EASY NAC

FREQUENTLY ASKED QUESTIONS

www.easynac.com

v3.2 240202

CONTENTS

Overview

Q. WHAT IS EASY NAC?

Easy NAC is a Network Access Control solution specifically designed to be simple and easy to deploy, while providing stronger security than traditional NAC solutions. Easy NAC provides visibility and Zero Trust 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, EDR, XDR, and other security solutions so it can quickly quarantine suspicious or infected devices.

Q. WHAT MAKES EASY NAC UNIQUE?

Network Access Control has a reputation of being difficult, time consuming, and expensive to implement. Easy NAC is different; It is an agent-less NAC solution that is simple and secure, without requiring changes to the network. It works with both managed and unmanaged networking equipment. No switch, endpoint, or spanning port configuration is required. At the same time, Easy NAC provides granular access control, complete network visibility, and options to extend protection to remote sites, making it the simplest NAC solution for centralized or distributed organizations.

Q. WHAT ARE THE KEY BENEFITS?

Easy NAC provides enhanced benefits over more complex NAC solutions. Key Benefits include:

- Real-time Visibility of all network devices
- Restricts untrusted devices from joining the network (LAN, WLAN, and VPN)
- Prevents the lateral spread of malware
- Protects against MAC spoofing
- Detects Hacking Activity (Deception feature)
- Provides Guest and BYOD registration
- Limits BYOD / Consultants devices to approved resources
- Validates managed devices are joined to the domain
- Validates Anti-Virus is enabled and managed
- Validates patch management is enabled and managed
- Comprehensive and continuous host integrity checks with an optional agent
- Provides Orchestration features to reduce the Mean Time to Response (MTTR)

Q. WHAT ARE THE KEY FEATURES OF EASY NAC?

The Easy NAC solution with CGX Access appliances provides the following features:

Agentless Visibility

CGX Access lets you see devices that join your network, without the use of agents. Visibility is immediate, with any untrusted device being immediately restricted, as desired. Devices will be both passively and actively profiled to determine operating system, manufacturer, and type of device.

Easy to Implement Enforcement

CGX Access uses ARP enforcement with DNS and HTTP redirection 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. For Remote Access VPN protection, Inline enforcement can be used.

Simple LAN \ WLAN Protection

It is easy to control which devices are allowed to access the network. Untrusted devices, rogue infrastructure, and non-compliant devices 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.

Automated MAC Address Whitelisting

CGX Access will regularly check with your Active Directory server and other end point security solutions to verify which devices are trusted. Devices that are confirmed as domain-joined or trusted will automatically be granted full access to the network. Devices that are not domain joined can be manually flagged as approved. In addition, device profiling can also be used to automate the process of flagging approved devices.

Anti-Spoofing Protection

CGX Access provides a fingerprint feature to protect against MAC address spoofing. All devices on the network are profiled for their MAC address, IP, Operating System, Hostname, and other attributes. This information can then be used to set a unique fingerprint for each device. Once a fingerprint has been set, the device(s) will be protected from spoofing.

Enforce Anti-Virus and Security Policies

CGX Access 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, CGX Access can enforce compliance with security policies. Devices out-of-compliance can be restricted at the point of network access.

Orchestration

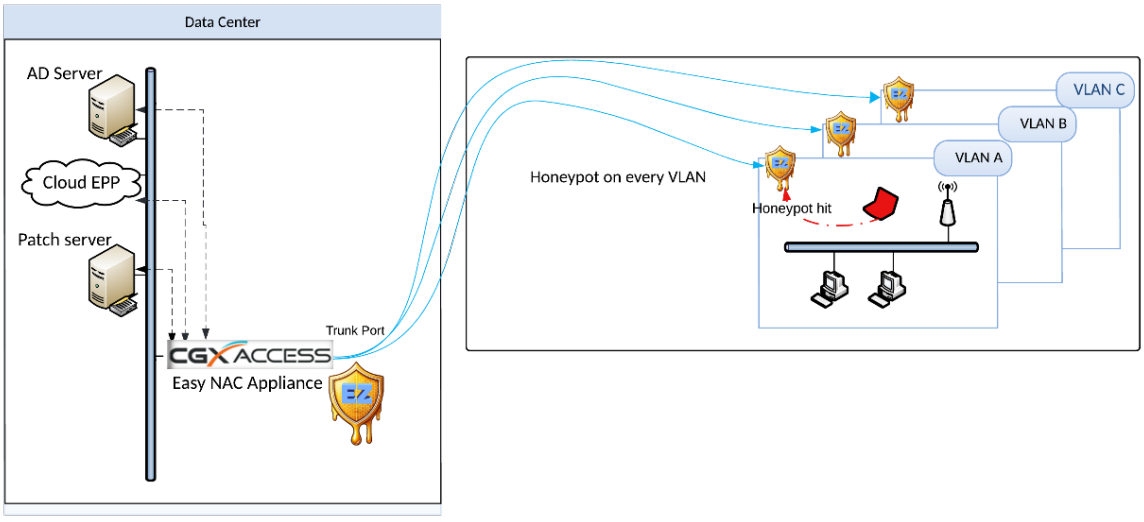
Security appliances that are designed to monitor devices and network traffic can send event-based alerts for administrative action. CGX Access can receive e-mail alerts or event-based syslog messages from Firewalls, XDR, IPS, SIEM, and many other types of security devices and then take immediate action when necessary. If CGX Access receives an alert that a device has malware, we can restrict it immediately.

