Genian NAC

Next-Gen Network Access Control for the IoT era

ARCHITECTURE

Completely out-of-band, Highly scalable

Genian NAC uses Layer 2 based non-disruptive sensing technology powered by its Device Platform Intelligence.

- Validate device platform information via the cloud
- Delivers the most accurate up-to-date device platform information to Policy Servers on a weekly basis

- Establishes security policies based on Node information collected by Network Sensors and Agents
- Distributes established policies to Network Sensors and Agents
- Integrates with user database and third-party security solutions
- Includes Built-in DHCP, RADIUS, Syslog server

Policy Server

* Can be hosted On-Prem or in the Cloud

- Scans and assesses networks (Wired, Wireless, Virtual)
- Detects all SSIDs by listening wifi signals
- Identifies who is accessing enterprise-owned, neighbor or rogue APs
- Enforces access control policies
- Supports 802.1q Trunk Port

Network Sensor

Agent

* Optional

- Manages installed HW/SW information
- Detects state changes in real time
- Performs incremental updates
- Controls all desktop configurations
- Provides Wireless Connection Manager (EAP-GTC)
- Supports Windows/macOS /Linux
- Lightweight Agent

You can install the Policy Server and Network Sensor software in either your Virtual or Physical machines (Intel Xeon or equivalent).

Actionable Intelligence For Cybersecurity

Genians has reimagined Network Access Control to maximize network security and IT operational effectiveness by leveraging its distinct Device Platform Intelligence (DPI).

DPI provides extremely accurate IT asset identification/classification based on its robust DPI, which allows for the full interrogation and gathering of all device platform information, combining technology-specific with business-contextual and risk-level data. DPI can enrich the way to manage IT security policices at a granular level.

Essential Cybersecurity Solutions

Delivers the major solutions that encompass both IT security and operations management very effectively.

- Network Surveillance
- Network Access Control
- Mobile, BYOD, Guest Management
- IP Address Management (IPAM)
- Switch Port Management
- WLAN Security
- Endpoint Security
- IT Security Automation

Multi-layered Access Control

Delivers the major solutions that encompass both IT security and operations management very effectively.

- Layer 2: ARP Poisoning (using Network Sensor)
- Layer 3: TCP reset (using Mirror Sensor)
- Layer 3: Inline enforcer (Dual-homed Gateway)
- Agent: NIC/Power Control, Alert Popup
- Built-in RADIUS server (802.1x)
- Built-in DHCP server

Interoperability

Integrates a wide range of IT security and business solutions (Firewall, IDS/IPS, VM, MDM, SIEM, APT, DLP, CMDB etc.) into each enterprise's Policy Server to ensure unified policy enforcement. Genian NAC supports custom integration using SNMP, Webhook, REST API, and Syslog.

Personalization

Monitors your network through personalized dashboards (Over 100 custom widgets to meet your network management needs).

Pricing

Simple! Genian NAC license model is based on the number of active devices. Nothing else.
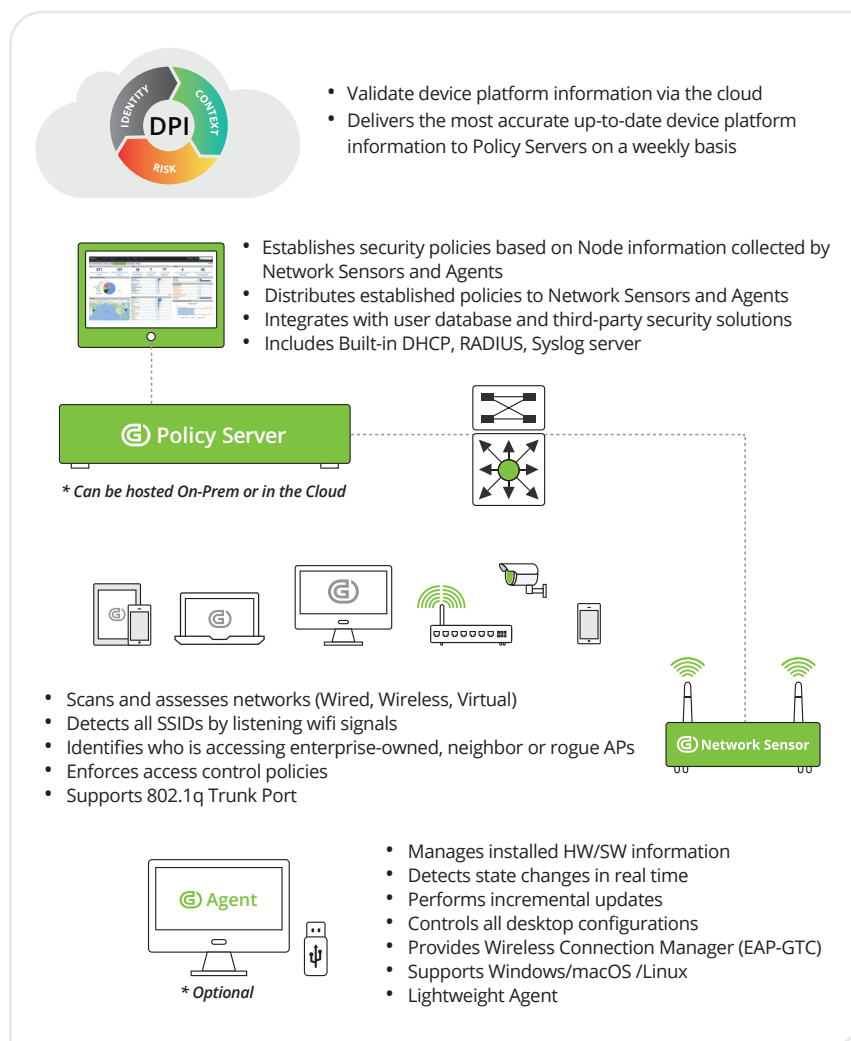
EDITIONS & VERSIONS

