SimgeNet Mühendislik

DESIGNED & ENGINEERED IN TÜRKİYE

NETWORK ACCESS CONTROL — INDUSTRIAL GRADE

# NAC Server

## The centre goes down.
## The site keeps running.

**Core + site-node network access control** for substations, rail systems, industrial plants and government networks. 802.1X/MAB decide who may connect, roles decide what they may do; when the link to the centre is lost, the site node keeps deciding. Built-in PKI, TACACS+ device administration, IEC 62443 — in one Simgenet software.

| 400K+ | 30 days | 1+1 | IEC 62443 |
|---|---|---|---|
| DECISIONS / DAY · SITE NODE | OPERATION WITHOUT THE CORE | STANDBY CORE | OT SECURITY |



Simgenet NAC Server · NAC Core hardware SMG-NAC104 · 1U 19" rack · site node runs the same software

01

COMPANY

# The Company That Builds, Protects and Proves the Network

Simgenet Mühendislik is a Turkish engineering company delivering industrial networking and critical-infrastructure communication systems. The NAC Server software is **entirely original**, developed in house at Simgenet; it is not an adaptation of an off-the-shelf package.

| 2000 | 500+ | 30+ | 100+ |
|---|---|---|---|
| FOUNDED | COMPLETED PROJECTS | COUNTRIES SERVED | PRODUCT TYPES |

### Why our own NAC

Who connects to the switches we install in substations and field networks, and who manages them — enterprise NAC products answered this with a head-office mindset: user laptops, guest portals, a permanent link to the centre. In the field there are IEDs, PLCs and RTUs; the WAN goes down; management happens on site. NAC Server was built for that reality, **together with our own switch, time server and test platform**.

### Why our own software

- **Technological sovereignty** — no dependency on foreign licences and roadmaps
- **Features to the specification** — the policy, report and integration the project requires are added
- **Ecosystem** — SMG-SW switch, GNSS time, SVP test platform from one source
- **Long service life** — support across a 15–20 year infrastructure lifecycle

**Our departments are separate.** The software of Simgenet-branded products is developed by our own **manufacturing and R&D department**; transmission systems and field deployment are delivered by separate specialist teams. We measure the access control we deploy with SVP and hand over the result with its standard reference.

### Our Mission

To deliver innovative, reliable and sustainable technology for industrial networks and critical-infrastructure communications, safeguarding our customers' business continuity.

### Our Vision

To become Türkiye's most trusted and innovative network-infrastructure technology partner, recognized as a global brand.

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

02

PLATFORM

# What is the Simgenet NAC Server?

A network access control server that **identifies every device joining the network and every person managing network devices, authorizes them by role and records every decision**. One **Core** defines the policy; **Site nodes** in the field run the same software and answer switch and access-point requests locally. Designed for industrial networks: device identity by certificate, MAC-based for IEDs and PLCs, administrator access via TACACS+; when the centre is lost, the site keeps running.

### Who may connect

Certificate-based IEEE 802.1X authentication, MAB for devices without certificates; an undefined device is rejected or placed in a monitoring VLAN. The decision is delivered to the switch as role → VLAN / access list.

### Who may manage

Administrator login to switches, routers and time servers via RADIUS and TACACS+ from the centre: privilege level, command authorization, accounting. Device certificates are distributed by the built-in PKI over SCEP/EST.

### Keeps running when cut off

The site node receives the policy signed from the core and works from a local decision table; authentication continues when the WAN is down. A standby core takes over and hands back; no standby node sits idle — it shares the load.

## Key Capabilities

- 802.1X EAP-TLS, PEAP / EAP-TTLS, MAB; dynamic VLAN (RFC 3580), Filter-Id / dynamic access list
- CoA / Disconnect (RFC 5176), re-authentication, quarantine
- Monitoring mode → enforcement mode: see first, then enforce; one-click revert
- Core + site-node architecture; signed policy distribution, A/B rollback
- Standby core with takeover / failback; load sharing
- RADIUS (incl. RadSec) and TACACS+ device administration (RFC 8907, with TLS 1.3)
- Built-in PKI: CA, SCEP, EST, OCSP, certificate-lifetime alarms, revocation
- Profiling with an OT device library (relay, RTU, PLC, IED, GNSS/PTP), inventory, "WHY?" on one screen
- Web (EN/TR/FR), REST API, SNMPv3 + MIB + notifications, CEF/TLS syslog, X.733 alarm management
- Backup/restore, signed updates, support bundle, daily report

**Built for industrial reality.** In the field there are no user laptops but IEDs, PLCs, RTUs and cameras; the link to the centre is not always there; the administrator logs into the switch from the console. Instead of guest portals and user agents, NAC Server is built on **device identity, local continuity and device administration**.

