

Let an AI run your server

Claude Code, or another AI tool that speaks MCP, can run Secretbase for you from any computer: publish apps, read their logs, turn on a database, put an earlier release back. Claude Code connects with an access token you make; Claude on the web, desktop or phone connects by signing in. Either way, it asks you first before it deletes an app or makes a new one public. A token reaches only the apps you choose, every app, or all of Secretbase (Full control).

Quick start

- 1 On the computer that runs Secretbase, run `secretbase tokens create --name cClaude`.
- 2 Copy the `cClaude mcp add` line it prints and run it where you use Claude Code.
- 3 To approve on your phone, turn on the online dashboard: `secretbase dashboard on`.
- 4 Ask Claude to publish your app from its git link.
- 5 See what it did: `secretbase activity`.

For Claude on the web, desktop or phone, see "Claude on the web, desktop or phone" below.

Three kinds of token

When you make a token, you choose what it may reach:

- **Only these apps:** the apps you pick, and nothing else. To this token your other apps don't exist. It can see them only (`read`) or also publish and change them (`deploy`), never `admin` . Best for one app, like a client's.
- **Every app on < machine >:** all apps on this computer, now and later, but not Secretbase's own settings. This is the kind `secretbase tokens create` makes unless you say otherwise.
- **Full control of Secretbase:** every app and Secretbase's own settings: addresses, backups, machines and tokens. It can make the other two kinds, never another Full control token, and when you revoke it, the tokens it made stop too.

A Full control token is made only by you, on the computer itself: run `secretbase tokens create --name <name> --master` there (at its keyboard or over SSH), or choose **Full control** on the dashboard on the computer. The online dashboard says "Full control can only be made on the computer itself." Once made, it works from anywhere. It lasts 30 days unless you choose `--expires 1d` , `7d` , `90d` or `never` .

Keep a Full control token like a master key: whoever has it has full control of Secretbase on that machine. It still can't approve anything, and it asks you first before it deletes an app, removes a backup place or deletes backups, signs a front door in or out, replaces the Cloudflare key or disconnects Cloudflare, pairs or unpairs a machine, or shows or enters the recovery key.

Make a token

On the computer, run `secretbase tokens create --name cClaude` as yourself, without sudo. It shows the token once and, after the line for a laptop, the line for Claude Code:

For Claude Code on any computer, run this (it holds the token):

```
claude mcp add --transport http <machine> https://<address>/mcp --header "Authorization: Bearer sbt_..."
```

Run that line once on each computer where you use Claude Code. `<machine>` is this computer's name. Before the token, it says what the token reaches, what it can do and when it ends, for example "Reaches: Every app on < machine > . Can: Publish and change. Ends: < date > ."

A token reaches every app and can deploy for 90 days unless you choose otherwise. `--scope` says what it may do:

- `read` : sees your apps, but not their logs or visitors.
- `deploy` (the default) : also publishes, reads logs, puts an earlier release back, takes apps offline, sets keys, turns databases on and off, reads the database, backs up and restores.
- `admin` : everything a token can do, also putting an app back online and managing git tokens.

`--expires` is `1d`, `7d`, `30d` or `90d`; `never` only with `--scope admin`. For example: `secretbase tokens create --name cClaude --scope read --expires 7d`.

On the dashboard, the AI tools page's **Access tokens** card does the same: **New access token**, then **What may it reach?**, **What can it do?** (**See only**, **Publish and change**, or for every app also **Everything but approvals**), **How long?** and a **Name**, then **Make token**. There, **Never** is offered only with Full control. The online dashboard makes and revokes tokens too, except Full control ones.

Give a client a token for just their app

To let someone work on one app and nothing else, make an app token:

```
secretbase tokens create --name acme --app acme-site
```

`--app` takes an app's name, and you can repeat it for more apps; add `--scope read` for a token that only looks. It says "Reaches: Only acme-site." and prints the `claude mcp add` line, which holds the token: give that line to the person, who runs it where they use Claude Code. On the dashboard, choose **Only these apps** and tick the apps.

With that token, Claude can publish that app again, read its logs and do everything else below, for that app only. To it, your other apps don't exist, and a new app is refused: "This token can only work on < apps > ." It can delete its own app only after you approve.

