EASY NAC

TECHNICAL FAQ

www.easynac.com

v2.3 -190404

CONTENTS

Overview

Q. WHAT IS EASY NAC?

Easy NAC is a Network Access Control solution specifically designed to be simple, easy to use, and cost effective. Easy NAC provides visibility and access control over all devices on the LAN and wireless network. It enhances security by preventing unknown devices from joining the network, enforces baseline security, ensures BYOD devices are properly registered, and guest accounts are managed. Easy NAC also integrates with Firewalls, APTs, and other security appliances so it can quickly quarantine unauthorized devices.

Q. WHAT MAKES EASY NAC UNIQUE?

Although NAC has a reputation of being difficult and expensive, Easy NAC is an agent-less NAC solution that is simple and affordable, because it doesn't make changes to the network. No switch, endpoint, or spanning port configuration is required. At the same time, Easy NAC has granular access control, complete network visibility, and remote site connectivity options making it the simplest NAC solution for centralized or distributed organizations.

Q. WHAT ARE THE KEY BENEFITS?

Easy NAC provides the same benefits as more complex NAC solutions. Key Benefits include:

- Full Visibility of all network devices
- Restricts untrusted devices from joining the network (LAN and WLAN)
- Quarantines misbehaving devices
- Provides BYOD registration features
- Limits BYOD devices and consultants to approved resources
- Provide guest access securely
- Validates managed devices are joined to the domain
- Validates Anti-Virus is enabled and managed
- Validates patch management is enabled and managed

Q. WHAT ARE THE KEY FEATURES OF EASY NAC?

Easy NAC is a Network Access Control that was designed to be simple, easy and cost effective to deploy.

Visibility

Easy NAC automatically detects and profiles new devices as they join the network. The web-based management system lets you see what's happening right now and lets you reconfigure access at any time.

Simple LAN / WLAN Protection

It is easy to control which devices are allowed to access the network. Unknown devices and rogue infrastructure that joins the network will immediately be detected and automatically restricted in real-time. Devices can be allowed access with simple ON / OFF controls or policies can be set for automated access.

Enforce Anti-Virus and Security Policies

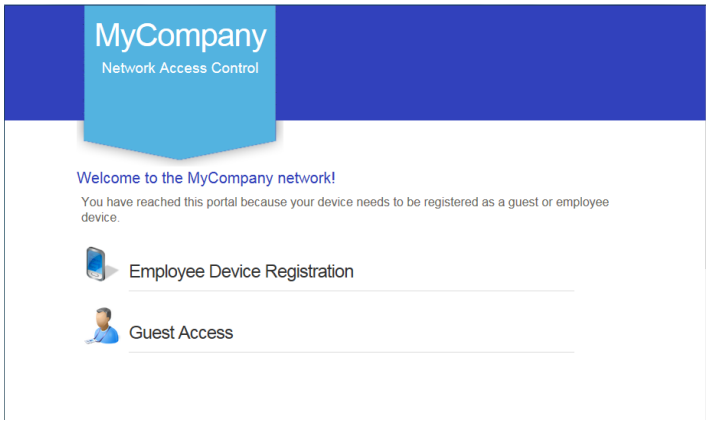
Easy NAC integrates with enterprise Anti-Virus vendors and leading endpoint management solutions, to verify endpoint security is active and up-to-date. By integrating with leading security solutions, Easy NAC can enforce compliance with security policies. Devices out-of-compliance can be restricted at the point of network access.

Automated Threat Response

Security appliances that are designed to monitor devices and network traffic can send event-based alerts for administrative action. Easy NAC can receive event-based syslog messages from all types for security devices and take immediate action when necessary. If Easy NAC receives an alert that a device has malware, we can restrict it immediately.

BYOD Registration

Easy NAC provides a self-registration portal to automate the BYOD registration process. Policies can be set, by groups, to limit the number and type of BYOD devices. It improves security by tracking device ownership, restricting the locations, and limiting network access.