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

03

ARCHITECTURE

# Core, Site Node and Standby Core

One software, two roles. **Decide at the centre, answer in the field:** policy, inventory, PKI and reporting live at the core; the authentication request is answered in the field, at the nearest node, within milliseconds. Everything between core and site is signed and versioned.

### NAC Core

Policy and role definition · device/user inventory · PKI and certificate lifecycle · device-administration AAA (RADIUS/TACACS+) · reports, alarms, management · signed distribution to site nodes

### NAC Site

Answers switch / access-point 802.1X and MAB requests locally (RADIUS) · local decision table · continues on the last approved policy when the core is lost · reports its state to the core

### Standby Core

Second core continuously synchronized · takes over when the primary fails, hands back when it returns · site nodes uninterrupted · the fleet visible from one place

### Core → site distribution

- Policy, role→VLAN, access lists and device records are distributed as a **signed, generation-numbered** package
- The site node verifies the signature, applies it, reads it back from the device; the result is visible at the core as **validated / applied / verified**
- Faulty generation: one-step **rollback** to the previous generation
- Software updates follow the same path: signed package, A/B installation, rollback

### Site node on its own

- Last approved policy and local decision table on the node; 802.1X/MAB and dynamic-VLAN decisions continue when the WAN is down
- Continuity modes (normal → restricted → continuity) on the panel and in the event log; up to 30 days on the last approved policy
- Time trust: GNSS/NTP source and certificate validity are part of the decision
- When the link returns, events are forwarded to the core and the policy difference closes automatically

### Scale and placement

- One region: 1 core + 1 standby core + N site nodes (every substation / station / plant is a node)
- A site node is fully featured on a 4–8 GB virtual machine; no features are cut on small nodes
- Site nodes are distributed across the two cores by "home core" — load sharing, no idle capacity
- The same switch sees several nodes as RADIUS servers — on node failure the switch falls back to the second

### With the Simgenet ecosystem

- **SMG-SW switch / SMGOS router:** 802.1X authenticator, MAB, dynamic VLAN, Filter-Id, CoA, device-administration RADIUS/TACACS+, common CA — enforcer and decision-maker from one source
- **Simgenet GNSS Server:** time trust and timing-port awareness
- **Simgenet SVP:** deployment acceptance is measured — 802.1X/MAB/CoA vectors, capacity and takeover time delivered as a report
- Standard RADIUS/TACACS+/CoA with third-party switches and access points; ready switch recipes for common vendors

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

04

ACCESS CONTROL

# Who May Connect, What They May Do

Every device plugged into a port first proves its identity; then it receives a VLAN and access list according to its role. An undefined device cannot join the network — or **becomes visible in the monitoring VLAN**. The decision is made in the field, within milliseconds.

## Authentication

- **IEEE 802.1X EAP-TLS** — device certificate and chain validation; certificate-to-MAC match is part of the decision
- **PEAP / EAP-TTLS** — username/password with the local user database
- **MAB** (MAC-based) — for IEDs, PLCs, cameras and sensors without certificates; local table, millisecond answer; MAC-spoofing suspicion detection
- Unregistered device: **reject** or **monitoring VLAN** — by policy
- Re-authentication period and session-end behaviour per role

## Authorization and enforcement

- **Role → VLAN** (RFC 3580 Tunnel attributes), **Filter-Id → access list** and dynamic ACL via vendor attributes
- **Port class:** timing / protection / general — a port carrying timing is known, and policy follows
- **CoA / Disconnect (RFC 5176):** session teardown, VLAN change and re-authorization from the centre; works with switches without CoA as well
- **Quarantine** and time-limited emergency override (break-glass): scoped, timed, logged

## Monitoring mode → enforcement mode

- Deployment always starts in **monitoring mode**: decisions are produced, not enforced, and reported; zero port changes
- The inventory fills, profiles are verified; the decision distribution is identical to enforcement mode
- Switching to enforcement is an administrator decision, **reverted with one click** — the fastest recovery in an incident

## Device profiling and inventory

- Passive collector: vendor (OUI), DHCP, SNMP traces; **OT device library** — relay, RTU, PLC, IED, GNSS/PTP
- Inventory: MAC, identity, profile, switch/port, last seen, role, policy generation
- Simgenet devices recognized instantly (our own OUI)
- Bulk import and registration via API

**"Why was it rejected?" on one screen.** The live authentication log lists every attempt with time, MAC, identity, profile, switch/port, policy, **failure reason**, authentication method and continuity state; the field engineer sees the answer before hanging up the phone.

