SimgeNet Mühendislik

TÜRKİYE'DE TASARLANDI VE GELİŞTİRİLDİ

AĞ ERİŞİM DENETİMİ — ENDÜSTRİYEL SINIF

NAC Server

Merkez kopar.
Saha durmaz.

Trafo merkezi, raylı sistem, endüstriyel tesis ve kamu ağları için **merkez + saha düğümlü ağ erişim denetimi**. 802.1X/MAB ile kim bağlanabilir, rol ile ne yapabilir; merkezle bağ kopsa da saha düğümü karar vermeye devam eder. Yerleşik PKI, TACACS+ cihaz yönetimi, IEC 62443 — tek Simgenet yazılımında.

400K+	30 gün	1+1	IEC 62443
KARAR / GÜN · SAHA DÜĞÜMÜ	MERKEZSİZ ÇALIŞMA	YEDEK MERKEZ	OT GÜVENLİĞİ



Simgenet NAC Server · NAC Merkez donanımı SMG-NAC104 · 1U 19" rack · saha düğümü aynı yazılım

01

KURUMSAL

Ağı Kuran, Koruyan ve Kanıtlayan Firma

Simgenet Mühendislik; endüstriyel ağ ve kritik altyapı haberleşme sistemleri sunan bir Türk mühendislik firmasıdır. NAC Server yazılımı **tamamen özgün** olarak Simgenet bünyesinde geliştirilmiştir; hazır bir paketin uyarlaması değildir.

2000	500+	30+	100+
KURULUŞ	TAMAMLANAN PROJE	HİZMET VERİLEN ÜLKE	ÜRÜN ÇEŞİDİ

Neden kendi NAC'ımız

Trafo merkezlerinde ve saha ağlarında kurduğumuz anahtarlara kim bağlanıyor, kim yönetiyor — bu soruya kurumsal NAC ürünleri şehir merkezi mantığıyla cevap veriyordu: kullanıcı cihazı, misafir portalı, merkeze sürekli bağlantı. Sahada ise IED, PLC ve RTU var; WAN kopar; yönetim yerinde yapılır. NAC Server bu gerçeklik için, **kendi anahtarımız, zaman sunucumuz ve test platformumuzla birlikte** geliştirildi.

Neden kendi yazılımımız

- **Teknolojik egemenlik** — yabancı lisans ve yol haritasına bağımlılık yok
- **Şartnameye göre özellik** — projenin istediği politika, rapor ve entegrasyon eklenir
- **Ekosistem** — SMG-SW anahtar, GNSS zaman, SVP test platformu aynı elden
- **Uzun ömür** — 15–20 yıllık altyapı yaşam döngüsü boyunca destek

Bölümlerimiz ayrıdır. Simgenet markalı ürünlerin yazılımı kendi **üretim ve Ar-Ge bölümümüzde** geliştirilir; transmisyon sistemleri ve saha kurulumu ayrı uzman ekiplerle yürütülür. Kurduğumuz erişim denetimini SVP ile ölçer, sonucu standart referansıyla birlikte teslim ederiz.

Misyonumuz

Endüstriyel ağ ve kritik altyapı haberleşme sistemlerinde yenilikçi, güvenilir ve sürdürülebilir teknoloji çözümleri sunarak müşterilerimizin iş sürekliliğini sağlamak.

Vizyonumuz

Ağ altyapısı teknolojilerinde Türkiye'nin en güvenilir ve yenilikçi çözüm ortağı olmak ve küresel ölçekte tanınan bir marka haline gelmek.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

02

PLATFORM

Simgenet NAC Server Nedir?

Ağa bağlanan her cihazı ve ağ cihazlarını yöneten her kişiyi **kimliğiyle tanıyan, rolüne göre yetkilendiren ve her kararı kayda geçiren** ağ erişim denetimi sunucusudur. Bir **Merkez** politikayı belirler; sahadaki **Saha düğümleri** aynı yazılımla anahtar ve erişim noktalarının isteklerini yerinde cevaplar. Endüstriyel ağ için tasarlandı: cihaz kimliği sertifikayla, IED/PLC için MAC tabanlı, yönetici erişimi TACACS+ ile; merkez kopsa da saha durmaz.

Kim bağlanabilir

IEEE 802.1X sertifikalı kimlik doğrulama, sertifikasız cihazlar için MAB; tanımlı olmayan cihaz reddedilir ya da izleme VLAN'ına alınır. Karar rol → VLAN / erişim listesi olarak anahtara iletilir.

