infoexpress

EasyNAC

EasyNAC is an agentless Network Access Control (NAC) solution that is simple to deploy and offers stronger security than traditional NAC solutions.The EasyNAC appliance utilizes ARP enforcement to deliver a true plug-and-protect solution, requiring no network changes, infrastructure modifications, or spanning ports.

Simple Control, Strong Security

www.easynac.com

sales@infoexpress.com | 2975 Bowers Avenue, Suite 323, Santa Clara, CA 95051 USA | Phone: +1 650-678-1541

v3.2.260127

EasyNAC

Simple Control ♦ Strong Security

infoexpress

www.easynac.com

OVERVIEW

EasyNAC is an agentless Network Access Control (NAC) solution that enhances security without network changes. It uses ARP enforcement to manage access, eliminating any network changes.

The EasyNAC appliance monitors devices across multiple subnets, quarantining unauthorized endpoints in real time. It supports flexible deployment, including physical connections, 802.1q trunk ports, and remote sites. It ensures seamless device access management while maintaining high network security with minimal complexity.

VISIBILITY / DEVICE PROFILING

EasyNAC allows you to see devices that join your network without requiring agents. Visibility is instant, enabling you to restrict untrusted devices immediately as needed. Devices are both passively and actively profiled to identify their operating system, manufacturer, and type.

LAN / VPN PROTECTION

EasyNAC utilizes ARP enforcement, DNS, and HTTP redirection to instantly detect and block unknown devices from joining the LAN. ARP enforcement operates as an out-of-band method, seamlessly working with any network infrastructure, including both managed and unmanaged switches, without requiring network changes. For VPN protection, it can be configured in-band to allow only authorized and compliant devices.

DECEPTION HACKING DETECTION

Leverage deception technology with a maintenance-free, distributed honeypot deployed across every subnet. This feature enables real-time detection of hacking attempts and malicious connections with near-zero false positives.

POSTURE ENFORCEMENT

EasyNAC integrates with enterprise AV/XDR vendors and leading endpoint management solutions to ensure endpoint security is active and up-to-date. Non-compliant devices can be restricted at the point of network access—no agents required. For advanced compliance needs, agents can be utilized.

ANTI-SPOOFING PROTECTION

EasyNAC includes a fingerprinting feature to protect against MAC address spoofing. All devices on the network are profiled based on their MAC address, IP, operating system, hostname, and more. This information is then used to create a unique fingerprint for each device.

AUTOMATED THREATS RESPONSE

EasyNAC can receive alerts via an API, event-based syslog or email messages from various security appliances and take immediate action when needed. If EasyNAC detects an alert indicating a device is infected with malware, it can instantly restrict network access. Additionally, EasyNAC offers Layer-2 security: ARP security and Malware Lateral Spread Protection to prevent worms or malware from spreading within the LAN.

SIMPLE TO DEPLOY

EasyNAC is a plug-and-protect appliance. Its agentless design enables rapid deployment and delivers immediate benefits. Devices can be granted access using simple ON/OFF controls, or policies can be configured for automated trust.

AUTOMATED ZERO TRUST

EasyNAC regularly checks with your Active Directory and XDR servers to verify domain-joined and trusted devices. Trusted devices can then be automatically granted full network access. Additionally, device profiling can streamline the approval process for IoT devices.

BYOD AND GUEST REGISTRATION WITH ROLE-BASED ACCESS CONTROL

EasyNAC offers a self-registration portal to streamline the BYOD (Bring Your Own Device) registration process. Policies can be configured by groups to control the number and type of BYOD devices allowed. Sponsors can pre-register guests or approve self-registered users through the captive portal. This enhances security by enforcing least privilege access—guests can be restricted to internet-only access, while BYOD and consultant devices are limited to approved resources.

CENTRAL VISIBILITY MANAGER (CVM)

EasyNAC
Simple Control ♦ Strong Security

The Central Visibility Manager (CVM) provides consolidated reporting and simplifies the management of multiple EasyNAC appliances. Key features of CVM include:

ADMINISTRATIVE PRIVILEGE MANAGEMENT

With CVM, administrative privileges can be managed so regional IT staff only have administrative access to the appliances and functionality relevant to their roles.