Claude on the web, desktop or phone

Claude on claude.ai, in Claude Desktop and in Claude's phone apps connects by signing in on Secretbase's own page: there is no token to copy.

- 1 On the computer, turn on the online dashboard with a password: `secretbase dashboard on`. Until it has one, `secretbase status` says "To connect Claude on the web or phone, turn on the online dashboard with a password: `secretbase dashboard on`."
- 2 Run `secretbase status` and copy the address after "AI address (MCP):".
- 3 Add it in Claude as a custom connector. Claude's help page gives these steps for Pro and Max plans: go to **Customize > Connectors**, click + **Add**, then **Add custom connector**. Enter a name (this computer's name is a good one), paste the address and click **Continue**, then **Continue** again on the sign-in settings Claude found. Under **Authentication**, choose **Sign in now** or **Sign in when needed**, not **No sign in**, and click **Add**. On a Team or Enterprise plan, an Owner adds it in **Organization settings > Connectors**, and you click **Connect** in **Customize > Connectors**.
- 4 When Claude signs in, Secretbase's page opens: "Sign in to connect <app>". Choose **Password** and sign in with the online dashboard's username and password, or choose **Access token**, paste a token you made and click **Continue**.
- 5 The next page, "Let <app> use Secretbase?", shows the app's name (only what it says it is), where it comes from and sends you back, and what it **Reaches**. Say yes only if you started connecting it yourself. Choose **What can it do?**, **How long?** and a **Name in your token list**, then click **Allow**.

What the connection gets depends on how you signed in:

- **With the password:** every app, **See only** or **Publish and change**, for 1 to 90 days (30 days unless you choose otherwise).
- **With an access token:** no more than that token: the same apps, at most what it can do, and never longer than it lasts ("No later than your token: <date>"). When you revoke the token, or it ends, the connection ends too.
- **With a Full control token:** the page shows "Full control of Secretbase on <machine>". Tick "I started this, and I want <app> to have full control." and click **Give full control**.

In a chat, Claude's "+" button on the lower left, then **Connectors**, turns it on or off for that conversation.

The connection is listed on the **Access tokens** card and in `secretbase tokens` under the name you gave, marked "<app> (says it is), signed in from <address>". **Revoke** on the card, or `secretbase tokens revoke <name>`, stops it at once.

Anyone with the online dashboard's password can make tokens for every app. Full control stays on the computer.

Claude's help page says custom connectors work on Free, Pro, Max, Team and Enterprise plans, and "Free users are limited to one custom connector": on the Free plan, Claude on the web or phone drives one machine. Claude Code has no such limit.

What the AI can do

Through this connection, Claude can:

- publish an app from its `https://` git link, and publish it again to update it;
- show your apps with their state and address, and an app's logs;
- take an app offline, or put its previous release back;
- turn an app's Postgres or Redis on or off, and read its Postgres: one read-only query, at most 1,000 rows or 100 KB, stopped after 10 seconds;
- list an app's keys by name, set a key it made itself (like a random session secret) and remove one;
- back up an app, list its backups and restore one;
- tell how much room is left, and what AI tools did here.

It never asks you to paste a password or API key into the chat. It gives you the place to type it: the app's **Settings** tab on the online dashboard, or the command to run on the computer.

It asks you first

Before Claude deletes an app or makes a brand-new app public, it shows you a link. Open it on your phone and sign in to the online dashboard. The page says what it asks, like "Claude asks to delete <app>": tap **Delete <app>** or **Make <app> public** to say yes, or **Keep it** to say no. Until you say yes, nothing is deleted, and a new app is built but stays private: "Waiting for your OK before <name> goes public."

Requests waiting for you are at the top of the dashboard's **AI tools** page, each with **Review**. On the computer, `secretbase approvals` lists them too, and `secretbase approve <id>` or `secretbase refuse <id>` answers one. With the online dashboard off, Claude shows that command instead of a link.

A request waits 24 hours. Refused or expired, nothing is deleted and a new app stays private. The AI can never approve a request, and through this connection even a Full control token asks first.

