AI Tool Private Control Center

with MCP powered by Code Creator

Start here

This server gives your AI applications a private, token-protected MCP endpoint. It includes one safe readiness tool so you can confirm that your client connection works before you add your own tools.

How This Server Works

AI Tool Private Control Center with MCP powered by Code Creator is a private access-control server for AI tools. It creates a secure HTTPS MCP endpoint that AI applications, agents, workflows, and custom integrations can use to connect to approved MCP tools.

At first boot, the server automatically creates your private endpoint, administrator configuration, starter client token, and an included safe readiness tool. Retrieve your connection details securely through SSH:

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

Use the endpoint and starter token in your MCP-compatible AI client or application.

Where You See Results

This product does not include a graphical AI chat dashboard. The public browser page confirms that the server is online and ready.

Tool results appear inside the AI client, agent, workflow, or custom application that connects to the MCP endpoint. The included readiness tool returns a result showing `status: ready`, confirming that your AI client authenticated successfully and can use an approved tool.

Opening the `/mcp` address directly in a browser will show a missing-token message. This is expected because browsers do not send your private MCP client token.

Managing Access

Administration is performed securely through SSH command-line utilities. Use the included commands to check server status, view the endpoint, review available tools, and create separate client tokens for each AI application.

The starter token is intentionally restricted to the included safe readiness tool. Create separate tokens and grant access only to the tools each AI application requires.

Important Product Scope

This server is not an AI model host, chatbot, or prebuilt catalog of business integrations. It is the private control layer that protects and manages MCP access between your AI applications and the tools you choose to connect.

What this server is for

Use this product as your private control point for MCP-enabled AI applications. Your AI client connects to the server over HTTPS, presents a bearer token, and can call only the tools you allow.

Important: This is not a hosted general-purpose AI model. The included `cc_readiness__get_control_center_status` tool is a safe connection and readiness check.

Your first 5 minutes

1	**Launch with a public IPv4 address.** No domain is required. The server creates a secure HTTPS address based on your public IP and nip.io.
2	**Wait for setup to finish.** First boot normally takes a few minutes. Do not try to use the MCP endpoint until status reports Ready.
3	**Connect by SSH.** Use the **Ubuntu** account supplied with your EC2 launch configuration.
4	**Check readiness.** Run the command below. When it says Ready, continue.

```
sudo codecreator-ai-tool-control-status
```

5	**Retrieve your private connection details.** The file below contains your personal MCP endpoint and starter token. Treat it like a password.

```
cat /home/ubuntu/FIRST_LOGIN.txt
```

Connect your AI or MCP client

In an MCP-compatible AI client, IDE, agent framework, or custom application, create a Streamable HTTP MCP connection using the details in `/home/ubuntu/FIRST_LOGIN.txt`

Transport	Streamable HTTP
MCP endpoint	`https://<your-public-ip>.nip.io/mcp`

Authentication	Bearer token from FIRST_LOGIN.txt
Test tool	`cc_readiness__get_control_center_status`
Expected result	status: ready

Browser note: Opening the server root URL in a browser shows a Ready page. Opening `/mcp` directly without a token returns an access-token error. That is expected and confirms the endpoint is protected.

Helpful server commands

`sudo codecreator-ai-tool-control-status`	Show first-boot and container status.
`sudo codecreator-ai-tool-control-url`	Show the current HTTPS endpoint.
`sudo codecreator-ai-tool-control-admin list tools`	List registered MCP tools.
`sudo codecreator-ai-tool-control-admin create mcp-client <client-name> --allow "cc_readiness"`	Create a separate limited client for testing.

Security essentials

- Keep the starter token private. Do not paste it into tickets, chats, source code, screenshots, or public configuration files.
- Use a separate client token for each AI application when you move beyond the included readiness test.
- Allow TCP 22 only from your administrator IP address. Allow TCP 80 and 443 only where your HTTPS users and AI clients require access.
- Do not open database or internal service ports such as 5432, 8000, or 8080 to the Internet.

Troubleshooting

Setup is still running	`Run sudo codecreator-ai-tool-control-status and wait until Status: Ready.`
Endpoint does not open	Confirm the instance has a public IPv4 address and that your security group permits TCP 80 and 443.
Browser shows token error at /mcp	Normal behavior. Use an MCP client that sends the bearer token from FIRST_LOGIN.txt.
Need more detail	`Run sudo journalctl -u codecreator-ai-tool-control-firstboot.service --no-pager -l.`

You are ready when your client can call `cc_readiness__get_control_center_status` and receives `status: ready.`