

BAŞLANGIÇ

Windows Güvenlik Duvarı ve portlar

MergenHub hangi portları kullanır, kurucu hangi kuralları ekler, nasıl açılır ya da kısıtlanır.

Çevrimiçi: mergenhub.envest.com.tr/tr/docs/firewall

BU SAYFADA

MergenHub'ın kullandığı portlar	Üçüncü parti güvenlik duvarı ve antivirüs
Kurucunun oluşturduğu kurallar	Doğrulama
Portları elle açma ya da değiştirme	Sorun giderme
Kimin bağlanabileceğini kısıtlama	

MergenHub varsayılan olarak iki TCP portunda dinler ve kurucu bunları Windows Güvenlik Duvarı'nda açar. Bu sayfa tüm portları, kurucunun oluşturduğu kuralları ve elle nasıl açılıp kısıtlanacağını listeler.

MergenHub'ın kullandığı portlar

PORT	YÖN	AMAÇ	NEREDEN DEĞİŞİR
8090 TCP	gelen	Web arayüzü, REST API, Data Bridge REST sunucusu, MCP ucu	Kurucu › <i>Sunucu adresi ve portlar</i> ; Ayarlar › <i>Web & REST API</i>
443 TCP	gelen	Aynı servisler için HTTPS (yalnız HTTPS açıkken)	Kurucu › <i>HTTPS</i> ; Ayarlar › <i>Web & REST API</i>
48010 TCP	gelen	OPC UA sunucusu (<code>opc.tcp://host:48010/MergenHub</code>)	Ayarlar › <i>OPC UA Sunucu</i> › <i>Endpoint'ler</i>
cihaz portları	giden	Modbus 502, S7 102, OMRON 9600 (FINS) / 44818 (CIP), DNP3 20000, IEC 104 2404, IEC 61850 102, MQTT 1883/8883, uzak sunuculara OPC UA istemci	kanal/cihaz başına
25 / 465 / 587	giden	E-posta bildirimleri için SMTP	Ayarlar › <i>E-posta</i>
443	giden	SMS sağlayıcı API'si, lisans portalı (etkinleştirme, tazeleme, güncelleme denetimi)	—

Giden bağlantılara Windows Güvenlik Duvarı normalde izin verir; yalnız gelen portlar için kural gerekir.

Kurucunun oluşturduğu kurallar

Kurucu `netsh advfirewall` ile şu gelen *allow* kurallarını ekler (tüm profiller, TCP):

KURAL ADI	PORT
MergenHub Web	seçtiğiniz web portu (8090)
MergenHub OPC UA	OPC UA portu (48010)
MergenHub HTTPS	HTTPS portu (yalnız HTTPS açıksa)

Kaldırıcı bunları siler. *Windows Defender Güvenlik Duvarı (Gelişmiş Güvenlik) > Gelen Kuralları* altında görürsünüz.

Portları elle açma ya da değiştirme

Yönetici komut isteminde:

```
netsh advfirewall firewall add rule name="MergenHub Web" dir=in action=allow protocol=TCP localport=8090
netsh advfirewall firewall add rule name="MergenHub OPC UA" dir=in action=allow protocol=TCP localport=48010
netsh advfirewall firewall add rule name="MergenHub HTTPS" dir=in action=allow protocol=TCP localport=443
```

PowerShell karşılığı:

```
New-NetFirewallRule -DisplayName "MergenHub Web" -Direction Inbound -Protocol TCP -LocalPort 8090 -Action Allow
```

Ayarlar'da portu değiştirdiyseniz yeni port için kural ekleyip eskisini silin:

```
netsh advfirewall firewall delete rule name="MergenHub Web"
```

Kimin bağlanabileceğini kısıtlama

Kuralı tüm dünya yerine belirli ağlarla sınırlandırın:

```
netsh advfirewall firewall set rule name="MergenHub OPC UA" new remoteip=10.0.0.0/24,192.168.10.0/24
netsh advfirewall firewall set rule name="MergenHub Web" new profile=domain,private
```

İnternete bakan sunucularda 443'te reverse proxy tercih edin ve 8090'ı `127.0.0.1` 'e bağlı tutun (*Ayarlar > Web & REST API*'de host'u `127.0.0.1` yapın). Bkz. [Domainde yayınlama](#).

Üçüncü parti güvenlik duvarı ve antivirüs

- Uç nokta güvenlik paketlerinin (Kaspersky, ESET, Sophos ...) kendi güvenlik duvarı vardır; aynı TCP portlarını orada da ekleyin.
- Bazı ürünler imzasız kurucuyu işaretler. Dosyaya sağ tık > *Özellikler > Engellemeyi kaldır* ya da `C:\Program Files\MergenHub` için istisna ekleyin.
- AppLocker / WDAC'li kurumsal bilgisayarlarda kurucu tamamen engellenebilir; yöneticiden yayıncıya ya da yola izin vermesini isteyin.

Doğrulama

- Başka bir makineden: `Test-NetConnection <host> -Port 8090` (PowerShell) — `TcpTestSucceeded: True` port açık demektir.
- Sunucuda: `netstat -ano | findstr :8090` dinleyen soketi ve `MergenHub` servisinin süreç kimliğini gösterir.
- Olay günlüğü* (... > Olay Günlüğü) servisler ayaktaiken `Web API listening on ...` ve `OPC UA server started` satırlarını gösterir.

Sorun giderme

BELİRTİ	OLASI NEDEN
Web arayüzü sunucuda çalışıyor, başka PC'lerden açılmıyor	Host <code>localhost</code> — <i>Ayarlar</i> > <i>Web & REST API</i> de <code>0.0.0.0</code> yapıp servisi yeniden başlatın; ya da güvenlik duvarı kuralı eksik
OPC UA istemcisi endpoint'i görüyor ama bağlanamıyor	Endpoint host adı istemcinin kullandığından farklı; sertifika güvenilirmiyor; güvenlik ilkesi uyuşmuyor
Tarayıcı HTTPS'te "bağlantı sıfırlandı" diyor	HTTPS açık ama <code>webpki\</code> altında geçerli <code>web.pfx</code> yok; olay günlüğüne bakın
Port zaten kullanımda	Başka bir program (çoğu kez başka bir OPC sunucusu) 48010 ya da 8090'ı kullanıyor; <i>Ayarlar</i> 'dan portu değiştirin