

09-mcp-github.md

kstack: book: Centerpoint Home
Lab chapter: AI & Automation
page: MCP GitHub Server tags:
[mcp, github, oauth2, ai, claude]

Overview

The MCP GitHub Server exposes GitHub's Model Context Protocol (MCP) server over HTTPS with OAuth 2.1 authentication, making it accessible to Claude.ai and other MCP-compatible AI clients from anywhere on the internet.

The stack consists of two containers:

- `mcp-github-proxy` — a custom Node.js OAuth 2.1 proxy (locally built image) that validates JWTs from Authentik before forwarding requests to the MCP server.
- `github-mcp-server` — the official GitHub MCP server running in HTTP mode, internal-only, with access scoped to repos and issues.

Access

Type	URL	Notes
Internal	<code>https://mcp-github.home.local</code>	LAN access via Step-CA TLS
External	<code>https://mcp-github.jeeves5454.ddns.net</code>	OAuth 2.1 authenticated — no Authentik ForwardAuth

The external route uses **OAuth 2.1** (not Authentik ForwardAuth) as the auth layer. GeoBlock and CrowdSec are still applied. The OAuth 2.1 issuer is Authentik.

Containers in This Stack

Container	Image	Role
mcp-github-proxy	mcp-github-proxy:latest (local build)	OAuth 2.1 proxy + MCP request forwarder
github-mcp-server	ghcr.io/github/github-mcp-server:latest	GitHub MCP server (HTTP mode, internal)

Configuration

Compose project: mcp-github **Compose file:** /home/jeeves/docker/mcp-github/proxy/docker-compose.yml

mcp-github-proxy Environment Variables

Variable	Value / Notes
PORT	3000
GITHUB_MCP_URL	http://github-mcp-server:8080
GITHUB_PERSONAL_ACCESS_TOKEN	REDACTED — PAT with read-only scopes (Contents, Issues, Metadata)
AUTHENTIK_ISSUER	https://auth.jeevesconsults.ca/application/o/mcp-github/
AUTHENTIK_JWKS_URL	https://auth.jeevesconsults.ca/application/o/mcp-github/jwks/
SERVER_URL	https://mcp-github.jeeves5454.ddns.net

github-mcp-server Environment Variables

Variable	Value / Notes
GITHUB_PERSONAL_ACCESS_TOKEN	REDACTED — same read-only PAT as proxy
GITHUB_TOOLSETS	repos,issues — restricts available tools
GITHUB_READ_ONLY	1 — belt-and-suspenders read-only flag

Security note: `GITHUB_READ_ONLY=1` has a known bug in HTTP mode (github/github-mcp-server #2156) — toolset flags may not fully enforce read-only behaviour. Primary read-only enforcement is the PAT scopes themselves (Contents/Issues/Metadata: read only).

Traefik Labels

```
# External route – GeoBlock + CrowdSec only (OAuth 2.1 handles auth)
traefik.http.routers.mcp-github-ext.rule: Host(`mcp-github.jeeves5454.ddns.net`)
traefik.http.routers.mcp-github-ext.entrypoints: websecure
traefik.http.routers.mcp-github-ext.tls.certresolver: letsencrypt
traefik.http.routers.mcp-github-ext.middlewares: plex-geoblock@file,crowdsec-bouncer@file
traefik.http.routers.mcp-github-ext.service: mcp-github-proxy-svc

# Internal route
traefik.http.routers.mcp-github-int.rule: Host(`mcp-github.home.local`)
traefik.http.routers.mcp-github-int.entrypoints: websecure
traefik.http.routers.mcp-github-int.tls.certresolver: step-ca
traefik.http.routers.mcp-github-int.service: mcp-github-proxy-svc

traefik.http.services.mcp-github-proxy-svc.loadbalancer.server.port: 3000
```

Note: Authentik ForwardAuth (`authentik-auth@docker`) is **not** used here. OAuth 2.1 is the authentication mechanism — the proxy validates the `Authorization` header JWT against Authentik's JWKS endpoint directly.

Sub-section: GitHub MCP Server

`github-mcp-server` runs the official GitHub MCP server in HTTP mode on port `8080`, internal-only. It is never directly exposed to Traefik or the host — all requests arrive through the `mcp-github-proxy` over the `mcp-github-internal` network.

The server is restricted to `repos` and `issues` toolsets, providing read-only access to repository content, metadata, and issues. Write operations are not available via the PAT scopes.

Proxy Image Build

The `mcp-github-proxy` image is built locally on Centerpoint before deployment:

```
cd /home/jeeves/docker/mcp-github/proxy
docker build -t mcp-github-proxy:latest .
```

Source files: `/home/jeeves/docker/mcp-github/proxy/{Dockerfile,package.json,src/}`

Volumes / Bind Mounts

No persistent volumes required. Both containers are stateless — the proxy holds no state, and the MCP server reads from GitHub's API on every request.

Networks

Network	Purpose
<code>traefik-net</code>	Exposes <code>mcp-github-proxy</code> via Traefik
<code>mcp-github_mcp-github-internal</code>	<code>mcp-github-proxy</code> ↔ <code>github-mcp-server</code> communication

`github-mcp-server` is on the internal network only — never on `traefik-net`.

Healthchecks

Both containers have healthchecks defined:

```
healthcheck:
  test: ["CMD", "wget", "-q0-", "http://localhost:<port>/health"]
  interval: 30s
  timeout: 5s
  retries: 3
```

- Proxy healthcheck: `http://localhost:3000/health`
- MCP server healthcheck: `http://localhost:8080/health`

Authentik OAuth 2.1 Provider Setup

In Authentik, an OAuth2/OIDC provider is configured for MCP GitHub with:

Setting	Value
Redirect URI	https://claude.ai/api/mcp/auth_callback
Issuer	https://auth.jeevesconsults.ca/application/o/mcp-github/
JWKS URL	<issuer>/jwks/

Dependencies

- Authentik (auth.jeevesconsults.ca) — proxy validates JWTs against Authentik JWKS
- GitHub API (internet access required for the MCP server to function)
- Traefik on traefik-net for both routes

Notes / Gotchas

- The GitHub PAT must be rotated before expiry. If it expires, all GitHub MCP tool calls will fail with 401 errors. Update in both container environment variables.
- The proxy image must be rebuilt after any source code changes:

```
cd /home/jeeves/docker/mcp-github/proxy
docker build -t mcp-github-proxy:latest .
docker compose up -d --force-recreate mcp-github-proxy
```

- Claude.ai connects to this server via the external URL. The redirect URI (https://claude.ai/api/mcp/auth_callback) must be registered in the Authentik OAuth2 provider — adding any other redirect URI will cause the OAuth flow to fail.
- GeoBlock allows CA, US, and IN. Claude.ai's servers may originate from other regions — if MCP calls fail, check Traefik logs for GeoBlock rejections and adjust the country allowlist accordingly.

Last Updated: 2026-06-16