DAY EIGHT

08 /10

Connecting Claude to Everything — *context, tools, and agents*

Claude is most useful when it can reach the things you actually work with — your documents, your calendar, your systems. Today is about the open standard that makes that possible, the connectors that bring it into the apps, and the agentic workflows it unlocks.

BY THE END OF DAY 8, YOU WILL BE ABLE TO TEACH OTHERS TO —

- Explain what MCP is and why it exists
- Describe what makes a workflow "agentic"
- Reason about trust and scope before connecting
- Use connectors in the Claude apps
- Keep a human in the loop on agent work
- Design one safe connected workflow

01 Why today matters

ORIENTATION

A brilliant assistant who can only see what you paste into the chat is working with one hand tied. The leap today is connection: giving Claude a safe, governed way to reach the documents, tools, and systems where your real work actually lives — so you stop being a courier between Claude and your data.

Two threads run through this day. One is MCP, the open standard that makes connection possible. The other is agentic work — what becomes possible once Claude can not only see your systems but take steps within them. Both are powerful; both demand the human-in-the-loop discipline that has run through this whole series.

PREREQUISITES

Day 2's connectors got a first mention; Day 6 and Day 7 touched MCP and tool use. Today pulls those threads together. No coding required — this is a concepts-and-judgement day.

02 MCP — a common standard for connection

CORE CONCEPT

The Model Context Protocol is an open standard for connecting AI assistants to outside tools and data sources. Before a common standard, every connection between an assistant and a system was a one-off. A shared protocol means a tool built once can be connected anywhere that speaks it.

> THE MENTAL MODEL
>
> **A universal plug.**
>
> Think of the way one connector shape replaced a drawer full of incompatible cables. MCP is that idea for AI: a standard "shape" for the connection between Claude and a system, so the two can be joined without custom wiring each time. Build the plug once; use it everywhere.

WHY A STANDARD MATTERS

- ✓ A connection built once can be reused across tools, not rebuilt each time
- ✓ It is open, so anyone can build a connector for their own system
- ✓ It gives connection a consistent shape — easier to reason about, and to secure

You met MCP already as the thing extending Claude Code's reach (Day 6) and underlying tool use (Day 7). Same idea, seen from the surface: a standard way to give Claude a new thing it can reach.

03 Connectors in the Claude apps

CORE CONCEPT

In the everyday apps, MCP shows up as connectors — connections you can switch on so Claude can work with a system directly, without you copying things back and forth.

3.1 What a connector changes

With the right connector enabled, "summarise the document I mentioned" or "what is on my calendar this week" becomes something Claude can act on directly. The work moves from you fetching and pasting to Claude reaching, with your permission.

3.2 The pattern to teach

- **Connect deliberately.** Each connector is a decision — turn on what serves the work, leave the rest off.
- **Know the scope.** Be clear on what a connector can see and do before you rely on it. Connection is access; access deserves thought.
- **Stay specific.** Day 3 still applies — "the Q3 planning doc," not "that file." A connector widens reach; it does not read your mind.

> KEY IDEA TO INSTALL
>
> A connector turns Claude from something you feed into something that can reach — within boundaries you set. The power is real; so is the responsibility to connect deliberately.

04 Agentic workflows

CORE CONCEPT

Once Claude can reach your tools, a new shape of work opens up. An agentic workflow is one where Claude does not just answer a question but carries out a multi-step task — gathering what it needs, taking steps, working toward a goal.

> THE SHIFT
>
> **From answer to errand.**
>
> A non-agentic exchange is a question and an answer. An agentic one is an errand: "look across these sources, pull the relevant points, draft the summary, and flag anything that needs my decision." Claude plans, takes steps, and uses what it is connected to — the way a capable assistant runs a task end to end.

You have seen this shape before. Claude Code is agentic — explore, plan, act, verify. Connectors bring the same capability to the conversational surfaces, pointed at your documents and tools instead of a codebase.

> *"A question gets an answer. An errand gets a result. Agentic work is the errand."*

05 Doing it safely

CORE CONCEPT

Reach and action together are exactly where care matters most. Three habits keep connected, agentic work trustworthy — teach them as inseparable from the capability, not as an afterthought.

- **Stay in the loop.** The human-in-the-loop principle reaches its peak here. An agent taking steps in your real systems should pause at the moments that matter — and you should be there for them.
- **Scope the access.** Connect what the task needs and no more. Broad access "just in case" is broad risk for no benefit. Match the connection to the job.
- **Mind the trust boundary.** When Claude reads from outside sources, it is reading content you did not write. Treat what comes in from connected systems with the same judgement you would apply to any external input — it is information to weigh, not instructions to obey.