CENTRALIZED MANAGEMENT AND REPORTING

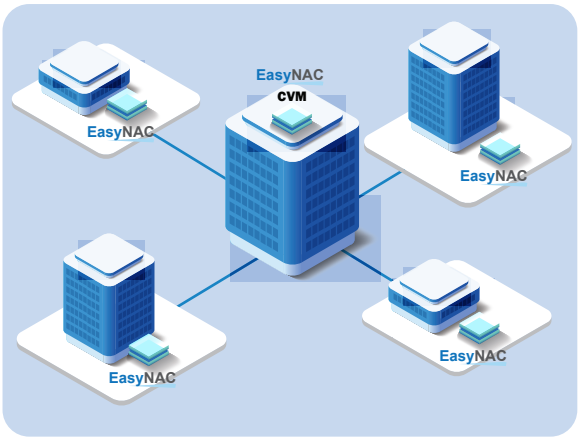
CVM also automates appliance backups and simplifies firmware \ update management. Reports from multiple appliances are consolidated and can be viewed as a whole or by regions.

DEPLOYMENT MANAGER

The deployment manager makes it easy to selectively syncronize settings between appliances. Preferred settings can be quickly uploaded to multiple appliance(s) on-demand.

DISTRIBUTED LICENSE MANAGEMENT

CVM offers a flexible licensing model, allowing a single bulk license to be divided and shared across multiple appliances. Customers can easily reallocate licenses as needed to align with changing business requirements.



TRANSPARENT DEVICE ROAMING

CVM enables trusted devices to move between offices while maintaining a seamless experience for end users.

EXTENDING PROTECTION

EasyNAC utilizes dedicated appliances to deliver strong network visibility and protection. For optimal operation, Layer 2 visibility within protected subnets is required. In environments where VLANs do not span across geographic locations, achieving this visibility at remote sites requires local enforcement.

To address this requirement, EasyNAC uses the Enforcer Sensor. The Enforcer Sensor can be deployed as software on Windows and Linux systems, or as a dedicated hardware option using supported Raspberry Pi devices. By placing an Enforcer Sensor locally at each branch, EasyNAC provides full Layer 2 visibility and protection without extending VLANs back to headquarters.

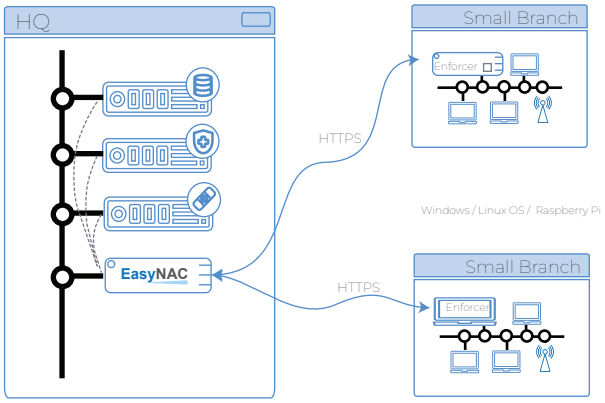
This approach ensures consistent enforcement, simplified architecture, and scalable protection across distributed environments.

ENFORCER SENSOR

The enforcer sensor communicates with the EasyNAC appliance to report, in real-time, the devices present on the local network. The EasyNAC appliance then profiles these devices and instructs the Enforcer Sensor on the appropriate access policies to enforce ARP-based enforcement locally.

Both MPLS and NAT'd network environments are supported. In NAT'd networks functionality may be reduced as the EasyNAC appliance may not be able to fully profile devices behind NAT.

Adding an Enforcer Sensor to extend EasyNAC protection to remote sites is a straightforward process: install the Enforcer Sensor software or image, then approve the sensor through the EasyNAC management interface for immediate visibility and control.