Kim yönetebilir

Anahtar, router ve zaman sunucularına yönetici girişi RADIUS ve TACACS+ ile merkezden: yetki seviyesi, komut yetkisi, hesap kaydı. Yerleşik PKI ile cihaz sertifikaları SCEP/EST üzerinden dağıtılır.

Kopsa da çalışır

Saha düğümü politikayı imzalı olarak merkezden alır ve yerel karar tablosuyla çalışır; WAN kesilince kimlik doğrulama sürer. İkinci merkez devralır, geri döner; yedek düğüm boşta beklemez, yük paylaşır.

Öne Çıkan Yetenekler

- 802.1X EAP-TLS, PEAP / EAP-TTLS, MAB; dinamik VLAN (RFC 3580), Filter-Id / dinamik erişim listesi
- CoA / Disconnect (RFC 5176), yeniden kimlik doğrulama, karantina
- İzleme modu → zorlama modu: önce gör, sonra uygula; tek düğmeyle geri
- Merkez + saha düğümü mimarisi; imzalı politika dağıtımı, A/B geri alma
- İkinci merkez ile devralma/geri dönüş; yük paylaşımı
- RADIUS (RadSec dahil) ve TACACS+ cihaz yönetimi (RFC 8907, TLS 1.3 ile)
- Yerleşik PKI: CA, SCEP, EST, OCSP, sertifika ömrü alarmı, iptal
- OT cihaz kütüphanesiyle profilleme (röle, RTU, PLC, IED, GNSS/PTP), envanter, "NEDEN?" tek ekran
- Web (TR/EN/FR), REST API, SNMPv3 + MIB + bildirim, CEF/TLS syslog, X.733 alarm yönetimi
- Yedek/geri yükleme, imzalı güncelleme, destek paketi, günlük rapor

Endüstriyel gerçeklik için. Sahada kullanıcı bilgisayarı değil IED, PLC, RTU ve kamera var; merkeze bağlantı her zaman yoktur; yönetici anahtara konsoldan girer. NAC Server misafir portalı ve kullanıcı ajanı yerine **cihaz kimliği, yerel süreklilik ve cihaz yönetimi** üzerine kurulmuştur.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

03

MİMARİ

Merkez, Saha Düğümü ve Yedek Merkez

Tek yazılım, iki rol. **Merkezde karar, sahada cevap:** politika, envanter, PKI ve raporlama merkezde; kimlik doğrulama isteği sahada, en yakın düğümde milisaniyeler içinde cevaplanır. Merkez ile saha arasındaki her şey imzalı ve sürümlüdür.

NAC Merkez

Politika ve rol tanımı · cihaz/kullanıcı envanteri · PKI ve sertifika yaşam döngüsü · cihaz-yönetim AAA (RADIUS/TACACS+) · raporlar, alarmlar, yönetim · saha düğümlerine imzalı dağıtım

NAC Saha

Anahtar / erişim noktası 802.1X ve MAB isteklerini yerinde cevaplar (RADIUS) · yerel karar tablosu · merkez kopunca son onaylı politikayla devam · durumunu merkeze bildirir

Yedek Merkez

İkinci merkez sürekli senkron · birincil düşünce devralır, dönünce geri verir · saha düğümleri kesintisiz · filo tek yerden görünür

Merkez → saha dağıtımı

- Politika, rol→VLAN, erişim listeleri ve cihaz kayıtları **imzalı ve nesil numaralı** paket olarak dağıtılır
- Saha düğümü imzayı doğrular, uygular, cihazdan geri okur; sonuç merkezde **doğrulandı / uygulandı / teyit edildi** aşamalarıyla görünür
- Hatalı nesil: tek adımda önceki nesle **geri alma**
- Yazılım güncellemesi de aynı yol: imzalı paket, A/B kurulum, geri dönüş

Saha düğümü tek başına

- Son onaylı politika ve yerel karar tablosu düğümde; WAN kopsa da 802.1X/MAB ve dinamik VLAN kararları sürer
- Süreklilik kipleri (normal → kısıtlı → süreklilik) panelde ve olay defterinde; son onaylı politikayla 30 güne kadar
- Zaman güveni: GNSS/NTP kaynağı ve sertifika geçerliliği kararın parçasıdır
- Bağlantı dönünce olaylar merkeze aktarılır, politika farkı otomatik kapanır