Malware Lateral Spread Protection– Zero-day Protection

CGX Access unique layer-2 visibility of the network allows for the immediate detection of suspicious behavior, such as devices making excessive connections attempts to endpoints on the same network segment. This real-time detection provides immediate protection against zero-day malware propagating on the network.

Deception – Hacking Detection

With its layer-2 protection, the Easy NAC solution will host fake services such SSH, Telnet, FTP, etc. on every VLAN or subnet it's protecting, creating a distributed honeypot. Theses fake services serves no real business purpose, so if any person or bot tries to login to these fake services, it's a strong indicator of hacking activity. With virtual honeypots on every VLAN, it provides early detection of hacking activity before hackers reach the core of the network.

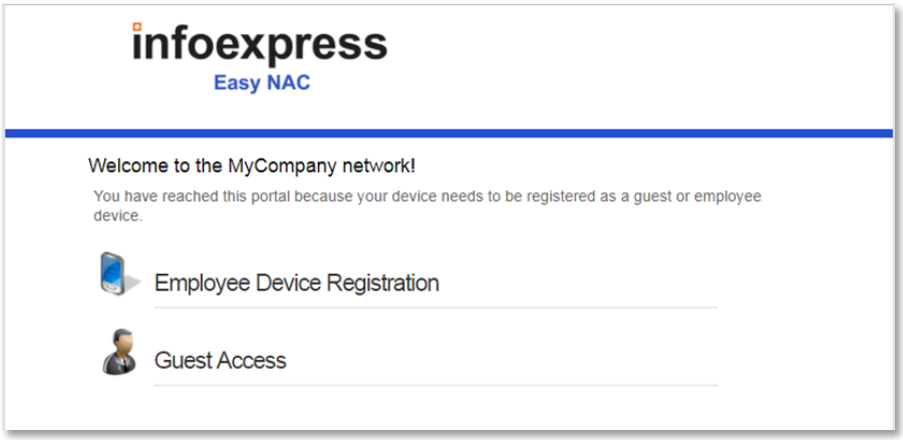


BYOD Registration

CGX Access 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 to approved resources.

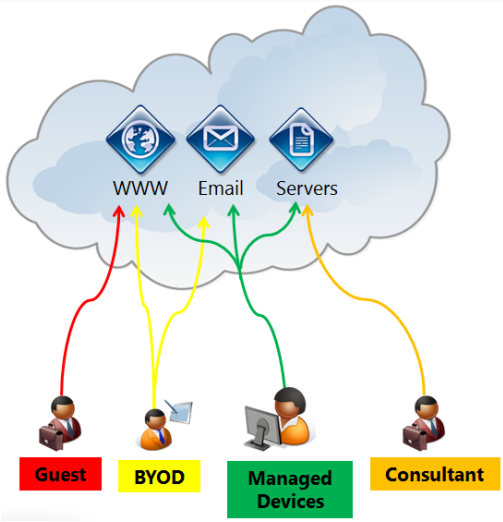
Guest Access

CGX Access 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 Control

CGX Access 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. DOES EASY NAC PROVIDE BEHAVIOR BASED ZERO-DAY PROTECTION?

During its normal operation, the CGX Access appliances are listening to broadcast traffic on the end-user segments. With this layer-2 visibility, CGX Access is in a unique position to detect devices making unusual connection attempts to other devices within the same segment. If an end-user device suddenly attempts to connect to an excessive number of devices on the same subnet or trying to connect to Dark IPs, that at not active on the network, this is very suspicious behavior. This behavior is indicative of a network scan being performed or malware in the recognizance phase as it attempts to spread. Easy NAC can detect this behavior and immediately quarantine this device so it can't spread malware laterally on the network.

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, and control, without network changes or agents. The use of ARP enforcement is easier to implement, and 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	RADIUS 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** when using SNMP 10+ minute enforcement delay is common	Often requires the use of digital certificates for 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	**Limited** - 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	Optional - Agents not required – typical compliance checks done by server integration	Optional - Agents are typically required to address compliance requirements	Typically 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
Malware – Lateral Spread Protection	Yes – Easy NAC has layer-2 visibility on each VLAN it's protecting	Visibility only at the core, can't see lateral movement on VLAN	No layer-2 visibility, so can't see lateral movement on VLAN
Deception – Hacking Detection	Yes – Built in	No comparable feature	No comparable feature

