PRACTITIONER · 6 MINUTE READ

Model connectors in practice: MCP across Claude, ChatGPT and Gemini

> Claude, ChatGPT, Gemini and Copilot Studio can all add MCP connectors; approve each one with a checklist, start read-only, and keep a person confirming changes.

What it is

Guide 13 explains connectors and least access. This guide is the practical side: where you add an **MCP** connector (Model Context Protocol, an open standard for connecting AI to tools and data) in the main assistants, and how to decide whether to approve one.

An **MCP server** is the program on the other end of the plug. It offers **tools** (actions the AI can call, such as "create task"), **resources** (data it can read) and **prompts** (ready-made instructions). A **remote server** runs on the internet. A **local server** runs on your own computer, with your access to your files.

Menus change often; this table is a snapshot as of November 2026; check the maker's page.

Assistant	Where you add a custom MCP server	Who controls it on business plans
Claude	Customize, then Connectors, then add a custom connector (remote). Local servers only in the desktop app's settings file	Team: Owners add connectors. Enterprise: Owners or a role with that permission. Members then connect individually
ChatGPT	Plugins, then Add custom MCP server (web only)	Business: admins and owners only. Enterprise and Edu: admins grant it by role and choose which actions each app may use
Gemini app	Settings, then Connected Apps, then Add a custom app (web, personal US accounts, 18 and over)	Not available on work or school accounts. Gemini Enterprise: an administrator registers the server and switches on each action
Microsoft Copilot Studio	In an agent's Tools page, add a Model Context Protocol tool	Power Platform data policies apply to MCP servers

Why it matters

- One server can work across several assistants, so the same approval questions recur.
- All four makers say that checking a third-party server is your responsibility, not theirs.
- **Write tools** (that create, change, send or delete) carry far more risk than **read tools**.
- Text that comes back from a server can carry hidden instructions (**prompt injection**, see guide 13).

How to do it

1. **Check** your organisation's list of approved connectors first.
2. **Ask** who built and runs the server, and where.
3. **List** every tool it offers and mark each one read or write.
4. **Find out** what data leaves: what is sent to the server and where it is stored. Read its privacy terms.
5. **Confirm** how people sign in: individual accounts are safer than one shared key that gives everyone the same access.
6. **Switch off** write tools you do not need (Claude, ChatGPT Enterprise and Gemini Enterprise all allow this).
7. **Test** with made-up data, then check the logs for what was read or changed.
8. **Review** approved connectors every few months and remove unused ones.

Example

A team asks to connect a task tracker's MCP server. The approver uses this checklist:

```
Connector: [name]   Requested by: [team]
Builder and host: [company / internal team], [country or cloud]
Remote or local: [ ]
Tools (R = read, W = write): [list each]
Write tools needed for the stated job: [list, or none]
Sign-in: individual accounts / shared key
Data sent to the server: [fields]   Stored for: [period]
Logs available to us: [yes/no, where]
Pilot: made-up data, [2] weeks, owner [name]
Decision: approve / approve read-only / decline
```

The server offers twelve tools, three of them write. The team only needs to read tasks, so the approver switches off the write tools and approves a pilot with made-up projects.

Common mistakes

- **Approving the server, not the tools.** Fix: approve tool by tool; updates can add tools.
- **Clicking "allow always" early.** Fix: keep confirmations on until the pilot ends. Claude's Research mode can call connector tools without asking, so disable write tools there.
- **Installing a local server from a link.** Fix: it runs code on your computer; treat it as a software install needing IT approval.

Try it this week

1. Find where connectors live in your approved assistant, using the table (3 minutes).
2. Open one approved connector and list its tools as read or write (5 minutes).
3. Fill in the checklist above for it, leaving blanks where you do not know (5 minutes).
4. Send the blanks to the connector's owner (2 minutes).

Going further

- The Gemini app currently asks you to confirm every write action. Gemini Enterprise lets a server mark tools as read-only so they skip confirmation; check those labels are honest during testing.
- In ChatGPT, new actions from an updated server stay off until an admin chooses.
- Claude reaches remote servers from the maker's cloud, so a server behind your firewall needs network changes.
- Copilot Studio supports MCP tools and resources, not prompts, and needs generative orchestration switched on.
- Builders: the MCP security guidance covers local server risks and narrow sign-in permissions.

Key words

- **MCP server**: the program that offers tools, data and prompts to an AI assistant through MCP.
- **Remote server**: an MCP server reached over the internet by web address.
- **Local server**: an MCP server that runs on your own computer.
- **Read tool / write tool**: a tool that only looks at information, or one that changes something.
- **Shared credential**: one key used by everyone, giving all users the same access.

Sources

- MCP architecture overview, https://modelcontextprotocol.io/docs/learn/architecture, checked 2026-11-03
- MCP security best practices, https://modelcontextprotocol.io/docs/tutorials/security/security_best_practices, checked 2026-11-03
- Claude Help Center, "Get started with custom connectors using remote MCP", https://support.claude.com/en/articles/11175166-get-started-with-custom-connectors-using-remote-MCP, checked 2026-11-03
- OpenAI Help Center, "Connecting custom MCP servers in ChatGPT", https://help.openai.com/en/articles/12584461-connecting-custom-mcp-servers-in-chatgpt, checked 2026-11-03
- OpenAI Help Center, "Connected apps in ChatGPT", https://help.openai.com/en/articles/11487775-connected-apps-in-chatgpt, checked 2026-11-03
- Gemini Apps Help, "Connect & manage custom apps for Gemini Apps", https://support.google.com/gemini/answer/17209137, checked 2026-11-03
- Google Cloud docs, "Set up a custom MCP server" (Gemini Enterprise), https://docs.cloud.google.com/gemini/enterprise/docs/connectors/custom-mcp-server/set-up-custom-mcp-server, checked 2026-11-03
- Microsoft Learn, "Extend your agent with Model Context Protocol", https://learn.microsoft.com/en-us/microsoft-copilot-studio/agent-extend-action-mcp, checked 2026-11-03
- Microsoft Learn, "Connect your agent to an existing MCP server", https://learn.microsoft.com/en-us/microsoft-copilot-studio/mcp-add-existing-server-to-agent, checked 2026-11-03