



Altos NAC: control access to your network

Identify every connection, decide the right access automatically and keep the proof.

SOLUTION · NETWORK ACCESS CONTROL

YOUR CHALLENGES

Is your network really under control?



Unknown devices

Any device plugged in gets access.



VLANs managed by hand

Every move requires an intervention on the switch.



No traceability

Impossible to say who was connected, where and when.



Poorly managed guests and Wi-Fi

Shared keys, access too broad for visitors.

Three functions, one decision engine



Identify and authenticate

802.1X certificate, MAC address or portal: every connection is recognised.



Authorise dynamically

VLAN, voice or quarantine assigned according to the decision, with no intervention.



Prove and audit

Every decision is logged and exportable to your SIEM.

FROM PLUG-IN TO DECISION

A decision in five steps

01

Connection

A device plugs in or joins the Wi-Fi.

02

Request

The switch queries the NAC over RADIUS.

03

Decision

Identity, role and device state evaluated.

04

Enforcement

VLAN, voice VLAN or quarantine applied.

05

Follow-up

Status change: reclassification by CoA.

Each device, its access method



802.1X by certificate

Corporate PCs, no password to type



Controlled MAB

Printers and IoT recognised by MAC address



Guest portal

Sign-up by SMS code, "My devices" list



Wi-Fi iPSK

One key per device, individually revocable



Dynamic VLAN

Quarantine and groups by certificate



IP telephony

Voice VLAN assigned by traffic class

Complete visibility of your estate



Live inventory

MAC, IP, VLAN, port and status of every device



IPAM and DNS

Synchronisation with your existing tools



SNMPv3 monitoring

Encrypted polling of switches



Reports

Periodic reports sent by email



SIEM export

Decision log in JSON format



AD / LDAP directory

Roles and groups from the directory

Observe first, enforce later



Observation mode

The NAC decides and logs, but lets everything through.



Correction

Inventory, certificates and exceptions handled.



Enforcement mode

Decisions enforced, with the option to return to observation.

A security tool that protects itself



HTTPS enforced

TLS-only interface, with HSTS



Two-factor authentication

Mandatory TOTP code, backup codes



Separate roles

Separated rights, protected network core



Protected secrets

Protected variables or Vault



Internal PKI

Issuance, revocation, alert before expiry



Audit log

Administrator actions traced

WHY ALTOS NAC

Ready for production



Shared PostgreSQL database

Several instances, least-privilege accounts.



Daily backup

Database, encryption key and configuration.



Tooled installation

Pre-deployment, deployment, verification and rollback, with no Internet on the server.



Quality verified in the lab

More than 600 automated tests; on-site validation to be planned with you.



Let's talk about your project, simply

A first conversation, no commitment. Contact: Serigne Ousmane, 00221
77 345 49 09, serigneousmane@altosystems.com

 **00221 77 345 49 09**

 **serigneousmane@altosystems.com**

 **www.altosystems.com**

 **Avenue Peytavin, Dakar**