V 3.2

EasyNAC

INSTALLATION AND CONFIGURATION GUIDE

EasyNAC and vLinks are trademarks of InfoExpress, Inc. Other product and service names are trademarks and service marks of their respective owners.

Copyright © 2026 InfoExpress Incorporated. All Rights Reserved. InfoExpress products and services are protected by one or more of the following U.S. Patents: 8347351, 8347350, 8117645, 8112788, 8108909, 8051460, 7523484, 7890658, 7590733. Additional patents pending.

www.easynac.com

infoexpress

Last Revised: May 11, 2026

TABLE OF CONTENTS

DISCLAIMER **10**

ABOUT THIS GUIDE **11**

Scope 11
Conventions Used in This Guide 11

OVERVIEW **12**

Product Architecture 12
Reference Deployment Models 13
Data Flow at Layer-2 13
Key Capabilities 15
Appliance Licensing Options 16
EasyNAC Appliance System Specifications *16*
Sizing & Capacity Planning 16
Headroom in Production *16*
Mapping Environment to Model *17*
Virtual Appliance Requirements *17*
Conditions That Affect Actual Ceilings *18*
When to Engage InfoExpress Support *18*
Device Licensing 19
EasyNAC Deployment Processes 20

DEPLOYMENT CONSIDERATIONS **21**

Layer-2 Enforcement Scope 21
Capacity Ceilings Per Appliance 21
Centrally-Managed Scenarios 21
Hardware-Appliance EOL/EOS 21

VIRTUAL MACHINE (VM) INSTALLATION **22**

Installing on VMware ESX / ESXi 22
Installing on Hyper-V Server 23
Installing on Nutanix AHV / Prism 24
Installing on Proxmox VE 25

CONFIGURING THE EASYNAC APPLIANCE **26**

Appliance Placement 26
Initial Configuration 26
Basic IP Configuration – Management IP *26*
Captive Portal IP Address *27*
Remediation Portal IP Address *28*
Certificate Management (Optional) *28*
Option 1 — Generate a Certificate Signing Request (CSR) From Your CA *28*
Option 2 — Upload a Certificate and Private Key to the EasyNAC Appliance *30*
Connecting to Active Directory *30*
AD Integration *31*

NOTIFICATIONS: EMAIL, SMS, SYSLOG, SLACK, TEAMS AND WHATSAPP **32**

Notification Contacts 32

© 2026 InfoExpress, Inc.

E-MAIL NOTIFICATIONS — SMTP 33
E-MAIL NOTIFICATIONS — MICROSOFT 365 (OAUTH2) 34
E-MAIL NOTIFICATIONS — GOOGLE WORKSPACE (OAUTH2) 36
CONFIGURING NOTIFICATIONS 38
E-MAIL ACTION BUTTON 38
MICROSOFT TEAMS NOTIFICATIONS (OAUTH2) 40
SLACK NOTIFICATIONS (SLACK APP) 42
WHATSAPP INTEGRATION 44
WhatsApp Integration Prerequisites *44*
WhatsApp Registration Process *44*
Enabling WhatsApp Alerts *47*

PROTECTING ADDITIONAL SUBNETS 48

ADDING NETWORK ADAPTERS 48
USING 802.1Q TRUNK PORTS 49
Configuring 802.1q Support on VMware ESX/ESXi *49*
Configuring 802.1q Support on Hyper-V *50*
Configuring 802.1q Support on Nutanix Prism *51*
Configuring 802.1q Support on Proxmox *52*
NETWORK GROUP 52

EXTENDING PROTECTION TO REMOTE SITES 54

ENFORCER SENSOR OVERVIEW 54
Enforcer Sensor (Microsoft Windows) Installation *55*
Enforcer Sensor (Linux) Installation *56*
Enforcer Sensor (Raspberry Pi) Installation *57*
Accepting the Enforcer Sensor *58*
ENFORCER SENSORS PAGE 59

ENFORCEMENT OVERVIEW 60

CONFIGURING ACCESS POLICIES IN EASYNAC 60
AUTO TRUST POLICY 62
Rules and Conditions *62*
Device Conditions *62*
Configuration Notes *66*
Default Rule Reference *66*
ROLES & ACCESS POLICY 68
Behavior *68*
Time and Location-Based Assignment *68*
Configuration Notes *68*
ACCESS GROUPS (ACLS) 69
Modifying an ACL *69*
Default Restricted ACL Behavior *69*
ACL RULE STRUCTURE 69
Supported Actions *69*
Supported Conditions *69*
Operators *70*
Notes *70*
ACL EXAMPLES 70

© 2026 InfoExpress, Inc.

TAGGING DEVICES AND ALLOWLISTING 72

TAGS 72
ALLOWLIST / BLOCKLIST / EXCLUDELIST / ROUTERLIST 74
Adding Devices to the Allowlist or Blocklist 75
The Excludelist 75
The Routerlist 75

DEVICE DISCOVERY 76

DHCP-BASED DISCOVERY 76
STATIC IP DISCOVERY 76
BROADCAST AND MULTICAST MONITORING 76
ACTIVE NETWORK SCANNING 76
SNMP-BASED DISCOVERY (OPTIONAL) 77
SUMMARY 77
DEVICE PROFILING 78
DHCP Profiling 78
Fingerbank 78
NMAP Profiling 78
Upnp Profiling 79
SNMP Scan 79
CONFIGURING DEVICE PROFILER POLICIES 80
Device Detail Data 80
Device Profiling Policies 80
NETWORK MAP 82

ANTI-SPOOFING PROTECTION 84

SETTING FINGERPRINTS 84
MAC Spoofing Detection 85
IP Spoofing Detection 85
Fingerprint Rescan Interval 85
Multi-Factor Authentication 85
Mismatched Authentication 87
Rogue DHCP Server Detection 87

TIME / LOCATION / LIST POLICIES 88

LOCATION POLICY 88
TIME POLICY 89
DEVICE-LISTS POLICY 89

CONFIGURING GUEST ACCESS 90

CUSTOMIZE CAPTIVE PORTAL 90
CUSTOMIZE GUEST PORTAL 90
GUEST REGISTRATION TEMPLATES 91
CUSTOMIZING DEVICE REGISTRATION TEMPLATES FOR GUESTS 92
SETTING UP SPONSORS 94
SPONSORING USERS 94

CONFIGURING DEVICE REGISTRATION 95

CUSTOMIZING THE DEVICE REGISTRATION PORTAL 95

Confirm Active Directory Settings 95
Customizing Device Registration Methods 95
User Experience 96

INTEGRATION MODULES 98

Integration Policies Page Structure 99
Settings Shared by All the Integrations 99
Vendor Categories 99
Bitdefender Integration 99
Carbon Black Cb Response Integration 100
Carbon Black Cloud Integration 101
CrowdStrike Integration 101
Cybereason Integration 102
Elastic Integration 103
ESET Antivirus Integration 103
Trellix Endpoint Security HX Integration (Formerly FireEye HX) 104
Google Workspace Integration 105
Headwind MDM Integration 106
HCL BigFix Integration 107
Ivanti Security Controls 107
Jamf Integration 108
Kaseya VSA Integration 109
Kaspersky Antivirus Integration 110
ManageEngine Desktop Central Integration 110
ManageEngine Patch Manager Integration 111
Microsoft Defender Integration 112
Microsoft Intune Integration 113
Microsoft SCCM / WSUS Integration 114
Microsoft Windows Management Instrumentation (WMI) 115
Moscii StarCat Integration 116
Okta Integration 117
Palo Alto Cortex XDR Integration 117
SentinelOne Integration 118
SolarWinds Integration 119
Sophos Integration 120
Sure MDM Integration 121
Symantec Endpoint Protection Manager - 14.X 122
Tenable Integration 122
Trend Micro Integration 123
Trellix ePolicy Orchestrator Integration 124
Webroot Integration 125

ORCHESTRATION EVENTS 126

Orchestration with Syslog 126
Syslog Event Creation 127
Orchestration Email Alert 128
Email Event Creation 128

ADVANCED SECURITY 130

Malware Lateral Spread Protection - Zero-Day 130
Policy-Based Response *131*
Clearing Zero-Day Events *131*
Handling Exceptions *131*
Deception – Hacking Detection 131
Policy-Based Response *132*
Credentials Used *132*
Edge Protection – Layer-2 Security 132
Policy-Based Notifications *132*

AGENT SUPPORT 133

Working with Agents 133
Hosting Agents 134
Installing Agents 134
On-Demand Agents (Recommended for Consultants) 134
Agent Compliance Policies 135
Policy Manager 136
Policies 137
Policies Best Practices *138*
Requirements to Pass a Policy 138
Requirements Priority *138*
Requirement Best Practices *139*
Remediation 139
Pop-Up Messages *139*
Remediation Actions *140*
Auto-Remediation *140*
Remediation Best Practices *140*
Using Active Directory User Group in Auto Trust Policy 141
Prerequisites *141*
DNS Server and Domain Settings for the EasyNAC Appliance *141*
Configure Active Directory User Group *142*
Joining the EasyNAC Appliance to Active Directory *142*
Cybergatekeeper Agent Authentication Plugin *142*
Add the User Group as a Condition in Auto Trust Policy *142*
Troubleshooting Agents 142
Installation Issues *142*
Connection Issues *143*

ADVANCED CONFIGURATION OPTIONS 145

Permission Manager - Administration Permissions 145
Pre-Defined Administrator Roles *148*
Granular Permission Grid *148*
Site Filter and Expiration *149*
Recommended Role Design *149*
Single Sign-on with SAML 150
Configuring 2FA for the EasyNAC Appliance Admin Login 151
Configuring RADIUS for EasyNAC Admin Login or BYOD Authentication 151
RADIUS Server Configuration *151*
EasyNAC Configuration *152*

© 2026 InfoExpress, Inc.

Customizing Landing Pages 153

EASYNAC API 154

Overview 154
What the API Does and Does Not Do 154
Authentication Model 154
Registering an Application 154
Token Issuance and Lifecycle 155
Sample API Call Structure 155
Rate Limits and Error Codes 155
Disabling or Revoking an Application 155
API Versioning and Deprecation Policy 156
Deprecation Timeline 156
Communications 156
Error Codes 156

HIGH AVAILABILITY 158

Requirements 158
Configuration – Standalone Appliances 159
Configuration – Centrally Managed Appliances 160
Configure the Cvm to Be an Arbiter (Optional) 160
Making HA Configuration Changes 162
Replace a Primary 162
Replace a Backup 162
Restore From a Backup Image 162
Upgrade to a New Version 162
Other Reconfiguration Changes 162

CENTRAL VISIBILITY MANAGER 163

Cvm Overview 163
Required Ports 163
Configuring a Central Visibility Manager 164
Configuring an Appliance to Be Centrally Managed 165
Deployment Manager 166
Software Updates 166
Central Visibility Manager – Device Roaming 167
Central Visibility Manager – Integration Proxy 167

MIGRATING FROM OTHER NAC SOLUTIONS 168

Pre-Migration Discovery Checklist 168
Migrating From Dynamic NAC (Legacy InfoExpress Product) 168
Pre-Migration Checklist 168
Import Procedure 169
Post-Import Validation 169
Migrating From Forescout 169
Source Data Mapping 169
Exporting Data From Forescout 169
Importing Into EasyNAC 170
Post-Import Validation 170

General Post-Migration Checklist 170

HARDENING CHECKLIST 171

1. Change Default Admin / Admin Credentials 171
2. Replace Default Self-Signed SSL Certificate 172
3. Restrict SSH Service Access with a Need to Know Basis. 172
4. Configure RADIUS, 2FA or SAML for Admin Authentication 172
5. Set Audit and Device-Record Log Retention 172
6. Configure Backup Destination and Automatic Backup 173
7. Verify NTP Servers Are Reachable 173
8. Apply Latest Software Update 173
9. Review Default Auto Trust Policy 173
10. Review Permission Manager Roles 174
11. Document Recovery Procedures 174

MAINTENANCE AND SUPPORT 175

Upgrading Firmware 175
Collecting Logs (Dump2) 176
SSL Certificate Manager 177
Account Manager 177
Software Update Procedure 177
Site Settings and Server Mode 178
Backup Destinations and Automatic Backup 178

APPENDIX A – INLINE ENFORCEMENT 179

Inline Enforcement Overview 179
Features 179
Requirements 179
Sample Test Network 180
Configuration 181
Location 181
Network Interfaces 181
Bridge IP 182
Access Control List 183
Enforcement Ranges 183

APPENDIX B – 802.1X RADIUS PROXY 185

RADIUS Proxy Overview 185
Requirements 185
Features 185
Configuring RADIUS Proxy Settings on the EasyNAC Appliance 185

APPENDIX C – USING NPS TO AUTHENTICATE EASYNAC USERS 187

Add Admin Group / Users to Active Directory 187
Configure Network Policy Server 188
Configure the EasyNAC Appliance to Allow Log in Using RADIUS 190
To Authenticate BYOD Users via Network Policy Server 190

APPENDIX D – VLINKS OVERVIEW 192

vLinks Central Setup 193

vLinks Remote Setup 193

APPENDIX E – FAILURE MODES 196

APPENDIX F – CONFIGURING THE CAPTIVE PORTAL API 197

Prerequisites 197
Configuration on the EasyNAC Appliance 197
Configuration on the Windows DHCP Server 197
Define the Predefined Option 197
Apply the Option Value to a DHCP Scope 198
Verification 198
Notes 198

APPENDIX G – DEPLOYMENT CHECKLIST 199

Phase 1 — Pre-Deployment Planning 199
Phase 2 — Virtual Machine Preparation 199
Phase 3 — Network Preparation 200
Phase 4 — Initial Appliance Configuration 200
Phase 5 — Active Directory Integration 201
Phase 6 — Notifications 202
Phase 7 — Policy Configuration 202
Phase 8 — Integration Setup 202
Phase 9 — Pre-Cutover Testing 203
Phase 10 — Production Cutover 203
Phase 11 — Post-Deployment Hardening 204

APPENDIX H – GLOSSARY 205

DISCLAIMER

The information in this document is provided for general guidance only and is subject to change without notice. While InfoExpress Inc. makes reasonable efforts to ensure the accuracy of the content at the time of publication, it is provided "as is" without any express or implied warranties, including, without limitation, warranties of accuracy, completeness, or fitness for a particular purpose.

Users are solely responsible for evaluating and determining the suitability of any products or information described in this document for their specific use cases. This document is intended to describe general product behavior and shall not be relied upon as a guarantee or representation of specific features or functionality in any particular product version.

This document forms part of the official product documentation. Product specifications and functionality may be updated or modified from time to time as described herein or in any accompanying materials.

The software described in this document is provided subject to the terms and conditions of the applicable license agreement and may be used only in accordance with those terms.

All product names, trademarks, and registered trademarks referenced herein are the property of their respective owners.

The information contained in this document is proprietary to InfoExpress Inc. and may not be reproduced, disclosed, or distributed without prior written permission.

© 2026 InfoExpress, Inc.

ABOUT THIS GUIDE

This guide describes how to install, configure, and operate the EasyNAC Network Access Control platform in an enterprise environment. It covers the EasyNAC Appliance, Enforcer Sensors, Central Visibility Manager, integration modules, and the operational practices required to run EasyNAC reliably at scale.

SCOPE

This guide covers:

- Installation of the EasyNAC Appliance on supported virtual and physical platforms.
- Initial configuration of network interfaces, Captive Portal, certificates, and Active Directory.
- **All built-in policy primitives** — Auto Trust, Roles & Access, Tags, Permission Manager, Time / Location / List policies.
- Each supported third-party integration, with prerequisites, configuration steps, and verification.
- High Availability, Central Visibility Manager, Enforcer Sensors, and vLinks.
- Operational maintenance, hardening, upgrade, backup, restore, and recovery procedures.

Out of scope:

- Detailed network design (VLAN architecture, firewall design, routing) of the host network. EasyNAC is deployed into the customer's existing network; the design of that network is the customer's responsibility.
- Endpoint hardening of devices that EasyNAC protects. EasyNAC reports on and enforces against endpoint state; it does not configure endpoints directly.
- Detailed third-party product configuration. Each integration chapter covers what EasyNAC needs from the third-party vendor; full product configuration is the third-party vendor's documentation.