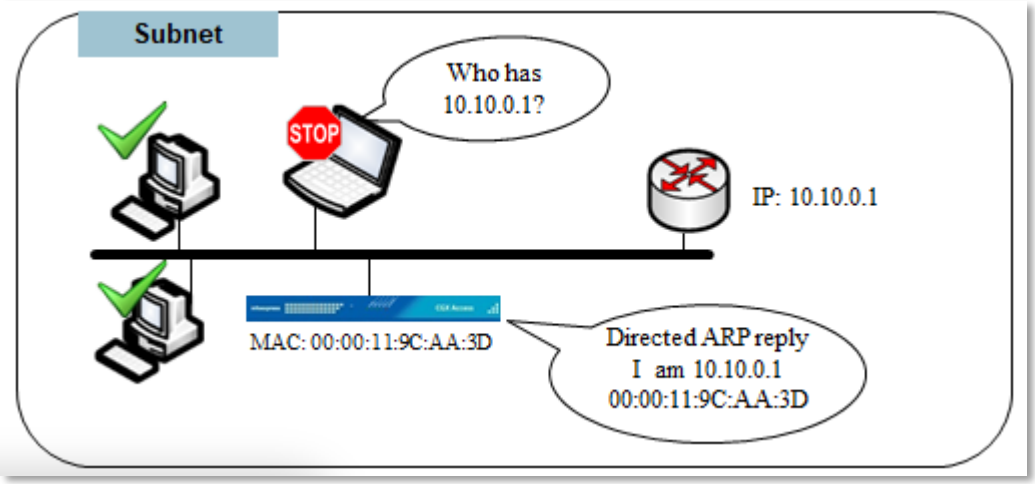
How Easy NAC Works

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 with policies. Trusted devices follow the normal path through the network and are unaffected.



Q. DOES EASY NAC SUPPORT IPV6?

Yes, iPv6 is supported. Easy NAC is compatible with endpoints running dual stack IPv4 and IPv6. IPv4 is required for management and most key features. Easy NAC would not be recommended for IPv6 only environments.

Q. HOW DOES EASY NAC DETECT AND TRACK DEVICES?

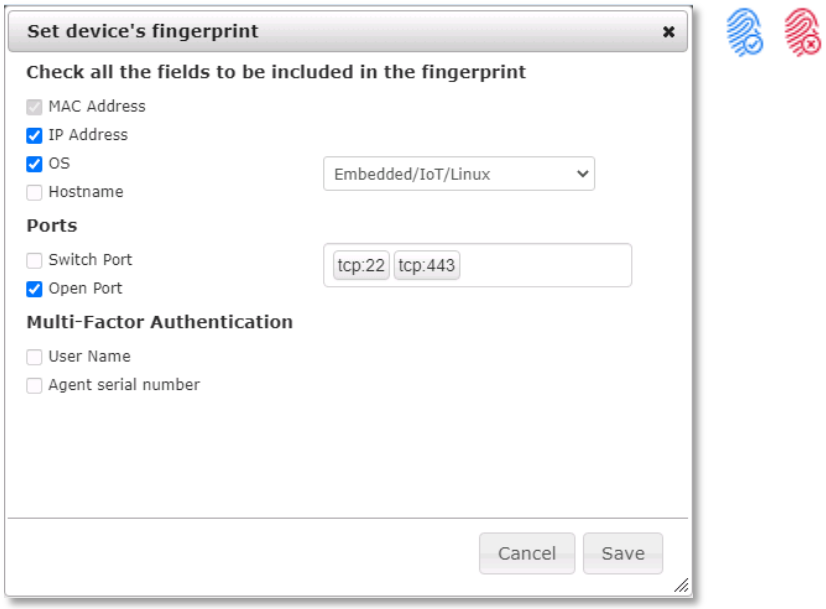
Easy NAC has layer-2 visibility on the subnets that it protects and will detect new devices immediately. When devices join a network, they typically send DHCP and ARP requests to initiate communications. Easy NAC will see these broadcast messages and will quarantine the device immediately. Devices are tracked and profiled by MAC addresses, with known trusted devices 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, DHCP requests and captive portal. Proactive methods include: NMAP scanning, SNMP, SMB NetBIOS scans, LLTD, PoF, UPnP, WMI scans, AD integration, optional agents, 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, Hostname, open ports, and other information. 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, Android 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 appliances (CGX Access) can be deployed with virtual appliances (software) and \ or physical appliances (hardware).

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

Appliance Specifications	Access Mini CGXA-S10	CGX Access CGXA-S100	Access 200 CGXA-S200	Access 500 CGXA-S500	Access 600 CGXA-S600	Access VM ENAC-VM
Scalability						
Maximum Devices	300*	2500*	5,000*	10,000*	10,000*	10,000*
Maximum Subnets	10	100*	100*	200*	200*	200*
Number of Ports	4	8	8	8	10 2 pairs of by-pass NICs.	8-10 virtual adapters

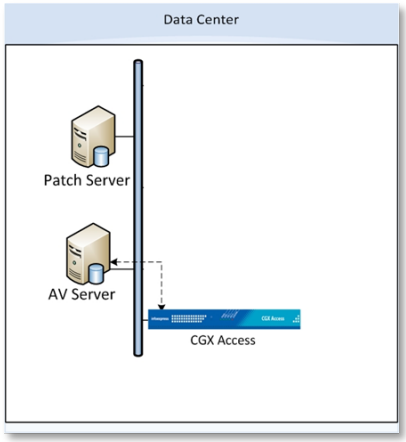
* Capacity is approximate and depends on network topology, endpoints, and features enabled. Hyper-V virtual appliances are limited to 8 interfaces.

