

Questions to ask an MCP vendor

Get clear answers about identity, billing, support, data retention and exit paths.

Updated October 29, 2026

Send the same questions to each shortlisted vendor. Ask for written answers with links to the relevant docs or contract. “Supported” needs a version, scope and owner.

Identity and permissions

How does the service bind an MCP user to the upstream account? Does it use the user's identity or a shared service account? Which scopes are required? Can we restrict access to a project, workspace or dataset? What happens after the user loses upstream access?

Ask the vendor to demonstrate a denied request. A successful demo shows that a connection works. A denied request helps show where its access boundary sits.

Data handling

Which request fields, tool results and error messages are logged? Where are logs stored? Who can view them? What are the retention and deletion terms? Are subprocessors involved? Ask whether payloads are used for training and where that promise is recorded.

Do not infer compliance from an encryption statement or a badge. Ask for evidence that covers the service you will use. Have your own reviewer assess its scope, date and exceptions.

Operations and support

Who handles an upstream API change? How are breaking tool changes announced? Can we pin a release? What are the support hours and escalation path? Is availability defined in a contract? Which incidents are excluded?

Ask what happens during rate limiting, an expired credential or a partial write. Can the client retry safely? Which actions need human approval? Who can revoke a connection during an incident?

Commercial terms and exit

What does a billable unit mean? Are failed requests charged? What is included in the plan? Ask for a quote for your pilot trace. Request cancellation, renewal and export terms.

Before approval, label each answer confirmed, unanswered or unacceptable. Assign an owner to every unresolved item. Do not let a sales demo replace an access-control test.

Sources

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

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

Frequently asked questions

What should a vendor answer in writing?

Ask about identity mapping, required scopes, data retention, billing units, support and exit terms.