

BAŞLANGIÇ

Domainde yayınlama

DNS, port yönlendirme, HTTPS sertifikası, reverse proxy (IIS / nginx / Caddy), uzaktan OPC UA.

Çevrimiçi: mergenhub.envest.com.tr/tr/docs/publish-domain

BU SAYFADA

Sunucuya nasıl ulaşılacağına karar verin

1. DNS

2. Portlar ve yönlendirme

3. HTTPS

4. Reverse proxy (isteğe bağlı ama önerilir)

5. İnternette OPC UA

6. Canlıya geçmeden kontrol listesi

MergenHub Windows servisi olarak çalışır; makinede kimse oturum açmasa da çalışmaya devam eder. Bir domain altında yayınlamak üç şey demektir: makineye işaret eden bir DNS kaydı, yönlendirici ve güvenlik duvarlarından geçen doğru portlar ve parolaların açık gitmemesi için HTTPS. Bu sayfa üçünü ve reverse proxy seçeneklerini anlatır.

Sunucuya nasıl ulaşılacağına karar verin

SENARYO	YAPILACAK
Yalnız bu bilgisayar	Kurucu varsayılanlarını koruyun (localhost).
Ofis / tesis ağı (LAN)	Host'u 0.0.0.0 yapın (tüm arayüzler); istemciler makinenin IP'sini ya da adını kullanır; kurucunun eklediği güvenlik duvarı kuralları yeter.
İnternet, kendi genel IP'niz	DNS A kaydı → genel IP; yönlendiricide port yönlendirme; HTTPS açın; kullanıcıları ve OPC UA'yı sertleştirin.
İnternet, reverse proxy arkasında	DNS → proxy; proxy HTTPS'i sonlandırıp 127.0.0.1:8090 'a iletir; OPC UA portu ayrıca yönlendirilir (TCP, HTTP değil).
Yalnız VPN	Dışarıdan OPC UA ve yazma erişimi için önerilir; port yönlendirme gerekmez.

Uyarı Web arayüzünü internete asla düz HTTP ile açmayın. HTTPS'i (aşağıda) açın ve güçlü parolalar kullanın; kurucu zayıf admin parolasıyla sunucuyu yerel dışı bir host'a bağlamayı reddeder.