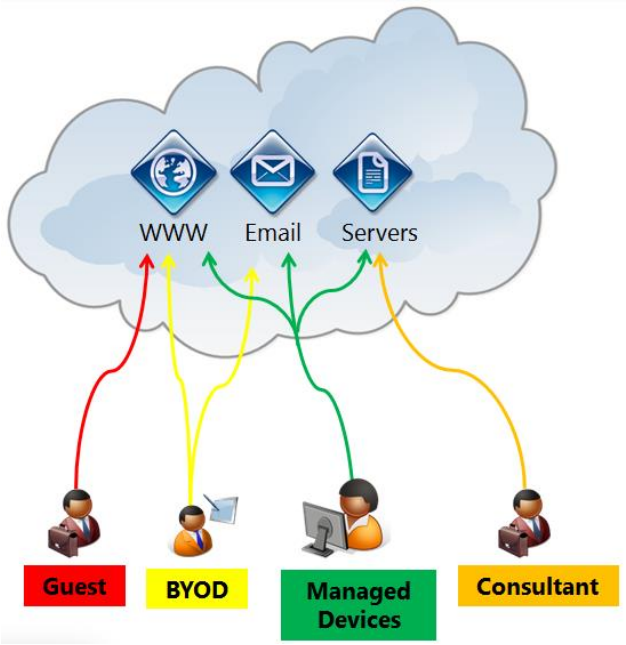


Guest Access

Easy NAC lets sponsors register guest accounts or authorize guests to create their own accounts via the landing page. Sponsors can authorize individual registrations or register groups for classes or meetings with configurable expiration times.

Role-based Access

Easy NAC enhances security by limiting devices to only the resources required. Guests are limited to internet only access. BYOD and consultant devices can be limited to specific resources.



Q. HOW DOES EASY NAC COMPARE TO OTHER NAC SOLUTIONS?

Easy NAC is a third generation plug and protect NAC solution designed to be easily deployed and affordably scale to many remote sites. The competition's products focus more on organizations with

homogeneous networks with limited sites. Competitive NAC solutions are significantly more complex to setup and manage, especially when enabling quarantine functionality.

Easy NAC provides immediate visibility, response, and control, without network changes or agents. The use of ARP enforcement is easier to implement, and also provides stronger and more granular enforcement. With ARP Enforcement, infected devices on the LAN will not be able to communicate with other workstations on the same LAN, and thus not be able to spread the infection. Competitive solution provides limited or weak protection against malware spreading on the LAN.

	Easy NAC	Spanning port approach	802.1x based approach
Enforcement Methods	ARP Enforcement	Block Port or TCP reset (virtual FW)	Quarantine VLAN
Network requirements	None- works with both unmanaged and managed switches and WLAN equipment	Requires available spanning port or mirror port. Require managed switches to block port	Requires managed switches and re-architecting networks to support dynamic VLAN assignments
Ease of Setup	**Easy** - no network changes required. Role-based control can also be enabled without changes	**Moderate to extensive** network changes	**Extensive changes** to rearchitect network for dynamic VLAN assignments.
Quarantine Rogue Devices	**Real-time** detection and immediate protection	**Slow detection and protection** – requires rogue to send traffic to core of network for faster detection	Immediate detection and protection
Quarantine Granularity	**Strong and flexible** – many different ACL's can be set based on policy. i.e., if AV is out-of-date, device can only access AV server	**Weak** – Port Blocking is not user friendly when AV is out-of-date. TCP reset does not isolate an infected machine or non-complaint machines	**Limited** - Using a quarantine VLAN for both infected machines and non-compliant machines puts non-compliant devices at risk
Visibility	Yes – real-time detection with device profiling of OS's	Yes - Good device profiling but, delay detecting rogue devices	Yes - OS profiling may be optional
Manage BYOD \ Guest Access	Yes – built-in	Yes – separate component	Yes – separate component
Agents	Agents not required – typical compliance checks done by server integration	Optional - Agents are typically required to address compliance requirements	Required
Integrations with 3rd party security solutions	Enterprise Edition provides Automated Threat Response with any solution that can send event-based Syslog or e-mail alerts	Add-on modules required $$	Limited