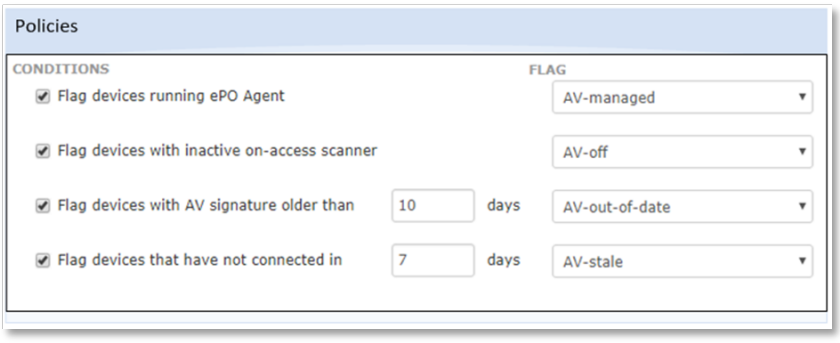
Q. HOW DO I SIZE A DEPLOYMENT?

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 cloud or on-premises enterprise AV servers to check the status of the endpoints. Easy NAC supports integration with enterprise AV, XDR, 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 3.2 integrates with Active Directory and supports the following endpoint solutions.

- Bitdefender
- Carbon Black Endpoint Standard
- CrowdStrike Falcon
- Cybereason
- Elastic Open XDR
- ESET Antivirus
- FireEye HX
- HCL BigFix
- Ivanti Security Controls
- Kaseya VSA
- Kaspersky Antivirus Integration
- ManageEngine Desktop Central
- ManageEngine Patch Manager
- Microsoft Intune
- Microsoft SCCM \ WSUS
- Moscii StarCat
- OKTA Verify
- Palo Alto Cortex XDR
- SentinelOne
- Sophos Enterprise Console and Sophos Central
- Symantec Endpoint Protection Manager
- Trend Micro OfficeScan, Apex Central, Vision One
- Trellix ePolicy Orchestrator
- Webroot

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

Q. CAN EASY NAC INTEGRATE WITH FIREWALL AND XDR 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 these event-based syslog messages and e-mail alerts from all types for security solutions and take immediate action when necessary. For example, if Easy NAC receives an alert that a device has malware, the appliance 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.

Q. CAN EASY NAC USE AGENTS?

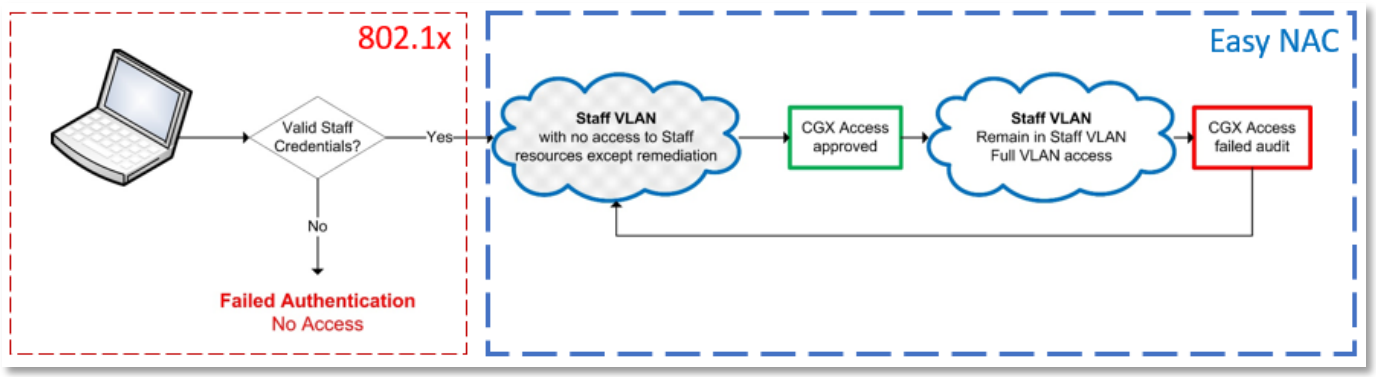
Easy NAC was designed to be agent-less, and agent-less deployments are the most common type of deployment. Agents are not required for typical compliance checks like Anti-virus and Patch compliance. However, for advance or more detailed compliance checks agents can be used.

Agents can also be used for continuous compliance checks and automated remediation of endpoints. The table below provides a comparison between agentless and agents. A hybrid approach can be used where the agent is deployed on laptops, with agentless checks for other devices.