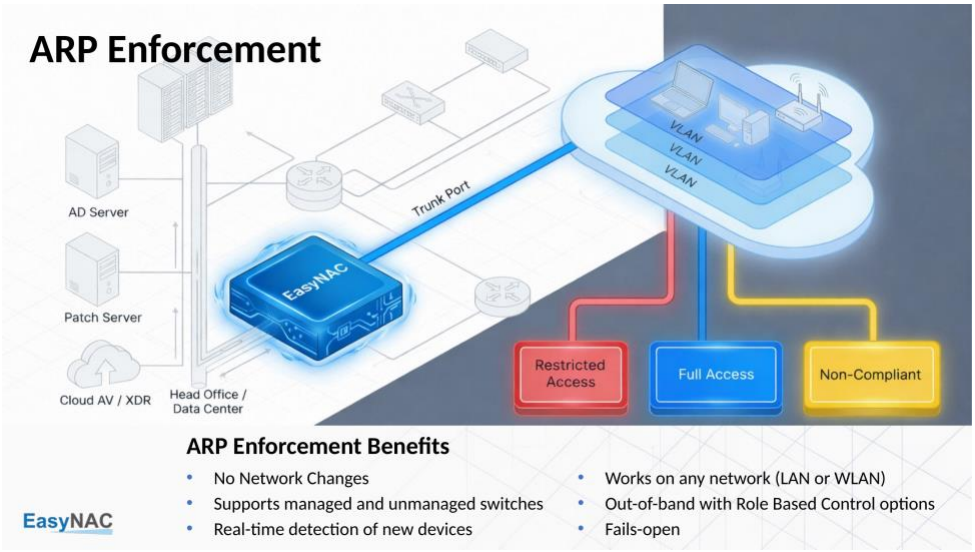
CONVENTIONS USED IN THIS GUIDE

- UI element names (buttons, menus, fields) appear in **bold**. Example: click **Save**.
- Menu paths use forward slash with spaces. Example: **Control / Network Map / Settings**.
- Code, CLI commands, file paths, and URLs appear in `monospace`.
- Placeholder values appear in angle brackets, e.g. `<your-domain>`.
- **Note** — informational only; reading is optional.
- **Tip** — helpful but not required for correct operation.
- **Caution** — indicates a security or correctness risk if the step is skipped or done out of order.
- **Warning** — indicates risk of data loss, service outage, or rollback difficulty.

© 2026 InfoExpress, Inc.

OVERVIEW

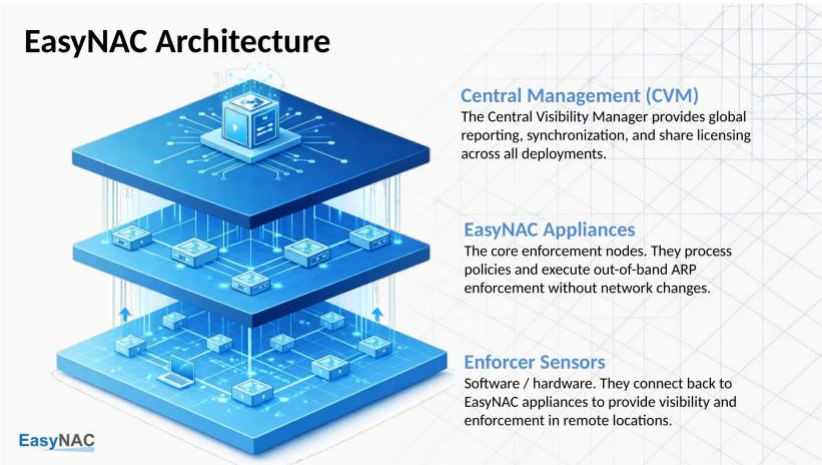
EasyNAC is a Network Access Control (NAC) platform that delivers Zero Trust security across wired and wireless networks. Designed to simplify enterprise NAC deployment and administration while maintaining comprehensive enforcement capabilities, EasyNAC provides immediate, agentless visibility into every device on the network and enforces granular access policies in real-time.



The EasyNAC Appliance sits out-of-band on the network, using ARP-based enforcement and DNS/HTTP redirection to control device access without becoming a single point of failure. The platform integrates with Active Directory, endpoint protection solutions, and leading SIEM/SOAR platforms to provide automated, policy-driven responses to security events.

PRODUCT ARCHITECTURE

The EasyNAC platform consists of three tiers: the EasyNAC Appliance (physical or virtual), optional Enforcer Sensors for remote subnet coverage, and the Central Visibility Manager (CVM) for multi-site management. Each appliance monitors all devices on its connected subnets using passive ARP inspection, building a real-time inventory of every network-connected endpoint.



© 2026 InfoExpress, Inc.

REFERENCE DEPLOYMENT MODELS

The same EasyNAC component set supports deployments from a single subnet at a small office to a multi-region enterprise estate. Four patterns cover the bulk of customer environments. Pick the pattern that matches the operational shape of your network, then size each appliance using the guidance under Sizing & capacity planning.

Pattern	When to use	Failure-mode behavior
Single appliance	Single site, single appliance protecting one or more locally-reachable subnets. Suitable for evaluations and for offices up to the supported device count of the chosen model.	No redundancy. If the appliance is unreachable, ARP enforcement stops; the network reverts to its baseline (no NAC).
HA pair	Single site, two appliances in active / standby. Production deployments where loss of NAC enforcement is unacceptable.	Automatic failover within the configured window. In-flight traffic for already-trusted devices is not disrupted; new-device profiling pauses briefly during failover.
Central appliance + remote Enforcer Sensors	One central appliance that holds all policy plus one Enforcer Sensor per remote subnet that is not directly reachable at Layer-2. This deployment model is commonly used in multi-site environments.	If a remote sensor is unreachable, enforcement at that remote subnet pauses; remaining subnets continue normally. The central appliance is the policy source of truth.
Multi-site with Central Visibility Manager (CVM)	Several site appliances managed by a CVM. Typical for large enterprises with regional admin teams or with regulated separation between sites. Adds cross-appliance reporting, tag synchronization and integration-proxy capabilities.	Each site appliance enforces independently. If the CVM is unreachable, sites continue to enforce on their last-known policy; centralized reporting and tag sync pause until reconnection.

Mixed deployments are supported — a CVM can manage a combination of standalone, HA-paired, and remote-sensor appliances. Choose the pattern per site rather than per estate.

DATA FLOW AT LAYER-2

EasyNAC enforces network access by participating in the ARP layer of each protected subnet. The appliance does not sit in the data path; client traffic is not forwarded through it.

When a device joins a protected subnet:

- The appliance observes the device through DHCP requests, ARP traffic, and (optionally) active scans.
- **The device is profiled** — operating system, hostname, MAC OUI, open ports, fingerprint attributes — and matched against the Auto Trust Policy.
- Auto Trust assigns the device a role; Roles & Access maps the role to an ACL or VLAN action.
- If the role permits full access, EasyNAC remains passive — the device communicates as if EasyNAC were absent.
- If the role restricts access, EasyNAC injects ARP responses that redirect the device's traffic toward the restricted destinations only (typically DNS, DHCP, captive / remediation portal). All other Layer-3 destinations become unreachable from that device.

© 2026 InfoExpress, Inc.

Two practical consequences:

- Restoration is instantaneous. Removing a device from restriction stops the ARP injection; existing client sessions resume in real-time.
- No switch reconfiguration is required. EasyNAC operates at the Ethernet broadcast domain, so any device that can reach the appliance via ARP can be enforced.

For subnets that the appliance cannot reach at Layer-2 — typically remote-site subnets behind a Layer-3 boundary — deploy an Enforcer Sensor at the remote subnet. The sensor extends ARP enforcement on behalf of the central appliance, communicating policy decisions over TCP 8889. See **Extending Protection to Remote Sites**.

© 2026 InfoExpress, Inc.

KEY CAPABILITIES

The EasyNAC Appliance provides a comprehensive set of network security capabilities across four pillars: visibility, enforcement, threat response, and access management.

Agentless Visibility Discover every device on the network instantly — no endpoint agents required. Covers IoT, OT, BYOD, and unmanaged devices.	**ARP-Based Enforcement** Layer-2 access control using ARP interception and DNS/HTTP redirection. No switch reconfiguration or 802.1X hardware needed.
LAN / WLAN Protection Unified policy enforcement across wired and wireless networks. Quarantine, redirect, or block untrusted devices automatically.	**Automated Allowlisting** Active Directory integration automatically trusts authenticated devices. AD-joined endpoints are allowlisted without manual intervention.
Anti-Spoofing Detection Behavioral fingerprinting detects MAC and IP spoofing anomalies. Suspect devices are flagged or auto-quarantined in real-time.	**AV / XDR Enforcement** Integrates with leading Antivirus and XDR solutions. Non-compliant endpoints are quarantined at network admission.
Threat Orchestration SIEM and SOAR platforms trigger automated quarantine via email, syslog, REST API for rapid incident containment.	**Zero-Day Protection** Detects lateral movement patterns indicative of malware propagation and ransomware — independent of signatures.
Deception Detection Honeypot services (SSH, Telnet, FTP, SMB) on every VLAN provide high-confidence early warning of insider threats and recon.	**BYOD Registration** Self-service portal for employees to register personal devices with configurable sponsorship workflows and access policies.
Guest Access Management Multi-workflow guest portal: sponsor-approved, self-registration, or pre-provisioned accounts with session time and bandwidth limits.	**Role-Based Access Control** Granular control using ACL rules by IP range, port, and protocol. Tailored profiles for every device category.

© 2026 InfoExpress, Inc.

APPLIANCE LICENSING OPTIONS

EasyNAC is available as a physical appliance or as a virtual appliance deployable on VMware ESX/ESXi, Microsoft Hyper-V, Nutanix, and Proxmox VE. The CVM can also be deployed in major cloud platforms including Microsoft Azure and Amazon AWS. Licensing is based on the number of endpoint devices managed. All hardware and virtual appliance models run the same software and support the same feature set.

For current pricing, available models, and licensing terms, contact your authorized InfoExpress partner or reach the InfoExpress sales team at sales@infoexpress.com.

EASYNAC APPLIANCE SYSTEM SPECIFICATIONS

	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*	10	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

** Capacity is approximate and depends on VLANs protected, endpoints, and features enabled.*

SIZING & CAPACITY PLANNING

The Appliance System Specifications table above lists the supported maxima per appliance model. Three considerations help translate those numbers into a procurement decision.

HEADROOM IN PRODUCTION

Plan production capacity at 70 percent of the published maximum. The remaining 30 percent absorbs short-term spikes (large deployments of new devices, BYOD-onboarding events, conference-room peaks) and provides margin for the additional load that integrations and profiling generate. Sustained operation above 80 percent of the published maximum is supported but reduces the appliance's ability to absorb spikes.

© 2026 InfoExpress, Inc.

MAPPING ENVIRONMENT TO MODEL

Use the following starting points; refine with InfoExpress Support if your environment has unusual integration density, deep NMAP profiling, or many small VLANs.

Environment shape	Suggested starting model	Notes
Up to 200 devices, single subnet, evaluation or branch office	S10 or ENAC-VM	S10 caps at 300 devices and 10 subnets; the VM scales as the host allows.
200–1,500 devices, several VLANs, small to mid-market enterprise	S100 or ENAC-VM	S100 supports 2,500 devices and 250 subnets — leaves headroom for two-to-three years of growth.
1,500–4,000 devices, many VLANs, several integrations	S200 or ENAC-VM (large)	S200 supports 5,000 devices and 400 subnets. This model is commonly deployed within mid-sized enterprise environments.
4,000–8,000 devices, dense integrations, regulatory environment	S500 or S600	S500 and S600 cap at 10,000 devices and 400 subnets. Difference is interface speed (S600 has 10G SFP+).
8,000+ devices on a single appliance	S500 / S600 with multi-site CVM	Above ~80 percent of the supported maximum, plan a multi-appliance deployment under a CVM rather than a larger single appliance.

VIRTUAL APPLIANCE REQUIREMENTS

The following minimum specifications apply when deploying the ENAC-VM. Size the VM to the number of devices the appliance will protect, with headroom per the guidance above.

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	8 vCPU / 16 GB RAM
Minimum Specs: 5,000+ devices	16 vCPU / 32 GB RAM
Virtual Storage Capacity	40 GB to 512 GB

© 2026 InfoExpress, Inc.

CONDITIONS THAT AFFECT ACTUAL CEILINGS

- Number of VLANs being protected. Each VLAN consumes a small amount of state.
- Number of integrations enabled and their polling frequency. Each API call consumes CPU and memory; aggressive polling against many integrations can shift the practical ceiling.
- Profiling depth. Active NMAP-based scanning is more expensive than passive DHCP profiling; deep scanning of every device on a 5,000-device network materially raises load.
- Logging verbosity. Debug-level logging at high event rates can saturate disk I/O before the device-count ceiling is reached.

WHEN TO ENGAGE INFOEXPRESS SUPPORT

Engage InfoExpress Support for sizing review if any of the following apply: planned operation above 80 percent of the supported maximum on day one; more than ten enabled integrations; subnets that exceed 250 protected VLANs per appliance.

© 2026 InfoExpress, Inc.

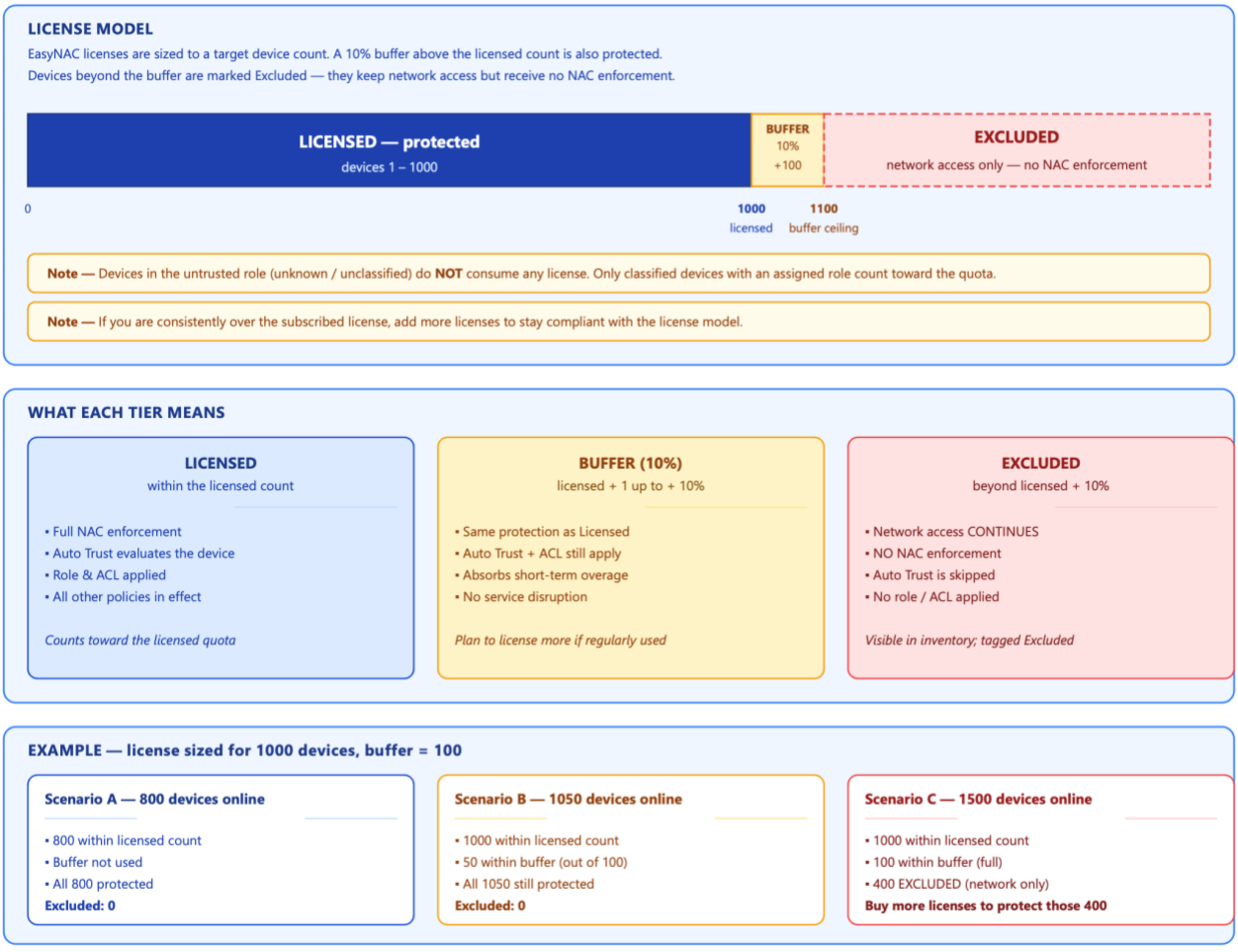
DEVICE LICENSING

EasyNAC uses a simple and scalable device-based licensing model designed to align with how modern networks operate. Licensing is based on the number of unique devices visible to the system within a rolling 5-minute window, rather than total installed assets or users. This ensures customers are only licensing actively connected devices at any given time, while maintaining flexibility for dynamic environments such as BYOD, IoT, and transient endpoints.