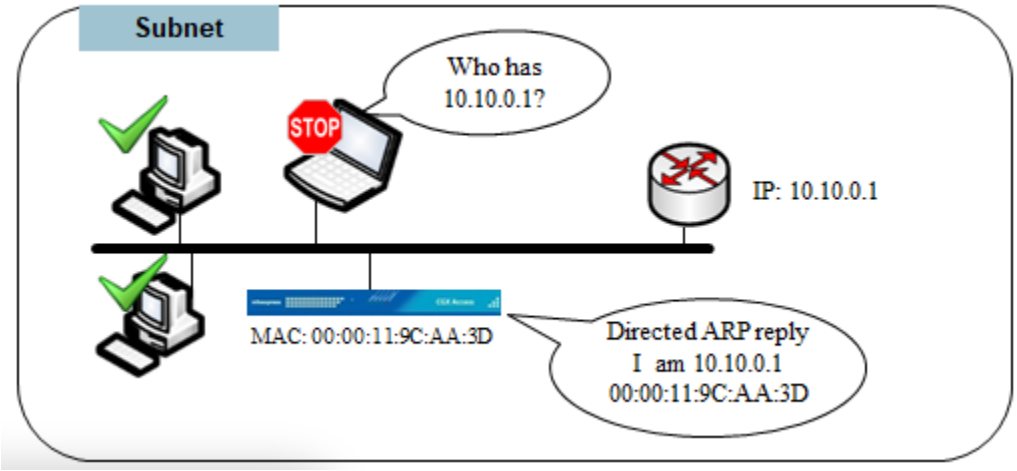
How Easy NAC Works

Q. HOW DOES EASY NAC ENFORCE TRAFFIC?

Easy NAC uses ARP enforcement to control which devices can access the network. ARP enforcement is an out-of-band enforcement method that doesn't require network changes. It works with any network infrastructure, both managed and unmanaged switches.

Q. HOW DOES ARP ENFORCEMENT WORK?

To quarantine a rogue device, the Easy NAC appliance will send ARP packets to direct the rogue's traffic to the appliance. The appliance blocks the rogue's traffic in accordance to policies. Trusted devices follow the normal path through the network and are unaffected.



Q. HOW DOES EASY NAC DETECT AND TRACK DEVICES?

Easy NAC has layer-2 visibility on the networks that it protects, and will detect new devices immediately. When devices join a network they typically send DHCP and ARP requests to initiate communications. Easy NAC will see these broadcast messages and will quarantine the device immediately. Devices are tracked and profiled by MAC addresses, with known good MAC addresses being provided access to the network.

Q. WHAT DEVICE PROFILING METHODS DOES EASY NAC USE?

Easy NAC has layer-2 visibility on the networks that it protects, and automatically profiles devices using both passive and proactive profiling methods. Passive methods include listening to ARP

requests and DHCP requests. Proactive methods include: NMAP scanning, SNMP, SMB NetBIOS scans, Web scans, WMI scans, AD integration, and integration with 3rd party endpoint solutions.

Q. CAN EASY NAC PROTECT AGAINST MAC SPOOFING?

Easy NAC uses MAC-based authentication, so MAC address spoofing can be a concern. Easy NAC provides a fingerprint feature to protect against MAC address spoofing. All devices on the network are profiled for their MAC address, IP, Operating System, and Hostname. This information can then be used to set a unique fingerprint for the device. Once a fingerprint has been set, the device(s) will be protected from spoofing. For example, a printer can include the host name and printer as its OS type. If a Windows, Apple or Linux device tries to spoof its MAC address, the spoof would be detected and the device can be restricted.

Q. IS EASY NAC A SOFTWARE OR HARDWARE SOLUTION?

Easy NAC consists of virtual appliances and physical appliances (CGX Access) and vLinks.

Appliances detects endpoints and control device access to connected subnets. Multiple appliances can extend protection beyond the number of devices listed. When using multiple appliances, a Central Visibility Manager can be used for centralized reporting and configuration management of the appliances.

vLinks connect remote sites without layer 2 access to the appliances. vLinks are used when there is no VLAN trunk or direct connections available from a remote network.