Ölçek ve yerleşim

- Bir bölge: 1 merkez + 1 yedek merkez + N saha düğümü (her trafo merkezi / istasyon / tesis birer düğüm)
- Saha düğümü 4–8 GB bellekli sanal makinede tam özellikli; küçük düğümde özellik kısılmaz
- Saha düğümleri "ev merkez" seçimiyle iki merkeze dağıtılır — yük paylaşımı, boşta bekleyen kapasite yok
- Aynı anahtar birden fazla düğümü RADIUS sunucusu olarak görür — düğüm arızasında anahtar ikinciye döner

Simgenet ekosistemiyle

- **SMG-SW anahtar / SMGOS router:** 802.1X authenticator, MAB, dinamik VLAN, Filter-Id, CoA, cihaz-yönetim RADIUS/TACACS+, ortak CA — zorlayan ve karar veren aynı elden
- **Simgenet GNSS Server:** zaman güveni ve zamanlama portu farkındalığı
- **Simgenet SVP:** kurulum kabulü ölçülür — 802.1X/MAB/CoA vektörleri, kapasite ve devralma süresi raporla teslim
- Üçüncü taraf anahtar/erişim noktalarıyla standart RADIUS/TACACS+/CoA; yaygın üreticiler için hazır anahtar reçeteleri

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

04

ERİŞİM DENETİMİ

Kim Bağlanabilir, Ne Yapabilir

Porta takılan her cihaz önce kimliğini kanıtlar; sonra rolüne göre VLAN ve erişim listesi alır. Tanımsız cihaz ağa giremez, ya da **izleme VLAN'ında görünür hâle gelir**. Karar milisaniyeler içinde, sahada verilir.

Kimlik doğrulama

- **IEEE 802.1X EAP-TLS** — cihaz sertifikası ve zincir doğrulama; sertifika ile MAC eşleşmesi kararın parçası
- **PEAP / EAP-TTLS** — kullanıcı adı/parola ile, yerel kullanıcı veritabanı
- **MAB** (MAC tabanlı) — sertifikasız IED, PLC, kamera ve sensörler için; yerel tablo, milisaniye cevap; MAC sahteciliği şüphesi tespiti
- Kayıtsız cihaz: **reddet** veya **izleme VLAN'ı** — politikaya göre
- Yeniden kimlik doğrulama süresi ve oturum sonu davranışı rol bazlı

Yetkilendirme ve zorlama

- **Rol → VLAN** (RFC 3580 Tunnel öznitelikleri), **Filter-Id → erişim listesi** ve üretici öznitelikleriyle dinamik ACL
- **Port sınıfı:** zamanlama / koruma / genel — zamanlama taşıyan port farkında olunur, politika buna göre
- **CoA / Disconnect (RFC 5176):** merkezden oturum düşürme, VLAN değiştirme, yeniden yetkilendirme; CoA desteklemeyen anahtarlarda da çalışır
- **Karantina** ve süreli istisna (break-glass): acil durumda kapsamlı, süreli, kayıtlı

İzleme modu → zorlama modu

- Kurulum her zaman **izleme modunda** başlar: karar üretilir, uygulanmaz, raporlanır; port değişikliği sıfır
- Envanter dolar, profiller doğrulanır; karar dağılımı zorlama moduyla birebir aynı
- Zorlamaya geçiş yönetici kararı, **tek düğmeyle geri alınabilir** — arızada en hızlı kurtarma

Cihaz profilleme ve envanter

- Pasif toplayıcı: üretici (OUI), DHCP, SNMP izleri; **OT cihaz kütüphanesi** — röle, RTU, PLC, IED, GNSS/PTP
- Envanter: MAC, kimlik, profil, anahtar/port, son görülme, rol, politika nesli
- Simgenet cihazları ilk anda tanınır (kendi OUI'miz)
- Toplu içe aktarma ve API ile kayıt

"Neden reddedildi?" tek ekranda. Canlı doğrulama günlüğü her denemeyi zaman, MAC, kimlik, profil, anahtar/port, politika, **red nedeni**, doğrulama yöntemi ve süreklilik durumuyla listeler; saha mühendisi telefonu kapatmadan cevabı görür.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

05

SÜREKLİLİK

Merkez Kopar, Saha Durmaz

Erişim denetiminin en tehlikeli arızası, merkeze ulaşılamadığında sahanın kilitlenmesidir. NAC Server bu senaryoyu ürünün merkezine koyar: **saha düğümü tek başına karar verir**, ikinci merkez devralır, hiçbir düğüm boşta beklemez.