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

05

CONTINUITY

# The Centre Goes Down, the Site Keeps Running

The most dangerous failure of access control is a site that locks up when the centre is unreachable. NAC Server puts this scenario at the heart of the product: **the site node decides on its own**, the standby core takes over, no node sits idle.

### Site-node continuity

- Continuity modes: normal (synchronized with the core) → restricted → continuity (local decision table, last approved policy); operation without the core **up to 30 days** (policy validity period, configurable)
- Every node carries the last good snapshot, policy generation and signature; 802.1X/MAB and dynamic-VLAN decisions continue when the WAN is down
- Continuity-readiness screen: local authorization, peer-node sync, last contact with the core, policy signature, time trust, certificate days left, rollback ready
- When the link returns, events are forwarded and the difference closes

### Standby core and load sharing

- **Second core** continuously synchronized; takes over when the primary fails, hands back when it returns — site nodes do not notice
- Single-writer principle: only one core writes at a time, no conflicts
- Site nodes distributed across the two cores by "home core" — **load sharing**, no idle capacity
- Node redundancy via multiple RADIUS/TACACS+ server entries on the switch side

### Change safety

- Policy and device records distributed as a **signed generation**; expiry and rollback
- Decision stages: validated → applied → verified (read back from the device)
- Software updates with a signed package, A/B installation, one-step rollback
- Backup / restore screen; integrity with manifest and checksum

### Licensing and operation

- Even when the licence expires, **authentication does not stop**; only management functions warn
- Password policy and brute-force lockout; secrets masked on screen and in logs, backup files accessible only to the administrator
- Small node fully featured: all functions on 4–8 GB of memory

## Failure Scenarios

**WAN goes down**
The site node continues on the last policy; events accumulate and are forwarded on return

**Core fails**
The standby core takes over; the site is uninterrupted; hands back when the primary returns

**Site node fails**
The switch falls back to the second node; the load-sharing peer node answers

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

06

AAA AND PKI

# Device Administration and Certificate Infrastructure

Who logged into a switch, router or time server, with which privilege, with which command — all defined at the centre and recorded. Device certificates are issued, distributed, monitored and revoked by the built-in PKI; **no certificates carried by hand**.

## RADIUS device administration

- Administrator login via RADIUS: privilege level (admin / operator / viewer), Service-Type and vendor attributes
- RFC 2865/2866/2869; **Message-Authenticator mandatory in both directions** — closed to BlastRADIUS-class attacks
- Accounting (Start / Interim / Stop); session duration and re-authentication
- **RadSec** (RADIUS/TLS, RFC 6614) server; Status-Server
- Built-in role mapping on Simgenet products (RFC 5607 privilege level); standard attributes on third-party devices

## TACACS+ device administration

- **RFC 8907 TACACS+**: authentication; session privilege level 0–15; **command authorization** — administrator-defined command sets (permit/deny patterns, assignment to a user or privilege-level range, default permit/deny) and built-in classes (view / all but configure / full); every command decision in the audit log; accounting
- **TACACS+ over TLS 1.3 (RFC 9887)** — management traffic encrypted
- Local fallback account policy on the device when the server is unreachable
- Device-administration AAA served from the core and the standby core; the switch knows both as servers

## Built-in PKI

- Internal certificate authority (CA), profile-based issuance, random serial numbers
- **SCEP (RFC 8894)** and **EST (RFC 7030)** for automatic device enrolment and renewal; old certificate revoked automatically on re-enrolment
- **OCSP** responder and CRL (signed distribution to sites); revocation check in EAP-TLS — a revoked certificate is rejected immediately
- Certificate-lifetime alarms (90 / 60 / 30 days); "next certificate installed" indicator

