then on you can ask "what can you see on Flow?" and the assistant answers with the folders you have opened to it.

MCP is the standard assistants use to connect to a data source. We mention it because it is the word you will find in assistants' settings.

Copy the block Flow gives you, not an example you read somewhere else: Flow's block already contains the real key. A block with a placeholder instead of the key installs just the same, and then the assistant replies that it knows nothing about Flow.

05 Connecting Cursor

In Cursor, the ready-made block goes in one of these two places, whichever you prefer:

- **Settings → MCP → Add server;**
- or the project's `.cursor/mcp.json` file, if you prefer the connection to stay with the project.

The block to paste is the second of those shown on the connection page, and it already contains the key. Once you have saved it, Cursor shows **flow** among the available servers.

The usual reminder applies: copy the block Flow gives you, not an example found elsewhere: a placeholder instead of the key goes unnoticed, and then the

assistant finds nothing.

06 Connecting Claude Desktop

Claude Desktop keeps its connections in a configuration file. You reach it from the app: **Settings** → **Developer** → **Edit Config**, which opens

```
claude_desktop_config.json.
```

Paste into that file the block the connection page shows for Claude Desktop, and then **restart Claude Desktop**: it reads connections at startup.

You do not need to install anything on Flow. To talk using the key, Claude Desktop uses a small bridge that downloads itself the first time: if the first answer takes a few seconds, that is why.

07 Connecting Codex

In Codex, the block goes in the `~/.codex/config.toml` file. From the app you reach it with **Settings** → **Configuration**; from the terminal there is also the command `codex mcp add`.

Once the file is saved, **restart Codex**. In the chat, `/mcp` lists the connected servers: **flow** is among them.

Two things to watch out for, both learned the hard way:

- the **"Connections"** item in Codex's settings is something else (remote control of the computer) and has nothing to do with assistants connected to Flow;
- if you paste an example block and leave the placeholder instead of the key, Codex still shows **"Authenticated"**, but then the assistant replies that it has no Flow tools. The right block is the one on the connection page, with the key already inside.

08 Connecting ChatGPT

ChatGPT takes a different route: **no key to copy**. You only give it your Flow address; it opens a Flow page where you sign in, choose the folders and confirm. The connection appears on its own in Account → Ai assistants, with the assistant's name, and from there you manage it like all the others.

The steps, inside ChatGPT:

1. **Settings → Security and access**, at the bottom, **Developer mode**: turn it on. ChatGPT flags it as "high risk": it is the warning it shows to anyone who adds their own server, and it is needed for that.
2. **Settings → Plugins → Browse plugins**.
3. At the top right, the **+** button, which opens the "New plugin" form.
4. Name **Flow**; in the link field, your Flow address followed by `/mcp`, for example `https://flow.kaigrid.ai/mcp`; authentication **OAuth**; tick "I understand and want to continue"; **Create**.
5. **Sign in with Flow**: the Flow page "... is asking to access Flow" opens, where you choose between Read only and Can edit, tick the folders and read the notice about your data. **Allow** (or **Don't allow**, and nothing happens).
6. In a new chat, choose Flow among the plugins and try it: "what can you see on Flow?".

On the consent page, in team spaces you see **only** the folders the administrator has opened: no padlocks, no list to decipher.

ChatGPT often renames its menu items: until recently plugins were called connectors. If an item is no longer called that, look for it by what it does.

09 Connecting Claude on the web

Claude on the web takes the same route as ChatGPT: **no key to copy**. You give it your Flow address; it opens a Flow page where you sign in, choose the folders and confirm.

In Claude: **Settings → Connectors → "Add custom connector"**, and as the address, your Flow address followed by `/mcp`, for example `https://flow.kaigrid.ai/mcp`.

From there it is identical: the page "... is asking to access Flow" opens, where you choose between Read only and Can edit, tick the folders and read the notice about your data. When you confirm, the connection appears on its own in **Account → AI assistants**, with the assistant's name, and you manage it like all the others: you change the folders, change what it can do, revoke it.

What applies to ChatGPT applies here too: in team spaces, on the consent page, you see **only** the folders the administrator has opened.

10 Changing your mind

Nothing you have chosen is permanent, and **you never have to create the key again**.

- **The folders:** from Account → Ai assistants, open the connection and change the ticks. The new folders apply from the assistant's next request, and you do not need to change anything in the assistant.
- **What it can do:** you switch from Read only to "Can edit" and back in the same way.
- **Revoke:** the assistant stops seeing Flow **immediately**. Use it when a project ends, when a computer is lost, or simply when you have finished.

For each connection, the page shows when you created it, **when it was last used** and its expiry: if nobody has used one for months, you can see it.

If the assistant tries to do something the connection does not allow (a change with a read-only connection, or in a folder where the administrator has not set Write), it receives a refusal explaining what is missing, and reports it to you instead of failing silently.