Saha düğümü sürekliliği

- Süreklilik kipleri: normal (merkezle senkron) → kısıtlı → süreklilik (yerel karar tablosu, son onaylı politika); merkezsiz çalışma **30 güne kadar** (politika geçerlilik süresi, ayarlanabilir)
- Her düğüm son iyi anlık görüntüyü, politika neslini ve imzasını taşır; WAN kopsa da 802.1X/MAB ve dinamik VLAN kararları sürer
- Süreklilik hazırlığı ekranı: yerel yetkilendirme, eş düğüm senkronu, merkeze son bağlantı, politika imzası, zaman güveni, sertifika kalan gün, geri alma hazır
- Bağlantı dönünce olaylar aktarılır, fark kapanır

Yedek merkez ve yük paylaşımı

- **İkinci merkez** sürekli senkron; birincil düşünce devralır, dönünce geri verir — saha düğümleri fark etmez
- Tek yazar ilkesi: aynı anda tek merkez yazar, çakışma olmaz
- Saha düğümleri "ev merkez" seçimiyle iki merkeze dağıtılır — **yük paylaşımı**, boşta bekleyen kapasite yok
- Anahtar tarafında birden fazla RADIUS/TACACS+ sunucu tanımı ile düğüm yedekliliği

Değişiklik güvenliği

- Politika ve cihaz kayıtları **imzalı nesil** olarak dağıtılır; süre sonu ve geri alma
- Karar aşamaları: doğrulandı → uygulandı → teyit edildi (cihazdan geri okuma)
- Yazılım güncellemesi imzalı paketle, A/B kurulum, tek adımda geri dönüş
- Yedek alma / geri yükleme ekranı; manifest ve sağlama ile bütünlük

Lisans ve işletme

- Lisans süresi dolsa da **kimlik doğrulama durmaz**; yalnız yönetim işlevleri uyarır
- Parola politikası ve brute-force kilidi; sırlar ekranda ve kayıtlarda maskeli, yedek dosyasına yalnız yönetici erişir
- Küçük düğüm tam özellikli: 4–8 GB bellekte tüm işlevler

Arıza Senaryoları

WAN kopar
Saha düğümü son politikayla devam eder; olaylar birikir, dönünce aktarılır

Merkez düşer
Yedek merkez devralır; saha kesintisiz; birincil dönünce geri verir

Saha düğümü düşer
Anahtar ikinci düğüme döner; yük paylaşımlı eş düğüm cevaplar

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

06

AAA VE PKI

Cihaz Yönetimi ve Sertifika Altyapısı

Anahtar, router ve zaman sunucularına kim, hangi yetkiyle, hangi komutla girdi — hepsi merkezden belirlenir ve kayda geçer. Cihaz sertifikaları yerleşik PKI ile üretilir, dağıtılır, izlenir ve iptal edilir; **elle sertifika taşıma yoktur**.

RADIUS cihaz yönetimi

- Yönetici girişi RADIUS ile: yetki seviyesi (admin / operatör / izleyici), Service-Type ve üretici öznitelikleri
- RFC 2865/2866/2869; **Message-Authenticator her iki yönde zorunlu** — BlastRADIUS sınıfı saldırılara kapalı
- Hesap kaydı (Start / Interim / Stop); oturum süresi ve yeniden doğrulama
- **RadSec** (RADIUS/TLS, RFC 6614) sunucu; Status-Server
- Simgenet ürünlerinde yerleşik rol eşlemesi (RFC 5607 yetki seviyesi); üçüncü taraf cihazlarda standart öznitelikler

TACACS+ cihaz yönetimi

- **RFC 8907 TACACS+**: kimlik doğrulama; oturum yetki seviyesi 0–15; **komut yetkilendirme** — yönetici tanımlı komut setleri (izin/yasak kalıpları, kullanıcıya veya yetki seviyesi aralığına atama, varsayılan izin/ret) ve hazır sınıflar (görüntüleme / yapılandırma hariç / tam); her komut kararı denetim kaydında; hesap kaydı
- **TACACS+ üzerinden TLS 1.3 (RFC 9887)** — yönetim trafiği şifreli
- Sunucu erişilemezken cihazda yerel yedek hesap politikası
- Cihaz-yönetim AAA merkez ve yedek merkezden sunulur; anahtar her iki merkezi sunucu olarak tanır