## Identity sources and trust

- Local user and device database; LDAP/AD directory; external RADIUS and TACACS+ identity sources
- Time trust is part of the decision: GNSS/NTP source and certificate validity window
- Role-based access for administrator accounts; **administrator audit log** including failed logins
- RADIUS attributes and MIB under our own enterprise identity (OID)

TACACS+ command decisions

```
user       priv   command              decision
operator   1      show version         PERMIT
operator   1      show running-config  DENY (pattern)
operator   1      configure terminal   DENY (default)
admin      15     configure terminal   PERMIT (full)
every decision → log + audit event
```

WHY? diagnosis

```
MAC 00:18:f8:09:cf:d7
switch   10.10.0.2  Gi1/0/5
method   MAB   profile ControlRTU
rule     ControlRTU → VLAN 30
         (generation 4, core-signed)
decision ACCEPT · VLAN 30
```

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

MANAGEMENT

# 07 Web Panel, Monitoring and Integration

Simple menu, table logic, the answer on one screen. The panel manages network devices, device records and policies with role-aware screens; the field engineer sees their own node, the central administrator the whole fleet.

## Web panel (HTTPS, EN/TR)

- **Status dashboard:** continuity mode, accept / reject / monitoring (24 h), authoritative policy generation, CPU/RAM/disk, decision rate, data age, latest decisions, alarm badge
- **Live authentication log** — every attempt, failure reason, authentication method, policy generation
- Menu: **Status · Devices · Switches · Audit · Simgenet NAC · Alarms · System**; under Simgenet NAC: role, sites, signed distribution, core HA, continuity, WHY?, switch recipes, certificate diagnosis, device profiles, emergency override, daily reports
- Role-aware view: admin / operator / viewer; only site items in the Site role; EN / TR / FR

## Alarms, events and reports

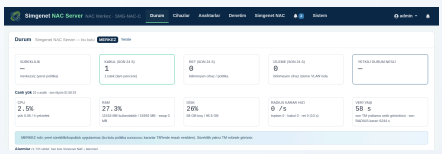
- Alarm management with **X.733** severities (critical / major / minor / warning): Alarms screen, acknowledgement, aggregated alarms, closure history, "to do" column; critical alarms in the top bar; thresholds configurable
- Event log: who, from where, when; no secrets in any record
- **Daily report**: decisions, events, administrator logins, end-of-day state; JSON/CSV export and API; 730-day retention
- **Support bundle** in one click: everything needed for diagnosis, personal data masked

## NMS / SIEM integration

- **SNMPv3** (authPriv) monitoring; SIMGENET-NAC-MIB; event → notification (trap)
- **Syslog CEF**, end-to-end over TLS (RFC 5425); directly to the SIEM
- **REST API** — device registration, policy, reports, automation
- Verified with common NMS and SIEM systems

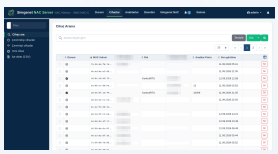
## Installation and operation

- **NAC Core: Simgenet SMG-NAC104 (1U 19" rack)**; site node on Simgenet hardware or a virtual machine; core and site node are the same image, the role is chosen on one screen at installation
- Site-node installation: core address + registration token (2 fields) → automatic registration, policy and certificate download themselves
- HTTPS; password policy; brute-force lockout
- Ready templates: 802.1X EAP-TLS, MAB, device administration, OT profiles, switch recipes; switch and device registration in 1 form each; policy = role→VLAN table + compile → sign → deploy



### Status dashboard

Continuity mode, accept/reject/monitoring, policy generation, live load.



### Device records

MAC, role, switch/port, last seen; filtering and CSV.

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

08

CAPACITY AND USE

# Scale, Scenarios and Acceptance

A capacity figure means nothing on its own; what matters is **all devices arriving at once on the morning shift, every substation in a region managed from a single pair of cores, and the site running through a WAN outage**. Values were measured with Simgenet SVP.