All core EasyNAC capabilities are included within the device license, providing full access to features such as device discovery, profiling, policy enforcement, segmentation, visibility, and reporting. This eliminates the need for feature-based add-ons and allows customers to deploy the solution without artificial limitations.

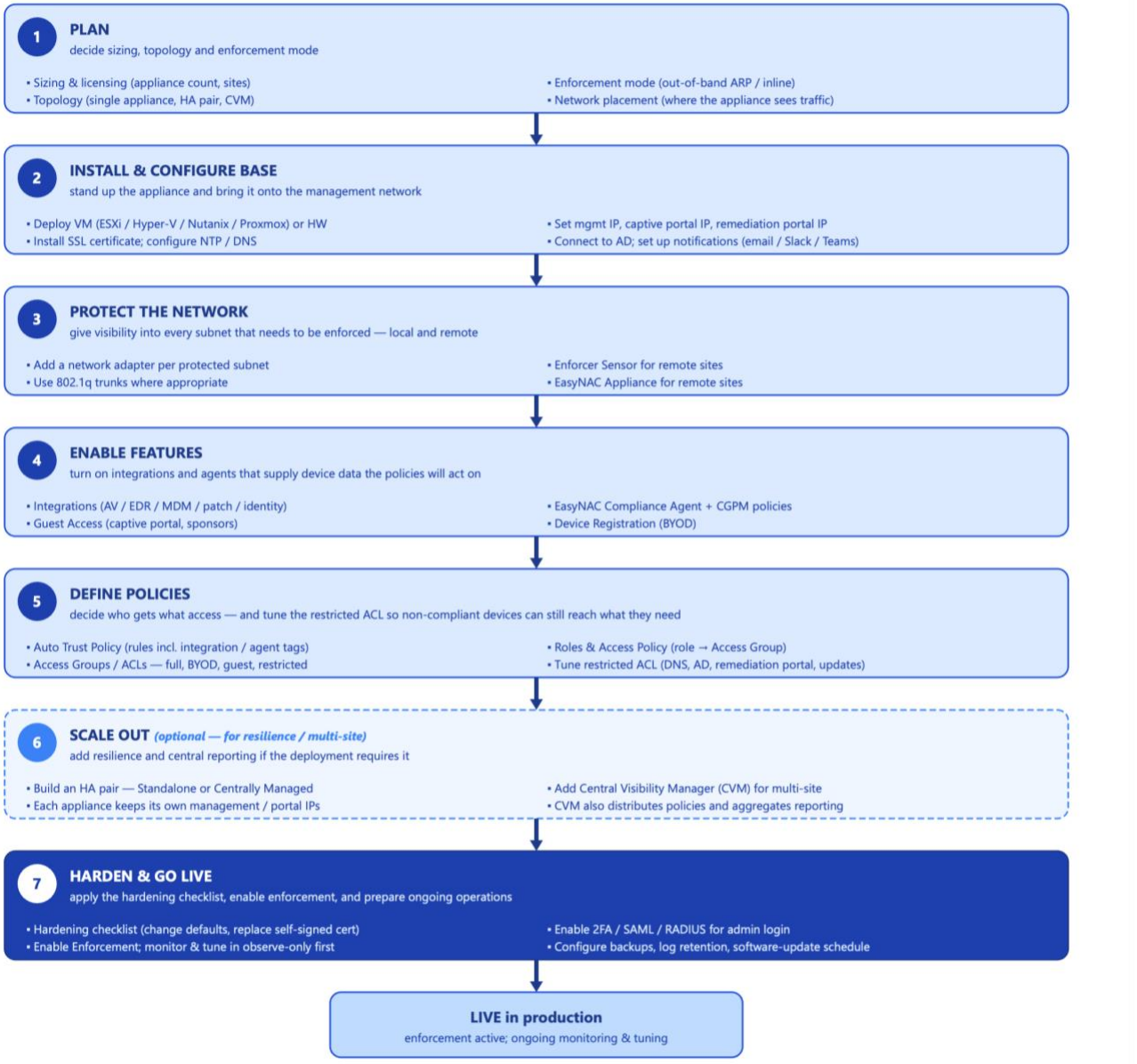
Optional components, including High Availability (HA), Central Visibility Manager (CVM), Enforcer Sensors, vLinks and the EasyNAC Compliance Agent, are licensed separately.

The model is straightforward to manage, cost-effective at scale, and well suited for both small deployments and large enterprise networks.



© 2026 InfoExpress, Inc.

EASYNAC DEPLOYMENT PROCESSES



© 2026 InfoExpress, Inc.

DEPLOYMENT CONSIDERATIONS

LAYER-2 ENFORCEMENT SCOPE

ARP-based enforcement is L2-scoped. EasyNAC controls access on subnets it has Layer-2 visibility into, either directly through a network adapter / 802.1Q trunk or via an Enforcer Sensor at a remote site.

- a subnet that is reachable from the appliance only at Layer 3 cannot be enforced. Discovery is possible (via SNMP or DHCP relay), but tags cannot be enforced as ACL actions.
- Deploy dedicated EasyNAC Appliance OR
- an Enforcer Sensor at the remote site.

CAPACITY CEILINGS PER APPLIANCE

The supported maximums in the EasyNAC Appliance System Specifications table are conservative figures that hold under typical conditions. Actual ceilings depend on:

- Number of VLANs being protected (each VLAN consumes a small amount of state).
- Number of integrations enabled and their polling frequency (each API call consumes CPU and memory).
- Profiling scan depth (NMAP-based deep scan is more expensive than passive DHCP profiling).
- Logging verbosity (debug-level logging at high event rates may saturate the disk).

If you intend to operate near the supported maximums, contact InfoExpress Support for a sizing review before going to production.

CENTRALLY-MANAGED SCENARIOS

In a CVM-managed deployment, the CVM is the source of truth for shared policy and integration data. If the CVM is unreachable from a managed appliance:

- Existing policy on the appliance continues to enforce normally.
- Roaming-device records and centralized tag updates pause until the CVM is reachable again.
- Integration-proxy data (where the CVM acts as the integration source) is unavailable until reconnection.
- Allocated licenses continue to function for up to 30 days

HARDWARE-APPLIANCE EOL/EOS

Each hardware appliance model has a published end-of-life and end-of-support date. After EOL, no new appliances of that model are sold; after EOS, security and bug fixes are no longer issued. The current EOL/EOS table is published on the InfoExpress support portal; contact InfoExpress Support before procuring or extending hardware close to or past these dates.

© 2026 InfoExpress, Inc.

VIRTUAL MACHINE (VM) INSTALLATION

EasyNAC is distributed as a virtual appliance in OVF format for VMware environments and as a pre-configured VHD package for Microsoft Hyper-V. The virtual appliance runs on a standard Linux OS and requires no additional software installation once deployed. Physical appliance deployments ship pre-installed and ready to configure; refer to the hardware quick-start guide included with the EasyNAC Appliance.

INSTALLING ON VMWARE ESX / ESXI

The EasyNAC virtual appliance is deployed on VMware ESXi using an OVF template. The OVF package is distributed as a compressed (.zip) archive; contact InfoExpress or your business partner if you do not have it.

Preparation

- Extract the archive to a location accessible from your workstation.
- Confirm access to the VMware vSphere Client.

Deployment Steps (vSphere Web Client)

- Log in to the vSphere Client using your web browser.
- In the inventory panel, right-click on your target host or cluster.
- Select Deploy OVF Template.

Note: *In legacy desktop clients, this option is located under the File menu.*

- Select Local file, browse to the OVF file, and click Next.
- Review the OVF template details, then click Next.

Note: *A security warning about an unsigned template is expected. Proceed if the file is from a trusted source.*

- Enter a name for the virtual machine, select a location if prompted, and click Next.
- Select the target compute resource (host or cluster) and click Next.
- Select the datastore for the virtual machine, then click Next.

Note: *Newer vSphere versions may also prompt for a storage policy.*

- Select the disk provisioning format (thin or thick) and click Next.
- Map the EasyNAC appliance interfaces to the appropriate port groups or distributed switches, then click Next.
- Review all configuration settings, then click Finish to begin deployment.

After Deployment

- The vSphere Client uploads and deploys the appliance.

© 2026 InfoExpress, Inc.

- When deployment completes, power on the virtual machine and proceed to the EasyNAC appliance configuration.

INSTALLING ON HYPER-V SERVER

The EasyNAC virtual appliance is deployed on Microsoft Hyper-V (Windows Server 2019 or later). The image is distributed as a compressed (.zip) archive; contact InfoExpress or your business partner if you do not have it.

Preparation

- Extract the archive to a location accessible from the Hyper-V host.
- Confirm Hyper-V Manager is installed and you have administrative access to the host.
- Create the Virtual Switch the appliance will use in advance; newer Hyper-V versions require explicit network assignment.

Deployment Steps (Hyper-V Manager)

- Open Hyper-V Manager.
- In the Actions panel, click Import Virtual Machine.
- On the Locate Folder screen, browse to the folder containing the extracted image, then click Next.
- Select the virtual machine listed (for example, EasyNAC-3.2) and click Next.
- For the import type, select Copy the virtual machine (create a new unique ID) and click Next.
- Specify the destination folders for the virtual machine configuration, snapshots (checkpoints), and virtual hard disks, then click Next.
- Confirm or select the destination folder for the virtual hard disk if prompted, then click Next.
- Review the configuration on the Summary screen, then click Finish to begin the import.
- The wizard imports and registers the virtual machine; once completed, it appears in Hyper-V Manager.

Post-Deployment Configuration

- Select the imported virtual machine and click Settings in the Actions panel.
- Select Network Adapter from the hardware list.
- Assign the appropriate Virtual Switch from the dropdown, then click Apply and OK.

After Deployment

- Verify CPU, memory, and disk settings before starting the virtual machine.
- Power on the virtual machine and proceed to the EasyNAC appliance configuration.

© 2026 InfoExpress, Inc.

INSTALLING ON NUTANIX AHV / PRISM

The EasyNAC virtual appliance is deployed on Nutanix AHV / Prism using a QCOW2 image. The image is distributed as a compressed (.zip) archive; contact InfoExpress or your business partner if you do not have it.

Preparation

- Extract the archive to a location accessible from the Nutanix Prism interface.
- Confirm access to the Nutanix Prism web console.

Deployment Steps (Nutanix AHV / Prism)

- Log in to the Nutanix Prism web interface.
- Navigate to Settings → Image Configuration and click Upload Image.
- In the Create Image window, enter the required details: Name (for example, EasyNAC-Image), Image Type: Disk, and Storage Container.
- Under Image Source, select Upload a File and choose the extracted .qcow2 file.
- Click Save to upload the image.
- Wait for the image to finish creating.

Note: *This may take approximately 30 minutes depending on the environment.*

- Confirm the image status shows as Active in the Image Configuration list.

Create Virtual Machine

- Navigate to VM → Table.
- Click Create VM.
    - Enter the virtual machine details: Name, vCPU(s), Number of Cores per vCPU, and Memory (RAM).

Note: *Use the specifications recommended by InfoExpress.*

- Under Disks, remove the default CD-ROM and click Add New Disk.
- Configure the new disk: Type: Disk; Operation: Clone from Image Service; Bus Type: SCSI; Image: the uploaded EasyNAC Appliance image. Confirm and add the disk.
- Configure Network: Under Network Adapters, click Add New NIC.
- Select the appropriate network for the appliance and click Add.
- Verify the NIC is listed, then click Save to complete VM creation.

After Deployment

- Power on the virtual machine and proceed with the EasyNAC Appliance configuration.

© 2026 InfoExpress, Inc.

INSTALLING ON PROXMOX VE

The EasyNAC virtual appliance is deployed on Proxmox VE using a Proxmox backup image (vzdump). The image is provided by InfoExpress; contact InfoExpress or your business partner if you do not have it.

Preparation

- Confirm access to the Proxmox web interface.
- Upload the backup image to the Proxmox server storage.

Note: *The file must be placed in the server dump directory (for example, /mnt/pve/<storage>/dump/).*

Deployment Steps (Proxmox)

- Upload the backup image to the appropriate storage dump folder on the Proxmox server using an SCP client such as WinSCP.
- Log in to the Proxmox web interface.
- Navigate to Server → Storage → Backups.
- Locate the uploaded backup file and click Restore.
- In the Restore window, select the target storage, click Unique to generate a new MAC address, and adjust other settings as required. Do not select Start after restore — review settings first.
- Click Restore to begin the process.
- Monitor the restore task until completion.

Note: *Wait until the status shows TASK OK before proceeding.*

Post-Deployment Configuration

- Once restored, the virtual machine appears under Virtual Machines.
- Select the virtual machine and review the hardware settings. By default, only one network adapter is configured.

  To add additional adapters: navigate to VM → Hardware and click Add → Network Device.

After Deployment

- Power on the virtual machine and proceed with the EasyNAC Appliance configuration.

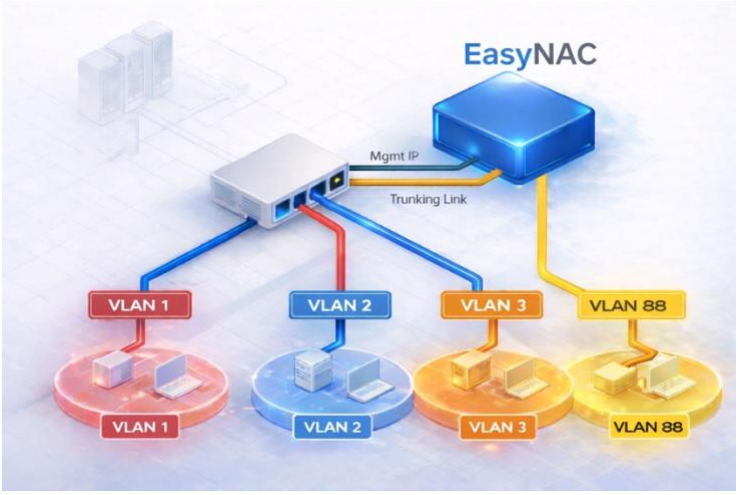
© 2026 InfoExpress, Inc.

CONFIGURING THE EASYNAC APPLIANCE

This section outlines the steps required to configure an EasyNAC Appliance, including initial deployment, network integration, and preparation for enforcing access control policies.

APPLIANCE PLACEMENT

The EasyNAC Appliance enforces access control on the subnets it connects to, providing full Layer-2 visibility. The appliance supports protection across up to 400 VLANs simultaneously using 802.1Q trunking.



The Management IP is the primary interface, used for administration and system communication. It must have connectivity to the Active Directory server, as this is required for policy enforcement and authentication.

For simple, single-subnet testing, the Management IP can be placed directly within the subnet where access control is required. For environments with multiple VLANs, additional interfaces or a trunk port should be configured to extend coverage across those networks.

INITIAL CONFIGURATION

The EasyNAC Appliance deployments typically require three IP addresses. One IP address is used for appliance management. The second IP address hosts the Captive Portal (landing page), and the third IP address hosts the remediation portal.

When protecting additional VLANs, each subnet requires one IP address within its respective network. For example, protecting ten subnets (one Management subnet and nine additional subnets) would require a total of twelve IP addresses. These additional IP addresses can be assigned dynamically using DHCP.

> **Note:** *The EasyNAC Appliance includes built-in ARP-based enforcement. Enforcement can be enabled across up to 400 VLANs, including the subnet where the Management IP resides.*

BASIC IP CONFIGURATION – MANAGEMENT IP

The Management IP provides administrative access to the EasyNAC Appliance and can be accessed via a web browser or SSH. SSH is typically required during the initial configuration process of the Management IP. Once the IP has been configured according to your corporate network, the appliance can be managed through the web interface.

