

MODULES

AI assistant (MCP server)

Connecting AI assistants over MCP, OAuth and tokens, the tool set, what it can and cannot do.

Online: mergenhub.envest.com.tr/docs/mcp-ai

ON THIS PAGE

What the assistant can do

Typical prompts

Connecting

Security notes

MergenHub includes an **MCP server** (Model Context Protocol) so AI assistants — Claude, ChatGPT-compatible agents, internal copilots — can query and configure the plant in natural language with the same permissions as the user who authorised them.

 **MergenHub**
OPC UA Gateway - v3.119

PROJE +

↳ Bağlantılar

↳  Simulation Examples 24

 Functions 24

↳ Eklentiler

↳ Virtual Tag'ler

↳ Tag Kısayolları

↳ Alarmlar

↳ Veri Logları

↳ Data Bridge

↳ MCP (AI)

admin
Root (super-admin)

TR TR

 Eklentiler > MCP (AI)

Sadece Konfig **Canlı Veri** 24/24 aktif tag Deneme 24/500

ⓘ MCP (Model Context Protocol): AI asistanlarının (Claude, Cursor...) sisteme GÜVENLİ bağlanması için token — yalnız okuma + SCADA ekran yapma + doküman; çizme/tag'e yazma, config ekle/sil YOK. Token yalnız SENİN yetkin dahilindeki araçları alır.

🔗 Dış Erişim — AI sağlayıcıya verilecek adres

http://localhost:8095/mcp  Kopyala  Keşif testini aç

ⓘ HTTPS: YOK — web tabanlı AI istemcileri yalnız **https://** adres kabul eder. Ayarlar → Web & REST API'den HTTPS'i aç (sertifika + domain).

ⓘ Erişilebilirlik: bu adres YEREL görünüyor — web AI istemcileri buraya İNTERNETTEN ulaşamaz. Sabit IP ya da domain + port yönlendirme gerekir. (Masaüstü istemciler aynı ağdaysa yerel adresle çalışır.)

Genel adres (public URL):  Kaydet

Boş = tarayıcının eriştiği adres kullanılır. Domain yayınında MUTLAKA doldur — OAuth keşif metadatası (issuer) bu adresle ilan eder.

DOMAİNE ÇIKARMA ADIMLARI (BİR KEZ)

Sabit IP edin (ISS'den) YA DA dinamik DNS kullan; domain'in **A kaydı**nı bu makinenin genel IP'sine yönlendir.

Modem/güvenlik duvarında **443** → **bu makine** port yönlendirmesi yap (MergenHub HTTPS portu).

Sertifika: **ücretsiz Let's Encrypt** önerilir — win-acme (wacs.exe) ile domain'e sertifika al (HTTP-01 doğrulaması için 80 portu geçici olarak bu makineye yönlendirilmeli), PFX olarak dışa aktar ve Ayarlar → REST API → Sertifika'dan yükle; sonra **HTTPS'i aç**. (Alternatif: self-signed üret — tarayıcı uyarı verir, claude.ai kabul etmeyebilir.) Let's Encrypt 90 günlük; win-acme görev zamanlayıcıyla yenilene kurar — yenilenen PFX'i tekrar yüklemeyi unutma.

Buradaki Genel adres alanına **https://domain** yaz ve kaydet.

"Keşif testini aç" ile metadatası'nın DIŞ ağdan da açıldığını doğrula (telefonda mobil veriyle dene).

🔑 Yeni MCP Token

Ad:

Süre:

İZİN VERİLEN ARAÇLAR — GRUBUN TAMAMINI VER YA DA "ARAÇLAR"DAN TEK TEK SEÇ

☐  **Tam Erişim — canlı tag değeri yazma HARIÇ her şey**
Tek tıkla: okuma + config/tag TANIMI + alarm + veri kaydı + üretim etiket + SCADA tasarımı/örizleme. **Canlı tag DEĞERİ yazma HARIÇ** (böyle bir araç yok). Her araç yine SENİN yetkinle sınırlı.

☒ **Etiketler (oku)** 3 araç  araçlar

☒ **Bağlantı (kanal / cihaz)** 4 araç  araçlar

☒ **Alarmlar** 3 araç  araçlar

Extensions > MCP (AI) — server status, tokens and connected clients

What the assistant can do

- **Read:** list channels/devices/tags, search tags, read live values and quality, device status and diagnostics, active and historical alarms, historian queries and charts, metrics and events, project overview.
- **Configure:** create/edit/delete channels, devices, tags, tag groups, virtual tags (with expression validation), aliases, alarms, log groups, Data Bridge agents; import/export projects.
- **SCADA:** create screens, add widgets from the real symbol library, draw pipes, set animations, render previews.
- **Documentation:** read the built-in manual (`list_docs` / `read_doc`).

What it can **never** do: write a live value to a device (no setpoint/command tool exists) — that stays with humans in the UI.

To talk to the assistant from INSIDE the application, see the [in-app AI assistant](#) (ChatGPT, Claude, OpenRouter, Ollama...) — same tools, same authorization.

Connecting

1. *Extensions* › *MCP (AI)* › enable the server. Endpoint: `https://<host>:<port>/mcp` (JSON-RPC over HTTP).
2. Authentication: **OAuth 2.0 with PKCE and dynamic client registration** (for assistants that support it) or a **bearer token** issued in the same page.
3. Two-tier authorisation: the token's scope × the user's permissions/ACL. A read-only token cannot configure even if the user could.
4. Every tool call is written to the audit log with the user and token name.

Claude Desktop / Claude Code example (`mcp.json`):

```
{ "mcpServers": { "mergenhub": { "url": "https://scada.example.com/mcp", "headers": {  
  "Authorization": "Bearer <token>" } } } }
```

Typical prompts

- "Which devices lost communication in the last hour?"
- "Create a Modbus TCP device at 10.0.0.9 with holding registers 40001–40020 as floats named Flow1...Flow10."
- "Add a high alarm on Plant.PLC1.Pressure above 6 bar with a 0.2 deadband and e-mail the operators group."
- "Plot Tank1.Level for the last 24 hours and tell me the minimum."
- "Build a screen with two tanks and a pump connected by pipes, animate flow when the pump runs."

Security notes

- Enable the MCP server only when needed; issue tokens per assistant and revoke them from the same page.
- Put the server behind HTTPS; the endpoint is rate-limited and audited.
- The assistant sees only what the token's user may see (resource ACL).