ENFORCER SENSOR SYSTEM SPECIFICATION AND REQUIREMENT

	Supported OS / Platform	Requirement	Recommended Subnets & Devices
Windows	Windows 10+ (x86 64bit)	Dual-Core CPU / 4GB RAM	10 subnets / 300 devices
Linux	AlmaLinux, Debian, Rocky Linux, Ubuntu (x86 64bit)	Dual-Core CPU / 4GB RAM	25 subnets / 500 devices
Raspberry Pi	EasyNAC Raspberry Pi OS	Raspberry Pi 4 or 5 / 4GB RAM / 64GB Storage	10 subnets / 300 devices

infoexpress

EasyNAC

Simple Control ♦ Strong Security

EASYNAC AGENT

The EasyNAC agent is an optional software component that improves the speed and depth of device posture assessment across Windows, macOS, and Linux systems. While EasyNAC already provides agentless network visibility and compliance checks, deploying the agent enables faster detection—typically within 10 seconds—and more detailed endpoint insight. It also allows real-time communication with users through pop-up messages.

When a compliance check fails, automated remediation actions can be initiated on the host system. These may involve executing custom scripts or programs—for example, triggering an update of endpoint protection software if it's outdated or inactive. This streamlines endpoint correction without requiring manual IT intervention.

In addition to enhanced posture assessment, the agent can control Wi-Fi adapters to prevent network bridging when a wired connection to the NAC appliance is present. This further strengthens policy enforcement and helps maintain a secure network environment.

EASYNAC APPLIANCE SYSTEM SPECIFICATION

	S10	S100	S200	S500	S600	ENAC-VM
Network Interfaces	4 x 1GbE	6 x 1GbE, 2 x 10G SFP+	6 x 1GbE, 2 x 10G SFP+	4 x 1GbE, 2 x 10GbE 2 x 10G SFP+	8 x 1GbE, 2 x 10G SFP+	10 x Virtual NICs
Maximum Devices*	300	2,500	5,000	10,000	10,000	10,000
Maximum Subnets*	20	250	400	400	400	400
VLAN Trunking	Yes	Yes	Yes	Yes	Yes	Yes
ARP Enforcement (Out of Band)	Yes	Yes	Yes	Yes	Yes	Yes
Inline Enforcement (VPN)	-	Yes	Yes	Yes	Yes (2 Pairs of By-pass NICs)	Yes
High Availability*	Yes	Yes	Yes	Yes	Yes	Yes

EASYNAC HARDWARE APPLIANCES SPECIFICATION

	S10	S100 / S200	S500	S600
				
Form Factor Height x Width x Depth	Mni-ITX 44.5mm x 195mm x 195mm	Mini-1U - Rack Mountable 43mm x 254mm x 226mm	1U - Rack Mountable 43mm x 437mm x 249mm	1U - Rack Mountable 44mm x 430mm x 450mm
Input Voltage	+12V DC - Power Adapter	+12V DC - Power Adapter	100v - 240V AC, 50 - 60 Hz	100v - 240V AC, 50 - 60 Hz
Power Configuration	ACPI Power Management Power-on Mode for recovery from AC power loss		200W Low Noise AC - DC power supply with PFC 80 Plus Gold Certified	300W Low Noise AC - DC power supply
Temperature	Operating Temperature: 0°C to 40°C (32°F to 104°F) Non-Operating Temperature: -40°C to 70°C (-40°F to 158°F)			Operating Temperature: 0°C to 45°C (32°F to 113°F) Non-Operating Temperature: -20°C to 70°C (-4°F to 158°F)
Electromagnetic Emission RoHS	FCC Class B, EN 55022 Class B, EN 61000-3-2/3-3, CISPR 22 Class B. / RoHS Compliant	FCC Class A, EN 55022 Class B, EN 61000-3-2/3-3, CISPR 22 Class A. / RoHS Compliant	FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 32 Class A. / RoHS Compliant	FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3 / RoHS Compliant
Electromagnetic Immunity	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)		EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11), CNS14336-1, CNS13438, GB4943.1-2011, GB9254-2008(Class A) and GB17625.1-2012	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11), EN 62368-1:2014+A11:2017
Safety	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)			CE Class A, SI 2016/1091,SI 2019/492, SI 2016/1101