Yerleşik PKI

- İç sertifika otoritesi (CA), profil tabanlı sertifika üretimi, rastgele seri numarası
- **SCEP (RFC 8894)** ve **EST (RFC 7030)** ile cihazların otomatik sertifika alması ve yenilemesi; yeniden kayıtta eski sertifika otomatik iptal
- **OCSP** yanıtlayıcı ve CRL (sahaya imzalı dağıtım); EAP-TLS'te iptal denetimi — iptal edilen sertifika anında reddedilir
- Sertifika ömrü alarmları (90 / 60 / 30 gün); "sonraki sertifika yüklü" göstergesi

Kimlik kaynakları ve güven

- Yerel kullanıcı ve cihaz veritabanı; LDAP/AD dizini; dış RADIUS ve TACACS+ kimlik kaynağı
- Zaman güveni kararın parçası: GNSS/NTP kaynağı ve sertifika geçerlilik penceresi
- Yönetici hesapları için rol tabanlı erişim; başarısız girişler dahil **yönetici denetim kaydı**
- Kendi kurumsal kimliğimiz (OID) ile RADIUS öznitelikleri ve MIB

TACACS+ komut kararları

```
kullanıcı  yetki  komut                karar
operator   1      show version         İZİN
operator   1      show running-config  RET (yasak)
operator   1      configure terminal   RET (varsayılan)
admin      15     configure terminal   İZİN (tam)
her karar → günlük + denetim olayı
```

NEDEN? teşhisi

```
MAC 00:18:f8:09:cf:d7
anahtar  10.10.0.2  Gi1/0/5
yöntem   MAB   profil KontrolRTU
kural    KontrolRTU → VLAN 30
         (nesil 4, merkez imzalı)
karar    KABUL · VLAN 30
```

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

07

YÖNETİM

Web Paneli, İzleme ve Entegrasyon

Sade menü, tablo mantığı, tek ekranda cevap. Panel; ağ cihazlarını, cihaz kayıtlarını ve politikaları rol duyarlı ekranlarla yönetir; saha mühendisi kendi düğümünü, merkez yöneticisi tüm filoyu görür.

Web paneli (HTTPS, TR/EN)

- **Durum panosu:** süreklilik kipi, kabul / ret / izleme (24 saat), yetkili politika nesli, CPU/RAM/disk, karar hızı, veri yaşı, son kararlar, alarm rozeti
- **Canlı doğrulama günlüğü** — her deneme, red nedeni, doğrulama yöntemi, politika nesli
- Menü: **Durum · Cihazlar · Anahtarlar · Denetim · Simgenet NAC · Alarmlar · Sistem**; Simgenet NAC altında rol (Merkez/Saha), siteler, dağıtım (imzalı politika), merkez HA, süreklilik, cihaz teşhisi (NEDEN?), anahtar reçeteleri, sertifika teşhisi, cihaz profilleri, acil geçiş, depolama, günlük raporlar
- Rol duyarlı görünüm: admin / operatör / izleyici; Saha rolünde yalnız saha kalemleri; TR / EN / FR

Alarm, olay ve rapor

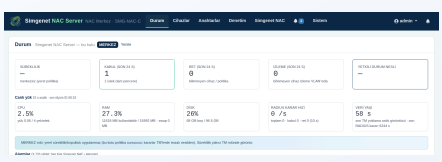
- Alarm yönetimi **X.733** şiddetleriyle (acil / majör / minör / uyarı): ayrı Alarmlar ekranı, "gördüm" onayı, toplu alarm, kapanma geçmişi, "yapılacak" sütunu; acil alarm her sayfada üst şeritte; eşikler ayarlanabilir
- Olay defteri: kim, nereden, ne zaman; sırlar hiçbir kayıtta yer almaz
- **Günlük rapor**: kararlar, olaylar, yönetici girişleri, gün sonu durumu; JSON/CSV dışa aktarım ve API; 730 gün saklama
- **Destek paketi** tek tıkla: teşhis için gereken her şey, kişisel veri maskeli

NMS / SIEM entegrasyonu

- **SNMPv3** (authPriv) izleme; SIMGENET-NAC-MIB; olay → bildirim (trap)
- **Syslog CEF**, TLS ile uçtan uca (RFC 5425); SIEM'e doğrudan
- **REST API** — cihaz kaydı, politika, raporlar, otomasyon
- Yaygın NMS ve SIEM sistemleriyle doğrulanmış