Appliance Specifications	Access Mini CGXA-S10	Access 100 CGXA-S100	Access VM CGXA-V50	Access VM CGXA-V100	Access VM CGXA-V200
Scalability					
Maximum Devices	300*	2500*	2,500*	5,000*	10,000*
Maximum Subnets	10	100	50	100	>200*
Number of Ports	4	6	10 virtual adapters	10 virtual adapters	10 virtual adapters

vLink	VL3
Scalability	
Maximum Devices	>20
Maximum Subnets	3
Number of Ports	3

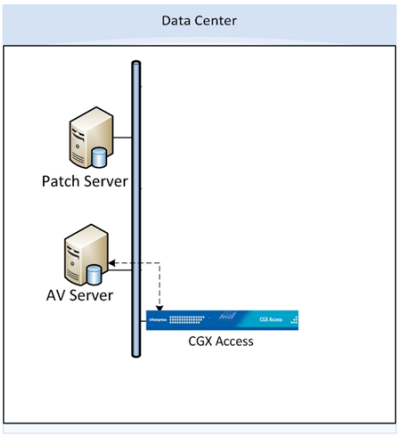
***** Capacity is approximate and depends on network topology, endpoints, and features enabled.

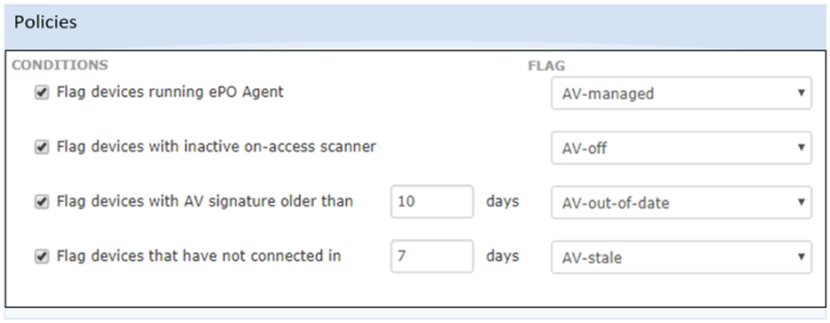
Q. HOW DO I SIZE A DEPLOYMENT?

Easy NAC can protect the entire network or only specific subnets. If the requirements are to protect only the end-user segments on the LAN, then the license should be large enough cover all the devices that are expected to be seen on these end-user segments. This may include end-user devices, printers, switches, etc. Licenses should be enough to cover each subnet that Easy NAC will be configured to protect. Licenses are not required for subnets that will not be monitored. For example, if VoIP or server segments will not be monitored, then it is not necessary for the license to cover these segments.

Q. HOW DOES EASY NAC CHECK ANTI-VIRUS COMPLIANCE?

Easy NAC integrates with on premise enterprise AV servers to check the status of the endpoints. Easy NAC supports integration with enterprise AV and endpoint management vendors. By leveraging the integration at the management server, Easy NAC can enforce compliance with security policies, without the use of agents. Devices out-of-compliance can be restricted and an administrator(s) alerted.





Q. WHAT ENDPOINT SOLUTIONS CAN EASY NAC INTEGRATE WITH?

Easy NAC version 2.3 integrates with Active Directory and supports the following on-premise endpoint solutions.

- Sophos Enterprise Console - 5.x + and Sophos Central
- Symantec Endpoint Protection Manager - 12.x, 14.x and cloud
- McAfee ePO - 5.x +
- Trend Micro OfficeScan - XG+
- Kaspersky Antivirus – 10.x+
- ESET Remote Administrator – 6.5+
- Microsoft SCCM and WSUS – 4.x +
- IBM BigFix – 9.x+
- Moscii StarCat 2013 and StarCat 10
- Carbon Black Cb Response – 6.x+

For other endpoint security solutions, Easy NAC also supports Windows Management Instrumentation (WMI). WMI can be used to check the endpoint's Windows Security Center and report the status of AV on that endpoint(s).

The Endpoint Compliance Module is sold separately, but included in the Enterprise Edition.

Q. CAN EASY NAC INTEGRATE WITH FIREWALL AND APT SOLUTIONS?

Yes, security appliances that are designed to monitor devices and network traffic can send event-based alerts for administrative action. Easy NAC can receive event-based syslog messages and e-mail alerts from all types for security devices and take immediate action when necessary. For example, if Easy NAC receives an alert that a device has malware, we can restrict it immediately.

Any solution that can send event-based syslog messages or e-mail alerts can be configured to work with Easy NAC.

The Firewall and APT integration modules are sold separately, but included in the Enterprise Edition.

