

MCP Apps: UI in AI

When Model Context Protocol (MCP)
can render HTML inside AI chat app



Aurelijus Banelis

Lead Software Engineer

aurelijus.banelis.lt

aurelijus@banelis.lt

PGP 0x320205E7**539B6203**

130D C446 1F1A 2E50 D6E3

3DA8 3202 05E7 539B 6203



TERMINOLOGY

MCP Apps: UI in AI tools

AI: Artificial Intelligence

MCP: Model Context Protocol

MCP Apps is part of MCP specification

UI: User Interface

AGENDA

What we'll cover

How it feels? 01

How it works? 02

How mature it is? 03

PART 01

How it feels?

DEMO time: How it looks from a non-technical user

- **01** How it feels?

- 02 How it works?

- 03 How mature it is?

4. ≡ Kaunas

5. ≡ Klaipėda

6. ≡ Šiauliai

7. ≡ Panevėžys

8. ≡ Alytus

9. ≡ Mažeikiai

10. ≡ Jonava

Send priorities to chat

Sent ✓



Prioritized:

1. Utena

2. Vilnius

3. Marijampolė

4. Kaunas

5. Klaipėda

6. Šiauliai

7. Panevėžys

8. Alytus

9. Mažeikiai

10. Jonava

Let's talk DEMO

<https://mcp-prioritization.netlify.app/mcp>

github.com/aurelijusb/mcp-prioritization

Claude is AI and can make mistakes. Please double-check responses.



Upgrade



@PrioritizeLet me
prioritize cities to visit



Called tool ▾

P

Prioritize

CSP off

Drag items to reorder, or focus an item (Tab) and
press Alt+↑/Alt+↓ to move it. ↑/↓ moves focus.

Full screen

1. ≡ Vilnius

2. ≡ Kaunas

3. ≡ Klaipėda

4. ≡ Šiauliai

5. ≡ Panevėžys

6. ≡ Alytus

7. ≡ Marijampolė

8. ≡ Mažeikiai



Ask anything



Think



0080 table items prioritizationtalk-mcp-apps

Give me to prioritize 0080 table items

Read 0080-support-matrix.md, used a tool >

Using Human prioritization: Human prioritization >

*

Allow Claude to use Human prioritization (Human prioritization)?

```
{
  "items": [
    "Claude Chat (desktop) - HTTP / stdio",
    "Claude Cowork (desktop) - HTTP / stdio",
    "Claude Chat (mobile) - HTTP",
    "Claude Code (CLI / VS Code) - no support",
    "GitHub Copilot (VS Code) - HTTP / stdio"
  ]
}
```

DenyAlways allow 2Allow once 3 Ctrl+Enter

Let's talk DEMO

tsx ./src/stdio.ts

github.com/aurelijusb/mcp-prioritization

MCP Apps: UI in AI

127.0.0.1:1111/slides#/6

Adoption

CLIENT	PLATFORM	MCP APPS SUPPORT
Claude Chat	desktop	HTTP / stdio
Claude Cowork	desktop	HTTP / stdio
Claude Chat	mobile	HTTP
Claude Code	CLI / VS Code	no support
GitHub Copilot	VS Code	HTTP / stdio

Microsoft Office Copilot also support, but it can cost ~2500k€/year.
Claude Haiku does not render MCP Apps, need at least Sonnet model.

OFFICIAL REFERENCE: SUPPORTED CLIENTS

STARTRESET

Slide 7 / 24

25m talk + 5m Q&A

0:00 / 30:00NOT STARTED

Adoption

CLIENT	PLATFORM	MCP APPS SUPPORT
Claude	desktop	HTTP / studio
GitHub Copilot	VS Code	HTTP / studio
Claude	mobile / web	HTTP
ChatGPT	mobile / web	HTTP
Claude	CLI / VS Code	no support
Codex	CLI / VS Code	no support

Microsoft Office Copilot also support, but it can cost ~2500k€/year.
Claude Haiku does not render MCP Apps, need at least Sonnet model.

[OFFICIAL REFERENCE: SUPPORTED CLIENTS](#)

PART 02

How it works?

Behind the SDK

01 How it feels?

■ 02 **How it works?**

03 How mature it is?

HTTP Schema for UI files

REQUEST · MY DEMO SERVER

```
curl -sS https://mcp-prioritization.netlify.app/mcp \
-H 'Content-Type: application/json' \
-H 'Accept: application/json, text/event-stream' \
-H 'MCP-Protocol-Version: 2026-07-28' \
-H 'Mcp-Method: tools/list' \
-d '{"jsonrpc":"2.0","id":1,
  "method":"tools/list",
  "params":{"_meta":{"
    "io.modelcontextprotocol/protocolVersion":
      "2026-07-28",
    "io.modelcontextprotocol/clientCapabilities":
      {}}}}' | jq
```

RESPONSE

```
{ "tools": [ {
  "name": "human_prioritization",
  "inputSchema": { ... },
  "_meta": {
    "ui": {
      "resourceUri": "ui://prioritization/list.html",
      "visibility": [ "model", "app" ]
    }
  }
} ] }
```

