

MODÜLLER

OPC UA sunucusu

Endpoint'ler, güvenlik ilkeleri, sertifikalar, adres uzayı, sistem tag'leri, geçmiş erişimi, UA üzerinden alarmlar.

Çevrimiçi: mergenhub.envest.com.tr/tr/docs/opc-ua-server

BU SAYFADA

Adres uzayı	Alarms & Conditions
Endpoint'ler	Metotlar
Güvenlik	Yaygın istemcileri bağlama
Oturum ve abonelik sınırları	Sorun giderme
Geçmiş erişimi	

MergenHub her kanal, cihaz ve tag'i tek adres uzayında sunan bir **OPC UA sunucusudur** (Data Access, Historical Access, Alarms & Conditions, Methods). Herhangi bir UA istemcisi — SCADA, MES, historian, PLC, başka bir MergenHub — bağlanır.

```
opc.tcp://<host>:48010/MergenHub
```

OPC UA Gateway - v3.119

PROJE

+

Bağlantılar

Simulation Examples

24

Functions

24

Ekentiler

Virtual Tag'ler

Tag Kısayolları

Alarmlar

Veri Logları

Data Bridge

MCP (AI)

admin

Root (super-admin)

TR TR

OPC UA SUNUCU

OPC UA Sunucu

OPC UA Kullanıcıları

Güvenilen Client'lar

Sunucu Sertifikası

WEB & BAĞLANTI

Web & REST API

Data Bridge

BİLDİRİMLER

E-posta

SMS

İletişim Merkezi

GÖRÜNÜM

Marka

SİSTEM

Lisans

Denetim

Saklama

Servisler

ERİŞİM

Kullanıcılar

OPC UA Sunucusunun dinlediği adres/port ve güvenlik politikaları. SCADA/İstemciler (UaExpert vb.) buraya bağlanır. [Detaylı yardım](#)

OPC UA Sunucu

Yardım

☒ Açık

Endpoint yolu

MergenHub

Tüm endpoint'ler bu yolu (path) paylaşır. Ağ adaptörü, port ve güvenlik her endpoint için ayrı ayarlanır.

SUNUCU ENDPOINT'LERİ

+ Endpoint Ekle

Sunucu birden fazla adres/portta aynı anda dinleyebilir (ör. localhost'ta güvensiz + LAN'da yalnız güvenli). Her satır bir dinleme endpoint'idir. Güvenlik policy'leri (Basic256Sha256 vb.) her endpoint satırının kalem düğmesindedir.

✓ Şu an etkin (canlı sunucu)

opc.tcp://localhost:48020/MergenHub

Basic256Sha256 · Sign

Basic256Sha256 · Sign & Encrypt

None

Yenile

Endpoint	Güvenlik
opc.tcp://localhost:48020/MergenHub	devralınan Basic256Sha256 (SE) None

☒ Güvenilmeyen sertifikaları otomatik kabul

OPC UA PROJE ÖZELLİKLERİ

☐ Log diagnostics (stack tanılama — yalnız sorun giderme)

☒ Alarmları OPC UA'dan yayınla (A&E — _Alarms koşulları)

Alarm motoru OPC UA'da AlarmConditionType olarak sunulur; istemci Server düğümüne olay aboneliği açar, ConditionRefresh ve Acknowledge kullanır. Kaynak tag yetkisine TABİDİR: tag'ı okuyamayan kullanıcı alarmı görmez, onay için okuma-yazma gerekir. Kapalıyken _Alarms düğümleri hiç kurulmaz.

Ayarlar > OPC UA Sunucu – endpoint'ler, güvenlik ilkeleri, sertifikalar ve proje özellikleri

Adres uzayı

```
Objects
├── <Kanal>
│   └── <Cihaz>
│       ├── <Tag> (Variable: değer, kalite, kaynak/sunucu zaman damgası, EngineeringUnits, Description)
│       ├── <TagGrubu>/...
│       └── _System (_Error, _NoError, _LastRead, _SuccessfulReads, _Enabled ...)
├── _Aliases
├── _AdvancedTags
├── _Alarms ("alarmları OPC UA'dan yayınla" açıkken)
└── _System (sunucu geneli istatistikler)
```

Node id'ler dizge tabanlıdır (`ns=2;s=Kanal.Cihaz.Tag`); yeniden başlatma ve dışa aktarmalarda sabit kalır.