	Agent	Agentless
Detection	Agent continuously detects changes in compliance within 10 seconds.	Compliance re-check interval depends on the interval specified. 5 to 15 minutes is fairly typical in most setups.
Supported OS	• Microsoft Windows 7 SP 1 or above (32bit and 64bit) • Apple MacOS • Linux	Any OS that is supported by Integration solutions.
Compliance checks	Compliance check can be customized to Include but not limited to the followings: • Running Process \ version info • Registry values • Files and locations • Machine names and OS check • Agent-based authentication	Agentless supports Integrations with: • Active Directory • Endpoint Security solutions • Patch Management solutions • WMI • Orchestration via Email or syslog
End-User Notifications	Pop-up messages	DNS or HTTP redirection
Real-time Wi-Fi adapters control	When connected to the corporate wired network, the wireless network adapter can be disabled automatically and re-enabled once wired NIC is disconnected	N/A
Automatic Remediation	When a compliance check fails, a remediation action can be initiated. It includes running scripts or executables on the host that has the agent installed. I.E., If AV out-of-date, the remediation script can start the AV update process.	N/A

Q. CAN EASY NAC WORK WITH 802.1X \ MAB?

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 quarantine VLANs.



Benefits of Easy NAC with 802.1x:

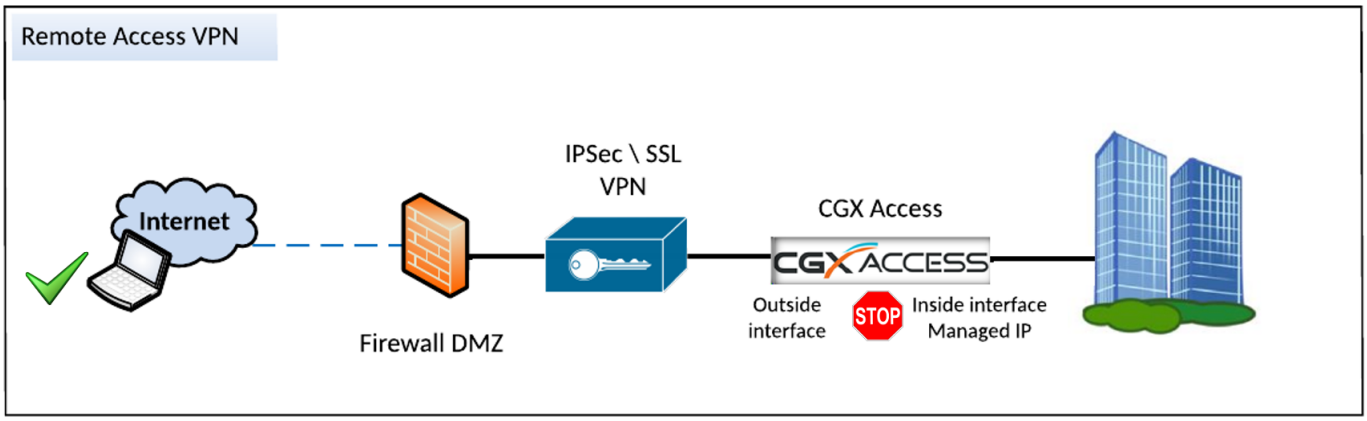
- Defense in Depth – 802.1x 1st layer with CGX Access 2nd layer of protection
- Eliminates need to architect Quarantine VLANs
- Better end-user experience: single sign-on, no IP changes, no VLAN changes or login delays
- Pre-connect checks with granular isolation (more secure) of non-compliant devices.
- Network Availability - 802.1x can be configured to fail-open with CGX Access maintaining security.
- Easy NAC will enhance the security of MAC Address Bypass functionality, with Fingerprinting to protect against MAC spoofing.

Q. CAN EASY NAC WORK AS A RADIUS PROXY?

Yes, in an 802.1x environment, the CGX Access appliances can be configured as a RADIUS server proxy. As a RADIUS proxy, the Easy NAC solution would also have visibility of the authentication process. This additional switch port visibility can be leveraged to enhance Fingerprinting (MAC spoofing protection) and also be used for providing Multi-Factor Authentication checks with or without agents.