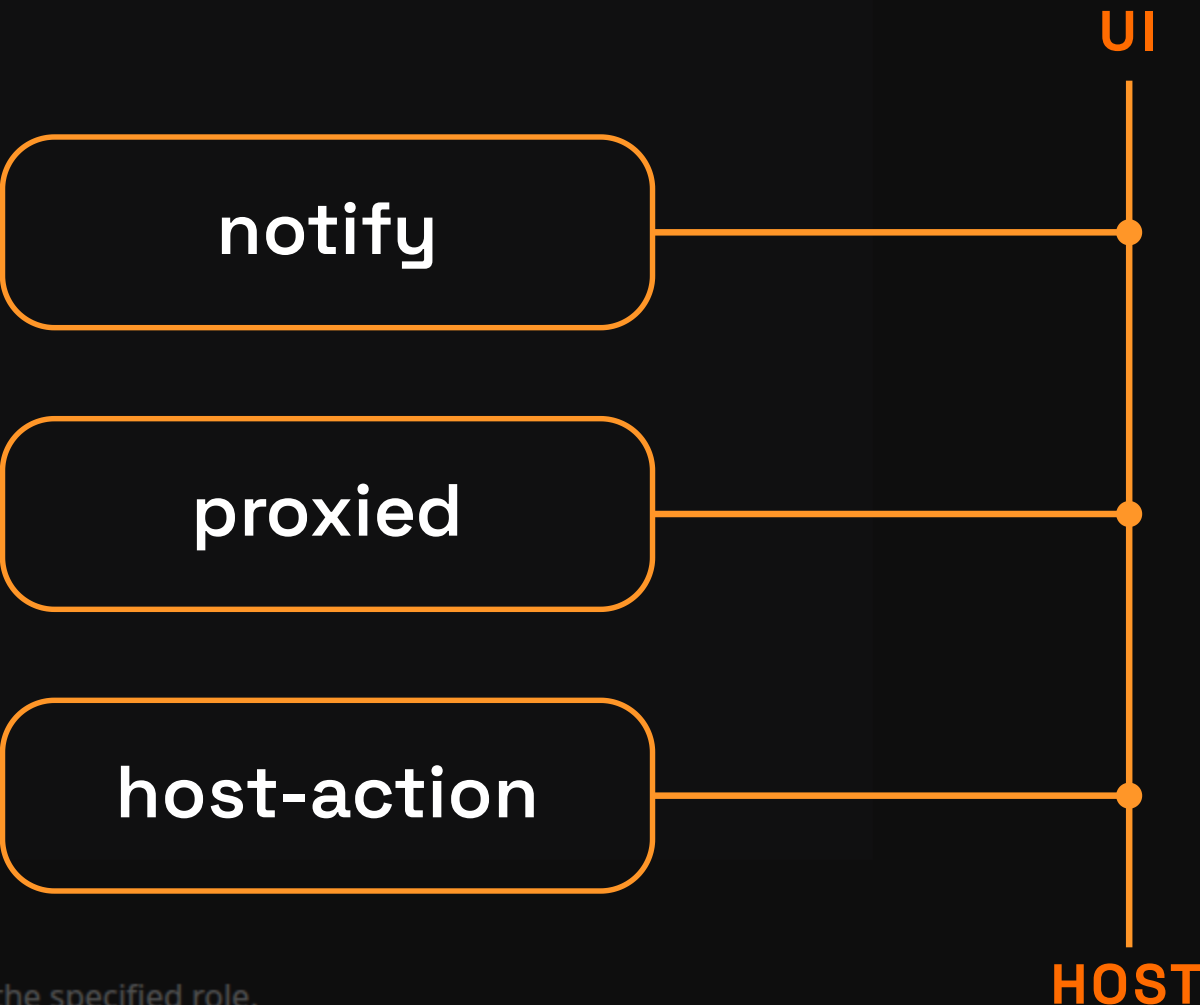
JSON-RPC over Stateless HTTP.

The UI is already declared in `tools/list`, before anything is called.

JavaScript Communication

Every message, in either direction, crosses one channel: `window.parent.postMessage`.

- **notify** — no id, fire and forget: *tool-input, tool-result*
- **host-action** — View → Host → Server: *tools/call, resources/read*
- **host-action** — terminates at the Host: *ui/open-link, ui/message, ui/request-display-mode, ui/update-model-context, ui/resource-teardown*



SPEC github.com/modelcontextprotocol/.../apps.mdx

- Host behavior:
- Host SHOULD add the message to the conversation context, preserving the specified role.
 - Host MAY request user consent.

`ui/request-display-mode` - Request host to change display mode

```
// Request
{
  jsonrpc: "2.0",
  id: 3,
  method: "ui/request-display-mode",
  params: {
```

PART 03

How mature it is?

