

AIKosh MCP

User Manual / Handbook

Official MCP URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>

Document version 1.0 . 2026-07-21 . Audience: End users, builders, researchers, enterprises

Note - Browser vs MCP client: Opening the MCP URL in a normal web browser may show a website "Page Not Found" response. That is expected for a tools endpoint. Always connect using an MCP-capable client (ChatGPT Connectors, Claude Connectors, Cursor, VS Code, etc.).

Contents

- [1. Introduction](#)
- [2. What is AIKosh MCP?](#)
- [3. Prerequisites & Access](#)
- [4. Official Endpoint](#)
- [5. Connect from ChatGPT](#)
- [6. Connect from Claude.ai](#)
- [7. Connect from Gemini \(Enterprise\)](#)
- [8. Connect from IDEs \(Cursor, VS Code, Windsurf, Antigravity\)](#)
- [9. Authentication \(OAuth\)](#)
- [10. Capabilities & Tools](#)
- [11. Example Conversations](#)
- [12. Security & Responsible Use](#)
- [13. Troubleshooting](#)
- [14. Support & References](#)
- [Appendix A - mcp.json templates](#)
- [Appendix B - Glossary](#)

1. Introduction

This handbook explains how to use AIKosh MCP, the Model Context Protocol server for IndiaAI's AIKosh platform. It follows the same structure used by leading AI platforms when documenting remote MCP connectors: overview, prerequisites, client setup, authentication, capabilities, security, troubleshooting.

Industry references informing this manual include OpenAI ChatGPT Connectors / Developer Mode (remote Streamable HTTP MCP), Anthropic Claude custom remote MCP connectors, Google Gemini Enterprise Custom MCP Server data stores, and IDE MCP configuration patterns used by Cursor, Visual Studio Code, Windsurf, and similar tools.

- **Who this is for:** Researchers and students discovering AIKosh datasets and models in chat.
- **Who this is for:** Builders wiring assistants and IDE agents into AIKosh.
- **Who this is for:** Enterprises enabling governed, per-user access to national AI assets.

2. What is AIKosh MCP?

Model Context Protocol (MCP) is an open standard that lets AI assistants call structured tools over a secure HTTP interface. AIKosh MCP wraps AIKosh's Dataset and Model APIs and exposes read-only tools so an assistant can search, inspect metadata, browse package contents, and obtain time-limited signed download URLs, acting as the signed-in user.

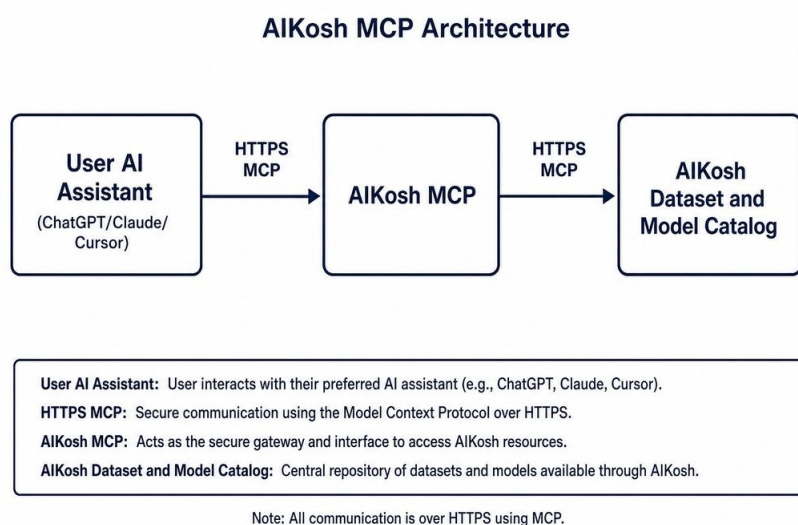


Figure 1. High-level flow: AI assistant - AIKosh MCP - AIKosh catalog APIs.

