05 AI control

AT A GLANCE

For	Working the box in plain words: "Set up a Pt100 and sweep it from 0 to 100 °C in 5 degree steps, 30 s each."
You need	**Built in:** the Companion, and a provider with a model (an online service with your API key, or a model on this computer). **Your own AI app** (Claude Code, Codex, Claude Desktop): the Local network API server running, **Allow AI control (MCP)** on, and the token.
Try it	Claude Code, after the token step below (port 8765). Then type `/mcp` in Claude Code: `ohmstar` is listed.

```
claude mcp add --transport http --scope user ohmstar http://127.0.0.1:8765/mcp --header
'Authorization: Bearer ${OHMSTAR_TOKEN}'
```

Built-in AI assistant

1. Open **AI assistant**. Choose **Provider** and **Model**; paste an **API key** if needed. **Test connection**.
2. Ask. Before any change to the box it shows exactly what it will send: **Allow**, **Allow for this conversation** or **Don't allow**.
3. **Keep beside pages** docks it next to any page.

Online	Anthropic (Claude), OpenAI, Google Gemini, DeepSeek, OpenRouter, Groq, Together AI, Mistral, xAI (Grok)
This computer	Ollama, LM Studio, llama.cpp server, vLLM. Nothing leaves the computer.
Custom	Any OpenAI- or Anthropic-compatible address
Sent to a provider	What you type, tool descriptions, the app's guide, tool replies. Never serial number, dates, USB chip serial or port.
API keys	Sealed by the operating system; each sent only to its own address.
Never asked	Stop sweep, define a custom sensor, make a table, save a sequence
Asked every time	Writing a table into a box slot (only the built-in assistant can)

Your own AI app (MCP)

1. Companion: connect the box, open **Local network API**, **Start**.
2. Switch on **Allow AI control (MCP)**. It is off at every app start unless **Keep on after restart** is ticked.
3. Press **Copy** on the token, then put it in `OHMSTAR_TOKEN`:

```
# macOS, Terminal
echo "export OHMSTAR_TOKEN=$(pbpaste)" >> ~/.zshrc
&& source ~/.zshrc
# Windows, PowerShell (then open a new terminal)
[Environment]::SetEnvironmentVariable('OHMSTAR_TOK
EN', (Get-Clipboard), 'User')
```

Client	Setup
Claude Code	The command above. Remove: `claude mcp remove ohmstar --scope user`
Codex	In `~/.codex/config.toml`: `[mcp_servers.ohmstar]` `url = "http://127.0.0.1:8765/mcp"` `bearer_token_env_var = "OHMSTAR_TOKEN"` Check: `codex mcp list`
Claude Desktop	**Save Claude Desktop extension**, open the `.mcpb` file, enter Token and Port when asked.

Apps opened from the Dock don't read `~/.zshrc`: start Claude Code or Codex from Terminal. Linux: add `export OHMSTAR_TOKEN=…` to your shell profile. Repeat after a new token.

Tools

Tool	Does	Tool	Does
`get_box_state`	Model, firmware, range, output, table, who has the box	`start_sweep`	List or range of ohms or sensor values, each held

Tool	Does	Tool	Does
`search_sensors`	Search the library and custom sensors	`stop_sweep`	Stops at once. Always allowed
`sensor_to_ohms`	Resistance at a value; sends nothing	`get_sweep_status`	Progress, time left, last result
`set_resistance`	Connects the output at `"100"`, `"4.7k"`, `"1.5M"`	`define_custom_sensor`	RTD by R0, thermistor by R25 and beta, Steinhart-Hart, points. Until the app closes
`set_sensor_value`	E.g. a Pt100 at 25 °C	`make_table`, `list_tables`	Save a table file in Tables; list them
`open_output`	Disconnects the terminals (broken wire)	`save_sequence`, `list_sequences`	Save a sequence file; list them
`close_output`	Reconnects, at the old or a new value	`run_sequence`	Starts a saved sequence on the Sequences page
`preview_sweep`	Values and duration; sends nothing	`read_reports`	Newest run reports, step by step

Limits

Sweep	1,000 values a pass, 100 loops, 10,000 values in all
Hold	1 s to 3,600 s a value; 24 h in all
Saved sequence	200 steps
Custom sensors	20, up to 1,000 points each
Values	Same checks as the Device page; refused, never clipped
MCP from	This computer only, even with other computers allowed

Refused or locked away

- **Refused while** the calibration bench, a table upload or a firmware update has the box, a sweep or sequence runs, or a table is active on the box. MCP also while AI control is off.
- **Never reachable:** calibration and its record, serial number and dates, firmware updates, raw commands, factory reset, power-up settings.
- Turning off AI control, stopping the server or closing the app stops what an AI started. **Recent AI actions** on the Local network API page lists what it did.