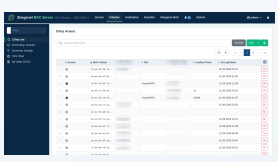
Kurulum ve işletme

- **NAC Merkez: Simgenet SMG-NAC104 (1U 19" rack)**; saha düğümü Simgenet donanım veya sanal makine; merkez ve saha düğümü aynı imaj, rol kurulumda 1 ekranda seçilir
- Saha düğümü kurulumu: merkez adresi + kayıt belirteci (2 alan) → otomatik kayıt, politika ve sertifika kendiliğinden iner
- HTTPS; parola politikası; brute-force kilidi
- Hazır şablonlar: 802.1X EAP-TLS, MAB, cihaz-yönetim, OT cihaz profilleri, anahtar reçeteleri; anahtar ekleme 1 form, cihaz kaydı 1 form, politika = rol→VLAN tablosu + derle → imzala → yükle
- Yedek alma / geri yükleme (onaylı), imzalı güncelleme, A/B geri dönüş; günlük saklama ve döndürme politikası



Durum panosu

Süreklilik kipi, kabul/ret/izleme, politika nesli, canlı yük.



Cihaz kayıtları

MAC, rol, anahtar/port, son görülme; süzme ve CSV.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

08

KAPASİTE VE KULLANIM

Ölçek, Senaryolar ve Kabul

Kapasite rakamı kendi başına anlam taşımaz; **sabah vardiyasında tüm cihazların aynı anda gelmesi, bölgedeki tüm merkezlerin tek çift merkezden yönetilmesi ve WAN kopukluğunda sahanın çalışması** anlam taşır. Değerler Simgenet SVP ile ölçülmüştür.

400K+ / gün
Tek saha düğümünde ölçülen karar sayısı; kararlar sahada, milisaniye sınıfında

30 gün
Merkezsiz çalışma — son onaylı politikayla kimlik doğrulama ve VLAN kararları kesintisiz

< 5 dk
Merkez devralma (geri dönüş < 6 dk) — 9 sahalı filoda 3 senaryoyla ölçüldü; politika dağıtımı 9 sahaya < 2 dk

Bu kapasite ne demek

- **Sabah 08:00 fırtınası:** bir trafo merkezindeki tüm IED, PC ve kameralar aynı anda gelse bile saha düğümü saniyeler içinde hepsini cevaplar
- **Bir bölge, tek çift merkez:** onlarca trafo merkezi / istasyon birer saha düğümüyle tek merkez + yedek merkezden yönetilir
- **WAN kopukluğu:** saha düğümü son onaylı politikayla 30 güne kadar çalışır; dönünce fark otomatik kapanır
- **Yük altında arıza:** devralma ve geri dönüş süreleri yük altında ölçülmüştür

Kabul testi (SVP ile)

- 802.1X / MAB / dinamik VLAN / CoA vektörleri — bilinen-PASS ve bilinen-FAIL kontrolüyle
- RADIUS güvenlik: Message-Authenticator, hatalı paket korpusu, tekrar saldırısı
- TACACS+ yetki ve komut yetkisi; yük ve bozuk paket seli altında davranış
- Kapasite ölçek testi; merkez devralma / geri dönüş; sonuç kilitlenebilir rapor

Enerji / trafo merkezi

IED, PLC, RTU ve kayıt cihazlarının MAB/EAP-TLS ile kaydı; zamanlama ve koruma portlarının sınıfıyla politika; bölge merkezi + yedek merkez; TACACS+ ile anahtar/router yönetimi; IEC 62443 uyumlu kayıt.

Raylı sistem / endüstriyel tesis / kamu

İstasyon ve tesis ağlarında envanter dışı cihaz reddi, izleme modundan zorlamaya kademeli geçiş, saha düğümüyle yerel süreklilik, merkezden tek politika; kamu ağlarında yönetici erişiminin merkezî kaydı.

Simgenet'e has ekosistem. Anahtarı (SMG-SW), zaman sunucusunu (GNSS Server), test platformunu (SVP) ve erişim denetimini aynı firma verir: zorlayan taraf, karar veren taraf ve ölçen taraf tek elden; kanıtlı rapor teslim edilir.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