2.1 Key product properties

- **Discovery:** Search datasets and models with official filters.
- **Exploration:** Inspect metadata, versions, and file trees before downloading.
- **Download assistance:** Receive time-limited signed URLs for packages or individual files.
- **Per-user auth:** OAuth 2.1 + PKCE with the user's own AIKosh API key.
- **Safety:** Read-only tools; the assistant cannot mutate the catalog.

2.2 How this compares to other MCP products

Like ChatGPT's remote MCP connectors, Claude's custom remote MCP connectors, and Gemini Enterprise's Custom MCP Server stores, AIKosh MCP is a public HTTPS Streamable HTTP

endpoint. You paste one URL, complete OAuth when prompted, and the client discovers tools automatically, the same pattern used across major AI vendors.

3. Prerequisites & Access

- An AIKosh account on <https://aikosh.indiaai.gov.in>.
- An AIKosh API key (from your AIKosh profile / developer settings).
- An MCP-capable client: ChatGPT (with Connectors / Developer Mode as applicable), Claude.ai, Gemini Enterprise, Cursor, VS Code, Windsurf, Antigravity, or MCP Inspector.
- Network access to the official MCP HTTPS endpoint.

Note - API key privacy: Never paste your API key into chat messages. Enter it only on the official AIKosh MCP authorize page during OAuth.

4. Official Endpoint

Use exactly this URL in every MCP client:

<https://aikosh.indiaai.gov.in/aikoshmcp/mcp>

4.1 Connection settings

- **Transport:** Streamable HTTP (preferred). Do not use stdio for remote clients.
- **Server URL:** <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>
- **Authentication:** OAuth 2.1 (authorization code + PKCE). Connector API-key Bearer is also supported where the client allows a static token.
- **Scopes:** mcp:tools (default). Finer scopes may restrict datasets, models, or downloads.

5. Connect from ChatGPT

ChatGPT supports remote MCP servers over HTTPS. For interactive Chat mode, OpenAI requires Developer Mode on eligible plans (Pro / Team / Enterprise / Edu). Steps below follow the Connectors pattern documented for ChatGPT remote MCP integrations.

5.1 Enable Developer Mode (when required)

- Open ChatGPT > Settings > Connectors (or Apps & Connectors).
- Under Advanced, enable Developer Mode (beta) if available on your plan.

5.2 Create the AIKosh MCP connector

- In Connectors, choose Create / Add custom connector.
- Name: AIKosh MCP
- Server URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>
- Authentication: OAuth (recommended).
- Confirm you trust the provider (IndiaAI / AIKosh).
- Save / Create, then complete the OAuth authorize page with your AIKosh API key.
- Navigate to <https://chatgpt.com/plugins>

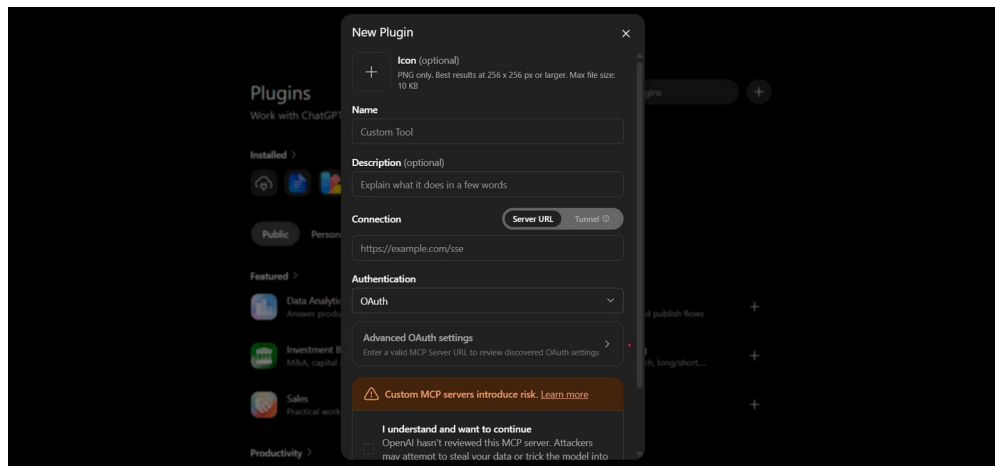


Figure 2. Illustrative ChatGPT connector dialog with AIKosh MCP URL (UI may vary by plan and product updates).