THE CONNECTION TRAP

"Connected" can feel like "handled." It is not. A connector is a capability, not a delegation of judgement. The more Claude can reach and do, the more your review and your boundaries are doing the real work of keeping it safe.

LAB 08 ~35 MIN

Design a safe connected workflow

Each learner designs one connected, agentic workflow for a real task — then stress-tests it against the safety habits before running what they can.

1. **Pick a real errand** — something multi-step that currently means fetching from several places and stitching it together by hand.
2. **Map the connections.** List exactly what Claude would need to reach to do it — and nothing more. Justify each one.
3. **Write it as an errand.** Phrase the task the way you would brief a capable assistant: the goal, the steps, what to flag for your decision.
4. **Stress-test it.** Walk Section 05: where should it pause for you? Is any access broader than the task needs? Where is it reading external content?
5. **Run what you safely can** with the connectors available to you — and note where a human checkpoint belongs.

a connected workflow the learner would actually trust — because they designed the checkpoints and the limits in, rather than bolting them on.

TEACHING NOTES

How to teach Day 8 well

OPEN WITH THIS

Ask the room to count how many times in a day they copy something out of one tool to paste it into Claude. That courier work is the problem connectors solve — and the count makes the value concrete before you name the standard behind it.

PACE & EMPHASIS

The "universal plug" framing (02) makes MCP land in one image — use it. Spend the back half of the day on safety (05): it is the part that is easy to underweight and expensive to get wrong. Connectors (03) are best shown live if you have one enabled.

DISCUSSION PROMPTS

· What is your most tedious copy-paste-between-tools task? · For one errand you would hand to an agent, where exactly should it stop and check with you? · What access would you be tempted to grant "just in case" — and should you?

COMMON MISCONCEPTIONS TO PRE-EMPT

"MCP is a product I have to buy or install."
It is an open standard — a shared shape for connections. Connectors are how you meet it in the apps.

"Agentic means it runs without me."
It means it carries out multi-step tasks. The human checkpoints are part of the design, not optional.

"Once it is connected, the task is handled."
Connected is a capability, not a delegation of judgement. Your review and limits do the safety work.

IF YOU ONLY HAVE 30 MINUTES Teach the universal-plug framing (02), what a connector changes (03.1), and all of the safety habits (05). Do Lab steps 1–4 on paper. The agentic-workflow framing can be a single sentence: “a question gets an answer; an errand gets a result.”

Day 8 Cheat Sheet

MCP	The Model Context Protocol — an open standard for connecting AI assistants to outside tools and data.
Universal plug	One standard “shape” for connection — build a connector once, use it anywhere that speaks MCP.
Connector	How MCP shows up in the apps — a connection you switch on so Claude can work with a system directly.
Connect deliberately	Each connector is a decision. Turn on what serves the work; leave the rest off.
Agentic workflow	Claude carrying out a multi-step task — gathering, taking steps, working to a goal — not just answering.
Answer vs. errand	A question gets an answer; an errand gets a result. Agentic work is the errand.
Stay in the loop	An agent acting in your real systems should pause at the moments that matter — and you should be there.
Scope the access	Connect what the task needs and no more. Broad access “just in case” is risk for no benefit.
Trust boundary	Content from connected systems is external input — information to weigh, not instructions to obey.

Check for understanding

Five questions. Learners should be able to answer all five before Day 9.

1. What is MCP, and what problem does having a common standard solve?
2. What does enabling a connector change about how you work with Claude?
3. What makes a workflow “agentic”? Give the answer-versus-errand distinction.
4. Name the three habits that keep connected, agentic work safe.
5. Why is “connected” not the same as “handled”?

> **Answer notes —** 1) An open standard for connecting AI assistants to outside tools and data; a common standard means a connection built once can be reused everywhere, instead of custom-wiring each one. 2) Claude can reach a system directly, with your permission — the work shifts from you fetching and pasting to Claude reaching. 3) Claude carries out a multi-step task rather than just answering — a question gets an answer, an errand gets a result. 4) Stay in the loop, scope the access, mind the trust boundary. 5) A connector is a capability, not a delegation of judgement — your review and your limits still do the real safety work.

Day 8 in five lines

- MCP is an open standard for connecting Claude to outside tools and data — a universal plug.
- Connectors are how that shows up in the apps: Claude reaches your systems instead of you pasting into it.
- An agentic workflow is an errand, not a question — Claude plans and takes steps toward a goal.
- Connected, agentic work demands the human in the loop at its strongest.
- Scope access tightly and treat external content as input to weigh — connected is not handled.

TOMORROW — DAY 9 → Claude Design — designing and building with Claude as your partner