KULLANICI KILAVUZU (UYGULAMA İÇİ, TAM)

MergenHub VPN (saha modemleri)

Çevrimiçi: mergenhub.envest.com.tr/tr/docs/kilavuz-vpn

BU SAYFADA

Ne işe yarar, nasıl kurulur
Saha modemi ekleme (sihirbaz)
İzleme: tag'ler, alarmlar, denetim kaydı
Sorun giderme

Ne işe yarar, nasıl kurulur

3.13 · FAZ 1

MergenHub VPN, MergenHub servisinin içinde çalışan, **WireGuard uyumlu** bir VPN sunucusudur. Saha modemleri (Teltonika, MikroTik, OpenWrt…) **tek bir UDP portu** üzerinden, her biri kendi anahtar çiftiyle hub'a bağlanır; modemin arkasındaki PLC'ler MergenHub sürücüleriyle tünel adresinden okunur. Ayrı bir VPN programı, ek Windows servisi ya da sahada açık port gerekmez: modem dışarıya doğru bağlanır.

Sayfa: sol menüde **Eklentiler › VPN**. Üç sekme vardır: **Genel Bakış** (durum, bağlı saha sayısı, trafik, dış adres, hub açık anahtarı), **Saha Cihazları** (tablo + **Saha ekle** sihirbazı) ve **Ayarlar** (dış adres, UDP portu, MTU, tünel adresi). Sayfayı görmek **Sunucu ayarları** yetkisi, değiştirmek ayrıca **VPN yönetimi** (`vpn.admin`) işlemini ister.

İLK KURULUM: ADIM ADIM

1. **Port yönlendirme.** Kurum güvenlik duvarında / modeminde **UDP 51820**'yi (ya da ayarlarda seçtiğiniz portu) MergenHub sunucusuna yönlendirin. İnternete açık tek port budur; web arayüzü ve OPC UA dışarı açılmaz. Windows Güvenlik Duvarı kuralını elle açmanız gerekmez (3. adım).
2. **Dış adres. Ayarlar** sekmesinde **Dış adres** kutusuna sunucunun genel **IPv4** adresini ya da **DNS adını**, isteğe bağlı portuyla yazın (ör. `vpn.musteri.gov.tr` , `vpn.musteri.gov.tr:51820` ya da `203.0.113.10`). Başka bir şey (boşluk, komut, yol) kabul edilmez. DNS Cloudflare'daysa kayıt **DNS only** (gri bulut) olmalıdır: Cloudflare vekili UDP taşımaz. **Kaydet**.
3. **Aç. Genel Bakış**'ta **VPN açık** anahtarını açın. İlk açılışta hub anahtar çifti üretilir, **MergenHub VPN** adlı ağ bağdaştırıcısı oluşturulur (kurulum paketiyle gelen WireGuardNT motoru Windows imzalı sürücüsünü kurar), `10.66.0.1/16` adresi atanır ve durum **Çalışıyor** olur. MergenHub aynı anda Windows Güvenlik Duvarı'na **"MergenHub VPN"** adlı gelen UDP kuralını (ayarlardaki port) kendisi ekler; port değişince kuralı günceller, VPN kapatılınca kaldırır.
4. **Saha ekle. Saha Cihazları** › **Saha ekle** ile ilk modemi tanımlayın (bkz. Saha modemi ekleme).

Durum: Kapalı	VPN bilerek kapatılmış.

Durum: Kullanılamıyor	Tünel motoru çalıştırılamıyor: motor dosyası (`wireguard.dll` ; kurulum paketi `C:\Program Files\MergenHub\` altına koyar) silinmiş ya da bozulmuş, işletim sistemi uygun değil ya da geliştirme sunucusunda yerel katman kapalı. Servis çalışmayı sürdürür; "VPN servisi kapalı" alarmı oluşur.
Durum: Hata	Bağdaştırıcı kurulamadı ya da yapılandırma uygulanamadı; ayrıntı satırda ve denetim kaydında (`vpn.apply.fail` , Win32 hata kodu). Servis dakikada bir yeniden dener.

Anahtarlar Hub'ın ve modemlerin özel anahtarları ile ön paylaşımlı anahtarlar (PSK) diskte **kayıtlı parolalar** kasasıyla şifrelenir (`keys\` klasörü); API yanıtında maskelenir, denetim kaydına yazılmaz. Anahtar yedekle taşınır: yedek başka sunucuda açılınca VPN anahtarları da açılır, dış adres DNS olarak verildiyse modemlere dokunmak gerekmez.

Kaldırma MergenHub kaldırılınca (Programlar ve Özellikler) "MergenHub VPN" güvenlik duvarı kuralı ve WireGuard sürücüsü de temizlenir.

Saha modemi ekleme (sihirbaz)

Saha Cihazları › **Saha ekle** dört adımlı bir sihirbaz açar. Önce **Ayarlar**'da dış adres girilmiş olmalıdır.