5.3 Use in a chat

- Start a new chat.
- Open + > More > Developer Mode (or Connectors) and enable AIKosh MCP for that chat.
- Try: "List healthcare datasets on AIKosh" or "Find Indic language models and show metadata."

6. Connect from Claude.ai

Anthropic documents custom connectors using remote MCP for Claude.ai, Claude Desktop, and related surfaces. The server must be reachable over the public internet.

6.1 Individual plans (Pro / Max / Free where available)

- Go to Customize > Connectors (or Settings > Connectors).
- Choose Add custom connector.
- Paste the remote MCP URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>
- Optionally open Advanced settings for OAuth client credentials if your organisation requires them.
- Click Add and complete OAuth when redirected.

6.2 Team / Enterprise

- An Owner adds the connector under Organization settings > Connectors.
- Members then enable it under Customize > Connectors.

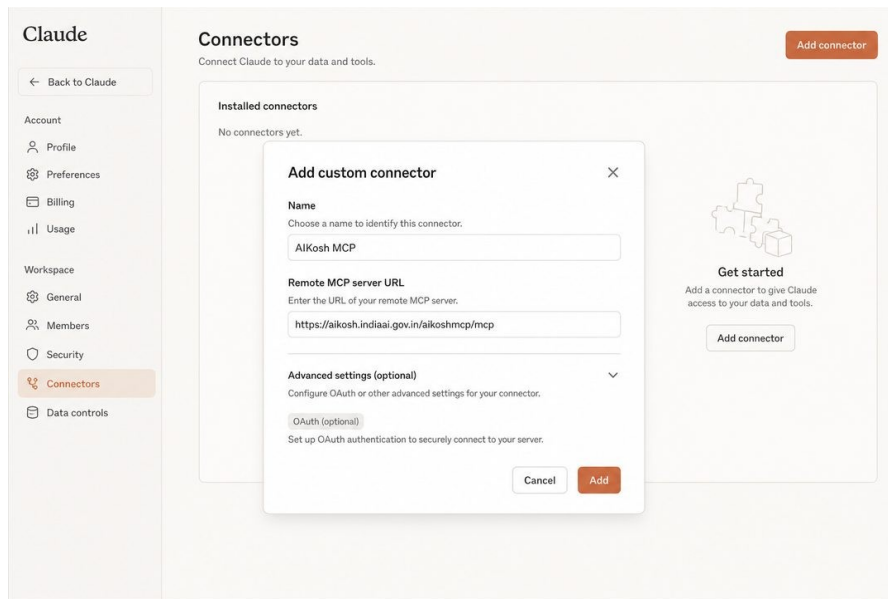


Figure 3. Illustrative Claude custom connector dialog for AIKosh MCP.

7. Connect from Gemini (Enterprise)

Google Gemini Enterprise supports Custom MCP Server connected data stores using Streamable HTTP. Administrators configure MCP Server URL plus OAuth Authorization and Token endpoints, then users authorize and enable tools.

- MCP Server URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>
- Authorization URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp/oauth/authorize>
- Token URL: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp/oauth/token>
- Follow Google Cloud Gemini Enterprise documentation for OAuth client redirect URIs required by Google.