09

TEKNİK ÖZELLİKLER

Simgenet NAC Server

ÖZELLİK	SİMGENET NAC SERVER
Ürün sınıfı	Endüstriyel ağ erişim denetimi (NAC) ve cihaz yönetimi AAA sunucusu; yazılım tamamen Simgenet bünyesinde
Roller	NAC Merkez (SMG-NAC-C) · NAC Saha düğümü (SMG-NAC-S) · Yedek Merkez — aynı yazılım imajı, rol kurulumda
Kimlik doğrulama	IEEE 802.1X-2020 EAP-TLS (RFC 5216) · PEAP / EAP-TTLS (yerel kullanıcı DB) · MAB · kayıtsız cihaz reddi / izleme (monitor) VLAN kipi · MAC sahteciliği şüphesi tespiti · yeniden doğrulama (RFC 2865 Session-Timeout / Termination-Action)
Yetkilendirme	Rol → VLAN (RFC 3580 Tunnel-*) · Filter-Id → erişim listesi · üretici öznitelikleriyle dinamik ACL · port sınıfı (zamanlama / koruma / genel) · karantina · süreli acil geçiş (break-glass, denetim kayıtlı)
Dinamik yetkilendirme	CoA ve Disconnect (RFC 5176, port 3799), Error-Cause; CoA desteklemeyen anahtarlar için yedek yol
RADIUS	RFC 2865 / 2866 / 2869 · Status-Server (RFC 5997) · Message-Authenticator iki yönde zorunlu (BlastRADIUS korumalı) · RadSec (RFC 6614) sunucu · hesap kaydı · yetki seviyesi (RFC 5607) · üretici öznitelikleri (kurumsal OID)
TACACS+	RFC 8907 — kimlik doğrulama (ASCII/PAP); yetkilendirme: oturum yetki seviyesi 0–15 ve komut yetkilendirme — yönetici tanımlı komut setleri (izin/yasak kalıpları, kullanıcı veya yetki seviyesi aralığına atama, varsayılan izin/ret), hazır sınıflar (görüntüleme / yapılandırma hariç / tam); her komut kararı denetim kaydında; hesap kaydı · TACACS+ üzerinden TLS 1.3 (RFC 9887)
PKI	İç CA · profil tabanlı üretim, rastgele seri (RFC 5280) · SCEP (RFC 8894, challenge parolalı) · EST (RFC 7030; ECDSA dahil, yeniden kayıtta eski sertifika iptali) · OCSP (RFC 6960) · CRL (sahaya imzalı dağıtım) · EAP-TLS iptal denetimi · ömür alarmları 90/60/30 gün · yenileme/iptal kayıtları denetim defterinde
Profilleme / envanter	Pasif toplayıcı (OUI, DHCP, SNMP) · OT cihaz kütüphanesi (röle, RTU, PLC, IED, GNSS/PTP) · cihaz kayıtları ve gruplar · toplu içe aktarma · API
Süreklilik	Saha düğümünde yerel karar tablosu ve son onaylı politika; kipler normal / kısıtlı / süreklilik; merkez kopukluğunda 802.1X/MAB ve dinamik VLAN kararları kesintisiz — 30 güne kadar (ayarlanabilir); cihaz-yönetim AAA (RADIUS/TACACS+) merkez ve yedek merkezden sunulur
HA / dağıtım	İkinci merkez (otomatik devralma / geri dönüş, tek yazar) · saha düğümleri "ev merkez" ile iki merkeze dağıtılır (yük paylaşımı) · imzalı nesil dağıtımı (çevrimdışı imza anahtarı, süre sonu, geri alma) · karar aşamaları doğrulandı → uygulandı → teyit edildi

Devamı sonraki sayfada: yönetim, izleme, güvenlik, kapasite, kurulum ve referans standartlar.

