EasyNAC

Compatibility

Traditional Network Access Control solutions requires integration with the network infrastructure. These integration requirements lead to incompatibility issues that often require expensive network refreshes. In addition, traditional NAC often requires the network to be rearchitected to support quarantine functionality. Rearchitecting networks can be a time-consuming process that requires extensive networking expertise, and often leads to project delays.

EasyNAC avoids both problems by being network independent. It doesn't require network integration so it can work with any type of switch and any type of wireless infrastructure. It also doesn't require any configuration changes to the network. These capabilities are what makes EasyNAC easy to deploy.

In addition, EasyNAC was also designed to work with any brand of VPN and support any 3rd party security appliance for Automated Threat Response. This agnostic design philosophy also makes it easy to secure work from home requirements and provide strong security with a rapid threat response.

Version 3.2.250801
Updated August 01, 2025

Switches for Enforcement

The EasyNAC solution uses ARP enforcement to protect the LAN. A key benefit of ARP enforcement is that no network integration is required, so any type of switch is supported.

Type	Compatibility
Managed Switch	Any brand, any version, any firmware
Unmanaged switch	Any brand, any version, any firmware
Hub	Any brand, any version, any firmware
Virtual Switch	Any brand, any version

Wireless Controllers for Enforcement

The EasyNAC solution uses ARP enforcement to protect the Wireless LAN. No network integration is required, so any type of wireless controller or Access point is supported.

Type	Compatibility
On-premise Controller	Any brand, any version, any firmware
Cloud Controller	Any brand, any version, any firmware
Unmanaged Access Point	Any brand, any version, any firmware
Consumer wireless	Any brand, any version, any firmware

SNMP scanning

SNMP scanning is an optional (free) feature to simply provide visibility of the switch and port a device is connect to. Read-only permission is required. SNMP v2c and v3 supported.

Supported brands include: 3COM, Aruba, Cisco, Cisco Small Business, F5, Allied Telesis, Fortinet, H3C, HP, HPE, Huawei, Juniper, Meraki, Mikrotik, PaloAlto, Sonicwall, Tplink, VMware.

VPN Protection

EasyNAC uses inline enforcement for VPN protection. A key benefit of Inline enforcement is no integration is required. The appliance is deployed in line behind the VPN like a transparent firewall and will only allow traffic to pass through from approved managed devices.

Type	Compatibility
SSL VPN*	Any brand, any version, any firmware
IPSEC VPN*	Any brand, any version, any firmware
PPTP VPN*	Any brand, any version, any firmware
Other Remote Access solutions*	Any brand, any version, any firmware

***** There are two requirements for setup: 1) Agents used for compliance checks 2) VPN must be configured using an IP pool, so each active connection has a unique IP address.

Integrations for Agentless Compliance Checks

EasyNAC supports integrations with 3rd party solutions for automated trust and simplified compliance checking. The following Integrations are supported.

Note: any brand of Anti-virus can be checked if using agents.

Endpoint Security	Compatibility
Bitdender GalaxyZone	Cloud and On-premise
Carbon Black	CB Response 6.x+ and Carbon Black Endpoint Standard - Cloud
Cortex XDR	Cloud
Crowdstrike Falcon	Cloud
Cybereason	Cloud
Elastic XDR	Cloud
ESET Antivirus	On-premise – 6.5+ and Cloud
FireEye HX	Cloud
Kaspersky Antivirus	On-premise – 10.x+

Microsoft Defender	Cloud
Okta Verify	Cloud
SentinelOne	Cloud
Sophos Enterprise Console and Sophos Central	On-premise 5.x and Cloud
Symantec Endpoint Protection	On-premise 14.x and Cloud
Tenable Vulnerability Management	Cloud
Trellix ePO	On-premise – 5.x+
Trend Micro OfficeScan, Apex Central, and Vision One	On-premise XG+ and Cloud
Webroot	Cloud

Patch, Desktop & Mobile Management	Compatibility
HCL Big Fix	On-premise – 9.x+
Ivanti Security Controls	On-premise – 2019.3+
Kaseya VSA	On-premise or Cloud
ManageEngine Patch Manager	On-premise or Cloud - API v1.3 and v1.4
ManageEngine Endpoint Central	On-premise or Cloud - API v1.3 and v1.4
Microsoft SCCM \ WSUS	On-premise – 4.x+ with SQL database
Moscii Starcat	On-premise -10.x
Microsoft Intune	Cloud
42Gears SureMDM	Cloud

Other Integrations	Compatibility
Microsoft Active Directory	On-premise
Microsoft Entra ID	Cloud
Microsoft WMI	On-premise - Active Directory joined devices
Tenable Vulnerability Management	Cloud
SolarWinds Observability	On-premise - Version 2025.2.1.3106 or later

Agents for Compliance checks

Agents are very versatile, and can check for any endpoint protection Software, network settings, applications, patches, etc. Custom compliance checks supported. Checks are continuous, both pre and post connection. Supported Operating Systems include:

Agents	Compatibility	Automatic Remediation
Windows Persistent	32-bit and 64-bit; Windows 7SP1+ and Windows 2008+	Yes
Windows on-demand agent	64-bit - Windows 10+	Yes* Depends on the logon user's permissions
Mac OSX	OS X 10.09+	Yes
Linux	Linux 4.12 Kernel+ x86	No

Automated Response Compatibility

EasyNAC is designed to be able to integrate with any existing security system to help reduce the Mean Time to Response (MTTR). As a network agnostic vendor, we designed a solution that can integrate with numerous brands for Automatic Threat Response.

Type	Compatibility
Firewall \ IPS*	Any brand, any version, any firmware
SIEM*	Any brand, any version, any firmware
Endpoint Protection Platforms*	Any brand, any version, any firmware
Endpoint Detection and Response systems*	Any brand, any version, any firmware
Mobile Device Management systems*	Any brand, any version, any firmware
Other security solutions*	Any brand, any version, any firmware

***** Automatic Threat Response works with any solution that can send e-mail or syslog alerts. An EasyNAC API is also available for customized integrations.

End of Document