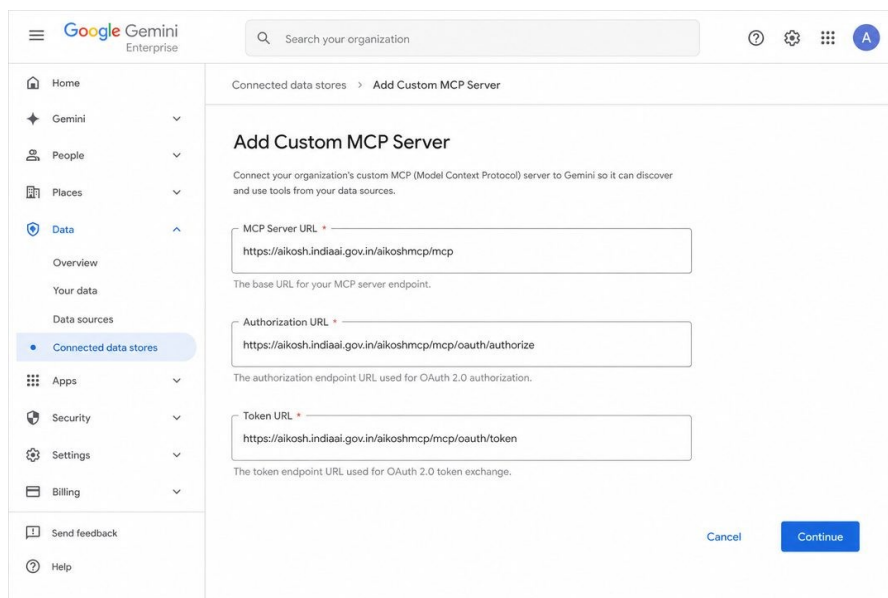


Figure 4. Illustrative Gemini Enterprise Custom MCP Server configuration for AIKosh MCP.

Note - Consumer Gemini apps: MCP connector availability differs between Gemini Enterprise / admin consoles and consumer Gemini surfaces. Prefer Enterprise documentation when enabling organisational access.

8. Connect from IDEs

Most coding agents configure remote MCP servers through an `mcp.json` (or `settings`) file. Below are recommended templates for AIKosh MCP. Field names may vary slightly by IDE version - prefer `type/url` (or `url + transport http`) over deprecated SSE-only configs.

8.1 Cursor

Create or edit `~/.cursor/mcp.json` (user) or project `.cursor/mcp.json`:

```
{
  "mcpServers": {
    "aikosh-mcp": {
      "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp",
      "headers": {
        "Authorization": "Bearer <API_Key>"
      }
    }
  }
}
```

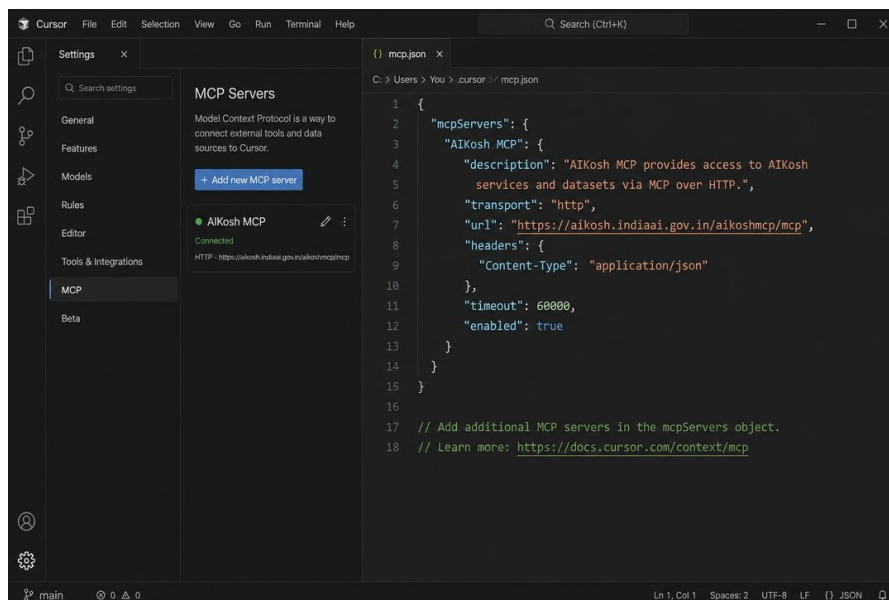


Figure 5. Illustrative Cursor MCP configuration for AIKosh MCP.