* Capacity figures are approximate and may vary based on factors such as network topology, number of endpoints, VLANs protected, and features enabled. For example, the S500 model can support up to 10,000 devices across 100 VLANs, or approximately 5,000 devices when 200 VLANs are configured.High Availability (HA) is supported and requires identical hardware or matching hypervisor environments. A minimum of 8 GB of RAM is recommended for optimal performance.

infoexpress

EasyNAC

Simple Control ♦ Strong Security

EASYNAC VIRTUAL APPLIANCES SPECIFICATION

	Virtual Appliance Requirements
Supported Hypervisor	Microsoft Hyper-V | Nutanix AHV | Proxmox VE | VMware ESX
Minimum Specs: 100+ devices	2 vCPU / 4 GB RAM
Minimum Specs: 500+ devices	4 vCPU / 8 GB RAM
Minimum Specs: 1,000+ devices	4 vCPU / 16 GB RAM
Minimum Specs: 5,000+ devices	8 vCPU / 32 GB RAM
Virtual Storage Capacity	40GB to 512GB

EASYNAC AGENT SUPPORTED PLATFORM

	Supported OS	Automatic Remediation
Windows	Persistent: Windows 7 SP1+, 2008+ (32/64-bit) On-demand: Windows 10+ (64-bit)	Yes (Persistent) Yes* (On-demand – depends on user permissions)
macOS / Linux	macOS: OS X 10.9+ Linux: Kernel 4.12+ (x86)	macOS: Yes Linux: No

CENTRAL VISIBILITY MANAGER (CVM) SYSTEM SPECIFICATION

	CVM-S100-HW	CVM-S200-HW	CVM-S500-HW	CVM-Virtual
Maximum Appliances	50	100	200	200
Maximum Devices	25,000	50,000	200,000	200,000
Platform Supported	Hardware Appliance			On-Premises: Microsoft Hyper-V, Nutanix AHV, Proxmox VE, VMware ESX Cloud: Amazon AWS, Microsoft Azure

CENTRAL VISIBILITY MANAGER (CVM) HARDWARE APPLIANCE SPECIFICATION

	CVM-S100-HW	CVM-S200-HW	CVM-S500-HW
Form Factor Height x Width x Depth	Mini-1U - Rack Mountable 43mm x 254mm x 226mm	Mini-1U - Rack Mountable 43mm x 254mm x 226mm	1U - Rack Mountable 43mm x 437mm x 249mm
Input Voltage	+12V DC - Power Adapter	+12V DC - Power Adapter	100v - 240V AC, 50 - 60 Hz
Power Configuration	ACPI Power Management Power-on Mode for recovery from AC power loss		200W Low Noise AC - DC power supply with PFC 80 Plus Gold Certified
Temperature	Operating Temperature: 0°C to 40°C (32°F to 104°F) Non-Operating Temperature: -40°C to 70°C (-40°F to 158°F)		
Electromagnetic Emission RoHS	FCC Class B, EN 55022 Class B, EN 61000-3-2/3-3, CISPR 22 Class B. / RoHS Compliant	FCC Class A, EN 55022 Class B, EN 61000-3-2/3-3, CISPR 22 Class A. / RoHS Compliant	FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 32 Class A. / RoHS Compliant
Electromagnetic Immunity	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)		EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11), CNS14336-1, CNS13438, GB4943.1-2011, GB9254-2008(Class A) and GB17625.1-2012
Safety	CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)		

CENTRAL VISIBILITY MANAGER (CVM) VIRTUAL APPLIANCES REQUIREMENT

	Virtual Appliance Requirements
Supported Hypervisor	On-Premises: Microsoft Hyper-V, Nutanix AHV, Proxmox VE, VMware ESX. Cloud: Amazon AWS, Microsoft Azure
Minimum Specs: 10 appliances	4 vCPU / 8 GB RAM
Minimum Specs: 25 appliances	4 vCPU / 12 GB RAM
Minimum Specs: 100 appliances	4 vCPU / 16 GB RAM
Minimum Specs: 200 appliances	8 vCPU / 32 GB RAM
Virtual Storage Capacity	40GB to 512GB

infoexpress