11 People working in the folder know

A folder opened to an assistant is not a private matter for whoever created the connection: the people who work in it need to be able to know.

That is why, next to the names of the folders and files an assistant can see, there is a **small icon**; hovering over it tells you which connection. In the file's information panel the same thing is written out in full: "**Visible to: Claude on the Dainese project**". Everyone who works there can see it, not just you.

The **Activity log** keeps a record of everything: when a connection is created, when its folders change, when it is revoked, **every read of content** (which connection, which file, when), every download link and every change. The assistants' log is always on.

What the log does **not** contain is the conversation: the administrator sees which files the assistant read, not what you asked it.

12 What the administrator decides

In team spaces, the company decides what can be opened to an assistant. The administrator does this in **Admin console → Ai assistants**, with "Edit the list": the same column tree, where every space and every folder has a box with **three states**, which you cycle through with a click.

- **No** (empty box): assistants cannot see it. This is the starting state of everything: a company that opens nothing exposes nothing.
- **Read** (the eye): assistants can read it.
- **Write** (the pencil): they can also change it, if the connection is "Can edit".

The state applies to everything the folder contains, and a subfolder can have a **different** one: the closest one always wins. The "Clients" space set to Read can contain "Drafts" set to Write; a folder set to Write can contain "Contracts" set to Read only. Subfolders show the level they inherit dimmed: one click changes it only there, another click restores it.

One thing is not possible: **setting "No" again inside an open folder**. No invisible holes: if a subfolder must stay hidden, you open its sibling folders and not the parent.

Personal spaces are not in that list: each user decides for themselves.

Removing or lowering an entry **takes effect immediately**, including for existing connections. So that it does not come as a surprise, next to each entry the page shows how many connections are using it. The same page has the list of **Company connections**: whose they are, on which folders, when they were last used.

13 Security and confidentiality

Documents that are read go out to the assistant's provider. When the assistant reads a file, that text reaches whoever provides the assistant (Anthropic, OpenAI or whoever acts for them) under the contract that you or your company have with that provider. Flow sends nothing on its own initiative: it sends what the assistant

requests, inside the folders you have opened to it. This is why it pays to open few folders and choose them carefully.

A document can contain instructions aimed at the assistant: lines written on purpose so that it reads and follows them. This applies to any assistant, and Flow puts four defences in place: by default the connection only reads; the text reaches the assistant marked as document content, not as an instruction; the assistant cannot create links to the outside; and everything it changes can be undone from the trash and versions.

A lost key can be revoked in one click, and the connection can have an expiry date from the start. The page shows when each one was last used.

An assistant never sees more than you do. The connection lives within your permissions: if you are removed from a space, your connections lose it at the same moment. And it works only for assistants: that key does not get you into the rest of Flow.

14 Frequently asked questions

Does the assistant see all my files? No: only the folders you ticked in the connection.

Can a colleague open a restricted folder to an assistant? Only if they can already see that folder themselves, and only if the administrator has made it available to open.

Can I change my mind later? Yes: you can change the folders or revoke whenever you like, and it takes effect immediately. The key stays the same.

Can the assistant delete my files? Only if you chose "Can edit" and only where the administrator has set Write. Even then, files go to the trash, from which they can be restored.

How do I know whether a folder is open to an assistant? It has a small icon next to its name, and the file's information panel says "Visible to", with the name of the connection.

I have lost the key. It cannot be recovered: revoke the connection and create a new one.

Does it work with ChatGPT? Yes, on the web. And with Claude Code, Claude Desktop, Cursor and Codex.

Do I need to install anything? Not on Flow, nothing. Claude Desktop uses a small bridge that downloads itself the first time it starts.

Can the administrator see what I ask the assistant? No. They see which files the assistant read or changed, not the conversation.

15 If something goes wrong

The assistant says it has no Flow tools, or does not know what Flow is. Almost always it is a block pasted by hand, with the placeholder left in place of the key. Some assistants still show "Authenticated" in that case. Copy the block again from the connection page, which already contains the key, and restart the assistant.

The assistant cannot see a folder I ticked. Check the connection in Account → AI assistants: if that folder has a **padlock**, the administrator has closed it to assistants, and closing it takes effect immediately, including on existing connections.

It says it cannot make changes. Either the connection is **Read only**, and you change that from its card, or that folder does not have the **pencil**: in team spaces, the administrator is the one who sets it.

The connection has expired. Expiry dates are the ones you chose when you created it. An expired connection cannot be extended: you create another one.

ChatGPT does not see the new features. ChatGPT keeps in memory the list of operations from when you created the plugin, and does not reload it on its own. Open the Flow plugin's card and click **Refresh**; if it is not there, delete the plugin and create it again. Then open a **new chat**. Permissions, however, always take effect immediately, whatever ChatGPT has in memory.

I revoked it by mistake. It cannot be restored: you create a new connection and go through the setup again in the assistant. It takes a minute.