

How to choose an MCP server

Start with a task, then check client support, permission scope and maintenance.

Updated October 29, 2026

Start with a task you can judge. “Find a document I can access and return its source link” is a testable goal. “Connect all our knowledge” is too broad for a pilot.

Define the boundary

Write the data source, allowed actions and user group. State whether the connection can read, create, update or delete. A read-only research task does not need a write token. Set a clear failure condition, such as returning a document outside the test user's permissions.

Check the exact client

Record the client name, version and deployment mode. Confirm its supported transport against the server's docs. Local stdio and remote Streamable HTTP have different setup and operational needs. A package name is not a transport. A remote endpoint is not an install command.

Use client-specific instructions for Claude, Cursor, Codex or your chosen client. Do not paste a configuration block from another client without checking its schema. Record the server release and package publisher alongside the instructions.

Review the source

Follow the repository and documentation links. Check the licence file for the exact release. Look for release notes, security reporting instructions and the current maintainer. Stars can show interest. A recent commit can show activity. Neither establishes safety, a support contract or legal permission to use the code.

Run a bounded pilot

Use test data and a restricted account. Check discovery, a valid read, a denied read and an upstream failure. Inspect the tool descriptions and arguments before letting an agent call them. MCP Inspector can help inspect and exercise a server. It does not certify production controls.

Save expected and actual results. Prefer a server that meets the task with a small permission scope. Keep a reason for rejecting each alternative. Recheck the decision when the package, tool schema or vendor terms change.

Sources

- [MCP specification: Transports, revision 2025-06-18](#). Fetched 2026-10-29.

- [MCP specification: Security best practices, revision 2025-06-18](#). Fetched 2026-10-29.
- [MCP documentation: Inspector](#). Fetched 2026-10-29.

Frequently asked questions

What should a pilot test?

Test the intended task, denied access, credential revocation and upstream failure with a restricted account.