- For physical appliances, connect an Ethernet cable directly to access the default IP address (10.0.0.250/24) via SSH. Alternatively, connect a keyboard and HDMI monitor for direct console access.
- For virtual appliances, open the VM console and power on the system.

Default user accounts are:

© 2026 InfoExpress, Inc.

— admin - used for initial setup and configuration as well as SSH access for maintenance tasks

— cguser - used for uploading files through SFTP.

Note: *The default passwords are the same as the username. These default passwords should be changed.*

Ensure the admin password is stored securely. If it is lost and no alternate administrative account is available, it may not be possible to recover access.

For hardware appliances, loss of access may require the unit to be returned to InfoExpress for RMA.

Log in via SSH or Console

Once the system has completed booting, you will be prompted to log in through SSH or the console.

- Login as ***admin*** with the default password ***admin***
- From the main menu choose 1 (Run Setup Wizard) by entering **1** and press **Enter** to get to the setup wizard
- Follow the prompts to configure the Time zone, Date and Time, Managed IP Address, Subnet Mask, Default Gateway, DNS Servers, and Hostname.

Once the setup wizard is complete, the system should be accessible on the network.

Note: *Verify connectivity by pinging the Management IP from a system on the same subnet, as well as from a system on a different subnet. If connectivity tests fail, check the physical or virtual network connections and confirm the IP configuration is correct.*

Login via web browser

- Access the EasyNAC Appliance web interface by opening https:// in a supported web browser (using the IP configured earlier).

- Log in as user admin (default password admin). A modern browser such as Chrome is strongly recommended.

Supported browsers include recent versions of:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Apple Safari

CAPTIVE PORTAL IP ADDRESS

The EasyNAC Captive Portal is the user-facing interface presented to devices that require authentication or registration before gaining network access. When any unauthorized device connects to a protected network, it is automatically redirected to the Captive Portal.

The portal supports employee device registration and guest access workflows and guest access, allowing users to identify themselves and complete the required authentication process. Based on the selected option and configured policies, EasyNAC will determine the appropriate level of network access.

© 2026 InfoExpress, Inc.

Configure Captive Portal IP

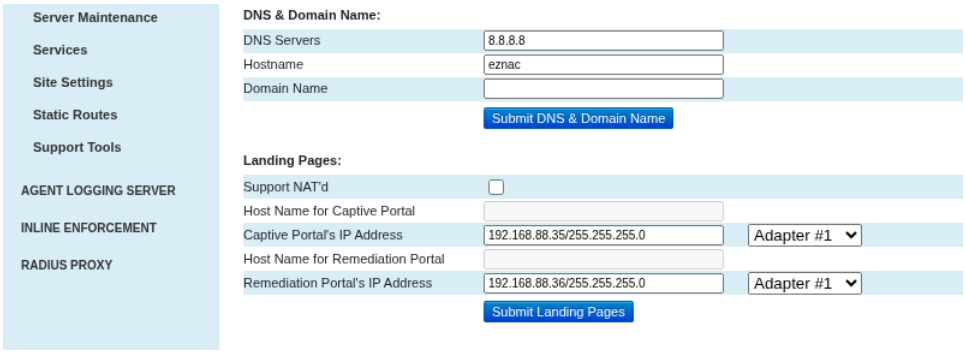
- In the EasyNAC Appliance GUI, navigate to Configuration → Appliance Settings → Networking.
- Enter the Captive Portal IP address using the format IP / Subnet Mask (for example, 10.0.0.251 / 255.255.255.0).
- Click Submit Landing Pages to apply the configuration.

REMEDIATION PORTAL IP ADDRESS

The Remediation Portal is a user-facing page presented to devices that do not meet compliance requirements. It informs users that their device has restricted or limited access and provides details on the reason for the restriction.

To support this functionality, an additional static IP address can be assigned to host the Remediation Portal. When configured, non-compliant endpoints will be redirected to this IP. The Remediation Portal IP is configured in the same way as the Captive Portal IP, using the steps outlined above.

> **Note:** *The Captive Portal and Remediation Portal are hosted on their respective configured IP addresses and must be reachable by all client devices within the protected network to ensure proper redirection and user interaction. Separate IP addresses are used to host the Captive Portal and Remediation Portal pages.*



CERTIFICATE MANAGEMENT (OPTIONAL)

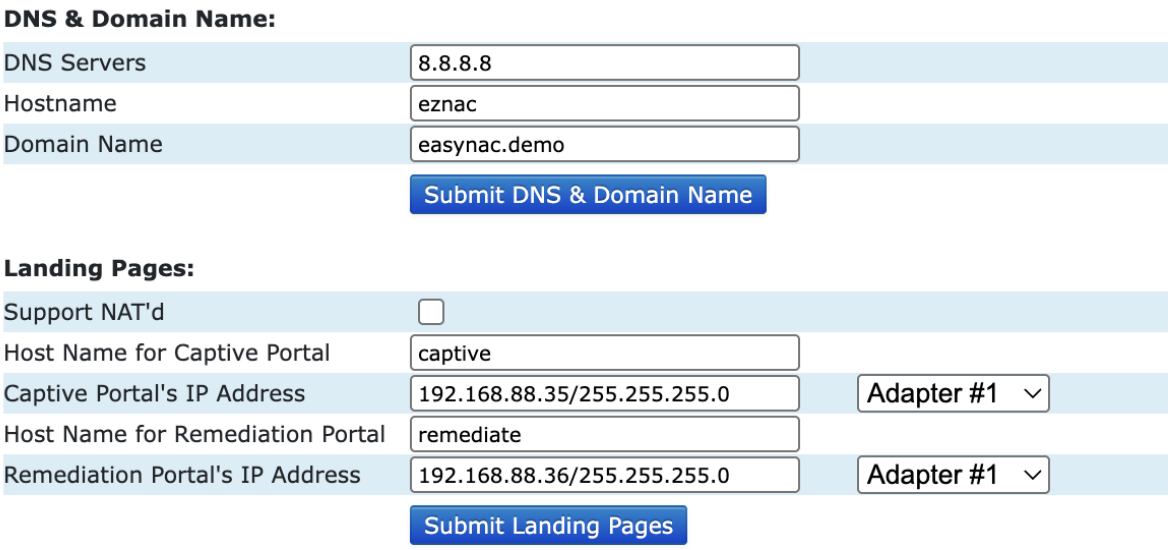
By default, The EasyNAC Appliance uses self-signed certificates which will not be trusted. To eliminate warnings on untrusted certificates, third-party certificates can be uploaded to the appliance.

OPTION 1 — GENERATE A CERTIFICATE SIGNING REQUEST (CSR) FROM YOUR CA

Please note: The EasyNAC Appliance could be using 3 hostnames, one for management-IP, Captive Portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

© 2026 InfoExpress, Inc.

- Log in to the EasyNAC Appliance using username **admin**, Go to Configuration → Appliance Settings → Networking.
- Configure DNS server, Hostname, Domain Name, Hostname for Captive Portal & Remediation Portal, and IP Address for Captive Portal & Remediation portal



- Click **Submit** to save the settings

Note: *Hostnames should match those entered in the certificate. Some settings may not be configurable until the DNS server and domain name are configured.*

- Navigate to Configuration → Appliance Settings → Server Maintenance → SSL Certificate Manager → Manage
- Click **Generate Private Key and CSR**
- Enter required details and click on **Generate**



- Save the generated CSR
- Provide the CSR to certification authority (CA) to generate the certificate.
- Once you obtain the certificate from CA, Click **Upload signed certificate**

- Choose the certificate file and upload
- New certificate will be uploaded and details will be shown
- Reboot the EasyNAC Appliance for the new certificate to take effect

Note: *You can use a single certificate for the Management IP, Captive Portal, and Remediation Portal, provided that the Subject Alternative Name (SAN) includes the appropriate fully qualified domain names (FQDNs).*

OPTION 2 — UPLOAD A CERTIFICATE AND PRIVATE KEY TO THE EASYNAC APPLIANCE

Please note: The EasyNAC Appliance could be using 3 hostnames, one for management-IP, Captive Portal, and Remediation portal. Therefore, it is advised that you create a wildcard certificate. (*.domain.com)

- Log in to the EasyNAC Appliance using username **admin**, Go to Configuration → Appliance Settings → Networking.
- Configure DNS server, Hostname, Domain Name, Hostname for Captive Portal & Remediation Portal, and IP Address for Captive Portal & Remediation portal
- Click **Submit** to save the settings
- Navigate to Configuration → Appliance Settings → Server Maintenance → SSL Certificate Manager → Manage
- Click Upload Certificate and Private Key
- Choose files to upload. (Enter password if required) and Click Upload



- Reboot the EasyNAC Appliance for the new certificate to take effect

CONNECTING TO ACTIVE DIRECTORY

Authentication credentials are commonly stored within Active Directory. Active Directory can be used to validate credentials for the following EasyNAC features:

- Employee Device Registration (see Configuring Device Registration)
- Sponsoring guest accounts (see Configuring Guest Access)
- Administrator permissions for accessing the management GUI (see Advanced Configuration)

Configure Active Directory Server Settings on the EasyNAC Appliance

- In the EasyNAC Appliance GUI, navigate to Configuration → General Settings.
- Click Active Directory Servers
- Under “Active Directory Server,” enter the host or IP address of the AD domain controller and the account suffix in the “Account Suffix” field. A username and password are typically required.
- Click the “Test LDAP Connection” button to verify the settings.
- Click Save to apply the settings

© 2026 InfoExpress, Inc.

Note: *The @ symbol should be included in the Account Suffix*
Up to 20 Active Directory servers can be configured per appliance.
The user credential requires read access to the Active Directory only. It does not require an administrator account.

AD INTEGRATION

Tip: *Enabling AD integration simplifies deployment by automatically identifying domain-joined devices as AD-managed and granting them full network access.*

- In the EasyNAC Appliance GUI go to Configuration → Integration
- Click Active Directory Integration
- Check "Enable Integration"
- Check "Tag devices that are domain computers"

Tip: *Enabling DNS can enhance AD-managed device identification, but inaccurate or outdated records may introduce false positives. Configure this under Configuration → Integration → Settings Shared by All Integrations.*

Note: *AD computer objects may be located in non-default OUs in certain environments. To ensure proper detection, adjust the queried OUs as needed. Custom OUs can be defined under Configuration → General Settings → Active Directory Server.*

If computer objects reside in the "Computers" container within the "USA" OU, use the following LDAP query: CN=Computers, OU=USA in the Computer Query Settings

If computer objects reside in the "Computers" within the "All-USA-PCs" OU under the parent "USA" OU, the corresponding LDAP query is: CN=Computers, OU=All-USA-PCs, OU=USA, in the Computer Query Settings.

Tip: *When Query Scope is set to "Entire Directory," the entire directory is queried. This can simplify configuration but may lead to longer query times in large-scale environments.*

© 2026 InfoExpress, Inc.

NOTIFICATIONS: EMAIL, SMS, SYSLOG, SLACK, TEAMS AND WHATSAPP

The EasyNAC Appliance can send notifications when critical events occur. You can send notifications using:

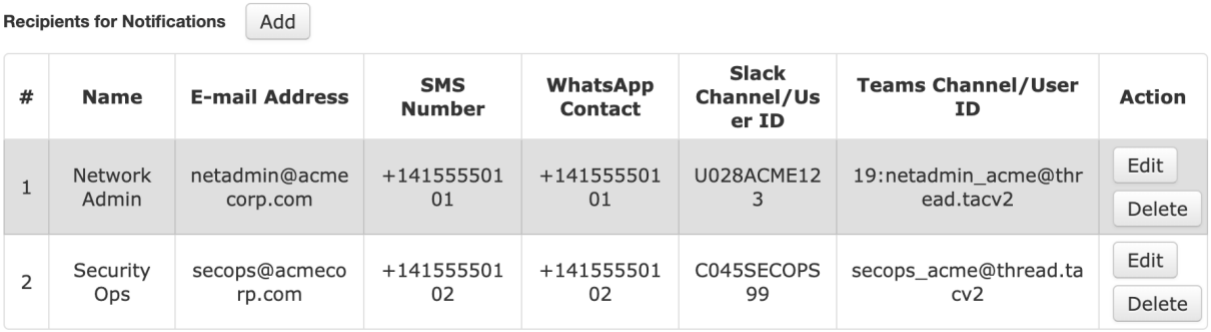
— Auto Trust Policy	— Device Profiling Policies
— Roles & Access Policy	— Guest registration Templates
— Monitoring Policies	

NOTIFICATION CONTACTS

Configuring notification contacts is essential to ensure that system-generated emails, alerts, and scheduled reports are delivered correctly. EasyNAC uses these contacts as notification recipients for administrative notifications. If they are not properly configured, email alerts and scheduled reports may not be delivered.

Navigate to Configuration → General Settings and click on the "Contact Information for Notifications" section.

Add or modify the contact details so that it can be used for sending relevant alerts to the relevant channel as needed to receive system notifications.



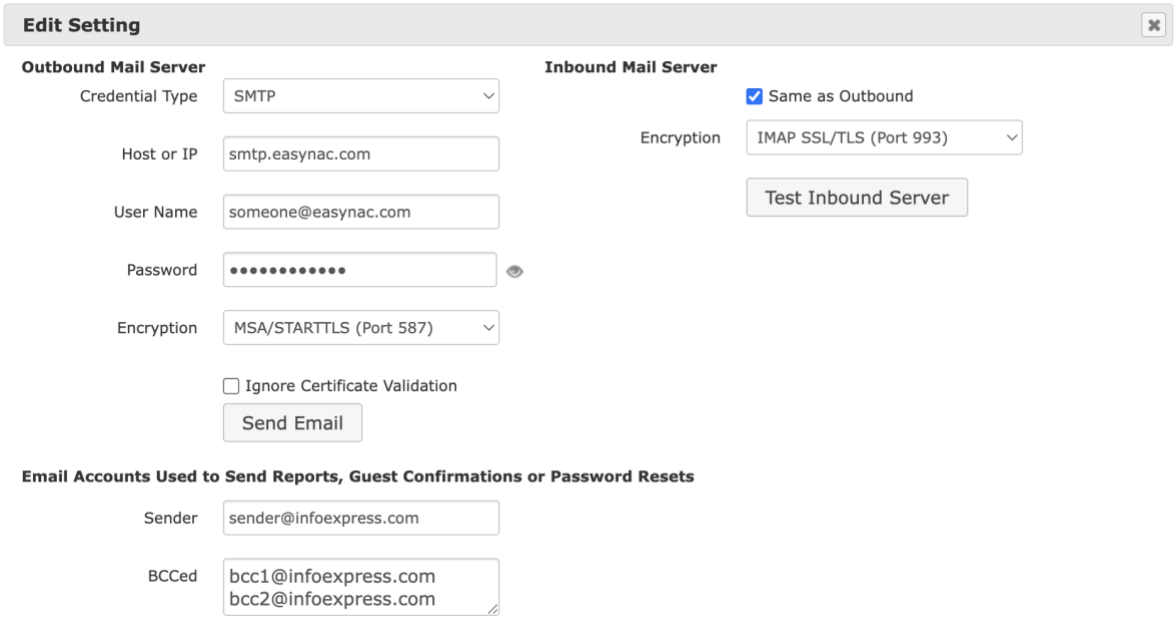
Note: *Ensure that the sender email address uses a valid and trusted domain configured on the email server. Emails sent from unrecognized or mismatched domains may be blocked by your mail servers configured.*

© 2026 InfoExpress, Inc.

E-MAIL NOTIFICATIONS — SMTP

To configure the SMTP email server used by the EasyNAC Appliance:

- Navigate to Configuration → General Settings
- Select E-mail Server



- Enter the required information
- Modify the email address used as sender address and the BCC recipients that will be blind carbon copy on guest registration emails.
- Click the Save button.