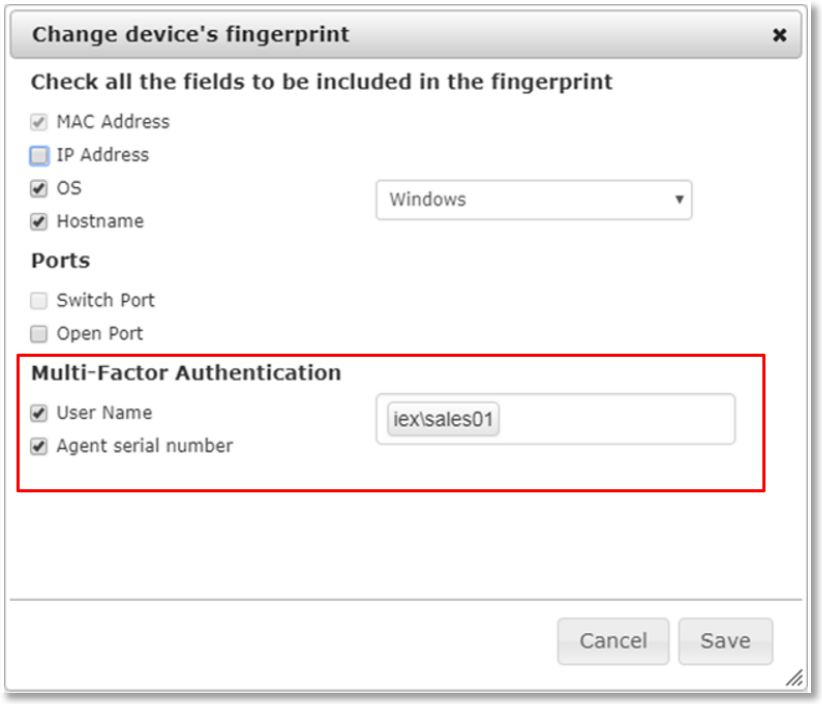
Q. CAN EASY NAC PROTECT REMOTE ACCESS?

Yes, CGX Access appliances support inline enforcement that can be used to control what devices are allowed to connect via the VPN. The CGX Access appliance is placed in bridge-mode between the remote access VPN server and the protected resources. Endpoints auditing with the appliance, using agents, are allowed to send traffic thru the appliance. While devices not auditing (untrusted) or devices failing a compliance check will have their traffic blocked.



MFA Authentication

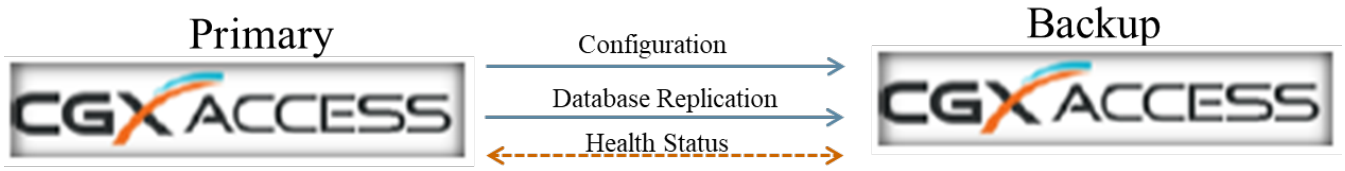
The Fingerprinting feature can provide a transparent multi-factor authentication. User credentials will be captured, and then associated with a specific device. Using the device's fingerprint, Easy NAC can provide 2FA (Something you know (password) and something you have a (specific device). Each CyberGatekeeper agent has a unique serial number providing strong verification the authenticated user is connecting from a unique and trusted device.



Q. DOES EASY NAC SUPPORT HIGH AVAILABILITY

Yes, Easy NAC offers a High Availability option to provide redundancy in the event an appliance or virtual appliance was to fail or be offline. HA is provided using a two-box design, where the Primary appliance syncs its database and configuration with a passive Backup appliance. If the Backup appliance determines the Primary appliance is offline, it will become active.

When the Primary appliance comes back online, the Backup will sync the configuration and database back to the Primary, and the Primary will become active again.