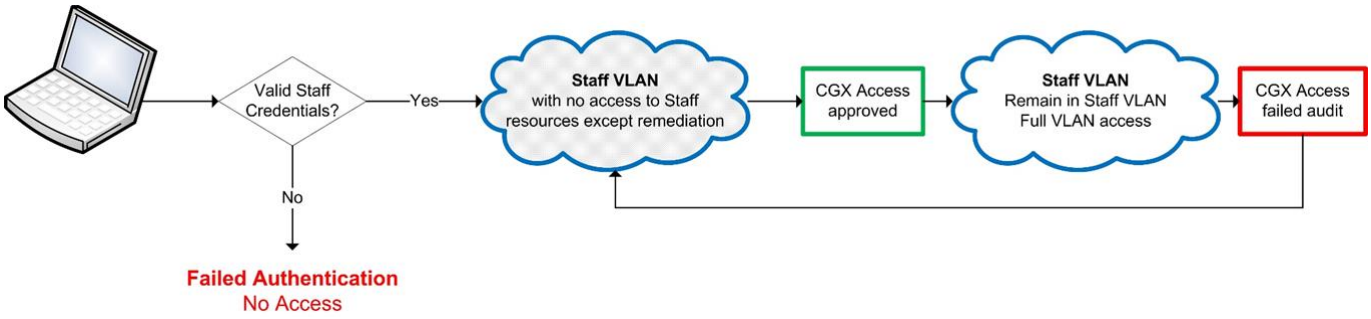
Q. DOES EASY NAC USE AGENTS?

Easy NAC was designed to be agent-less, and agentless deployments are the most common type of deployment. Agents are not required for typical compliance checks like Anti-virus and Patch compliance. However, for advance or more detailed compliance checks agents can be used.

Agents can also be used for continuous compliance monitoring and automated remediation of end-points.

Q. CAN EASY NAC WORK WITH 802.1X?

Yes, 802.1x is an authentication standard that is widely supported. Easy NAC is authentication agnostic, and can co-exist with any authentication method. When CGX Access is deployed on an 802.1x enabled network it provides multiple layers of access control, that is simple to implement and more secure. Easy NAC can quarantine endpoints without rearchitecting the network to support dynamic VLANs \ quarantine VLAN assignments.



Benefits of Easy NAC with 802.1x:

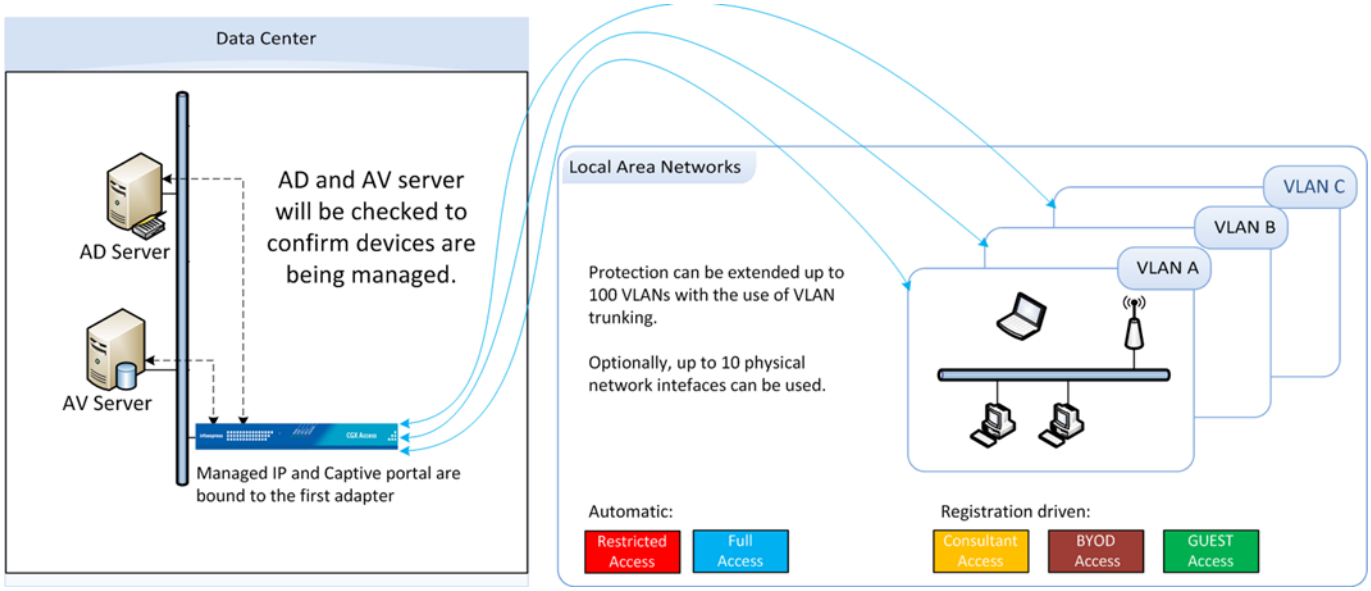
- Defense in Depth – 802.1x 1st layer with CGX Access 2nd layer of protection
- Eliminates need to architect Dynamic VLAN's or Quarantine VLAN's
- Better end-user experience: single sign-on, no IP changes, no VLAN changes or login delays
- Granular isolation (more secure) of non-compliant devices.
- Network Availability - 802.1x can be configured to fail-open with CGX Access maintaining security

