interweb

Generated on 15/11/2026 00:12

KNOWLEDGE BASE · PUBLIC DOCUMENT

What an MCP server is, and why people ask for one

How AI Works

CODE	VERSION	COUNTRY · LANGUAGE
RLX-AO-KB-940	v2026.10.10	Angola · English

Interweb Angola
RLX Angola, Lda. · Group RLX Holdings
Tax ID (NIF) 500 260 5724 · Commercial registration no. 26464-25/250724

https://www.meu.interweb.ao/knowledgebase/940

What an MCP server is, and why people ask for one

How AI Works Created on **October 10, 2026** 3 min read



MCP (Model Context Protocol) is an open protocol that defines a common way for an AI application to talk to tools and data: read files, query a database, create an event, send a message. An **MCP server** is the small program that exposes those abilities; the AI application, acting as the client, connects to it and can use them. Think of it as a standard socket: the same plug fits many tools.

Interweb does not sell MCP servers or install them. When someone asks for "an MCP", they nearly always mean one of two different things: using one that already exists, or writing their own and putting it on a server. This article helps you tell them apart.

The three things an MCP server can offer

What	What it is	Example
Tools	Actions the model can ask to run	Create a task, send an e-mail, write to a sheet
Resources	Data the model can read	Files, rows of a database, documentation pages
Ready-made prompts	Reusable request templates	"Summarise this contract with these precautions"

Local or remote: where it runs

1. **Local.** It runs on your computer, started by the AI application itself. No server, no domain. It is the most common case and the easiest to try out.

2. **Remote.** It runs on a server behind an HTTPS address, and several people or applications connect to it over the internet. Here you need a VPS (or equivalent), a domain and authentication. See **HTTPS and a domain for an application**.

3 **In both cases** the AI application decides when to use the tool, and the MCP server is what runs it with your permissions. That is where the risk comes from.

A simple remote MCP server could in theory run as a Node.js application in cPanel, within the limits of a shared account. One that has to be always on, take constant connections or run heavy tasks belongs on a VPS. See **why an agent needs a VPS**.

Every MCP server is code with access.
A third-party server you install can read the data you connect it to, and can make the model do things. Install only servers from sources you trust, read what they ask for and give them the minimum: a read-only database account instead of the main one, a folder instead of the whole disk.

Text from strangers is dangerous.
If the model reads a page or an e-mail with hidden instructions and has a tool that writes or sends, it may obey them. Do not combine powerful tools and content from unknown sources in the same agent.

If you are putting one on a server of your own

1 **Decide first whether you need remote.** If only you use it, a local one is usually enough.

2 **Add authentication.** A remote server without it is an open door for anyone who finds it. See **ports and firewall**.

3 **Keep keys out of the code.** See **environment variables and secrets**.

4 **Follow the documentation of the protocol and of the library you use.** They change fast, and this article does not replace either.

Test each new tool with a test account and test data before connecting it to real data.

RECOMMENDED
Need a VPS to run an application, with a domain and HTTPS? See the plans.
See VPS plans →

SEE ALSO

- Hosting an AI agent: why it needs a VPS and not shared hosting
- OpenClaw security: what it can reach, and how to limit it
- What a webhook is, and how to test one with curl
- VPS plans

interweb

Interweb Angola

RLX Angola, Lda. · Group RLX Holdings

TAX ID (NIF)	500 260 5724
COMMERCIAL REGISTRATION NO.	26464-25/250724
REGISTERED OFFICE	Rua Direita do Patriota, Bairro Dangereux Belas, Luanda, Angola
CONTACT	info@interweb.ao · +244 942 011 191 · www.interweb.ao
OPENING HOURS	Monday to Friday - 08 AM to 04 PM Saturday & Sunday - Closed

Online version of this document

RLX-AO-KB-940 · v2026.10.10 · Generated on 15/11/2026 00:12