1. DNS

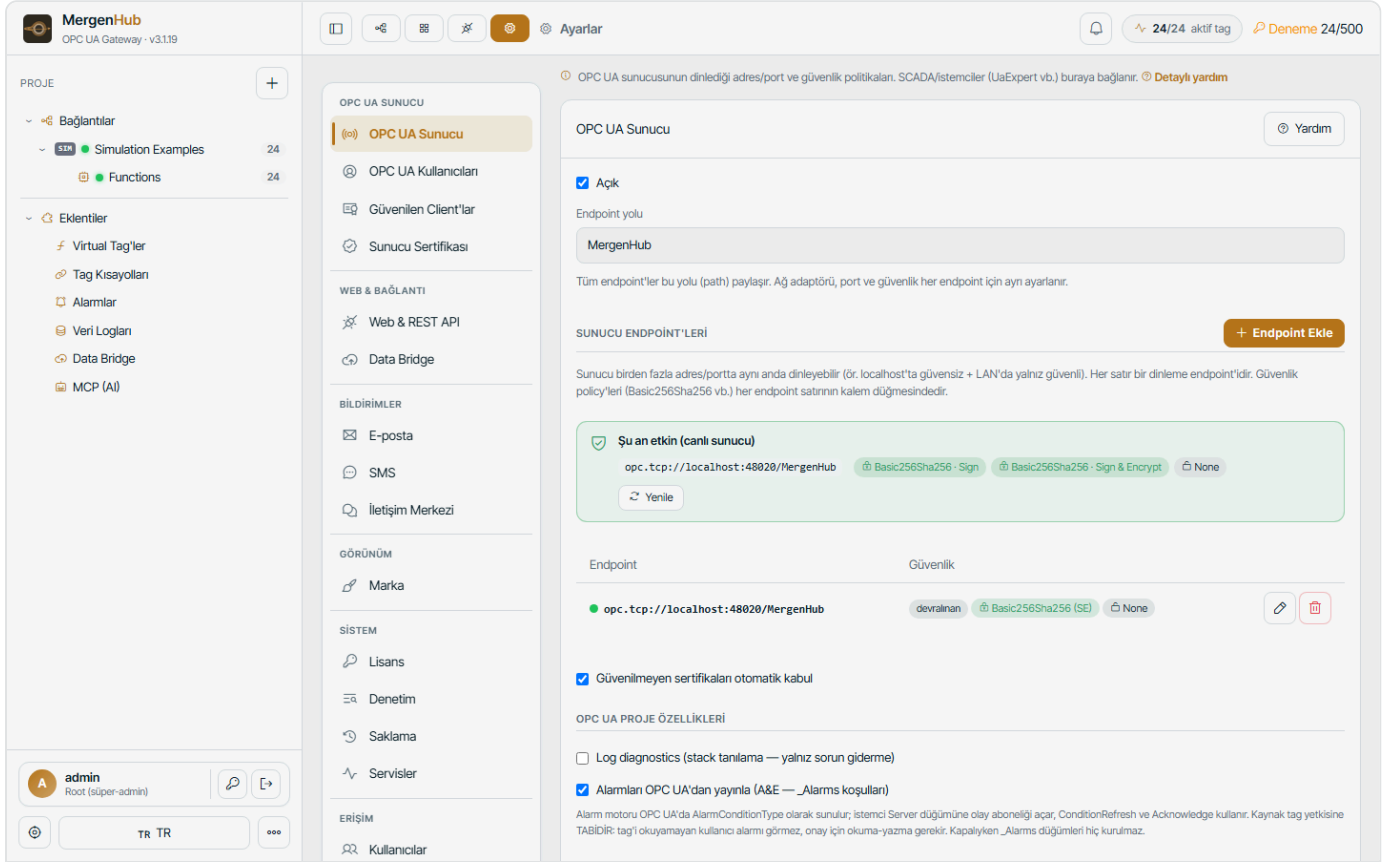
İstediğiniz ad için (ör. `scada.example.com`) internet bağlantınızın genel IP'sine (ya da reverse proxy / bulut sunucunuza) işaret eden bir **A kaydı** oluşturun. ISS adresiniz değişiyorsa dinamik DNS servisi kullanın.

Kurucunun **Domain ve DNS kontrolü** sayfası domaini girdiğinizde adın bu makinenin genel adresine çözülüp çözülmediğini söyler.

2. Portlar ve yönlendirme

TRAFİK	PORT (VARSAYILAN)	PROTOKOL	GEREKLİ OLDUĞU YER
Web arayüzü + REST API	8090, HTTPS'te 443	TCP	Tarayıcılar, REST istemcileri, Data Bridge REST sunucusu
OPC UA	48010	TCP	OPC UA istemcileri (SCADA, MES, historian)

Yönlendiricide dış portu MergenHub makinesinin LAN IP'sine yönlendirin. Makinenin kendisinde kurucu Windows Güvenlik Duvarı kurallarını zaten oluşturdu; bkz. [Windows Güvenlik Duvarı ve portlar](#). Portları *Ayarlar > Web & REST API* ve *Ayarlar > OPC UA Sunucu* dan değiştirebilirsiniz.



Ayarlar > OPC UA Sunucu — endpoint'ler, güvenlik ilkeleri ve sunucunun dinlediği port

3. HTTPS

Üç seçenek var.

A) SELF-SIGNED SERTİFİKA (EN HIZLI)

Kurucuda *HTTPS – self-signed* seçin ya da sonradan yönetici olarak çalıştırın:

```
"C:\Program Files\MergenHub\MergenHub.exe" gencert "scada.example.com"
```

C:\ProgramData\MergenHub\webpki\web.pfx yazılır. Sertifika genel bir otorite tarafından imzalı olmadığından tarayıcılar bir kez uyarır; iç kullanım için yeterlidir.

B) KENDİ SERTİFİKANIZ (PFX)

PFX'i `C:\ProgramData\MergenHub\webpki\web.pfx` olarak, parolasını `web.pfx.pass` (düz metin) olarak kopyalayın ya da kurucuda dosyayı seçin. `MergenHub` servisini yeniden başlatın.

