

A community server is assessed before anyone connects it

You practise this in the course

Question	Finding
Who maintains it?	One individual; active in the last month
What can it read?	Records and files in the configured folder
What can it change?	update_record and delete_file
Where does data go?	Not stated in the README

Decision

- Pilot with read tools only; write tools disabled
- Confirm the data flow with the maintainer first
- Review after 30 days

YOU START WITH

A community MCP server someone wants to use, with its README and requested access.

WHAT YOU PRACTISE

Checking source, maintainer, scopes and data flow, then limiting access to what the task needs.

THE PROMPT USED

“Summarise this community MCP server’s README and requested permissions into our trust checklist: who maintains it, what it can read and write, where data goes, and anything unclear.”

THE FINISHED OUTPUT CONTAINS

- Maintainer, source and update history
- Read and write tools listed separately
- A decision with conditions

STILL NEEDS HUMAN CHECKING

- The repository and maintainer yourself
- Every write tool’s purpose
- Where data is sent

RELATED COURSE

[Claude MCP: Connect and Configure](#) ·
Module: Trust and access control