

MODÜLLER

Uygulama-içi yapay zekâ asistanı

Sağlayıcı seçimi (bulut ve yerel LLM), yetkiler ve izin akışı, ağ teşhisi, SCADA ekran tasarımı, ekler, beceriler, bağlam yönetimi.

Çevrimiçi: mergenhub.envest.com.tr/tr/docs/ai-asistan

BU SAYFADA

Sağlayıcı seçimi	Veri ve gizlilik
Davranış ayarları	Veri işleme onayı (KVKK / GDPR)
Asistan neler yapar	Fiyat, maliyet ve model bilgisi
Yetki ve izin akışı	Onay kipleri
Konuşmalar, bağlam ve beceriler	Betikler, ekran görme ve yetkiler

MergenHub'ın içinde, **oturumdaki kullanıcının yetkileriyle** çalışan bir yapay zekâ asistanı vardır. Üst çubuktaki ✨ düğmesi ya da Eklentiler > **Yapay Zekâ Asistanı** ile sağ tarafta bir panel (dock) olarak açılır; istenirse ayrı pencereye çıkarılır (masaüstü uygulamasında yerel ikinci pencere). Dışarıdan bağlanan asistanlar için ayrıca [MCP sunucusu](#) vardır — ikisi aynı araç kataloğunu ve aynı yetki denetimini kullanır.

Sağlayıcı seçimi

Yönetici (Ayarlar yetkisi) asistan panelindeki ⚙ > **Sağlayıcılar** sekmesinden bir ya da birden çok model sağlayıcısı tanımlar:

- Bulut:** OpenAI (ChatGPT), Anthropic (Claude), OpenRouter, Google Gemini, Mistral, DeepSeek, Groq, xAI, Together, Fireworks, Perplexity, Cerebras, Cohere, Azure OpenAI.
- Yerel (anahtarsız):** Ollama, LM Studio, vLLM, llama.cpp server (Unsloth GGUF), LocalAI, Jan, text-generation-webui, KoboldCpp, LiteLLM/OpenWebUI vekili. "**Yerel sunucuları tara**" ayakta olanları bulur, tek tıkla profil ekler.
- Özel:** herhangi bir OpenAI-uyumlu ya da Anthropic-uyumlu uç.

Her profilde Base URL, API anahtarı (yalnız sunucuda saklanır, maskeli döner), varsayılan model ("Modelleri getir" ile listeden), bağlam penceresi (bilinmiyorsa elle) ve etkin/varsayılan işareti vardır. Sohbet başlığındaki model çipinden profil ve model **aramalı listeden** seçilir; seçim konuşmaya kaydedilir.

İlk kurulumda sağlayıcı yoksa asistan paneli yöneticiye **3 adımlı sihirbaz** gösterir (sağlayıcı → anahtar → model, test). Asistan kapalıysa menü girişi soluk görünür; tıklayınca nereden açılacağı söylenir.

Davranış ayarları

- Asistan açık** — kapalıyken kimse sohbet edemez.

- **Asistan deęişiklik yapabilir** — kapalıyken yalnız okuma araçları; açıkken yapılandırma/alarm/log/SCADA yazma araçları **kullanıcının kendi yetkisi ölçüsünde** kullanılır ve her yazma denetim günlüğüne `kullanıcı (AI asistan)` olarak düşer. Cihaza **canlı deęer yazma aracı hiçbir durumda yoktur**.
- **Düşünme / muhakeme** (kapalı/düşük/orta/yüksek) — OpenAI o-serisi ve GPT-5, Claude (extended thinking), Gemini 2.5, OpenRouter, Groq, DeepSeek-R1 destekler; düşünce akışı katlanır blok olarak görünür.
- Sıcaklık, yanıt token üst sınırı, tur başına araç adımı, **yönetici talimatları** (tesise özel kurallar).

Asistan neler yapar

Bir SCADA/otomasyon uzmanı gibi çalışır: önce okur, sonra hedefli yazar, sonra doğrular.