C) LET'S ENCRYPT İLE ÜCRETSİZ GENEL SERTİFİKA

- **win-acme** MergenHub makinesinde: `wacs.exe --target manual --host scada.example.com --store pfxfile --pfxfilepath C:\ProgramData\MergenHub\webpki --pfxfilename web.pfx --pfxpassword <pw>` + yenileme görevi; parolayı `web.pfx.pass` dosyasına yazın. Doğrulama sırasında 80 portu erişilebilir olmalı (ya da DNS doğrulaması).
- **Caddy** reverse proxy sertifikayı kendisi alır ve yeniler — aşağıda. Üretim için en basit yol budur.

HTTPS'i ve portu *Ayarlar > Web & REST API*'de (ya da kurucuda) açın. Eski yer imleri çalışsın diye HTTP yönlendirmesini açık tutun.

4. Reverse proxy (isteğe bağlı ama önerilir)

Aynı makinede ya da bir geçit sunucusunda reverse proxy TLS'i sonlandırır, iç portu gizler ve tek IP arkasında birden çok uygulama barındırmanızı sağlar.

CADDY (OTOMATİK HTTPS)

```
scada.example.com {  
    reverse_proxy 127.0.0.1:8090  
}
```

Caddy sertifikayı kendisi alır ve yeniler. MergenHub arkada HTTP `127.0.0.1:8090` olarak kalır.

NGINX

```
server {  
    listen 443 ssl http2;  
    server_name scada.example.com;  
    ssl_certificate /etc/ssl/scada.crt;  
    ssl_certificate_key /etc/ssl/scada.key;  
    client_max_body_size 64m;  
    location / {  
        proxy_pass http://10.0.0.20:8090;  
        proxy_http_version 1.1;  
        proxy_set_header Host $host;  
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;  
        proxy_set_header X-Forwarded-Proto https;  
        proxy_read_timeout 300s;  
    }  
}  
  
server { listen 80; server_name scada.example.com; return 301 https://$host$request_uri; }
```

IIS (URL REWRITE + APPLICATION REQUEST ROUTING)

1. *URL Rewrite* ve *ARR* kurun, *Server Proxy Settings > Enable proxy* açın.
2. `scada.example.com:443` bağlı, sertifikalı bir site oluşturun.

3. Gelen kural ekleyin: `(.) eşleşmesi, eylem *Rewrite → http://127.0.0.1:8090/{R:1}` , *Append query string* işaretli.
4. Büyük SVG sembol kütüphaneleri yüklüyorsanız *Request Filtering*'de izin verilen içerik uzunluğunu artırın.

Not OPC UA ikili bir TCP protokolüdür, HTTP değildir — HTTP reverse proxy'den geçmez. 48010 portunu doğrudan yönlendirin (ya da VPN kullanın).

5. İnternette OPC UA

- *Ayarlar* > *OPC UA Sunucu*'da host'u genel DNS adı olan bir **endpoint** ekleyin (`opc.tcp://scada.example.com:48010/MergenHub`). İstemciler sunucu sertifikasını bağlandıkları ada göre doğrular.
- Güvenlik ilkesi **Basic256Sha256 – Sign & Encrypt** kullanın, *Anonim*'i kapatın; yalnız gereken haklara sahip bir OPC UA kullanıcısı oluşturun.
- *Güvenilmeyen sertifikaları otomatik kabul*'ü kapatın; istemcileri *Ayarlar* > *Güvenilen istemciler*'de açıkça güvenilir yapın.
- Host adını değiştirdikten sonra sunucu sertifikasını yeniden üretin (*Ayarlar* > *Sunucu sertifikası*).

6. Canlıya geçmeden kontrol listesi

- [] Güçlü admin parolası; sınırlı rollü operatör hesapları ([Kullanıcılar ve güvenlik](#))
- [] HTTPS açık; HTTP yönlendiriliyor
- [] Yalnız 443 ve (gerekiyorsa) 48010 yönlendirilmiş; diğerleri kapalı
- [] OPC UA anonim erişim kapalı, güvenilen istemci listesi bakımlı
- [] Oturum politikası ve denetim saklama süresi gözden geçirilmiş ([Loglar](#))
- [] `C:\ProgramData\MergenHub` yedeği zamanlanmış ([Yedekleme](#))
- [] Lisans etkinleştirilmiş; deneme penceresi taramayı durdurmasın ([Lisanslama](#))