### 400K+ / day

Decisions measured on a single site node; decisions made in the field, in the millisecond class

### 30 days

Operation without the core — authentication and VLAN decisions uninterrupted on the last approved policy

### < 5 min

Core takeover (failback < 6 min) — measured in a 9-site fleet with 3 scenarios; policy distribution to 9 sites < 2 min

## What this capacity means

- **The 08:00 storm:** even if every IED, PC and camera in a substation arrives at once, the site node answers them all within seconds
- **One region, one pair of cores:** dozens of substations / stations, each with a site node, managed from one core + one standby core
- **WAN outage:** the site node runs up to 30 days on the last approved policy; the difference closes automatically on return
- **Failure under load:** takeover and failback times were measured under load

## Acceptance test (with SVP)

- 802.1X / MAB / dynamic VLAN / CoA vectors — with known-PASS and known-FAIL controls
- RADIUS security: Message-Authenticator, malformed-packet corpus, replay attack
- TACACS+ authorization and command authorization; behaviour under load and malformed-packet floods
- Capacity scale test; core takeover / failback; result as a lockable report

## Power / substation

Registration of IEDs, PLCs, RTUs and recorders via MAB/EAP-TLS; policy by timing- and protection-port class; regional core + standby core; switch/router management via TACACS+; IEC 62443-aligned records.

## Rail / industrial plant / government

Rejection of non-inventoried devices on station and plant networks, gradual transition from monitoring to enforcement, local continuity with the site node, one policy from the centre; central records of administrator access on government networks.

**An ecosystem unique to Simgenet.** The switch (SMG-SW), the time server (GNSS Server), the test platform (SVP) and access control come from the same company: enforcer, decision-maker and measurer from one source; an evidence-based report is delivered.

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

09

TECHNICAL SPECIFICATIONS

# Simgenet NAC Server

| FEATURE | SIMGENET NAC SERVER |
|---|---|
| **Product class** | Industrial network access control (NAC) and device-administration AAA server; software developed entirely in house at Simgenet |
| **Roles** | NAC Core (SMG-NAC-C) · NAC Site node (SMG-NAC-S) · Standby Core — same software image, role chosen at installation |
| **Authentication** | IEEE 802.1X-2020 EAP-TLS (RFC 5216) · PEAP / EAP-TTLS (local user DB) · MAB · rejection of unregistered devices / monitoring VLAN mode · MAC-spoofing suspicion detection · re-authentication (RFC 2865 Session-Timeout / Termination-Action) |
| **Authorization** | Role → VLAN (RFC 3580 Tunnel-*) · Filter-Id → access list · dynamic ACL via vendor attributes · port class (timing / protection / general) · quarantine · time-limited emergency override (break-glass, audited) |
| **Dynamic authorization** | CoA and Disconnect (RFC 5176, port 3799), Error-Cause; fallback path for switches without CoA |
| **RADIUS** | RFC 2865 / 2866 / 2869 · Status-Server (RFC 5997) · Message-Authenticator mandatory both ways (BlastRADIUS-protected) · RadSec (RFC 6614) server · accounting · privilege level (RFC 5607) · vendor attributes (enterprise OID) |
| **TACACS+** | RFC 8907 — authentication (ASCII/PAP); authorization: session privilege level 0–15 and command authorization — administrator-defined command sets (permit/deny patterns, assignment to a user or privilege-level range, default permit/deny), built-in classes (view / all but configure / full); every command decision in the audit log; accounting · TACACS+ over TLS 1.3 (RFC 9887) |
| **PKI** | Internal CA · profile-based issuance, random serial (RFC 5280) · SCEP (RFC 8894, challenge password) · EST (RFC 7030; incl. ECDSA, old certificate revoked on re-enrolment) · OCSP (RFC 6960) · CRL (signed distribution to sites) · EAP-TLS revocation check · lifetime alarms 90/60/30 days · renewal/revocation records in the audit log |
| **Profiling / inventory** | Passive collector (OUI, DHCP, SNMP) · OT device library (relay, RTU, PLC, IED, GNSS/PTP) · device records and groups · bulk import · API |
| **Continuity** | Local decision table and last approved policy on the site node; modes normal / restricted / continuity; 802.1X/MAB and dynamic-VLAN decisions uninterrupted when the core is lost — up to 30 days (configurable); device-administration AAA (RADIUS/TACACS+) served from the core and the standby core |
| **HA / distribution** | Standby core (automatic takeover / failback, single writer) · site nodes distributed across the two cores by "home core" (load sharing) · signed generation distribution (offline signing key, expiry, rollback) · decision stages validated → applied → verified |