1. **Saha:** saha adı (ör. *Serbest Bölge Kuyu 1192*; benzersiz, en çok 64 karakter), modem modeli: **Teltonika RUT / RUTX / TRB**, **MikroTik RouterOS 7**, **OpenWrt** ya da **Diğer**; isteğe bağlı **Bu modemi kullanan cihazlar**. GSM sahada çoğunlukla her cihazın kendi modemi olur: o cihazı seçin, hangi `.conf` 'un hangi cihaza ait olduğu tabloda (**Cihazlar** sütunu) ve cihazın ••• › **VPN modemi** menüsünde görünür. Bir cihaz yalnız bir modeme bağlanabilir; bir modemin arkasında birkaç cihaz olabilir.
2. **LAN:** erişim modu. **Yönlendirmeli**: sahanın LAN'ı benzersizse (ör. `192.168.21.0/24`); cihazlar gerçek IP'leriyle okunur, hub bu aralığı tünele yönlendirir. **Sadece modem**: PLC modemin port yönlendirmesiyle açıksa; sürücüde cihaz adresi modemin tünel IP'sidir (ör. `10.66.0.11:502`). **Denetle** düğmesi aralığı tünel ağıyla (`10.66.0.0/16`), eşleme bloğuyla (`10.100.0.0/16`), öteki sahaların LAN'larıyla ve sunucunun kendi ağlarıyla karşılaştırır. Çakışma varsa sihirbaz ilerlemez. **Eşlemeli (1:1 NAT)** mod Faz 3'te gelecektir.
3. **Özet: Oluştur** modem anahtar çiftini ve PSK'yı üretir, saha bloğundaki (`10.66.0.0/22`) sıradaki boş adresi verir (ilk adres `10.66.0.10`), peer'ı servis yeniden başlatılmadan canlı ekler ve yönlendirmeyi yazar. Bağdaştırıcıya uygulanamazsa kayıt yazılmaz.
4. **Kurulum:** tek kullanımlık bağlantılar: **WireGuard .conf**, **QR kodu** ve MikroTik / OpenWrt için **komut dosyası**; altında modele özel adım adım kurulum. Pencere modemin bağlanmasını bekler; ilk el sıkışmada **Modem bağlandı** yazar.

Tek kullanımlık bağlantı Her bağlantı **bir kez** ve **24 saat** çalışır; giriş gerektirmez (sahadaki teknisyene gönderilebilir). Yapılandırma modemin özel anahtarını taşıdığı için **yerel ağ dışından yalnız HTTPS ile** indirilir: bağlantı internetten `http://` ile açılırsa reddedilir (bağlantı harcanmaz); Ayarlar'da HTTPS'i açıp `https://` ile açın. Kullanılmış ya da süresi dolmuş bağlantı "bağlantı daha önce kullanıldı / süresi doldu" der ve denetim kaydına `vpn.config.link_reuse` olarak yazılır. Yenisi için satırın ••• menüsünde **Yeni indirme bağlantısı**. QR kodu da bağlantıyı harcar: yalnız **QR kodunu göster**'e basınca yüklenir.

SATIR MENÜSÜ (•••)

Ayrıntı ve kurulum adımları	Tünel IP, hub'daki izinli adresler, son el sıkışma, dış uç nokta, hız, açık anahtar, tag yolu ve kurulum adımları.
Bu modemi kullanan cihazlar	Modeme bağlı proje cihazlarını ekler / çıkarır. Başka bir modeme bağlı cihaz listede görünmez.
Cihaz adreslerini tünel IP'sine çevir	Yalnız "Sadece modem" sahasında. Modeme bağlı cihazların adresini (Modbus `<IP>.birim`, S7, FINS…: cihaz kimliğinde; BACnet: cihaz IP alanında; DNP3, IEC 104: kanalda) modemin tünel IP'sine çevirir. Önce eski → yeni listesi gösterilir, **Uygula** ile kaydedilir (cihaz / kanal düzenleme yetkisi gerekir). Modeme cihaz bağlanınca da kendiliğinden önerilir.
Bu sahaya yeni cihaz ekle	Bağlantılar'da kanal sihirbazını açar ve cihaz adresine ne yazılacağını söyler.
Devre dışı bırak / Etkinleştir	Peer hub'dan geçici çıkarılır / geri konur. Gerekçe zorunludur (denetim kaydına yazılır).
İptal et (sil)	Peer hemen çıkar, o anahtarla gelen paketler sessizce düşer. Geri alınamaz; yeniden eklemek yeni anahtar üretir.