See what it did, and undo it

What AI tools did, on the **AI tools** page on the computer and in the online dashboard, lists what AI tools did here, newest first: when, what it did and to which app, which token, the agent's name (only what it says it is) and how it stands. A row you can undo has a button: **Undo**, **Put online**, **Remove key**, **Turn Postgres back on** or **Turn Redis back on**, and, on the computer, **Restore from the last backup** for a deleted app. Only you can press them.

In a terminal, `secretbase activity` shows the same, with the command that undoes each row. Add `--since 1h`, `1d` or `7d`, or `--token <name>`.

Room for more apps

The first line of `secretbase status`, and the line under **Projects** on the dashboard, say how many more apps fit: "room for about <N> more". It counts free memory, free disk and, while they are limited, free public addresses. Claude can ask for the same, with the free memory and disk: "Room for about <N> more apps (<M> GB memory, <D> GB disk free)."

Stop a token

`secretbase tokens` lists your tokens with what each reaches, what it can do, when it was last used and when it ends. `secretbase tokens revoke claude` stops one at once, everywhere; so does **Revoke** on the **Access tokens** card. Revoking a Full control token also stops the tokens it made. An expired token stops by itself. A connected app stops the same way, by the name you gave it.

Several machines

Each machine is its own connection: make a token on each one and run its `claude mcp add` line. Every answer says which machine it came from. A token works only on its own machine, never on your paired machines. In Claude on the web, desktop or phone, each machine is its own custom connector at its own AI address, and you sign in on each.

Your own name for the AI address

With Cloudflare connected (`secretbase cloudflare connect`, see "Use your own domain" in the Setup guide), the online dashboard and the AI address can go on a name of your own domain, like `console.yourname.com`. On the computer, run:

```
secretbase dashboard domain console.yourname.com
```

or type the name under **Your own name** in **Settings** > **Open from anywhere** and click **Use this name**. Once it is live, the AI address is `https://console.yourname.com/mcp`: `secretbase status`, the `claude mcp add` line and the dashboard show it first, and the Tailscale addresses keep working. `secretbase dashboard domain` shows how it is going; `secretbase dashboard domain --remove` takes the name off.

Moving to another computer? Run the same command there. Secretbase asks you to approve moving the name (`secretbase dashboard domain approve console.yourname.com`), then the name points at the new computer.

Two limits:

- Tokens and AI connections stay on each computer: after a move, sign in again on the same address.

- Through Cloudflare, your dashboard password and tokens pass through Cloudflare's servers.

Good to know

- It works with Claude Code and other AI tools that connect to an MCP address over HTTP and send the token in a header, and with Claude on the web, desktop or phone, which signs in instead.
- Through this connection Claude publishes git links, not folders. To let Claude Code publish a folder from your laptop, see "Connect your AI tool" in the home server guide.
- `secretbase status` shows "AI address (MCP):" and the address Claude connects to. When that address isn't on port 443, `status` also suggests a Tailscale key (`secretbase tailscale-key`), which gives it an address of its own on 443. Claude Code works at either; Claude on the web, desktop or phone needs the address on 443.
- A connected app's sign-in renews by itself until the time you chose under **Lasts** ends. Connected apps count toward the 20 access tokens a computer can have.
- Everything Claude reads from your apps (logs, error messages, database rows, app names) is marked as data, never as instructions to follow.

If something goes wrong

- "This access token is wrong or was revoked": make a new token and run its `claude mcp add` line.
- "This access token expired on <date>": make a new one.
- "This token's scope is <scope>; this needs <needed>": make a token with that scope.
- "This token can only work on <apps>": the token is an app token; make one that reaches that app.
- "Full control can only be made on the computer itself.": make it on the computer, with `secretbase tokens create --name <name> --master`.
- "This request isn't here any more": requests are kept for a day, and restarting the computer clears them. Ask Claude again.
- "Too many wrong tries from your address": wait 15 minutes.
- "This sign-in request expired or was already answered": start connecting again from Claude.
- "Secretbase doesn't know this app" or "This app's return address isn't one it registered": start connecting again from Claude.
- "This sign-in code expired or was already used": connect again from Claude.
- "You refused this app's access. Nothing was connected.": connect again from Claude if you meant to approve.
- "This connected app's sign-in ended": Claude renews it by itself; if it can't, connect it again and sign in.