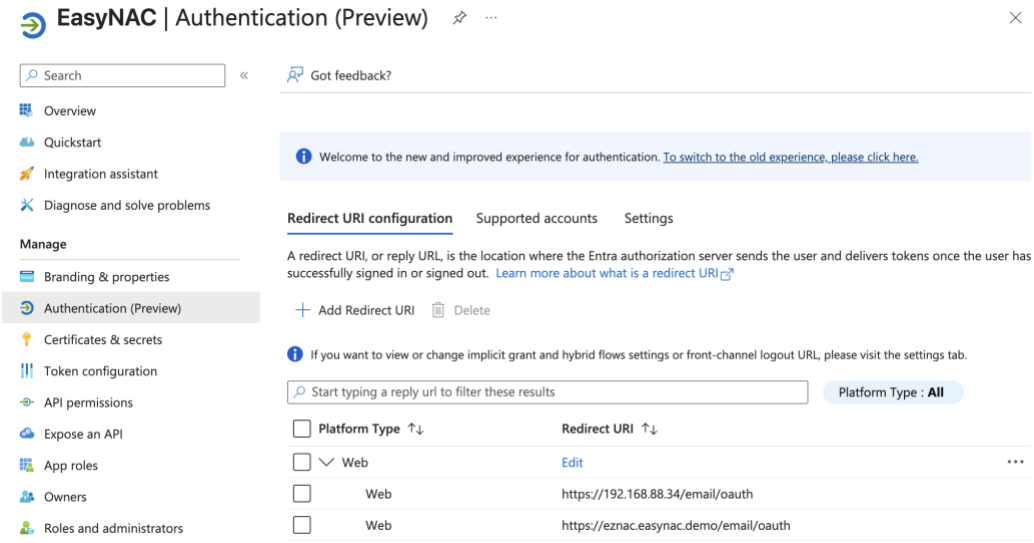
© 2026 InfoExpress, Inc.

E-MAIL NOTIFICATIONS — MICROSOFT 365 (OAUTH2)

- The following settings configure the mail server used by EasyNAC to send notification emails to administrators and alert emails to users using Microsoft 365 Email (OAuth2) with Microsoft Graph.
- Follow the steps below to complete the configuration.

Register an Application

- **Sign in to the Microsoft Entra admin center** - https://entra.microsoft.com/
- If you have access to multiple tenants, switch to the correct tenant first.
- Go to Entra ID → App registrations.
- Select New registration.
- Enter a Name for the application, say EasyNAC.
- Under Supported account types, select Single tenant only – [Your Organization Name]
- Under Redirect URI (optional):
- Select Web
- Enter: https://{easynac-ip-or-domain}/email/oauth
- If using both hostname and IP, you can add the second URI later under the Authentication
- Click Register.



Note: *If EasyNAC is configured with a domain/hostname, please register both the domain/hostname and the IP address as Redirect URIs.*

- After registration is complete, record the following values for later use:
- Directory (tenant) ID
- Application (client) ID

Configure Permissions

- Go to API permissions of the "EasyNAC" application in Microsoft Entra
- Select Add a permission.
- Select Microsoft Graph.
- Select Delegated permissions.
- Add the following permissions:
- **Outbound (Send emails)** - Mail.Send

© 2026 InfoExpress, Inc.

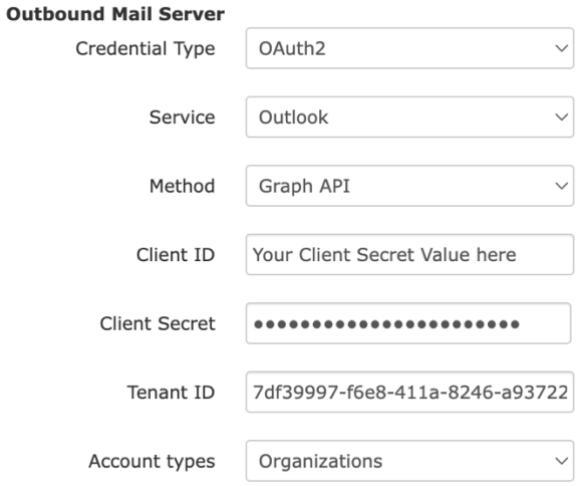
- **Inbound (Read emails)** - Mail.ReadWrite
- **Required** - User.Read

Add a Client Secret

- Go to Certificates & secrets of the "EasyNAC" application in Microsoft Entra
- Select Client secrets → New client secret
- Enter:
- Description
- Expiration
- Click Add
- Copy the Value and Secret ID

Configure the Email Server in the EasyNAC Appliance

- To configure the Microsoft 365 Email (OAuth2) used by the EasyNAC Appliance:
- Navigate to Configuration → General Settings
- Select E-mail Server
- Select Credential Type as **OAuth2**
- Select Service as **Outlook**
- Select Method as **Graph API**
- In the Client ID, enter the Client secrets' **Value**
- In the Client Secure, enter the **Secret ID**
- In the Tenant ID, enter the **Directory (tenant) ID**
- Select Account Type as **Organization**
- Under the Inbound Mail Server, select "**Same as Outbound**"
- Update the sender email address and the BCC addresses used for guest registration emails.
- Click **Sign in With Microsoft** to authenticate. Once completed, click Save to confirm the changes.



E-MAIL NOTIFICATIONS — GOOGLE WORKSPACE (OAUTH2)

The following settings configure the mail server used by EasyNAC to send notification emails to administrators and alert emails to users using Google Workspace (OAuth2) with Gmail API.

Follow the steps below to complete the configuration.

Create a Project

- **Go to the Google Cloud Console** - https://console.cloud.google.com/
- In the top navigation bar, click the Project selector
- Click New Project
- Enter a Project name (EasyNAC-GmailAPI)
- Click Create

Enable Gmail API

- **In the upper left menu, go to** - APIs & Services → Library
- Search for "Gmail API"
- Click Enable button to activate the API.

Configure OAuth Consent Screen

- **In the upper left menu, go to** - APIs & Services → OAuth consent screen
- Click the **Get Started** button
- **App Information** – Enter App Name (EasyNAC) and User Support Email
- Click Next
- Under the Audience, Select External
- Click Next
- Confirm the Contact Information
- Click Next
- Agree the Google API Services: User Data Policy by selecting the checkbox
- Click Create

Configure Data Access (Scopes)

- Go to Data Access
- Click Add or remove scopes
- In Manually add scopes, add **https://mail.google.com/**
- Click Add to Table and Click Update

Add Test Users

- Go to Audience
- Click Add Users under Test Users
- Enter one or more Google account email addresses to be used by EasyNAC, then click Save

© 2026 InfoExpress, Inc.

Create Credentials

- **In the upper left menu, go to** - APIs & Services → Credentials
- Click Create credentials → OAuth client ID
- Select: Web application as the Application Type
- Enter a name for it (EasyNAC WebApp)
- **Under the Authorized JavaScript Origins** – Click the Add the URI and key in the FQDN of your EasyNAC Appliance (**https://eznac.easynac.com**)
- **Under the Authorized redirect URIs** – Click the Add the URI and key in the FQDN of your EasyNAC Appliance follows by "email/oauth" suffix (**https://eznac.easynac.com/email/oauth**)
- Click Create
- A dialog box is displayed, containing your Client ID and Client Secret.

In EasyNAC, Test users are the Google accounts authorized to complete the OAuth2 sign-in when connecting to Gmail. When you select "Sign in with Google" in EasyNAC, you must log in using one of the accounts added as a Test user. These accounts grant EasyNAC permission to send and receive emails via the Gmail API. If an account is not listed as a Test user, it will not be able to authenticate while the application is in testing mode.

Configure the Email Server in the EasyNAC Appliance

To configure the Google Workspace (OAuth2) used by the EasyNAC Appliance:

- Navigate to Configuration → General Settings
- Select E-mail Server
- Select Credential Type as **OAuth2**
- In the Client ID, enter the OAuth **Client ID** generated
- In the Client Secure, enter the OAuth **Client Secret** generated
- Under the Inbound Mail Server, select "**Same as Outbound**"
- Update the sender email address and the BCC addresses used for guest registration emails.
- Click **Sign in With Google** to authenticate. Once completed, click Save to confirm the changes.

© 2026 InfoExpress, Inc.

CONFIGURING NOTIFICATIONS

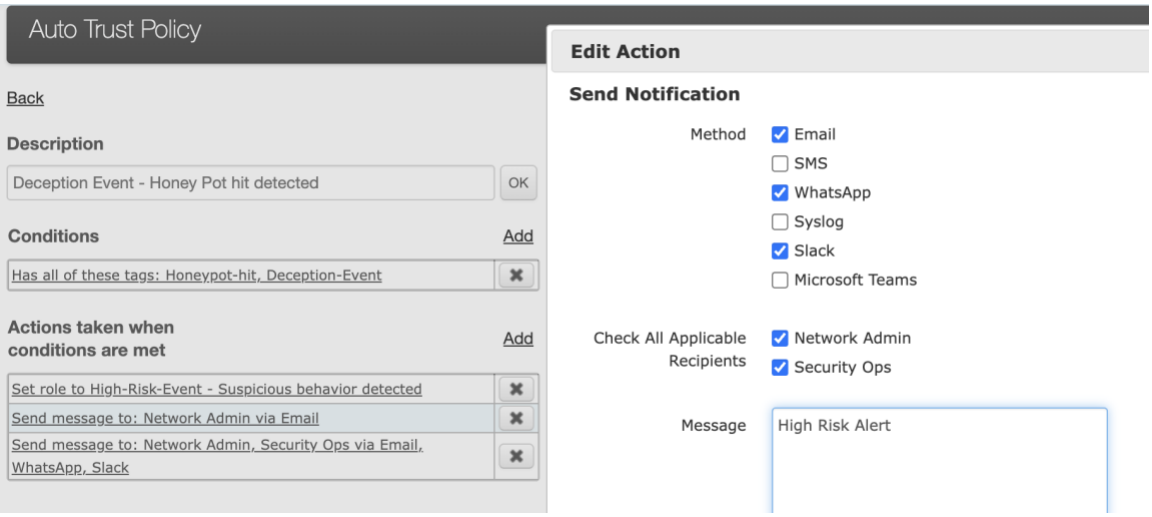
Notifications can be configured across multiple policy types, including Auto Trust Policy, Roles & Access Policy, Monitoring Policies, and Device Profiling Policies. Each policy enables administrators to define specific conditions and associate one or more actions, such as sending notifications, when those conditions are met.

When a policy condition is triggered, EasyNAC automatically executes the configured actions, ensuring timely alerts and improved operational visibility.

The example below illustrates how to configure notifications using an Auto Trust Policy.

Within an Auto Trust Policy, administrators can define actions to be taken when the specified conditions are satisfied. This includes selecting Send Notification as an action, allowing EasyNAC to automatically generate and deliver alerts to configured contacts whenever a device meets the defined trust criteria.

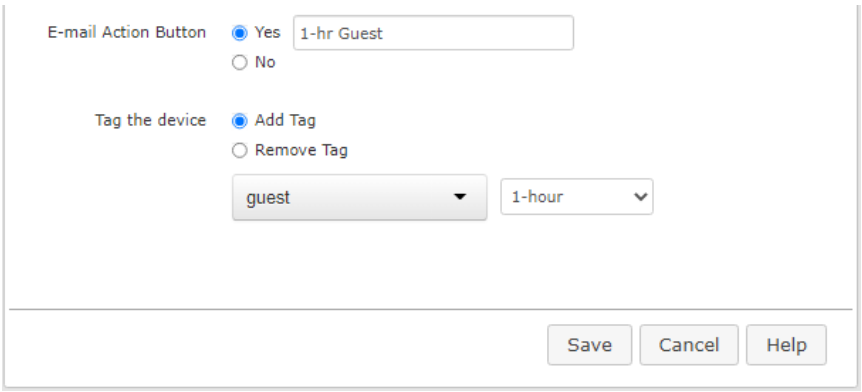
- Select a rule within the Auto Trust Policy to open its definition.
- Click Add next to Actions to be taken when the specified conditions are met.
- Select Notify → Send Notification.
- Configure the notification settings, including the alert method, recipients, and message content.
- Click Save
- Click Activate to commit changes.



E-MAIL ACTION BUTTON

When configuring email-based notifications, an Action Button can be included to enable quick responses directly from the email. This allows recipients to take immediate action without accessing the EasyNAC interface.

In the example below, a Monitoring Policy is configured to send an email notification when a new device is detected on the network for the first time.



The Action Button within the email is configured to apply a “guest” tag to the device for a duration of one hour when clicked by the recipient. This provides a convenient way for administrators to take timely action directly from the notification.

Note: *For this integration to operate as expected, the email recipient must have network connectivity to the appliance’s Management IP address. Authentication is not required. In addition, an Auto Trust Policy must be configured to assign Guest Access to any device tagged with guest.*

© 2026 InfoExpress, Inc.

MICROSOFT TEAMS NOTIFICATIONS (OAUTH2)

The following settings configure the Microsoft Teams integration used by EasyNAC to send notifications to administrators or users via Microsoft Teams.

Follow the steps below to complete the configuration.

Register an Application

- **Sign in to the Microsoft Entra admin center** - https://entra.microsoft.com/
- If you have access to multiple tenants, switch to the correct tenant first.
- Go to Entra ID → App registrations.
- Select New registration.
- Enter a Name for the application, say EasyNAC-Teams.
- Under Supported account types, select Single tenant only – [Your Organization Name]
- Under Redirect URI (optional):
- Select Web
- Enter: https://{easynac-ip-or-domain}/teams/oauth
- If using both hostname and IP, you can add the second URI later under the Authentication
- Click Register.
- Record the following values:
- Directory (tenant) ID
- Application (client) ID

Configure Additional Web and Spa Settings

- Go to: Entra ID → App registrations → [EasyNAC-Teams] → Authentication
- Select Settings
- Make sure these 2 options are selected
- Access tokens (used for implicit flows)
- ID tokens (used for implicit and hybrid flows)

Add a Client Secret

- Go to Certificates & secrets of the “EasyNAC-Teams” application in Microsoft Entra
- Select Client secrets → New client secret
- Enter:
- Description
- Expiration
- Click Add
- Copy the Value and Secret ID

Configure the Microsoft Teams Integration in the EasyNAC Appliance

- To configure the Microsoft Teams integration (OAuth2) used by the EasyNAC Appliance:
- Navigate to Configuration → General Settings
- Select Other Servers
- Select Teams App
- In Tenant ID, enter your **Directory (tenant) ID**

© 2026 InfoExpress, Inc.

- In the Client ID, enter the OAuth **Client ID** generated
- In the Client Secure, enter the OAuth **Client Secret** generated
- Optionally, you can select **Enable approve guest from Teams**, if you are using it for Guest Account Approval.
- Select Sign in with Microsoft and accept the Permission requested.
- Click Save

Note: *Please use a dedicated account for this purpose, as the signed-in account will be used exclusively as the sender for EasyNAC.*

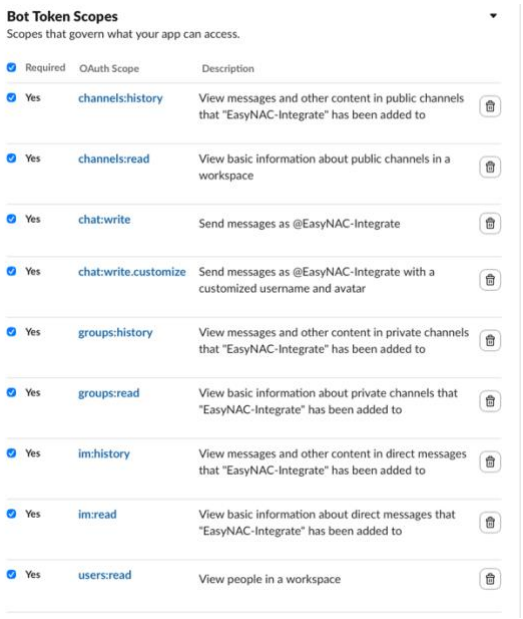
The account can only send messages to team members or channels it has joined. Ensure it is added to the appropriate teams and channels before use.

© 2026 InfoExpress, Inc.

SLACK NOTIFICATIONS (SLACK APP)

The following settings configure the Slack integration used by EasyNAC to send notifications to administrators or users via Slack App.

Follow the steps below to complete the configuration.