Easy NAC Deployment

Q. WHERE IS EASY NAC CONFIGURED ON THE NETWORK?

The Easy NAC appliances are placed anywhere there is layer 2 or layer 3 connectivity to each location. There are three ways to connect a subnet to an appliance:

- **Method 1 – Physical connection:** Add additional network adapter and plug-in to a normal switch access port to extend protection to an additional subnet.
- **Method 2 – 802.1q trunk:** Use 802.1q trunk ports so multiple VLANs can be protected with each ethernet adapter. Multiple adapters are recommended if there is extensive traffic from devices being restricted with ACLs.
- **Method 3 – vLink:** For remote sites without either 802.1q or direct ethernet connections, place a vLinks at that site to provide connectivity to the appliance.



Q. ARE THERE ANY SWITCH OR NETWORK REQUIREMENTS?

There are no special networking requirements to deploy Easy NAC. It works with any brand of switches, hubs, or wireless infrastructure. This includes:

- Enterprise and consumer routers and switches
- Enterprise and consumer wireless network equipment
- Unmanaged switches

Q. HOW IS EASY NAC SOLD?

Easy NAC is typically sold with a perpetual license for software and hardware purchases for appliances and vLinks. Licensing depends on the network devices, remote subnets, and feature options. Easy NAC keeps tracks of the number of devices (unique MAC addresses) it has seen in the past 24 hours. Please contact your authorized partner or InfoExpress for up-to-date information on licensing. sales@infoexpress.com

Q. WHAT IS A TYPICAL DEPLOYMENT LIKE?

Each deployment will vary depending on the endpoints and network topology. Deployments can be a fast as a few days, but a more conservative deployment would be two weeks, with most of the time spent in monitoring mode. Because there will be no changes to the existing network, operations will not be affected during the deployment, and after-hours work is not required. Typically, a three-stage deployment is recommended:

Phase 1 – Infrastructure setup (1-3 days)

- Installation of CGX Access appliances and vLinks
- Setup integration with Active Directory
- Setup AV and Patch integration
- Configure BYOD, Consultants, and Guest Access policies
- Configure and fine tune Access Control Lists for Restricted, BYOD, Consultants and Guests

Phase 2 –Monitor mode – (1 week)

- Educate staff and have them register their personal devices
- Educate staff on how to register guests
- Monitor subnets – For devices that need to be whitelisted or flagged for access
- Add flags and white-lists configurations as appropriate

Phase 3 - Protection Enabled (1-2 days)

- Enabled Enforcement 1 subnet at a time

Q. WHAT HAPPENS IF A LICENSE IS OVER-SUBSCRIBED?

Easy NAC keeps track of each unique MAC address that it has seen in the past 24 hours. Each MAC address will use a license, with the exception of restricted devices. Restricted devices don't consume a license. If the license is exceeded, a warning indicator will be shown on the management interface, but the solution and protection will continue to work as per normal.

If the license is exceeded by more than 10%, enforcement protection will be disabled for any new device that is attempting to join the network and needs to be quarantined.