

PRACTITIONER · 7 MINUTE READ

AI that acts for you: browser and computer use

Some assistants can now click, type and fill in forms for you, in your browser or on your computer, if you give permission.

What it is

Most of this guide series is about AI that drafts and suggests. A newer kind of feature lets the assistant **act**: open web pages, click buttons, fill in forms, move between apps and finish a task on your computer. You stay in control of what it may touch.

This guide uses Claude as its worked example because its safety settings are publicly documented; ChatGPT, Microsoft Copilot and Gemini offer comparable features. One example is the **Claude desktop app**. When you allow it, Claude can work in your Chrome browser through the **Claude in Chrome** extension, and on macOS and Windows it can also operate other apps on your screen. It tries the most precise route first: a connector if one exists (guide 13), then the browser, and only then the screen itself. The other main assistants (ChatGPT, Microsoft Copilot and Gemini) also offer browser or computer agents, but names, plans and features change often, so check what your approved tool offers today. When checked, operating other desktop apps was a beta feature on some individual plans and not available on every business plan, so check what your organisation's plan allows.

Think of it as letting a capable assistant sit at your desk while you watch. Useful, but you decide which drawers it may open.

Checked October 2026. These features are new, often in beta, and change quickly.

How permission works (Claude as the example)

- **You install and switch it on.** Nothing acts on your computer until you set it up and allow it.
- **App by app.** On the desktop, Claude asks before it uses each application, and you approve it.
- **Action by action in the browser, if you choose.** Claude in Chrome lets you approve each action yourself, or let it work with automatic safety checks. A setting that skips all approvals exists; do not use it at work.
- **Some things are blocked.** Claude in Chrome blocks certain actions in every mode, such as making purchases, creating accounts, executing trades and permanently deleting files. It asks before visiting financial sites. On the desktop, some apps (such as trading and cryptocurrency apps) are blocked by default, and you can block others.
- **It sees your screen.** It works from screenshots, so anything visible can become part of the conversation.

Why it matters

- It can finish repetitive web and app tasks that have no connector, such as collecting information from several sites into one table.
- Once you trust a task, it can work through multiple steps while you get on with other work, with checkpoints for your approval.
- It also brings new risks: a web page or email can contain hidden instructions aimed at the AI ("prompt injection"). The provider adds defences, and says openly that the risk is not zero.
- Mistakes happen in real systems, not just in a draft.

How to do it

1. **Check** with your IT team that the feature is approved for work, and on which accounts.
2. **Start** with a low-risk, read-mostly task, such as "collect the opening hours and addresses of these five suppliers into a table".
3. **Close** sensitive tabs, apps and files before you begin, since the AI can see your screen.
4. **Choose** the approval setting where it asks before each action, at least until you trust the task.
5. **Write** a specific instruction: which sites or apps, what to collect or do, where to stop.

6. **Watch** the first runs, and stop it if it goes somewhere unexpected.
7. **Check** the result against the source before you use it.
8. **Keep** the final step human: you press submit, send or pay.

Example

Task: preparing a comparison of three conference venues.

Open the websites of [venue A], [venue B] and [venue C].
For each, collect: capacity for 80 people seated, price per day, catering options, distance from [our office], cancellation terms.
Put them in a table. Do not fill in any booking or contact form.
Stop and show me the table when done.

The AI visits each site, gathers the details and builds the table. You check two figures against the sites, then decide which venue to call.

Common mistakes

- **Skipping approvals to save time.** Fix: keep "ask before acting" for anything that changes, sends or submits.
- **Leaving sensitive things open.** Fix: close banking, health, HR and customer records first. Avoid using these features for banking, medical or legal tasks, as the provider itself advises.
- **Vague instructions.** Fix: name the sites, the data and where to stop.
- **Trusting what the page tells the AI.** Fix: remember that web content can try to give the AI orders. Limited access and your approval are the real protection.
- **Using a personal account for work.** Fix: approved work accounts only.

Try it this week

If your organisation has approved it:

1. Pick a 15-minute web research task you do regularly.
2. Write the instruction using the example above as a pattern.
3. Run it with approval required for every action, and watch.
4. Time it against doing it yourself, and note what you had to correct.

Going further

- **Prefer connectors** where they exist: they are faster and more precise than clicking through a screen.
- **Use blocklists** for apps and sites the AI must never touch.
- **Check the activity history** after a task to see what it opened and did.
- Combine with skills (guide 11): a saved instruction for a recurring browser task helps it follow the same safe steps each time.

Key words

- **Browser agent:** an AI that can navigate websites and act in your browser.
- **Computer use:** an AI operating apps on your screen by clicking and typing.
- **Approval mode:** the setting that decides whether the AI asks before each action.
- **Blocklist:** apps or sites the AI is never allowed to use.
- **Prompt injection:** hidden text on a page or in a document that tries to give the AI new instructions.