8.2 Visual Studio Code

Use VS Code MCP settings / `.vscode/mcp.json` (wording depends on VS Code MCP support version):

```
{
  "servers": {
    "AIKosh-MCP": {
      "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp",
      "headers": {
        "Authorization": "Bearer <API_Key>"
      }
    }
  },
  "inputs": []
}
```

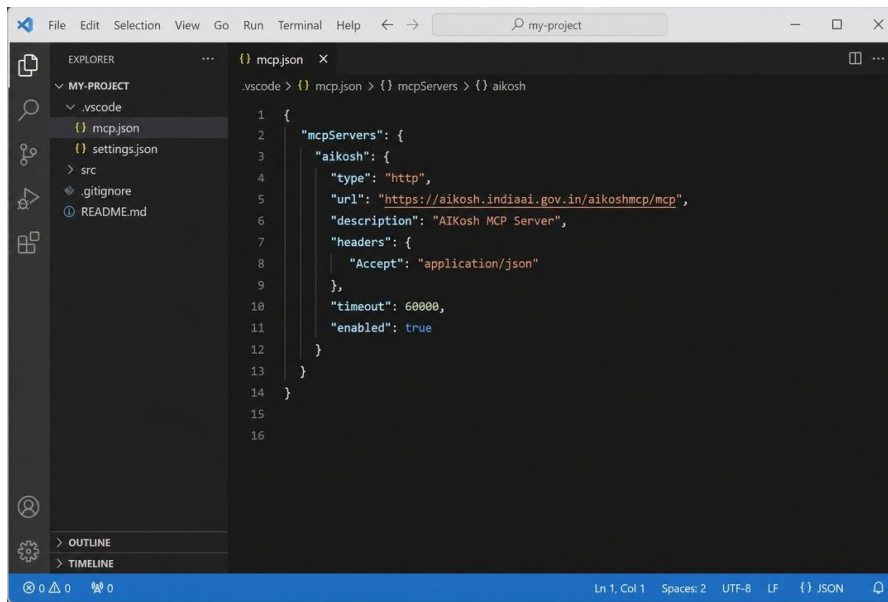


Figure 6. Illustrative VS Code MCP configuration for AIKosh MCP.

8.3 Windsurf

Add a remote MCP server in Windsurf MCP settings, or via mcp.json-compatible config:

```

{
  "mcpServers": {
    "aikosh-mcp": {
      "serverUrl": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp",
      "headers": {
        "Authorization": "Bearer <API_Key>"
      }
    }
  }
}