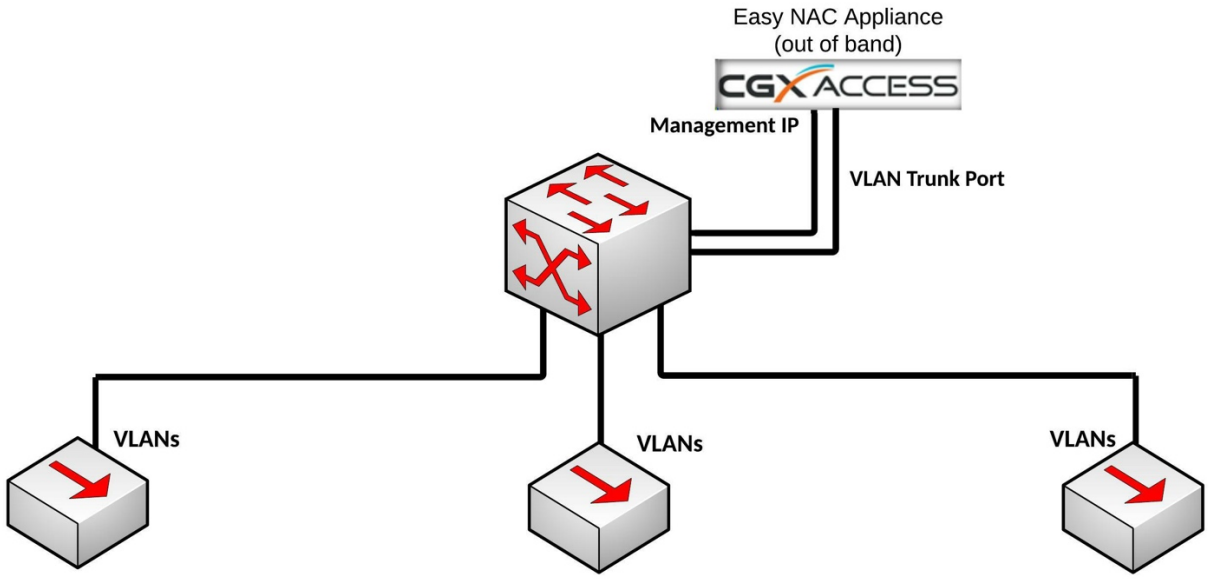


Easy NAC Deployment

Q. WHERE IS EASY NAC CONFIGURED ON THE NETWORK?

The CGX Access appliances are placed anywhere there is layer 2 connectivity for the subnets to be protected. 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 – vLinks or Enforcer Sensors (Agent)**: For remote sites without either 802.1q or direct ethernet connections, place a vLinks or Enforcer Agent at the remotes sites to provide visibility and control back to the appliance.

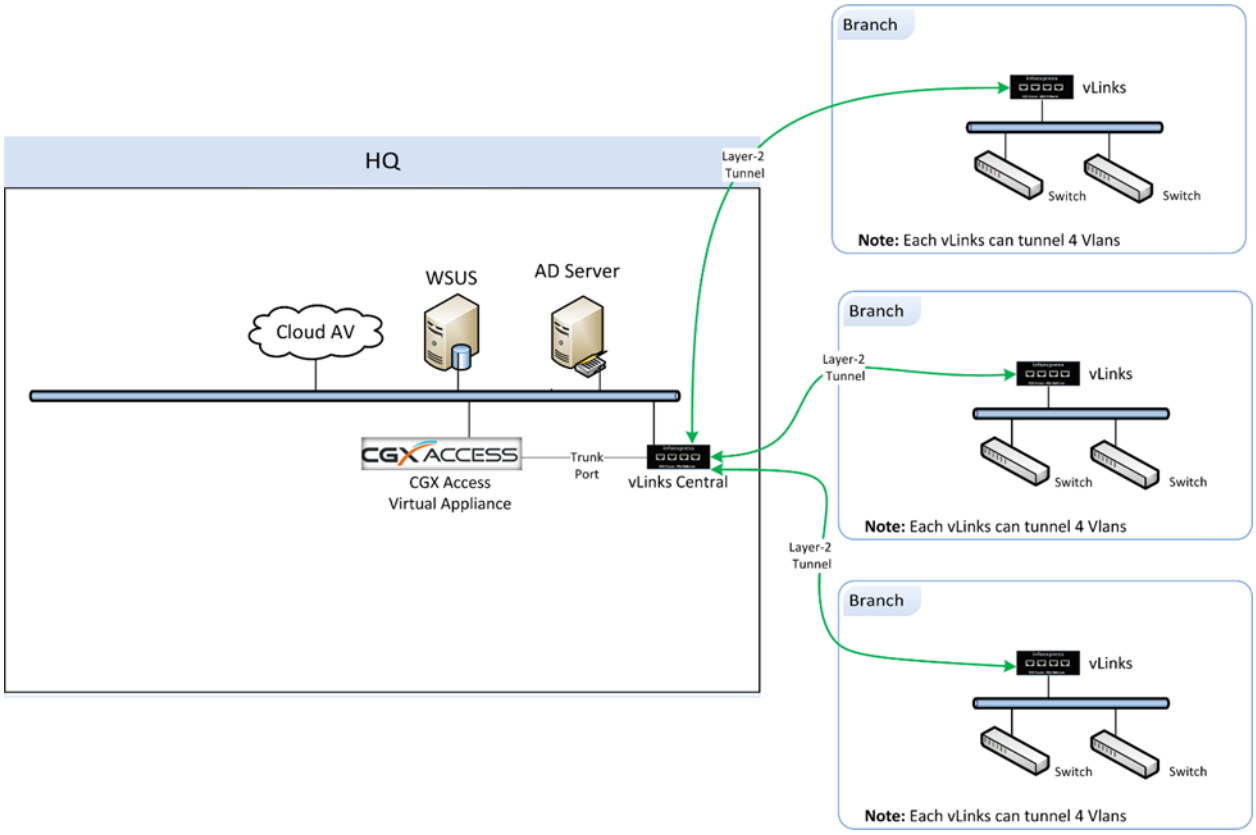


Q. WHAT IS THE VLINKS SOLUTION AND HOW DOES IT WORK?

The CGX Access appliance requires layer-2 visibility of the subnets it's protecting. Having layer-2 visibility at the main site can be easily achieved with trunk ports or standard access ports. However, getting layer-2 visibility for remote sites can be more challenging. The vLinks solution is designed to extend the reach of the CGX Access appliances so it can also protect your smaller remote sites with cost effective hardware.

The vLinks architecture is shown below. At remote sites, a vLinks appliance is placed on the network for layer-2 visibility. This layer-2 traffic is then tunneled back to a vLinks Central appliance. This tunneled traffic is sent over the existing corporate WAN, so an existing WAN network is required. MPLS and NAT'd network types are supported.