Create a Slack App

- Navigate to https://api.slack.com/apps
- Click Create New App
- Select From scratch
- Provide an App Name and select your Workspace
- Click Create App to proceed

Configure Permissions (Scopes)

- In your Slack app settings, go to OAuth & Permissions
- Scroll down to the Scopes section
- Under Bot Token Scopes, click Add an OAuth Scope
- Add the following scopes:
- channels:history, channels:read, groups:history, groups:read, im:history, im:read, users:read, chat:write, chat:write.customize

Note: *Ensure all scopes are added under Bot Token Scopes, not User Token Scopes.*

Install the App to Workspace

- In your Slack app settings, go to OAuth & Permissions
- Scroll to OAuth Tokens for Your Workspace
- Click Install to Workspace
- Complete the authorization in the Slack prompt

Obtain the Bot Token

- In OAuth & Permissions, locate OAuth Tokens for Your Workspace
- Copy the Bot User OAuth Token
- This information is required during EasyNAC configuration

Enable Messaging Capability

- Navigate to App Home under Features
- Scroll to Show Tabs
- Enable: **Allow users to send Slash commands and messages from the messages tab** under the Messages Tab

Add App to a Channel (Optional) - If Notifications Should Be Sent to a Channel:

- Open the desired channel in Slack
- Click the channel name → Integrations

© 2026 InfoExpress, Inc.

- Select Add apps
- Search for your app and add it to the channel

Configure the Slack Integration in the EasyNAC Appliance

To configure the Slack (Slack App) used by the EasyNAC Appliance:

- Navigate to Configuration → General Settings
- Select Other Servers
- Select Slack App
- In Bot User OAuth Token, enter your **Bot User OAuth Token** generated earlier
- Optionally, you can select Enable approve guest from Slack, if you are using it for Guest Account Approval.
    - Configure approval keywords
        - **Approve guest when matching pattern** - E.g. approve, yes
    - Configure rejection keywords
        - **Reject guest when matching pattern** - E.g. reject, no
- Click Save

Note: *To configure notification recipients, navigate to Configuration → General Settings → Configuration Settings → Contact Information for Notifications. Enter the appropriate Slack Channel ID or User ID from your workspace, and use the Support button if you need assistance retrieving the required ID.*

© 2026 InfoExpress, Inc.

WHATSAPP INTEGRATION

The EasyNAC Appliance supports administrative notifications via WhatsApp and can also be used for guest access approval workflows.

Notifications

To prevent spam on the WhatsApp network, Meta requires all business messaging to be sent through approved third-party API providers.

EasyNAC integrates with Twilio as its WhatsApp API provider. Therefore, enabling this feature requires both a Twilio account and WhatsApp Business approval.

WHATSAPP INTEGRATION PREREQUISITES

- Create a Twilio Account
- Register for a Twilio account: https://www.twilio.com/whatsapp
- This provides the API used to send WhatsApp messages from EasyNAC
- Purchase a Twilio Phone Number
- Buy a Twilio phone number (credit card required)
- This number will be used for WhatsApp messaging

Note: *You may use any number that suits your requirements; however, a US number is generally the most cost-effective option. For pricing details, please refer to Twilio.*

- **Facebook Business Manager ID** - https://business.facebook.com
  Follow the instructions provided by Meta to set up a Business Manager account.

Note: *A Facebook account is required to create a Facebook Business Manager account. Each department, such as IT, can create and manage its own Business Manager account if needed.*

WHATSAPP REGISTRATION PROCESS

- Request Access for WhatsApp
- To enable your Twilio number(s) for WhatsApp, complete the Request Access form with accurate and up-to-date information, including your Facebook Business Manager ID.
- When prompted whether you are working with an ISV or a third-party vendor, select No.
- After submitting the form, you will receive a confirmation email. Once your account is reviewed, you will receive an email indicating that you are pre-approved to use Twilio APIs for WhatsApp. Final approval is granted by WhatsApp after completing the sender profile in the next step.
- Submit a Sender Profile
    - To create a new sender profile, go to the Twilio Console and navigate to Messaging → Senders → WhatsApp Senders, or use the direct link provided. Click "Submit a WhatsApp Sender" and follow the prompts to complete the setup.

Note: *Your Sender "Display Name" must be the business name used in the Facebook Business Manager account.*

- Authorize Twilio to Send Messages on Your Behalf
    - After Twilio submits your Display Name and phone number to WhatsApp, you must grant approval for Twilio to send messages on your behalf.
    - You will receive a notification email prompting you to approve this request via Facebook Business Manager.
    - To complete the authorization:
        - Log in to the same Facebook Business Manager account used in Step 1.
        - Go to Business Settings
        - Navigate to the Requests section
        - Locate the request titled "Approve Twilio to message on behalf of…".
        - Click Approve to grant access.

© 2026 InfoExpress, Inc.

        - Alternatively, you can access the request directly using the link provided in the email notification.
        - Once approved, Twilio will be authorized to send WhatsApp messages on your behalf.
- Verify Your Facebook Business Manager Account
    - Once you have approved Twilio to send messages on your behalf, you can proceed with verifying your business.
    - To begin the verification process:
        - Log in to your Facebook Business Manager account.
        - Navigate to Business Settings.
        - Locate the Verification section.
        - Click Start or Continue to initiate the verification process.
    - During this process, you may be required to submit official documentation to confirm your business identity. Ensure all documents are valid and match your business details.
    - For detailed requirements, refer to Facebook's official guidance on business verification and document submission. The verification process may take several days to complete.
- Twilio Completes WhatsApp Sender Registration
    - After you have approved Twilio to send messages on your behalf, Twilio will proceed with completing the registration of your WhatsApp sender profile.
    - Once the process is finalized, you will receive an email confirmation indicating that your WhatsApp sender has been successfully registered.
- Submit Message Templates
    - To comply with WhatsApp's anti-spam policies, outbound messages must use pre-approved templates.
    - To create and submit message templates:
        - Navigate to Messaging → Senders → WhatsApp Templates in your Twilio console.
        - Submit templates for approval before they can be used in production.
    - For EasyNAC integrations, the following four message templates must be created:
        - Template 1: System Notifications

Template Name	**system_notifications**
Template Category	Alert Update
Language	English
Buttons	None
Message Body:	
System Alert Notification on: {{1}} EasyNAC IP: {{2}}	

        - Template 2: Device Profiler Notifications

Template Name	**device_profiler_notification**
Template Category	Alert Update
Language	English
Buttons	None
Message Body:	
Device Profiler Alert Notification on: {{1}}	

        - Template 3: Device Notifications

Template Name	device-notification
Template Category	Alert Update
Language	English
Buttons	None
Message Body:	
Device Alert Notification on: IP: {{1}} MAC: {{2}} Hostname: {{3}} Location: {{4}} Access Group: {{5}} Role: {{6}} OS: {{7}} First Seen: {{8}} Tags/Lists: {{9}} EasyNAC IP: {{10}} Message: {{11}} See Visibility - Alerts and Notifications for details.	

- Template 4: Guest Access Notification

Template Name	guest-notification
Template Category	Alert Update
Language	English
Buttons	None
Message Body:	
Device Alert Notification on: {{1}} just sent you a network access request. MAC: {{2}} IP: {{3}} Fullname: {{4}} Email: {{5}} Phone: {{6}} Company: {{7}} To grant guest access: Please enter: {{8}} To deny guest access: Please enter: {{9}}	

Note: *Additional guest templates may be required, depending on how the guest registration process is configured within your organization.*

© 2026 InfoExpress, Inc.

ENABLING WHATSAPP ALERTS

Once the registration process is complete, you can enable EasyNAC to send administrative alerts via WhatsApp.

1. Configure the WhatsApp Sender
    - Navigate to Configuration → General Settings → Other Servers
    - Select WhatsApp Provider Tab
    - Enter the WhatsApp number that has been approved as the sender
    - Enter the Account SID and Auth Token
        - This information can be found in the Twilio Console under Account → General Settings
    - Optionally, you can select Enable approve guest from WhatsApp, if you are using it for Guest Account Approval.
        - Configure approval keywords
            - **Approve guest when matching pattern** - E.g. approve, yes
        - Configure rejection keywords
            - **Reject guest when matching pattern** - E.g. reject, no
        - Go to Configuration → Device Registration Templates → Guest Registration Templates
        - Within these guest templates, specify the WhatsApp number to which guest requests should be sent. Each template may be configured with a different WhatsApp approver, allowing requests to be routed to the appropriate recipient.
2. Configure Admin Contact Details
    - Navigate to Configuration → General Settings → Contact Information for Notifications
    - Enter the WhatsApp numbers of the administrators who should receive alerts

© 2026 InfoExpress, Inc.

PROTECTING ADDITIONAL SUBNETS

When using ARP enforcement, EasyNAC requires Layer-2 visibility of ARP broadcast traffic to detect and restrict devices. To extend this visibility across multiple subnets, the following methods can be used:

- **Method 1 – Additional Adapters**: Install additional network adapters and connect them to standard access ports to extend protection to other subnets.
    - Physical appliances support up to the maximum number of network adapters available for the specific hardware model.
    - Virtual appliances support up to 10 network adapters (Microsoft Hyper-V supports up to 8 adapters)

- **Method 2 – 802.1Q Trunking**: Use 802.1Q trunk ports to monitor multiple VLANs through one or more network adapters.
    - Supports up to 400 VLANs per deployment (depending on hardware model)
    - Recommended for environments with multiple VLANs
    - Deploy multiple adapters if there is significant traffic, particularly when enforcing restrictions using ACLs
    - Virtual EasyNAC Appliances also support 802.1Q trunking. Additional configuration may be required on the hypervisor to enable VLAN tagging

Note: *Protection can also be extended to remote sites using Enforcer Sensors*

ADDING NETWORK ADAPTERS

EasyNAC Appliances—whether deployed as a virtual appliance or on physical hardware—support multiple network adapters. Virtual appliances are typically pre-configured with up to 10 virtual network adapters, while physical appliances support the maximum number of adapters available for the specific hardware model.

To configure network adapters:

- In the EasyNAC Appliance GUI go to Configuration → Appliance Settings → Networking
- Select the network adapter to configure and choose how the IP address will be assigned (e.g., DHCP or Static).
- If using a static IP address, enter the required IP configuration details.
- The Location field is optional but recommended for environments using location-based policies.
- To apply and confirm the network configuration changes, click **Submit Network Changes**.

Note: *The Metric field is automatically configured by the system and should not be modified. Changing this value may result in network routing issues and could impact connectivity to the appliance.*

© 2026 InfoExpress, Inc.

USING 802.1Q TRUNK PORTS

Networks configured for VLAN tagging allow for straightforward addition of new VLANs.

Configure 802.1Q Trunking on Physical Switch Port

The following example demonstrates how to configure trunking on a Cisco switch. For other switch platforms, refer to the vendor's documentation for instructions on configuring trunk ports.

In this example, VLANs 2, 3, 5, and 100 are allowed on the trunk, with VLAN 1 configured as the native VLAN (Cisco VLAN 1 corresponds to Hyper-V VLAN 0).

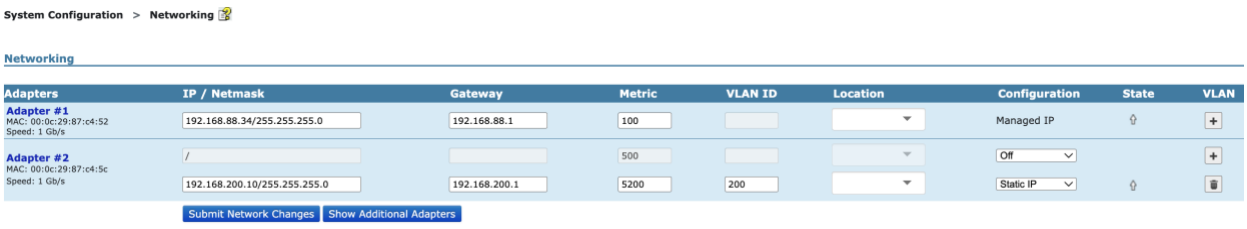
```
Switch# configure terminal
Switch(config)# interface fastEthernet 0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 2,3,5,100
Switch(config-if)# switchport trunk native vlan 1   ! Optional: change native VLAN if required
Switch(config-if)# exit
```

Note: *When adding network adapters to the EasyNAC Appliance, ensure they are properly connected to the network. For virtual deployments, adapters must be provisioned on the host and attached to the virtual appliance. For physical deployments, adapters must be connected to the appropriate switch ports.*

If VLAN trunking is required, verify that the switch ports are correctly configured to allow all intended VLANs. Failure to do so may prevent EasyNAC from detecting and protecting devices on those VLANs.

To add a VLAN via 802.1Q Trunk Port in EasyNAC

- In the EasyNAC Appliance GUI go to Configuration → Appliance Settings → Networking
- Click "+" button on the adapter attached to a trunk port
- Complete VLAN ID and static IP address information, if necessary. DHCP can be used
- To confirm the network changes, click the "Submit Network Changes" button…



CONFIGURING 802.1Q SUPPORT ON VMWARE ESX/ESXI

To enable 802.1Q VLAN tagging for the EasyNAC virtual appliance, configure a port group on the VMware virtual switch to support VLAN trunking.

Follow the steps below using the VMware vSphere Client:

- Log in to the vSphere Client.
- Select the ESX / ESXi host from the inventory
- Go to the Configure tab

- Under Networking, select Virtual switches.
- Identify the vSwitch used by the EasyNAC Appliance and click Add Networking (or edit an existing port group).
- Create or edit a Port Group.
- In the VLAN ID field, enter **4095** to enable trunking of all VLANs.
- Ensure the corresponding physical switch port is configured as a trunk and allows the required VLANs.
- Click Save to apply the configuration.
- Assign the EasyNAC virtual appliance to connect to the port group configured

Note: *If your environment is using a VMware Distributed Switch, you can create a Distributed Port Group and specify a VLAN range (or the full VLAN range of 0–4094). Assign this distributed port group to the EasyNAC (CGX-Access) trunk interface to enable VLAN trunking across the required networks.*

CONFIGURING 802.1Q SUPPORT ON HYPER-V

To enable 802.1Q VLAN tagging for the EasyNAC virtual appliance in a Microsoft Hyper-V environment, the virtual network adapters must be configured to support VLAN tagging. This requires additional configuration using Windows PowerShell.

Before enabling trunking, ensure the following:

— The Hyper-V host's physical network adapter supports 802.1Q VLAN tagging

— The switch port connected to the EasyNAC trunk interface is configured for 802.1Q trunking and allows the required VLANs

— In Virtual Switch Manager, the virtual switch is configured as an External Network

— Assign Virtual Switch to EasyNAC Network Adapter

— Follow these steps to assign a virtual switch to the EasyNAC virtual appliance in Microsoft Hyper-V:

— Open Hyper-V Manager.

— In the Virtual Machines list, select the EasyNAC VM.

— From the right-hand Actions pane, click Settings.

— In the Settings window:

— Select the desired Network Adapter (e.g., Network Adapter 1, Network Adapter 2).

In the right pane, locate the Virtual switch dropdown.

Select the appropriate External Virtual Switch that is connected to your physical network.

Click Apply, then OK to save the configuration.

Configuring VLAN Trunking on Hyper-V (PowerShell)

To configure a network adapter on the EasyNAC virtual appliance as a trunk port in Microsoft Hyper-V, use Windows PowerShell.

Configure Trunk Mode in Hyper-V Host

- Open Windows PowerShell with administrative privileges.
- Run the following command to configure Network Adapter as a trunk port. Modify the values as required for your environment:

```
Set-VMNetworkAdapterVlan
-VMName "EasyNAC-3.2"                    # EasyNAC virtual machine name
-VMNetworkAdapterName "Network Adapter 1"  # Target network adapter of EasyNAC VM
-Trunk                                   # Enable trunk mode
```

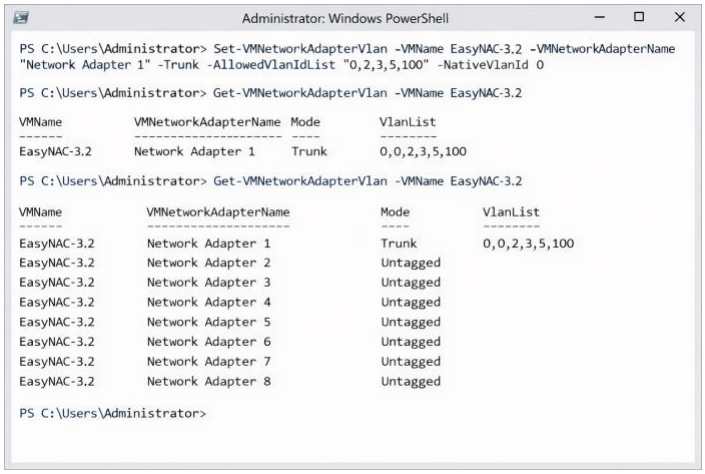
© 2026 InfoExpress, Inc.

```
-AllowedVlanIdList "0,2,3,5,100"        # Allowed VLANs
-NativeVlanId 0                         # Untagged/native VLAN
                                        #(Cisco switches typically use VLAN 1)
```

The example above configures the VM named EasyNAC-3.2 on its "Network Adapter 1" as Trunk Port. The VLANs allowed are 0,2,3,5,100 and Native VLAN as 0 (Native VLAN is 1 on Cisco switches)

To verify enter following command.