```

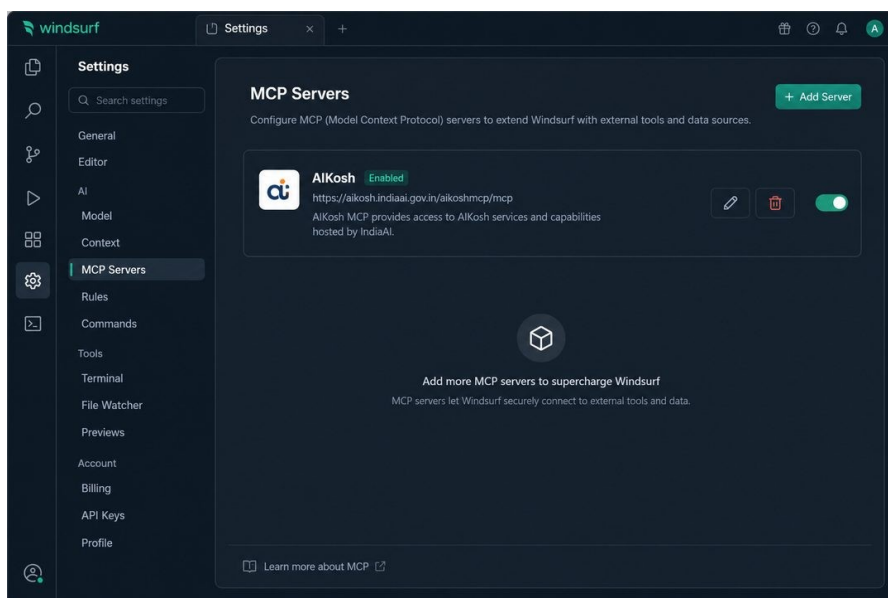


Figure 7. Illustrative Windsurf MCP settings for AIKosh MCP.

8.4 Antigravity

In Antigravity MCP / Integrations settings, add a remote HTTP MCP server:

```

{

```

```

"mcpServers": {
  "AIKosh MCP": {
    "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp",
    "headers": {
      "Authorization": "Bearer <API_Key>"
    }
  }
}

```

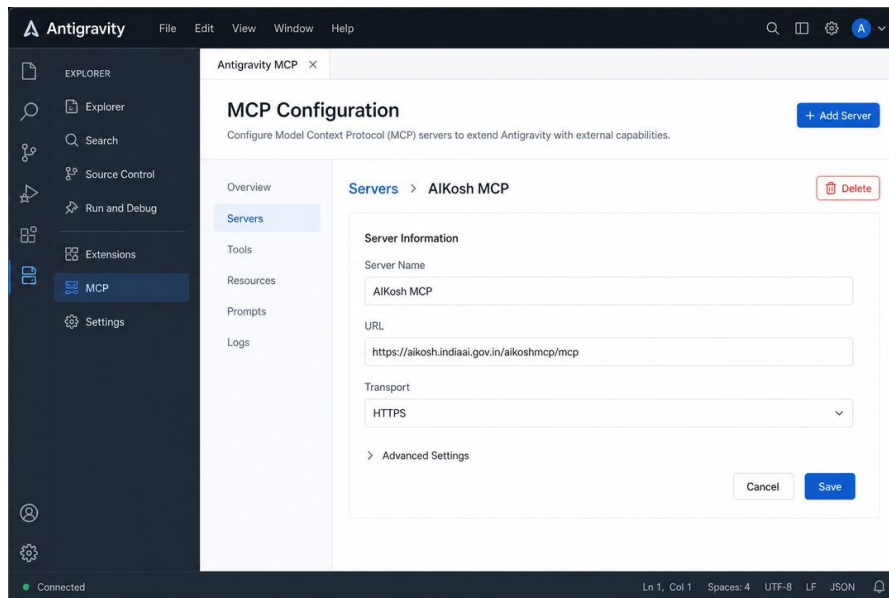


Figure 8. Illustrative Antigravity MCP configuration for AIKosh MCP.

8.5 Claude Desktop / Claude Code (reference)

Claude Desktop config (claude_desktop_config.json) remote HTTP example:

```

{
  "mcpServers": {
    "aikosh-mcp": {
      "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp",
      "headers": {
        "Authorization": "Bearer <API_Key>"
      }
    }
  }
}

```

Claude Code CLI (illustrative):

```

claude mcp add --transport http aikosh-mcp
https://aikosh.indiaai.gov.in/aikoshmcp/mcp

```

9. Authentication (OAuth)

When a client connects without a token, AIKosh MCP returns HTTP 401 with a WWW-Authenticate header pointing to OAuth protected-resource metadata. Compatible clients then open the authorize page.

9.1 Typical user flow

- Client discovers authorization server metadata under the MCP issuer.

- You are redirected to the AIKosh MCP authorize page.
- Paste your AIKosh API key and approve access.
- Client receives an access token and can call tools.

9.2 Connector API-key mode

Some IDE connectors accept Authorization: Bearer <AIKosh_API_KEY> directly. When the Bearer value matches API-key shape, AIKosh MCP binds a session for that key. Prefer OAuth in browser-based assistants when available.

