

Manage and share conversations

Cover history, continuing an earlier chat, supported management actions, and the limits of a shared conversation snapshot.

Conversation history lets you return to earlier work without repeating all of its context. Treat each conversation as a working record: give it a recognizable purpose, continue it while the context is still relevant, and start a new one when the audience, source material, or objective changes.

Find and continue a conversation

1. Open Chat or Chat History and locate the conversation by its title or recent activity.
2. Open it and reread the most recent request, sources, assumptions, and result before continuing.
3. Add new instructions or source material in a follow-up, and state when newer information replaces something earlier in the chat.
4. Verify important facts again when the conversation depends on files, policies, connected data, or events that may have changed.

Keep conversation history useful

- Use one conversation for one coherent outcome instead of mixing unrelated work.
- Rename a conversation when the generated title does not make it easy to recognize later.
- Move durable source material to My Files, a Knowledge Base, or a project instead of relying on one chat as the only copy.
- Start a new conversation when old instructions or attachments could confuse the next task.

Share with care

A shared conversation may expose the messages, attached context, generated outputs, or a snapshot of the work to its recipients, depending on the supported sharing option. Review the entire conversation before sharing, remove material that the audience should not receive, and prefer sharing the final approved deliverable when recipients do not need the working history.

What sharing does not do

Sharing a conversation does not necessarily grant access to every linked file, project, Knowledge Base, agent, or connection. Recipients may be able to read the shared record while still being unable to open a restricted source. Never use a shared chat to distribute passwords, access tokens, API keys, authentication codes, or other secrets.