Get-VMNetworkAdaptervlan -VMName EasyNAC-3.2



Enable MAC Address Spoofing on the EasyNAC Adapter

EasyNAC enforces access by injecting ARP responses to redirect traffic from untrusted endpoints. By default, Hyper-V can block frames from a virtual machine that use a source MAC different from the adapter's assigned MAC, which prevents ARP-based enforcement from taking effect. Enable MAC address spoofing on the EasyNAC virtual network adapter so this enforcement traffic is permitted.

- In Hyper-V Manager, right-click the EasyNAC virtual machine and select Settings.
- Under the Network Adapter used by EasyNAC, expand Advanced Features.
- Tick "Enable MAC address spoofing". Click Apply, then OK.

Or via Windows PowerShell on the Hyper-V host:

Set-VMNetworkAdapter -VMName "EasyNAC-3.2" -MacAddressSpoofing On

Note: *If enforcement actions appear to take effect in the EasyNAC management interface but devices on the network are not actually being restricted, MAC address spoofing is the most common cause on Hyper-V deployments.*

CONFIGURING 802.1Q SUPPORT ON NUTANIX PRISM

Configuring VLAN Trunking on Nutanix

VLAN trunking requires additional configuration through the Nutanix CLI.

- Access the Nutanix CLI and enter the following command to launch the ACLI interface:
- Run the following command:
  vm.nic_create <VM_NAME> network=<NETWORK_NAME> trunked_networks=<VLAN_IDs> vlan_mode=kTrunked
- An example is provided below:
  acli # Enter Nutanix CLI
  vm.nic_create EASYNAC-VM # Target VM name
  network=EZNAC-NET-TRUNK # Network configured for trunking

```
trunked_networks=100,101        # VLANs allowed on this trunk
vlan_mode=kTrunked              # Enable trunk mode
```

- Verify the new network adapter appears in the VM settings within Prism.

CONFIGURING 802.1Q SUPPORT ON PROXMOX

Proxmox does not use a "trunk command" like Hyper-V or Cisco. Instead, trunking is achieved by creating a VLAN-aware Linux bridge, which allows VLAN-tagged traffic to pass through to VMs.

Configuring a VLAN-Aware Bridge on Proxmox (GUI Method)

- Log in to the Proxmox web interface.
- Navigate to:
  - Node → System → Network
- Click Create → Linux Bridge (or edit an existing bridge such as vmbr0).
- Configure the following settings:
- Bridge ports: Select the physical network interface (e.g., eno1) connected to the trunk port
- Enable VLAN aware
- (Optional) Specify VLAN IDs (VIDs), for example: 2,3,5,100 or a range like 2-4094
- Click Create (or OK if editing an existing bridge).
- Click Apply Configuration to activate the changes.

The bridge becomes VLAN-aware, meaning it can pass tagged VLAN traffic

- This effectively turns the Proxmox bridge into a trunk interface
- Multiple VLANs can now traverse a single physical NIC

Configure EasyNAC adapter to attach to the VLAN-aware bridge (e.g., vmbr0)

Note: *Do NOT set VLAN Tag. All VLAN tags to pass through to the EasyNAC VM and it handles the VLAN tagging inside.*

NETWORK GROUP

Network Groups Definition

The Network Groups page (Control / Network Group), labelled "Network Groups Definition", is used to create and manage Network Groups.

This page is limited to basic group administration and includes the following actions:

- **Add Network Group** — create a new group by name (e.g. HQ, Branch Office, Asia, Europe)
- **Remove Selected** — delete one or more existing groups

This page does not assign any objects to a group; it only maintains the list of available group names.

Where Group Assignment Occurs

Assignment of objects to Network Groups is performed in other sections of the system:

- Subnets are assigned via Control / Network Map
- Enforcer Sensors are assigned via Control / Enforcer Sensors

Usage and Limitations

Network Groups are intended purely as a management convenience for applying bulk configuration changes.

They cannot be used as a condition or filter in:

- Auto Trust Policy
- Access Control Lists (ACLs)
- Permission Manager (site filtering)
- Network Map filtering

© 2026 InfoExpress, Inc.

EXTENDING PROTECTION TO REMOTE SITES

To provide effective visibility and protection, the EasyNAC Appliance requires Layer-2 visibility of the subnets it monitors. At the main site, this can be achieved using trunk ports or standard access ports.

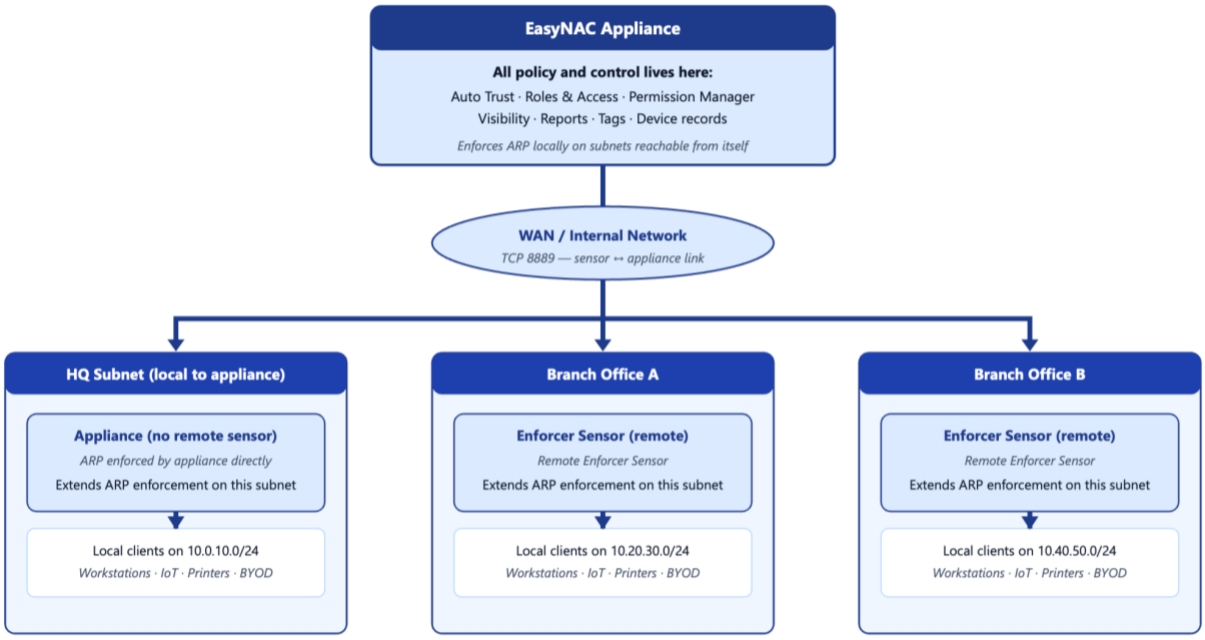
For remote sites, additional EasyNAC Appliances can be deployed. However, for a more cost-effective approach, EasyNAC also supports alternative methods to extend protection without deploying full appliances at each location.

1) Enforcer Sensors

2) vLinks Network Extenders (See Appendix D)

ENFORCER SENSOR OVERVIEW

Refer to the Enforcer Sensor architecture below.



The Enforcer Sensor is designed to extend EasyNAC visibility and enforcement to remote sites without requiring a full appliance deployment.

The Enforcer Sensor software can be installed on the following platforms:

- Windows (64-bit)
- Linux (Ubuntu 24.04 or later)
- Raspberry Pi (pre-built hardened image available)

Once deployed, the Enforcer Sensor communicates with the EasyNAC Appliance in real-time to report devices detected on the local network. The EasyNAC Appliance profiles these devices and determines the appropriate access policies. These policies are then enforced locally by the Enforcer Sensor using ARP-based enforcement.

Both MPLS and NAT network environments are supported.

© 2026 InfoExpress, Inc.

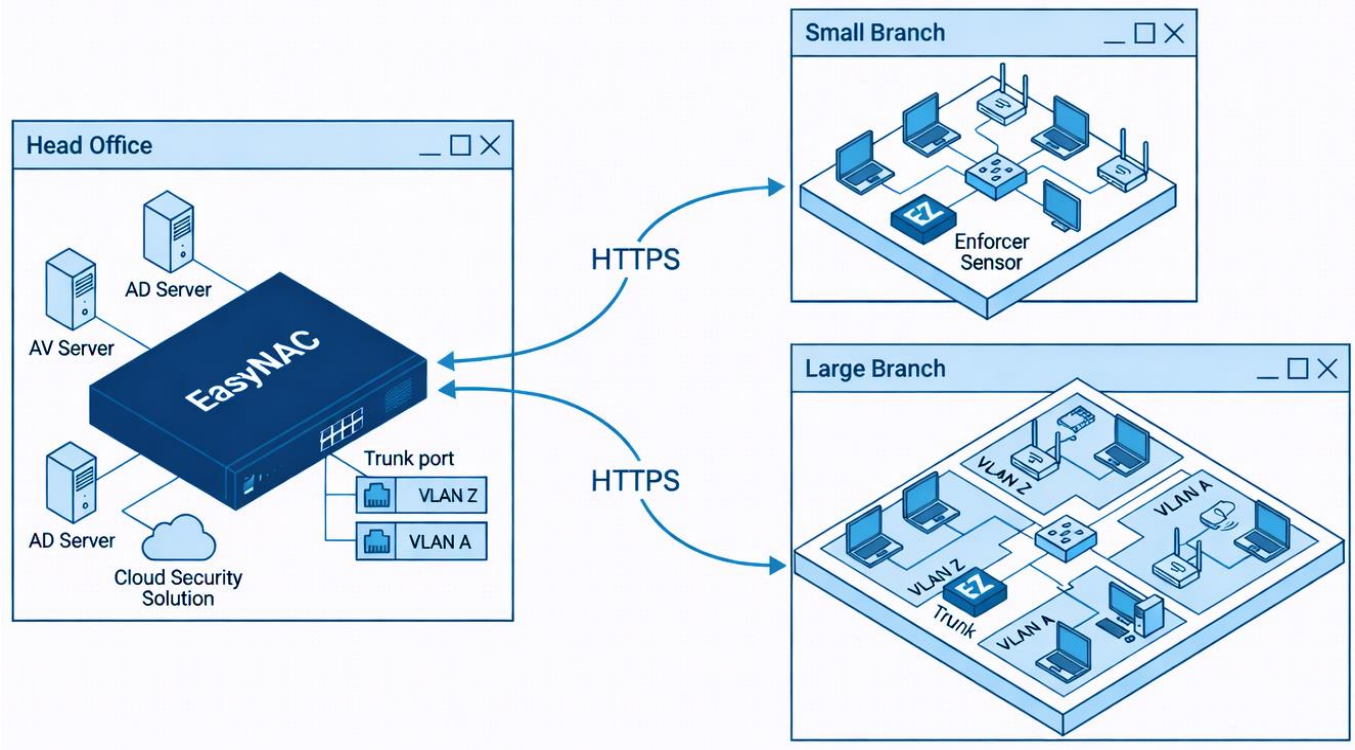
However, in NAT environments, functionality is limited to rogue device prevention, as the EasyNAC Appliance may not be able to fully profile devices behind NAT. Adding an Enforcer Sensor to extend EasyNAC protection to remote sites is a straightforward process. It involves installing the Enforcer Agent and then approving the sensor in the EasyNAC management interface.

Obtain the Enforcer Sensor installer from your InfoExpress partner, representative, or support team. The latest versions are also available from the InfoExpress Support Portal.

Enforcer Sensors are compatible with EasyNAC Appliances version 3.1.220317 and above using default shared settings. Enforcer Agents are licensed separately.

Note: *If your organization is using the EasyNAC Compliance Agent (CyberGateKeeper Agent) with customized shared settings, you may need to generate a compatible Enforcer Sensor package using the EasyNAC (CyberGateKeeper) Policy Manager.*

The Enforcer Sensor communicates with the EasyNAC Appliance over TCP port 8889. Ensure this port is open and reachable between the Enforcer Sensor and the EasyNAC Appliance.



ENFORCER SENSOR (MICROSOFT WINDOWS) INSTALLATION

The Enforcer Sensor supports:

- Windows 10 or later
- Windows Server 2016 or later
- 64-bit systems only

The installer is lightweight and operates within minimum OS requirements. Refer to the EasyNAC datasheet for recommended hardware specifications.

The installation package is provided as a compressed folder containing:

- nsagent.msi (installer)
- nsagent.ini (configuration file)

Ensure both files are located in the same directory before starting the installation.

Installation

- Configure Server Address
    - Edit the nsagent.ini file and look for the line

```
ServerAddr = "cgx-access";
```

    - update the ServerAddr value (cgx-acess) to point to the management IP address of your EasyNAC Appliance. Alternatively, a DNS entry can be used in place of the IP address.
    - Save the changes.

- Install the Sensor
    - Right-click the MSI installer and select Open (administrative privileges are required).
    - The installation runs silently in the background. If prompted by User Account Control (UAC), click Yes to proceed.

- Once the installation is completed, the Enforcer Sensor runs as a Windows service that starts automatically.

ENFORCER SENSOR (LINUX) INSTALLATION

The Enforcer Sensor supports:

- Ubuntu / Debian
- AlmaLinux / Rocky Linux
- 64-bit systems

Installation

- Download or copy the appropriate installation package to the Linux.
    - Ubuntu / Debian:
        - ES-Ubuntu-Debian-<version>
    - AlmaLinux / Rocky Linux:
        - ES-Alma-Rocky-<version>
    - Extract the package if required.

- Navigate to the extracted folder and run the appropriate script:
    - Ensure the script is executable and run it with administrative privileges:
        - Ubuntu / Debian:

```
chmod +x debian.sh
sudo ./debian.sh
```

        - AlmaLinux / Rocky Linux:

```
chmod +x rhel.sh
sudo ./rhel.sh
```

Configuration

- The Linux-based Enforcer Sensor includes a built-in web management interface for basic configuration and monitoring.
- Open a web browser and access the Enforcer Sensor using its IP address over TCP port 8443:
  - Example:
    - https://192.168.88.222:8443
  - If accessing from the same subnet, you may also use:
    - https://espi.local:8443
- The Enforcer Sensor Web GUI should be displayed, allowing you to manage and monitor the sensor.
- The log on credential is your Linux logon credential.
- Go to Settings, change the CGXA Address to the DNS or IP address of your EasyNAC Appliance.

ENFORCER SENSOR (RASPBERRY PI) INSTALLATION

The Enforcer Sensor can be deployed on Raspberry Pi for lightweight and cost-effective remote site protection. If preferred, InfoExpress also offers a hardware version of the Raspberry Pi–based Enforcer Sensor, which can be purchased directly from InfoExpress.

Supported Platform:

- Raspberry Pi 4 or above
- Minimum 4GB RAM
- 32GB SD card (or larger)

Installation

- Download Enforcer Sensor Pi Image
  - Obtain the pre-built Enforcer Sensor image from InfoExpress.
  - Flash the image onto the SD card using a tool such as Raspberry Pi Imager
- Deploy Raspberry Pi Sensor
  - Insert the SD card into the Raspberry Pi, connect it to the network, and power it on.
  - Ensure the device is connected to the appropriate network segment for monitoring.

Configuration

- The Raspberry Pi Enforcer Sensor includes a built-in web management interface for basic configuration and monitoring.
- Open a web browser and access the Enforcer Sensor using its IP address over TCP port 8443:
  - Example:
    - https://192.168.88.222:8443
  - If accessing from the same subnet, you may also use:
    - https://espi.local:8443
- The Enforcer Sensor Web GUI should be displayed, allowing you to manage and monitor the sensor.
- The log on credential is admin/admin; you are prompted to change the password.
- Go to Settings, change the CGXA Address to the DNS or IP address of your EasyNAC Appliance.