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

TEKNİK ÖZELLİKLER

10 Yönetim, Güvenlik ve Kapasite

ÖZELLİK	SİMGENET NAC SERVER
Yönetim	HTTPS web (TR/EN/FR; rol duyarlı admin / operatör / izleyici; Saha kapsamı) · yönetici girişi için dış TACACS+/RADIUS/LDAP · REST API (tam) · CLI (sistem) · cihaz yönetimi (TACACS+) ekranı: NAS listesi, komut setleri, atamalar · canlı kararlar · "NEDEN?" teşhis ekranı · hazır şablonlar ve anahtar reçeteleri · destek paketi (sırsız, takma kimlikli)
İzleme	SNMPv3 (authPriv) + SIMGENET-NAC-MIB + bildirimler · X.733 alarm yönetimi (acil/majör/minör/uyarı; onay, toplu alarm, kapanma geçmişi) · eşikler · zaman güveni izleme (PTP/GNSS NTP, kademeli) · günlük rapor (JSON/CSV/API, 730 gün) · ortak teşhis olay şeması (SMG ürün ailesiyle aynı)
Kayıt / SIEM	Syslog CEF (RFC 5424), TLS ile (RFC 5425) · yönetici denetim kaydı (başarısız girişler dahil) · zaman damgalı karar günlüğü · saklama ve döndürme politikası · sır içermeyen kayıt
Güvenlik	IEC 62443-4-2 ilkeleri (en az yetki, oturum/kilit, denetim) · parola politikası ve brute-force kilidi · sırlar ekranda ve kayıtlarda maskeli; yedek dosyasına yalnız yönetici erişir · zaman güveni (GNSS/NTP) kararın parçası
Yedek / güncelleme	Yedek alma / geri yükleme ekranı (manifest + sağlama, onaylı) · imzalı yazılım paketi, A/B kurulum, geri dönüş · politika neslinde geri alma
Kapasite (ölçülmüş)	Tek saha düğümü 421.000+ karar/gün · merkez devralma 161–245 s, geri dönüş 234–315 s (9 saha, 3 senaryo) · merkezsiz çalışma 30 güne kadar · politika dağıtımı 9 sahaya < 2 dk · rapor saklama 730 gün · eşzamanlı istemci ve NAS kapasitesi projeye göre ölçek testiyle
Kimlik kaynakları	Yerel kullanıcı/cihaz veritabanı · LDAP / AD · dış RADIUS · dış TACACS+ · sertifika (EAP-TLS) · MAC envanteri
Entegrasyon	SMG-SW anahtar / SMGOS router (802.1X, MAB, dinamik VLAN, Filter-Id, CoA, cihaz-yönetim AAA, ortak CA) · Simgenet GNSS Server (yönetim AAA, CoA, zaman güveni) · Simgenet SVP (uygunluk vektörleri) · standart RADIUS/TACACS+/CoA ile üçüncü taraf anahtar ve erişim noktaları, yaygın üreticiler için hazır reçeteler
Donanım ve kurulum	**NAC Merkez: Simgenet SMG-NAC104** — 1U 19" rack, Intel® Xeon® E3-1200 v5, DDR4 64 GB'a kadar, 4 × PCIe Gen3 x8, 220 VAC 250 W, −20…+60 °C, IEC 61000-4 Seviye 3 · **NAC Saha:** Simgenet donanım veya sanal makine · Merkez 4 vCPU / 8 GB / 100 GB · Saha 2–4 vCPU / 4–8 GB / 60 GB · saha kurulumu: imaj + kayıt belirteci → otomatik kayıt
Dil	TR / EN / FR
Kapsam dışı	Bulut/SaaS · posture/uyumluluk ajanı · misafir/captive portal · BYOD self-servis · Wi-Fi denetleyici işlevi

Referans Standartlar

IEEE 802.1X-2020 · RFC 5216 (EAP-TLS) · RFC 2865 / 2866 / 2869 (RADIUS) · RFC 5997 (Status-Server) · RFC 3580 (802.1X RADIUS kullanımı) · RFC 5176 (CoA / Disconnect) · RFC 5607 · RFC 6614 (RadSec) · RFC 8907 (TACACS+) · RFC 9887 (TACACS+ TLS) · RFC 7030 (EST) · RFC 8894 (SCEP) · RFC 6960 (OCSP) · RFC 5280 (X.509 / CRL) · RFC 5424 / 5425 (syslog, TLS) · RFC 3411–3418 (SNMPv3) · RFC 5905 (NTP) · IEC 62443-3-3 / 62443-4-2 · X.733

© 2026 Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

SimgeNet Mühendislik

Neden Simgenet NAC Server

Merkez kopar, saha durmaz

Saha düğümü yerel karar tablosu ve imzalı son politikayla çalışır; ikinci merkez devralır; yedek düğüm yük paylaşır.

Endüstriyel cihazlar için

Sertifikalı 802.1X ve MAB; IED, PLC, RTU ve kamera için izleme modundan zorlamaya kademeli geçiş; zamanlama portu farkındalığı.

Cihaz yönetimi ve PKI yerleşik

RADIUS ve TLS'li TACACS+ ile kim hangi komutu çalıştırdı; iç CA, SCEP/EST, OCSP ile sertifika elle taşınmaz.

Özgün, ekosistemli, kanıtlı

Yazılım tamamen Simgenet bünyesinde; anahtar, zaman ve test platformu aynı elden; kabul SVP raporuyla teslim.

BİZE ULAŞIN

Adres
Kartal / İstanbul, Türkiye

Telefon
+90 555 600 4506

E-posta · Web
info@simgenet.net · simgenet.net

Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

Ürün Broşürü · SMG-UB-NAC-TR · Rev. 3 · © 2026

Türkiye'de Geliştirildi