**Continued on the next page:** management, monitoring, security, capacity, installation and reference standards.

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

TECHNICAL SPECIFICATIONS

# 10 Management, Security and Capacity

| FEATURE | SIMGENET NAC SERVER |
|---|---|
| **Management** | HTTPS web (EN/TR/FR; role-aware admin / operator / viewer; Site scope) · external TACACS+/RADIUS/LDAP for administrator login · REST API · CLI · device administration (TACACS+) screen: NAS list, command sets, assignments · live decisions · "WHY?" screen · templates and switch recipes · support bundle (secret-free) |
| **Monitoring** | SNMPv3 (authPriv) + SIMGENET-NAC-MIB + notifications · X.733 alarm management (acknowledgement, aggregated alarms, closure history) · thresholds · time-trust monitoring (PTP/GNSS NTP) · daily report (JSON/CSV/API, 730 days) · common diagnostic event schema (SMG product family) |
| **Logging / SIEM** | Syslog CEF (RFC 5424), over TLS (RFC 5425) · administrator audit log (incl. failed logins) · time-stamped decision log · retention and rotation policy · secret-free records |
| **Security** | IEC 62443-4-2 principles (least privilege, session/lockout, audit) · password policy and brute-force lockout · secrets masked on screen and in logs; backup files accessible only to the administrator · time trust (GNSS/NTP) part of the decision |
| **Backup / update** | Backup / restore screen (manifest + checksum, confirmed) · signed software package, A/B installation, rollback · rollback within a policy generation |
| **Capacity (measured)** | Single site node 421,000+ decisions/day · core takeover 161–245 s, failback 234–315 s (9 sites, 3 scenarios) · operation without the core up to 30 days · policy distribution to 9 sites < 2 min · report retention 730 days · concurrent-client and NAS capacity by scale test per project |
| **Identity sources** | Local user/device database · LDAP / AD · external RADIUS · external TACACS+ · certificate (EAP-TLS) · MAC inventory |
| **Integration** | SMG-SW switch / SMGOS router (802.1X, MAB, dynamic VLAN, Filter-Id, CoA, device-administration AAA, common CA) · Simgenet GNSS Server (management AAA, CoA, time trust) · Simgenet SVP (conformance vectors) · third-party switches/APs via standard RADIUS/TACACS+/CoA, ready recipes |
| **Hardware and installation** | **NAC Core: Simgenet SMG-NAC104** — 1U 19" rack, Intel® Xeon® E3-1200 v5, DDR4 up to 64 GB, 4 × PCIe Gen3 x8, 220 VAC 250 W, −20…+60 °C, IEC 61000-4 Level 3 · **NAC Site:** Simgenet hardware or virtual machine · Core 4 vCPU / 8 GB / 100 GB · Site 2–4 vCPU / 4–8 GB / 60 GB · site installation: image + registration token → automatic registration |
| **Languages** | EN / TR / FR |
| **Out of scope** | Cloud/SaaS · posture/compliance agent · guest/captive portal · BYOD self-service · Wi-Fi controller function |

## Reference Standards

IEEE 802.1X-2020 · RFC 5216 (EAP-TLS) · RFC 2865 / 2866 / 2869 (RADIUS) · RFC 5997 · RFC 3580 · RFC 5176 (CoA) · RFC 5607 · RFC 6614 (RadSec) · RFC 8907 (TACACS+) · RFC 9887 · RFC 7030 (EST) · RFC 8894 (SCEP) · RFC 6960 (OCSP) · RFC 5280 · RFC 5424 / 5425 (syslog) · 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

# Why Simgenet NAC Server

### The centre goes down, the site keeps running

The site node works from a local decision table and the signed last policy; the standby core takes over; the standby node shares the load.

### For industrial devices

Certificate-based 802.1X and MAB; gradual transition from monitoring to enforcement for IEDs, PLCs, RTUs and cameras; timing-port awareness.

### Device administration and PKI built in

Who ran which command, via RADIUS and TLS-protected TACACS+; internal CA, SCEP/EST, OCSP — no certificates carried by hand.

### Original, ecosystem, proven

Software entirely developed in house at Simgenet; switch, time and test platform from one source; acceptance delivered with an SVP report.

GET IN TOUCH


Address
**Kartal / İstanbul, Türkiye**

Phone
**+90 555 600 4506**

E-mail · Web
**info@simgenet.net · simgenet.net**

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



Product Brochure · SMG-UB-NAC-EN · Rev. 3 · © 2026


**Engineered in Türkiye**