

Getting started with an MCP server safely

Use a test account, follow client-specific docs and keep a record of the working setup.

Updated October 29, 2026

Choose a small read-only task. Use data that can be exposed during a pilot. Keep production customer data out of the first connection.

Find the primary instructions

Open the server's official docs from the listing. Confirm the repository or package publisher. Check the licence and exact release. Find the install instructions for your client. Claude, Cursor, Codex and other clients can use different configuration formats and setup flows.

This guide does not provide a universal install block. Copy only the block documented for your client and inspect the command, arguments and endpoint before running it. Keep credentials in the supported secret mechanism rather than in a shared document.

Connect a restricted account

Decide which data and actions the test needs. Create or use an account restricted to that scope. Follow the documented authorization flow. For a local package, review which filesystem paths and network services it can reach.

Use MCP Inspector when you need to examine tool discovery and request behaviour separately from the AI client. Read its installation and security guidance first. Do not expose a development inspection service to untrusted users.

Verify success and denial

Ask for a known record and compare the returned result with the source. Ask for a record outside the test account's access. Check the error and logs. Verify that a disconnected or revoked account stops working. If the task needs writes, introduce them only after a separate review and an approval rule.

Save a short test record: client version, server artifact, transport, permission scope, expected result, actual result and evidence link. Remove secrets from screenshots and logs.

Prepare the handover

Name the owner for updates and incidents. Document how to stop the process or disable the remote connection. Record how to revoke the upstream credential. Share the approved setup through your team's normal review process. Recheck it when the client, server or requested permissions change.

Sources

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

Frequently asked questions

Can I reuse any client configuration?

Use the instructions for your exact client and server version. Inspect commands, endpoints and permissions before use.