Usages in the real world

01 How it feels?

02 How it works?

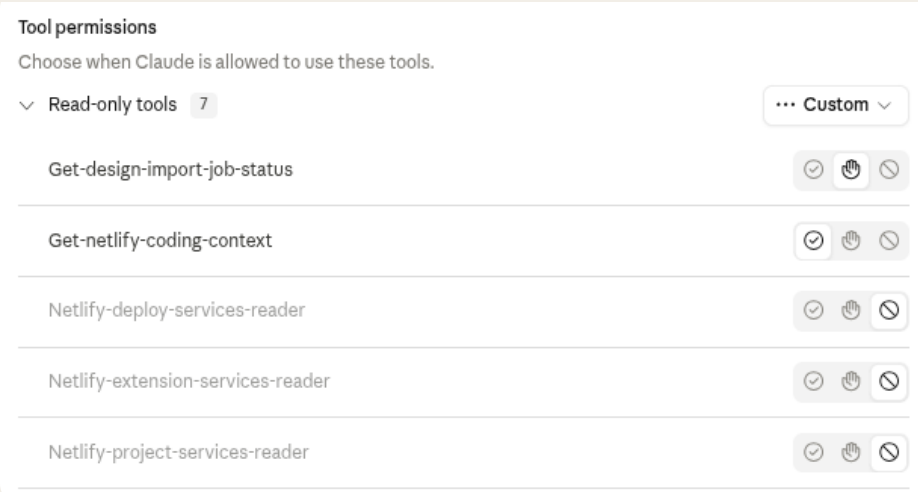
■ 03 How mature it is?

No single MCP Apps store

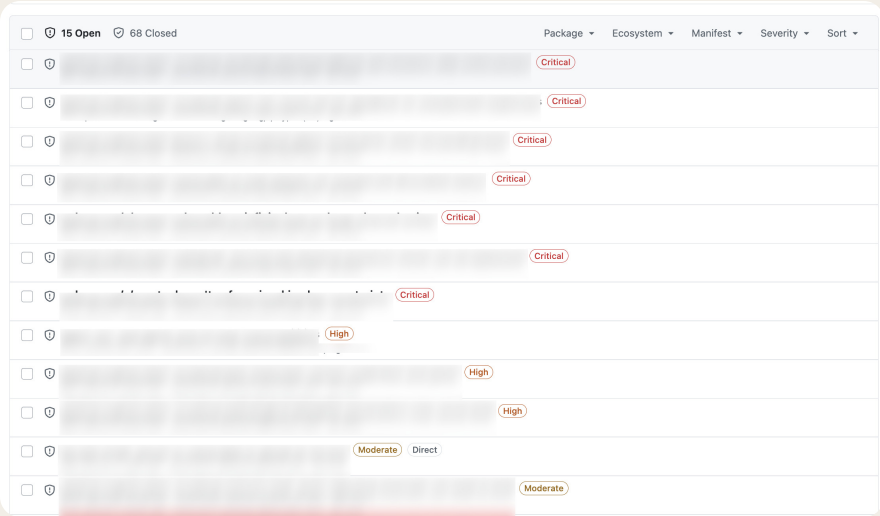


HOST	NAME
Claude	Claude Connector or Claude App that ships UI
ChatGPT	ChatGPT App build on MCP with some OpenAI-only features
VS Code	Microsoft's curated MCP gallery
Goose	Goose extensions
Cursor	Cursor marketplace
PulseMCP	The cross-host MCP server directory
...	...

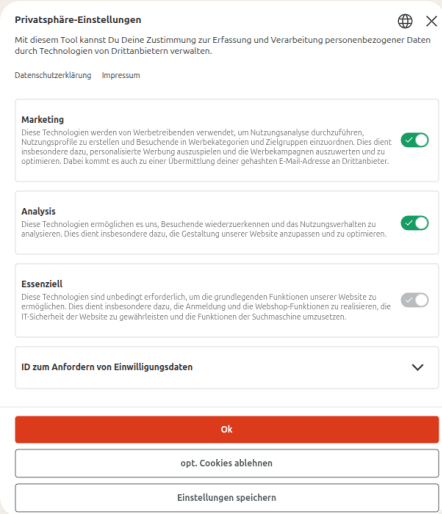
Security and privacy edge cases



Tool trust poisoning — Invariant Labs, Apr 2025 — a sleeper server advertises an innocuous tool, then swaps it *after* you approved it. CyberArk extended this to the whole schema, not just descriptions *



Supply chain — postmark-mcp shipped 15 clean versions, then a one-line BCC backdoor in v1.0.16 — 1,643 downloads before removal. CVE-2025-6514 in mcp-remote scores 9.6 *



GDPR — ePrivacy Art. 5(3) and TDDDG §25 are technology-neutral and name local storage directly. MCP simply has no consent logging — a compliance burden

```
max_results: 1
```

×

Copy

POTENTIAL

MCP Apps: The next IDE

Biggest MCP Apps potential is still for technical people.

Human review on low level code will become a bottleneck.

Visualization and interaction is like a high level programming language.

Q&A

MCP Apps: UI in AI

Aurelijus Banelis · aurelijus.banelis.lt