At the main site, a vLinks Central will consolidate the layer-2 traffic from multiple vLinks and share it with the CGX Access appliance using a port directly connected to the CGX Access appliance. With this connectivity in place, CGX Access will detect rogue devices at the branches and quarantine these devices real-time. All Easy NAC features including compliance checks, captive portals, Automated Threat Response, etc., are supported.

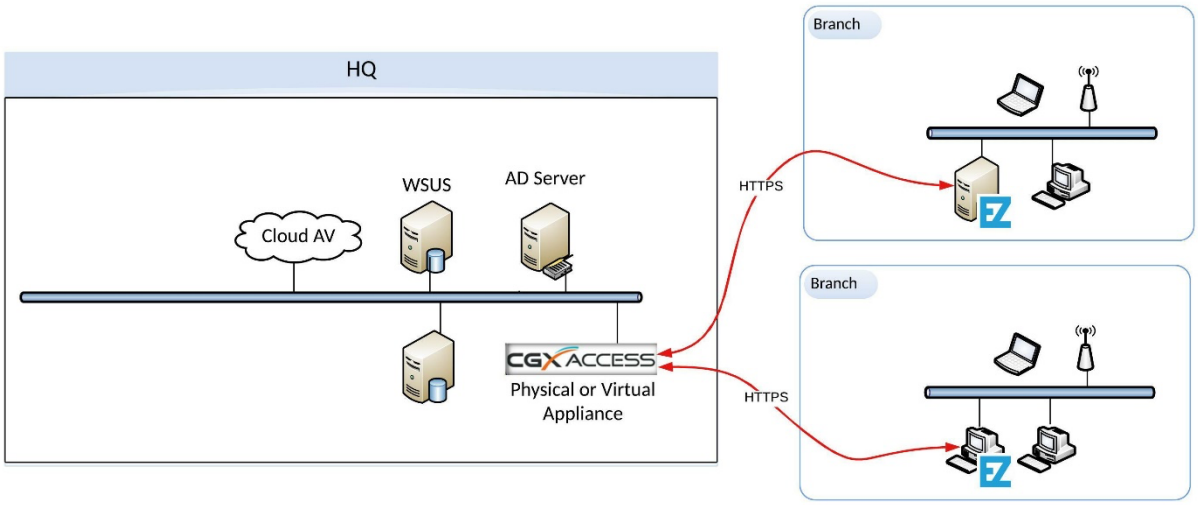


Q. WHAT ARE ENFORCER SENSOR (AGENT) AND HOW DOES IT WORK?

The Easy NAC solution uses CGX Access appliances for visibility and protection of the network. To provide visibility and protection, the CGX Access appliance requires layer-2 visibility of the subnets it's protecting. Having layer-2 visibility at the main site can be easily achieved with trunk ports or standard access ports. However, getting layer-2 visibility for remote sites can be more challenging. At the remote sites, the Enforcer Sensor (Agent) can be deployed on Windows or Linux platforms to get this visibility and local enforcement at remote sites.

The Enforcer Sensor (Agent) architecture is shown below. At remote sites, the Enforcer Sensor software is installed on a Windows 64-bit OS. The agent would then communicate back to the CGX Access appliance to report in real-time what devices are on the network. The CGX Access appliance

would then profile these devices and tell the Enforcer Agent what access should be assigned. The Enforcer Sensor would then apply the ARP enforcement. Both. MPLS and NAT'd network types are supported. However, with NAT'd networks only rogue prevention features are supported, as the CGX Access appliance may not be able to fully profile the remote devices. If using NAT'd subnets, the vLinks solution may be a better approach to extend the protection.



Adding Enforcer Sensors to extended CGX Access protection to remote sites is a simple process that consists on installing the Enforcer Sensor (Agent) and then accepting this agent in the CGX Access management interface.

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, wireless infrastructure or remote access VPNs. This includes:

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

Q. HOW IS EASY NAC SOLD?

Easy NAC is typically sold with a perpetual license for software and hardware appliance purchases. Software subscription options are also available. The licensing depends on the number of network devices and number of remote subnets that need protection. From a licensing perspective, Easy NAC keeps tracks of the number of devices (unique MAC addresses) it has seen in the past 24 hours. Agents, if desired, are purchased separately. 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 number of locations, network segments to be protected and the number of devices on the network. Deployments can be as fast as a few days, but a more conservative deployment would be two weeks, with most of the time spent in monitoring mode. Larger distributed networks may take 1 to 3 months. Because there will be no changes to the existing network, operations will not be affected during the deployment, and after-hours work is not normally required. Typically, a three-stage deployment is recommended:

Phase 1 – Infrastructure setup (1-10 days)

- Installation of CGX Access appliances and vLinks at necessary sites
- 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 – (1-2 weeks)

- 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, except for Untrusted devices. Untrusted 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 additional device that joins the network and needs to be quarantined or protected.

End of Document