You Choose, We Deliver

Choose the edition that best meets your business requirements. Upgrade between editions as your network evolves without losing your original investment.
The editions can be delivered in 3 different ways:

	BASIC Network Surveillance	PROFESSIONAL Network Access Control	ENTERPRISE Automation
On-Premises	Free up to 300 devices*	30 days free trial	Contact a Genians Partner
Cloud-Managed Policy Server in the Cloud	30 days free trial Support up to 3,000 devices*		
MSP-Ready NAC as a service	Contact Genians		

* Only count the number of active devices

EDITIONS & FEATURES

CATEGORY	FEATURES	BAS	PRO	ENT
Visibilty	Detect/Monitor IP-enabled Device	•	•	•
	Device Platform Intelligence (Name, Type, Picture, EOL, Connection, CVE)	•	•	•
	Switch Port Information	•	•	•
	WLAN Monitoring / Security (Rogue AP)	•	•	•
	Basic Endpoint Information (OS, HW, Software) by Windows/macOS Agent	•	•	•
	Condition based Dynamic Node Group	•	•	•
	Customizable Dashboards (Over 100 Widgets)	•	•	•
	Track Changes / Audit Logs	•	•	•
	Network Anomaly Detection (MAC Spoofing, Rogue Gateway, Ad-hoc)	•	•	•
	Basic Reports (Node, WLAN, Log)	•	•	•
	Custom Reports		•	•
User Authentication	Captive Portal Login		•	•
	Active Directory SSO		•	•
	External User Directory Integration (LDAP/RADIUS/SMTP/POP3/IMAP)			•
	Multifactor Authentication (For both Admin and User)	•	•	•
Network Access Control	Role based Access Control		•	•
	ARP based Layer 2 Control		•	•
	802.1x based Control (RADIUS Server)			•
	Port Mirroring (SPAN) based Control		•	•
	Switch integration (SNMP) based Control		•	•
	DHCP Server		•	•
Desktop Management	Compliance Check (Antivirus, Required SW,HW, Desktop Settings)		•	•
	OS Configuration (Screenlock, Internet Options, DNS)			•
	OS Updates			•
	External Device Control (USB)			•
	802.1x Connection Manager			•
	WLAN Control (SSID Whitelist, SoftAP block)			•
Integration	User Directory Sync (RDBMS, LDAP)			•
	Webhook / Syslog / SNMP trap (Outbound)			•
	REST API (Inbound)			•
	Syslog Listener (Inbound)			•
Business Process	Consent Pages			•
	Request/Approval Process (IP, Device, User, External Device)			•
	Role based Administrator			•
	Customized Fields (Node, Device, User)			•
	Captive Portal Pages for Purposes			•
	Multilingual Support			•
Scalability and Availability	High Availability (Policy Server / Network Sensor)			•
	Interface Channel Bonding			•
	Disastor Recovery (DB Replication, Policy Server Backup)			•