CİHAZDAN: VPN MODEMİ

Bağlantılar'da cihazın ••• menüsü › **VPN modemi**: cihaz bir modeme bağlıysa modemin adı, durumu, tünel IP'si, cihaz adresine ne yazılacağı ve son el sıkışma görünür (**Bu cihazı modemden çıkar** ve **VPN sayfasında aç**). Bağlı değilse **Bu cihaz için modem ekle** sihirbazı adı ve cihazı hazır doldurulmuş açar; ya da **Var olan modeme bağla** ile bir modem seçilir.

Durum renkleri: **Bağlı** (son el sıkışma < 3 dk), **Gecikmeli** (3–10 dk), **Koptu** (> 10 dk), **Bekliyor** (hiç bağlanmadı).

İzleme: tag'ler, alarmlar, denetim kaydı

VPN durumu 5 saniyede bir okunur ve **_System.VPN** altında tag olarak yayınlanır: SCADA ekranları, veri kaydı, alarmlar ve OPC UA istemcileri ek kod olmadan kullanır.

`_System.VPN.Enabled`	1 = bağdaştırıcı açık (UP).
`_System.VPN.ConnectedPeers`	Son 3 dakikada el sıkışan peer sayısı.
`_System.VPN.Peers.<ad>.Online`	1 = son el sıkışma < 180 sn.
`….LastHandshake`	Son el sıkışma (metin; sayı değeri Unix saniye).
`….Endpoint`	Modemin dış IP:port'u (operatör / hat değişimi takibi).
`….RxBytes`, `….TxBytes`	Toplam trafik (bayt).
`….RxRate`, `….TxRate`	Anlık hız (kbit/s; hücresel kota takibi).

Saha adındaki nokta tag yolunda alt çizgiye döner (*Kuyu.7* → `Kuyu_7`).

ALARMLAR (KENDİLİĞİNDEN TANIMLANIR)

VPN servisi kapalı (kritik)	VPN açık istenmişken `_System.VPN.Enabled` = 0 (30 sn). VPN bilerek kapatılınca tanım kalkar.
Saha VPN bağlantısı koptu: <ad> (yüksek)	En az bir kez bağlanmış sahada `Online` = 0, 5 dakika sürerse. Hiç bağlanmamış ("Bekliyor") saha alarm üretmez. Saha silinince tanım kalkar.

Bildirim kanalları ve öncelik **Alarmlar** sayfasında tanım düzenlenerek değiştirilebilir.

DENETİM KAYDI

Bütün VPN işlemleri **Ayarlar › Denetim günlüğü**'nde **VPN** kategorisinde, olay koduyla yazılır: `vpn.interface.enable/disable/update`, `vpn.peer.create/update/disable/enable/revoke`, `vpn.config.issue/download/link_reuse`, `vpn.session.up/down`, `vpn.endpoint.change`, `vpn.apply.fail`. Anahtarlar yalnız parmak iziyle (açık anahtarın ilk 8 karakteri) anılır; özel anahtar, PSK ve indirme belirteci hiçbir kayda yazılmaz.

Sorun giderme

Kullanılamıyor: wireguard.dll bulunamadı	Kurulum paketi motoru `C:\Program Files\MergenHub\wireguard.dll` olarak koyar. Dosya silinmiş ya da bir güvenlik yazılımı tarafından karantinaya alınmışsa aynı sürümün kurulum paketini yeniden çalıştırıp kurulumu onarın, sonra servisi yeniden başlatın.
Modem "Bekliyor"da kalıyor	Dış adres ve port doğru mu (modemin günlüğünde el sıkışma denemesi)? UDP portu kurum güvenlik duvarında / modeminde sunucuya yönlendirilmiş mi? Windows Güvenlik Duvarı'nda "MergenHub VPN" kuralı var mı (VPN açıkken kendiliğinden eklenir; başka bir güvenlik duvarı yazılımı kullanılıyorsa portu orada açın)? DNS Cloudflare'da "DNS only" mi? Modemin saati doğru mu?
İndirme bağlantısı "yalnız HTTPS" diyor	Bağlantı yerel ağ dışından şifresiz HTTP ile açılmış. Ayarlar'da HTTPS'i açın ve bağlantıyı `https://` ile açın; bağlantı bu denemede harcanmamıştır.
Bağlı ama PLC okunamıyor	Yönlendirmeli modda PLC'nin ağ geçidi modem olmalı ve modemde tünelden LAN'a iletim açık olmalıdır (komut dosyası bunu yapar). Sadece modem modunda PLC portu modemde yönlendirilmiş olmalıdır.
Saha dalgalı (bağlanıp kopuyor)	Hücresel hatta MTU 1380 önerilir; 25 sn canlı tutma açık kalmalıdır.
LAN aralığı çakışıyor	Sahaların çoğu 192.168.1.0/24 kullanır; aynı aralık iki sahaya verilemez. Eşlemeli (1:1 NAT) mod Faz 3'te gelecek; şimdilik sahanın LAN'ını değiştirin ya da Sadece modem modunu seçin.

Ayrıca bkz Alarmlar İşlem başvurusu