- **Envanter ve teşhis**: kanal/cihaz/tag, canlı deęer ve kalite, cihaz durumu, alarmlar, historian, olaylar, denetim günlüğü, kullanıcılar ve yetkiler, ayarlar — yetkiniz dahilinde hepsi.
- **Ağ testleri**: `ping`, TCP port testi (Modbus 502, S7 102, OPC UA 4840...), DNS çözümleme, yerel dinlenen portlar. "Cihaz haberleşmiyor" sorusuna tahminle deęil ölçümle yanıt verir.
- **Yapılandırma**: kanal/cihaz/tag, virtual tag (ifade doğrulamalı), alias, alarm (ISA-18.2), log grubu, Data Bridge ajanı oluştur/düzenle/sil.
- **SCADA ekranı**: gerçek sembol kütüphanesi, boru hatları ve akış animasyonu, tank/pompa sahneleri, bağlamalar, önizleme. Yerleşik **"SCADA ekran tasarımı"** becerisi yerleşim ızgarası, ISA-101 renk dili, gezinme ve doğrulama kurallarını verir.
- **Sistem**: ayarları kısmi güncelleme (OPC UA portu, HTTPS...), HTTPS sertifikası (self-signed ya da sohbete eklenen PFX), Windows güvenlik duvarı portları, servis yeniden başlatma. Örnek: "alan adım X, 443'te HTTPS yayınla" → DNS → port boş mu → sertifika → ayar → güvenlik duvarı → restart → doğrulama.
- **Ekler**: görsel (PNG/JPG...), PDF, CSV/JSON/TXT, SVG ve PFX sohbete eklenir; görseller vision-destekli modele gider, `add_widget type=image` ile ekrana konabilir, CSV/JSON içerięi bağlam olur.

Yanıtlardaki `Kanal.Cihaz.Tag` referansları tıklanabilir — ana uygulamada o yere gider. Araç çağrıları argüman/sonuç/önizlemesiyle kart olarak görünür; "Düşünüyor / Ekran oluşturuyor / Portları test ediyor" durum satırı işin nerede olduğunu gösterir.

Yetki ve izin akışı

Güvenlik katmanları: (1) **"Yapay zekâ asistanını kullanma" yetkisi** — kullanıcı/grup bazında verilir, yoksa asistan kapalıdır; (2) her araç çağrısı kullanıcının **kendi yetkisiyle** sınırlıdır; (3) yönetici **yazma kapısı**; (4) **onay** — varsayılan olarak her deęişiklik sohbette Onay/Reddet ile bekler, asistan sormadan yapmaz; (5) **denetim günlüğü** — asistanın her araç çağrısı (okumalar dahil) ve sohbet mesajları loglanır; (6) canlı deęer yazma aracı yoktur.

Token ekonomisi: modele her turda tüm araçlar deęil, çekirdek gruplar + kompakt bir katalog gider; gereken gruplar konuşma sırasında yüklenir. Şablonlar: "bu cihaz tipini şablon yap" denince asistan beceri olarak kaydeder, sonra tek cümleyle o tipte kanal/cihaz/tag/alarm/ekran üretir.

Asistan token kullanmaz: **oturumdaki kullanıcı** kimdir, o yetkilerle çalışır. Bir araç yetki (ör. ConfigWrite) ya da yazma kapısı yüzünden reddedilirse asistan nedenini açıkça söyler ve sorar; yönetici kartta **"İzni aç ve yeniden dene"** ile kapıyı açabilir. Dolanma ya da uydurma yoktur.

Konuşmalar, bağlam ve beceriler

- Konuşmalar kullanıcıya özeldir; yeniden adlandırma, klasör, sabitleme, arşiv ve arama vardır.

- **Bağlam göstergesi** son turun token sayısını modelin penceresine oranlar; %75 dolunca eski turlar otomatik özetlenir (ekranda tam geçmiş kalır). Elle sıkıştırma göstergeye tıklayarak yapılır.
- **Beceriler** (`DataRoot/ai/skills/*.md`): tesise özel talimat paketleri. Yerleşik iki uzman beceri açık gelir (SCADA ekran tasarımı; alarm/veri kaydı/köprü/virtual tag mühendisliği); yönetici düzenler, kapatır, yenilerini ekler. Sistem istemine yalnız ad ve açıklama girer, içerik gerekince yüklenir.
- **Dış MCP sunucuları**: ERP, doküman deposu ya da başka bir MergenHub gibi sistemlerin araçları da asistana eklenebilir (Streamable HTTP + isteğe bağlı bearer token).

Veri ve gizlilik

Sohbetler, ekler ve beceriler MergenHub veri dizininde (`ai/`) tutulur; API anahtarları yalnız `settings.json` içinde saklanır ve arayüze maskeli döner. Sağlayıcıya yalnız o turda gereken metin/görsel gider; yerel sağlayıcı (Ollama, LM Studio...) seçilirse veri makineden çıkmaz.