Endpoint'ler

Sunucu aynı anda birden çok endpoint'te dinleyebilir (*Ayarlar > OPC UA Sunucu > Endpoint'ler*): örneğin yerel istemci için güvensiz `localhost` ve LAN/genel host için `Basic256Sha256 – Sign & Encrypt`. Her endpoint'in kendi host, port ve izinli güvenlik ilkeleri vardır. Değişiklik runtime yeniden başlatılınca geçerli olur.

Güvenlik

AYAR	ÖNERİ
Güvenlik ilkeleri	None yalnız localhost'ta; başka her yerde Basic256Sha256 Sign & Encrypt
Anonim erişim	üretimde kapalı

MergenHub · OPC UA sunucusu · mergenhub.envest.com.tr/tr/docs/opc-ua-server

2 / 4

AYAR	ÖNERİ
Kullanıcı doğrulama	<i>Ayarlar › OPC UA Kullanıcıları:</i> rollü kullanıcı/parola hesapları; sertifika desteklenir
Güvenilmeyen sertifikaları otomatik kabul	üretimde kapalı; istemcileri <i>Ayarlar › Güvenilen istemciler</i> 'de güvenilir yapın
Sunucu sertifikası	kurulumda üretilir; host adı değişince yeniden üretin (<i>Ayarlar › Sunucu sertifikası</i>)

Kullanıcı bazlı **kaynak ACL** OPC UA'da da geçerlidir: arayüzde bir kanalı göremeyen kullanıcı adres uzayında da görmez; yazma için yazma izni gerekir. Bkz. [Kullanıcılar ve güvenlik](#).

Oturum ve abonelik sınırları

Varsayılanlar: 128 oturum, oturum zaman aşımı 20 dk, 450K izlenen öge kanıtlanmış. Yayın aralığı 100 ms'ye kadar; sunucu istemcinin istediği örnekleme hızına uyar (tarama modu *istemci hızına saygı*) — aboneler taramayı sürükleyebilir.

Geçmiş erişimi

Bir historian log grubuna ait tag'ler **HistoryRead** isteklerini (ham ve işlenmiş toplamalar) doğrudan historian veritabanından yanıtlar; UA istemcileri ayrı historian olmadan trend çizebilir. Bkz. [Historian](#).

Alarms & Conditions

Alarmları OPC UA'dan yayınla açıkken her alarm tanımı `_Alarms` altında bir `AlarmConditionType` olur; istemciler Server nesnesine olay aboneliği açar, `ConditionRefresh` ve `Acknowledge` kullanır. Durum eşlemesi ISA-18.2'yi izler (aktif/onaylı/silinmiş). Bkz. [Alarmlar](#).

Metotlar

Runtime kontrolü için (kanal yeniden başlat, okumaya zorla) sunucu tarafı metotlar yalnız yetkili kullanıcılara açıktır.

Yaygın istemcileri bağlama

- UaExpert** — Add server › endpoint URL'sini girin › güvenlik seçin › sunucu sertifikasına güvenin; *otomatik kabul* kapalıysa UaExpert sertifikasını *Ayarlar › Güvenilen istemciler*'de güvenilir yapın.
- Kepware / Ignition / Siemens WinCC** — aynı endpoint; imzalı oturumlar için MergenHub sertifikasını (`pki\own`) istemcinin güven deposuna alın.
- Başka bir MergenHub** — bu sunucuyu kanal olarak *OPC UA istemci* sürücüsüyle kullanın.

Sorun giderme

BELİRTİ	ÇÖZÜM
<code>BadCertificateHostNameInvalid</code>	İstemci sertifikada olmayan bir adla bağlanıyor — o host'la endpoint ekleyip sunucu sertifikasını yeniden üretin
<code>BadSecurityChecksFailed</code> / <code>BadCertificateUntrusted</code>	İstemci sertifikasına güvenin (<i>Ayarlar › Güvenilen istemciler</i>) ya da geçici otomatik kabul açın
<code>BadIdentityTokenRejected</code>	Anonim kapalı ve kullanıcı/parola yanlış
İstemci Bad kalite görüyor	Cihaz çevrimdışı ya da deneme penceresi dolmuş — <i>Bağlantılar</i> ve Olay günlüğü
Arayüzde sunucu "çalışmıyor"	Portu başka bir OPC sunucusu kullanıyor; <i>Endpoint'ler</i> 'den portu değiştirin

