EXPLAINER · AI AND INTEGRATIONS · 2026

What Is MCP? The Model Context Protocol in Plain English

What it is, how it differs from an API, what it lets an AI assistant do, and the security questions to settle first.

> MCP is a **shared plug standard for AI**. A business system publishes one MCP server, and any compatible assistant can discover and use the tools and information it offers.

The key facts

Question	Answer
Who created it?	Anthropic, 25 November 2024
Who looks after it now?	Agentic AI Foundation, Linux Foundation (Dec 2025)
Who supports it?	Claude, ChatGPT, Gemini, Copilot, VS Code, Cursor and more
How many servers?	10,000+ published by December 2025
How is access granted?	An authorisation model based on OAuth 2.1

The three parts

- Host: the app the person uses
- Client: the part inside it that speaks MCP
- Server: the adaptor in front of your system

What a server offers

- Tools: actions, such as booking or texting
- Resources: information to read
- Prompts: ready-made instructions

MCP versus an API

	API	MCP server
Used by	Developers	AI assistants
Capabilities found by	Reading documentation	Asking the server
Needs underneath	The system	Usually an API

Before you connect an assistant

- [ ] We know exactly what data it can reach
- [ ] It starts read-only; write tools are added one at a time
- [ ] Credentials sit with the server, never in the chat
- [ ] A person approves anything that changes data
- [ ] Servers come only from sources we trust
- [ ] We know where the AI service processes and keeps data
- [ ] Every tool call is logged
- [ ] We have checked APP 11 and APP 8 if the Privacy Act covers us

Prompt injection

Text an assistant reads, from an email, a web page or a customer message, can contain hidden instructions. Treat tool results as information, not orders, and keep risky actions behind a human approval.

Where phone data fits

1. **Records:** can call records, transcripts and summaries be read through a documented API?
2. **Events:** are missed calls and voicemails pushed to other systems straight away?
3. **Actions:** can SMS and user changes be made without the portal?

Uniden Voice

Australian owned and operated. Open REST API and webhooks across voice, SMS, numbers, users and AI transcripts; Zapier, Make and Power Automate; AI Agents with calendar, transfer, SMS and webhook tools. General information only. Book a demo at unidenvoice.com/get-started/book-a-demo or call 1300 881 662.