Veri işleme onayı (KVKK / GDPR)

Bulut sağlayıcısı (OpenAI, Anthropic, OpenRouter, Google...) kullanılmadan önce yöneticinin **veri işleme onayı** vermesi gerekir; onay verilmeden bulut profiliyle sohbet açılmaz. Metin şunları kapsar: veri sorumlusunun siz olduğunuz ve sağlayıcının üçüncü taraf olduğu; aktarılan veriler (mesajlar, ekler, araç çıktıları: proje yapılandırması, tag değerleri, alarm/olay kayıtları, kullanıcı adları — anahtar ve parolalar maskelenir); yurt dışına aktarım (KVKK m.9) için hukuki dayanağın veri sorumlusunda olduğu; saklama; kullanıcıların aydınlatılması (KVKK m.10); güvenlik; onayın kim tarafından ve ne zaman verildiğinin kaydı ve geri alınabilirliği. Yerel sağlayıcılarda (Ollama, LM Studio, vLLM...) veri makineden çıkmaz; onay gerekmez.

Fiyat, maliyet ve model bilgisi

API anahtarı girildiği anda model listesi otomatik çekilir; her model için bağlam penceresi ve fiyat (1M token girdi/çıktı) gösterilir. Fiyatlar herkese açık OpenRouter kataloğundan alınır (24 saat önbellek), yerel modeller ücretsiz sayılır; bilinmeyen modelde dolar yerine yalnız token sayısı görünür. Her turun ve konuşmanın tahmini maliyeti sohbet altında ve konuşma listesinde görünür. Model, konuşma sırasında da değiştirilebilir; "Düşünme" çipiyle konuşma başına muhakeme düzeyi seçilir.

Onay kipleri

Değiştiren araçlar için üç kip: **Her değişiklikte sor** (varsayılan), **Konuşmada bir kez onaylanana hatırla**, **Sormadan uygula** (yalnız yönetici; kapalı ortamlar için). Onay kartında "bu konuşmada bir daha sorma" ve "her zaman izin ver" seçenekleri vardır; kalıcı izinler Ayarlar > Davranış'ta listelenir ve kaldırılabilir. Her kipte tüm araç çağrıları denetim günlüğüne yazılır.

Betikler, ekran görme ve yetkiler

Asistan, hesap/rapor/dönüştürme gibi işler için **kum havuzunda** Python veya PowerShell betiği çalıştırabilir. Bu özellik **kapalı gelir** ve yalnız **sistem yöneticisi (Root)** açar: Ayarlar > Yapay Zekâ > Davranış > *Betik çalıştırma*. Açmadan önce riskleri anlatan metin okunup onaylanır; onay, kim ve ne zaman verdiğiyle birlikte silinemez uyum defterine yazılır.

Betikler nasıl sınırlanır:

- Ayrı ve **düşük yetkili bir Windows hesabıyla** çalışır (MergenHubSandbox), MergenHub veri klasörünü okuyamaz.

- **Ağ varsayılan olarak kapalıdır.** Açarsanız izin listesi verirsiniz (IP, IP bloğu ya da alan adı); listede olmayan hiçbir adrese paket çıkamaz. Bu kısıt işletim sistemi güvenlik duvarında uygulanır.
- Betik **canlı tag yazamaz.** Sahaya yazma yalnız ayrı onay kartlarıyla yapılır.
- Zaman aşımı ve çıktı sınırı vardır; çalışma klasörü koşu sonunda silinir.
- **Her çalıştırmada kod size gösterilir ve onay istenir.** "Sormadan uygula" kipi ve "her zaman izin ver" listesi bu araca işlemez. Her koşu (kodun özeti, çıkış kodu, süre) denetim günlüğüne ve uyum defterine yazılır.
- **Acil durdurma** düğmesi çalışan tüm betikleri anında durdurur ve yeni betiği kilitler; kilidi yalnız sistem yöneticisi açar.

Asistan gerektiğinde **ekranınızı da görebilir**: "burası bozuk", "bu eğriyi yorumla" gibi durumlarda izin ister; onaylarsanız o anki ekranın görüntüsü yalnız o konuşmaya eklenir.

Yeni yetkiler (Ayarlar › Kullanıcılar › Yetkiler):

YETKİ	ANLAMI
Yapay zekâ asistanını kullanma	Asistanla sohbet
MCP köprüsü	Dış istemciyle (Claude Desktop, IDE) bağlanma — asistandan ayrıdır
Asistan betik çalıştırabilir	Tehlikeli; rol varsayılanıyla gelmez, yalnız Root tek tek verir
Asistan/MCP güvenlik yönetimi	Betik özelliği, onay kipi, kalıcı izinler, dış MCP sunucusu — yalnız Root

Asistan ayrıca **lisans ve paket durumunuzu** okuyabilir: kaç tag ekleyebilirsiniz, lisans süresiz mi abonelik mi, bakım (yeni sürüm hakkı) ne zaman bitiyor, daha yeni sürüm var mı ve yenileme nereden yapılır. "Kaç tag hakkım kaldı?" diye sorabilirsiniz.