10. Capabilities & Tools

AIKosh MCP exposes read-only tools for datasets and models (illustrative catalog):

10.1 Dataset tools

- `get_dataset_filters` - allowed sectors, licenses, organisations, formats
- `list_datasets_tool` - browse / filter the catalog
- `get_dataset_metadata` - full metadata for one dataset
- `get_dataset_file_structure` - browse files inside a version
- `get_dataset_download_url_tool` - signed URL for a full package
- `get_file_download_url_tool` - signed URL for one file
- `search_datasets_and_get_download_urls` - search with download links
- `search_datasets_with_signed_urls` - organisation-oriented search
- `ping` - connectivity check

10.2 Model tools

- `get_model_filters_tool`
- `list_models_tool`
- `get_model_metadata_tool`
- `get_model_file_structure_tool`
- `get_model_download_url_tool`
- `get_model_file_download_url_tool`

Note - Access types: RESTRICTED assets may refuse downloads for your key. REDIRECT / externally hosted assets may return an external URL (for example Hugging Face) instead of a hosted signed URL.

11. Example Conversations

- "What sectors can I filter AIKosh datasets by?"
- "Find agriculture datasets and summarise the top three."
- "Show metadata and files for dataset id <uuid>."
- "List Indic translation models and give me a download link for Indic Trans2."
- "Datasets published by AI4Bharat with download options."

12. Security & Responsible Use

- Use only the official HTTPS endpoint above.
- Do not share API keys, OAuth tokens, or signed URLs in tickets or screenshots.
- Signed URLs expire quickly; request a new one when needed.

- Respect dataset/model licenses and organisational access policies.
- Report suspected abuse through AIKosh support / grievance channels.

13. Troubleshooting

Browser shows Page Not Found for the MCP URL

Expected for many deployments. The endpoint is for MCP clients, not a human HTML page. Connect via ChatGPT / Claude / IDE instead.

401 Unauthorized

Complete OAuth again, or refresh the connector token. Confirm your API key is active.

OAuth page does not appear

Confirm the client is using the full URL including /aikoshmcp/mcp. Check corporate firewall / proxy allowlists for aikosh.indiaai.gov.in.

Tools fail with permission / restricted

Your AIKosh account may lack download entitlement for that asset. Try an Open / HOSTED item.

IDE cannot connect

Validate JSON syntax in mcp.json, restart the IDE, and confirm HTTPS outbound access.

14. Support & References

- AIKosh portal: <https://aikosh.indiaai.gov.in>
- AIKosh MCP: <https://aikosh.indiaai.gov.in/aikoshmcp/mcp>
- IndiaAI programme: <https://indiaai.gov.in>
- MCP specification: <https://modelcontextprotocol.io>
- OpenAI ChatGPT MCP / Connectors documentation (vendor site)
- Anthropic Claude remote MCP connectors help centre
- Google Cloud Gemini Enterprise Custom MCP Server docs

Appendix A - mcp.json templates

Minimal remote HTTP template (Cursor-style):

```
{
  "mcpServers": {
    "aikosh-mcp": {
      "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp"
    }
  }
}
```

Typed HTTP template (VS Code / Claude Desktop-style):

```
{
  "mcpServers": {
    "aikosh-mcp": {
      "type": "http",
      "url": "https://aikosh.indiaai.gov.in/aikoshmcp/mcp"
    }
  }
}
```

Appendix B - Glossary

- **MCP:** Open standard for AI tool calling over transports such as Streamable HTTP.
- **AIKosh:** India's national AI dataset and model platform under IndiaAI.
- **OAuth 2.1 / PKCE:** Industry-standard login flow used by AIKosh MCP for per-user access.
- **Streamable HTTP:** Current recommended remote MCP transport used by ChatGPT, Claude, and Gemini Enterprise.
- **Signed URL:** Time-limited HTTPS link to download a package or file.

-- End of document --