© 2026 InfoExpress, Inc.

ACCEPTING THE ENFORCER SENSOR

Once the Enforcer Sensor is installed and running, it must be approved in the EasyNAC Appliance before enforcement begins.

- Log in to the EasyNAC Appliance web interface.
- Navigate to:
  - Control → Enforcer Sensors
- Locate the pending Enforcer Sensor connection request (identified by the sensor's IP address).
- Click Accept to approve the sensor.
- (Optional) Enter a Location name to help identify the site or subnet associated with the sensor.

Verification

- After approval, the Enforcer Sensor status should change to Active
- The monitored subnet will appear under:
  - Control → Network Map
- The sensor will be flagged as an Enforcer
- Click Refresh, you will see the subnet range that is being protected and when the agent was last seen.

Note: *You can configure alerts to notify administrators if the Enforcer Sensor goes offline due to network issues or system shutdown.*

In NAT environments, it's necessary to add a line to the Restricted ACL to allow restricted devices to reach the Captive Portal via the Enforcer Sensor.

© 2026 InfoExpress, Inc.

ENFORCER SENSORS PAGE

The Enforcer Sensors page (Control / Enforcer Sensors) is the management page for sensors deployed at remote sites. It provides a single inventory of every sensor that has registered with this appliance.

At the top of the page are

- ES Installers (the link for sensor installation packages that can be used for upgrade),
- Refresh (manually re-poll), and
- a global Enforcer Sensors activity Enable / Disable control.
- There is also an Export button.

Per-sensor columns

- **IP Address** — the sensor's address.
- **Subnets** — the subnets the sensor advertises and is prepared to enforce.
- **Last seen** — when the sensor last contacted the appliance.
- **State** — the sensor's current state.
- **Location** — the Network Group the sensor belongs to.
- **Behind NAT** — whether the sensor is reachable directly or sits behind NAT.
- **Version** — the sensor's software version.
- **Actions** — per-row controls (view, configure, remove).

View types and bulk operations

View type: Ungrouped, Grouped, or By Group (using Network Groups to organize the display).

The Apply Action to selected ES bar runs bulk operations on the selected sensors:

- **Schedule Alerts on Enforcers** — schedule notification rules for the selected sensors.
- **Change Enforcers settings** — change configuration settings for the selected sensors in one step.
- **Change Enforcers group** — move the selected sensors into a different Network Group.

Assigning a sensor to a Network Group

- Use the Change Enforcers group bulk operation (or the per-row equivalent) to place sensors into a Network Group. Once grouped, configuration changes made via Change Enforcers settings can be applied to every sensor in the group at the same time.
- **The group is a management container only** — assigning a sensor to a group does not affect Auto Trust evaluation, ACL evaluation, or the Permission Manager.

© 2026 InfoExpress, Inc.

ENFORCEMENT OVERVIEW

The EasyNAC uses ARP-based enforcement to control network access and redirect users to a landing page when required. This approach keeps deployment straightforward, as it does not require any changes to the existing network infrastructure.

On top of enforcement, EasyNAC provides role-based access control through configurable Access Groups (ACLs). These can represent different types of users or devices such as restricted, limited, full access, guest, consultant, or BYOD. Each group can be tailored to align with the organization's security policies and operational needs.

By default, all subnets start in monitoring mode. This allows you to observe network activity and fine-tune policies before enforcing any controls. It's best practice to complete the initial setup, refine ACLs, enable integrations, and allow-list known devices before switching enforcement on.

When any subnet remains in monitoring mode, the system clearly indicates this with a status message at the top of the management console, so there's always visibility on the current enforcement state.

When ready, enforcement can be enabled in the Network Map under Control in the EasyNAC Appliance web interface.

Note: *VRRP and HSRP Redundancy*

For EasyNAC to operate correctly, it must be aware of the MAC and IP addresses of the routers or gateways within each subnet. In environments where redundancy protocols such as VRRP or HSRP are used, both the virtual MAC address and the physical MAC addresses of the participating routers must be defined in the Routerlist under the subnet configuration in the Network Map.
To configure this:

1. Navigate to Control → Network Map
2. Locate the relevant subnet and select Show Configuration

EasyNAC can detect the presence of VRRP or HSRP. When such protocols are identified, a warning will appear against the subnet in the Network Map.
The virtual MAC address will be automatically detected and classified as network infrastructure, so no action is required for it. However, you will still need to obtain the MAC addresses of the physical routers participating in the redundancy setup and add them to the Routerlist.

CONFIGURING ACCESS POLICIES IN EASYNAC

This section outlines the required steps to configure access policies in EasyNAC as part of a standard deployment.

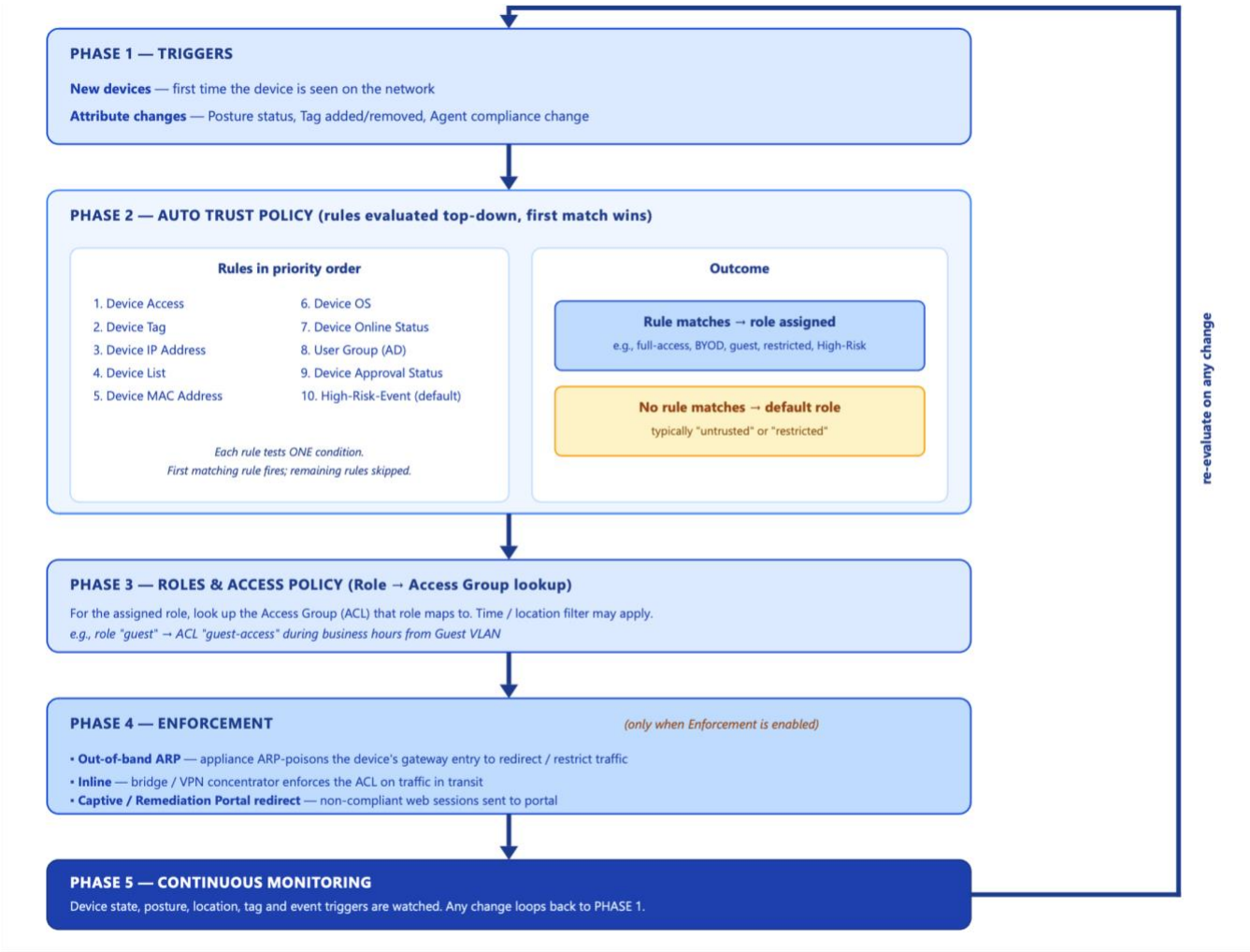
Access control in EasyNAC is implemented as a five-phase lifecycle that runs continuously for every device on the network:

- **Triggers** – Evaluation runs whenever a new device is detected, or when an existing device's attributes change (posture status, tag, agent compliance, or other monitored event).
- **Auto Trust Policy** – Rules are evaluated top-down in priority order. The first rule whose condition matches the device fires and assigns a Role; the remaining rules are skipped. If no rule matches, the default role applies (typically *untrusted* or *restricted*).
- **Roles & Access Policy** – The assigned Role is looked up against the Roles & Access Policy, which returns the Access Group (ACL) that role maps to. Time and location filters may further constrain the mapping.
- **Enforcement *(only when Enforcement is enabled)*** – The selected ACL is applied at the network layer using one or more of: Out-of-band ARP (the appliance redirects the device's gateway via ARP), Inline (a bridge or VPN concentrator enforces the ACL on traffic in transit), or Captive / Remediation Portal

© 2026 InfoExpress, Inc.

redirect for non-compliant web sessions. With Enforcement disabled, the Role and ACL are computed and recorded for visibility but not applied to traffic.

- **Continuous monitoring** – Device state, posture, location, tag, and event triggers are watched continuously. Any change feeds back into the Trigger phase, restarting the cycle so the device's role and access remain current.



AUTO TRUST POLICY

The Auto Trust Policy is used to evaluate devices and assign them a Role based on defined conditions. EasyNAC includes a set of preconfigured rules that cover common deployment scenarios. These rules can be modified to meet specific enterprise requirements.

Navigation: Go to Policies → Auto Trust



RULES AND CONDITIONS

— Rules are evaluated in a top-down order

— The first rule that matches all conditions is applied

— If a rule contains multiple conditions, all conditions must be satisfied

— If no rules match, the device is assigned the Untrusted role (restricted by default)

DEVICE CONDITIONS

Device Conditions are used within Auto Trust rules to evaluate endpoint attributes and determine the appropriate Role assignment.

Each condition supports logical evaluation such as ANY (OR), ALL (AND), or NONE (NOT), depending on the condition type.

© 2026 InfoExpress, Inc.

Device Authentication

Checks the authentication and domain status of the endpoint.

Configuration:

— Requirement:

— Match any (OR)

— Match all (AND)

— Available Checks:

— User Authenticated

— Not User Authenticated

— AD Computer

— Not AD Computer

Notes:

- *"User Authenticated" requires authentication methods such as 802.1X or Active Directory*
- *"AD Computer" requires the Compliance Agent*

Device Access

Checks the current access state of the device.

Configuration:

— Granted Access

— Denied Access

Use Case:

- *Used to distinguish between devices that already have access and those that are currently restricted.*

Device Tag

Checks whether a device has one or more assigned tags.

Configuration:

— Requirement:

— Match any (OR)

— Match all (AND)

— Match none (NOT)

— Tags to Check:

— Select from tags defined under:

— Configuration → Global Defaults → Names Used by Policies

Notes:

- *For mixed logic (include some tags but exclude others), use multiple conditions*

Device IP Address

Checks whether the device IP address falls within a defined range.

© 2026 InfoExpress, Inc.

Configuration:

— Condition:

— IP is within range

— IP is outside range

— IP Address Range Format:

— 10.0.0.1-10.0.0.255

— (One range per line. Multiple ranges supported.)

Device List

Checks whether a device matches a predefined list of IP or MAC addresses.

Configuration:

— Condition:

— Address is in list

— Address is not in list

— Check All Applicable:

— Select one or more predefined lists

Device MAC Address

Checks the MAC address prefix (OUI) of the device.

Configuration:

— Requirement:

— Match prefix

— Do not match prefix

— MAC Address Prefix Format:

— Use uppercase with colon separators

— Examples:

— AA:BB:CC

Use Case:

- *Identify device vendors such as printers, IoT devices, or specific manufacturers.*

Device OS

Checks the operating system of the endpoint.

Configuration:

— Requirement:

— Match any selected OS (OR)

— Do not match selected OS (NOT)

— Check All Applicable:

— Select from the list of detected operating systems

Device Online Status

Checks whether the device is currently active on the network.

Configuration:

— Online within X minutes

— Offline for more than X minutes

Use Case:

- *Used to identify inactive or stale devices.*

User Group

Checks whether the logged-in user belongs to a specific group.

Configuration:

— Requirement:

  — Match any (OR)

  — Match none (NOT)

— Check All Applicable:

  — Select from groups defined under:

  — Configuration → Global Settings → Names Used by Policies

Notes:

- *User group information can come from:*
- *Active Directory*
- *RADIUS attributes (VSA)*
- *Compliance Agent*
- *Compliance Agent is required for full functionality*

Device Approval Status

Checks whether the device meets defined approval or compliance criteria.

Configuration:

— Requirement:

  — Approved

  — Not approved

— Audit Methods:

  — Completed guest or device registration

  — Passed agent audit

  — Failed agent audit

  — No agent audit

  — Passed fingerprint check

  — Failed fingerprint check

  — No fingerprint set

© 2026 InfoExpress, Inc.

CONFIGURATION NOTES

— Rules can be reordered by dragging them up or down in the list

— Individual rules can be enabled or disabled as required

— Disabled rules are not evaluated

— After making any changes, click Activate to apply the configuration

DEFAULT RULE REFERENCE

The default Auto Trust policy contains the rules below. Customers who upgrade from earlier builds and have customized these rules should review the differences.

Rule	Conditions	Action
Device is on Routerlist	Device is on Routerlist	Set role to full-access — Device is on Routerlist
Device is on Allowlist	Device is on Allowlist	Set role to full-access — Device is on Allowlist
Device is on Blocklist	Device is on Blocklist	Set role to restricted — Device is on Blocklist
Deception Event – Honey Pot hit detected	Has all of these tags: Deception-Event	Set role to High-Risk-Event — Suspicious behavior detected; Send message to Admin via Email
Fingerprint Mismatch	Has any of these tags: FP-mismatched	Set role to High-Risk-Event — Device failed fingerprint check
Malware Lateral Spread Risk – Scan Detected	Has all of these tags: Dark-IP-Scan, Scan-detected	Set role to High-Risk-Event — Excessive network scanning activity was detected
Orchestration Event	Has any of these tags: SIEM-Event, IPS-Event, infected, FW-Event, APT-Event	Set role to High-Risk-Event — Malware or suspicious behavior has been detected
Passed Agent Audit	Passed Agent Audit	Set role to full-access — Passed agent audit
Failed Agent Audit	Failed Agent Audit	Set role to failed-agent-audit — Failed agent audit
Endpoint Security Non-Compliance (agent-less checks)	Has any of these tags: AV-off, AV-out-of-date, No-AV, non-compliant, Sensor-off, Sensor-out-of-date, stale-device	Set role to non-compliant — Device is NOT compliant with the corporate endpoint security policy
Patch Non-Compliance (agent-less checks)	Has any of these tags: patch-failed, patch-pending, patch-stale	Set role to non-compliant — Device is NOT compliant with the

© 2026 InfoExpress, Inc.

		corporate patch management policy
Trusted Managed Device	Has any of these tags: AD-managed, AV-managed, managed-device, patch-managed, XDR-managed	Set role to full-access — Assigned trusted managed device tag
Trusted IOT Device	Has any of these tags: enforcer, network-infrastructure, printer, switch, VoIP	Set role to full-access — Assigned trusted IOT device tag
BYOD Registration	Has any of these tags: byod	Set role to BYOD — Device registered with authorized credentials
Consultant Registration	Has any of these tags: consultant	Set role to consultant — Device registered as consultant
Guest Registration	Completed Guest or Device Registration	Set role to guest — Device registered by guest

If none of the above conditions are met, a device is assigned to the Untrusted Role.

ROLES & ACCESS POLICY

The Roles & Access Policy maps assigned Roles to Access Groups (ACLs). Default policies are provided and can be adjusted as needed.

Navigation: Go to Policies → Roles & Access

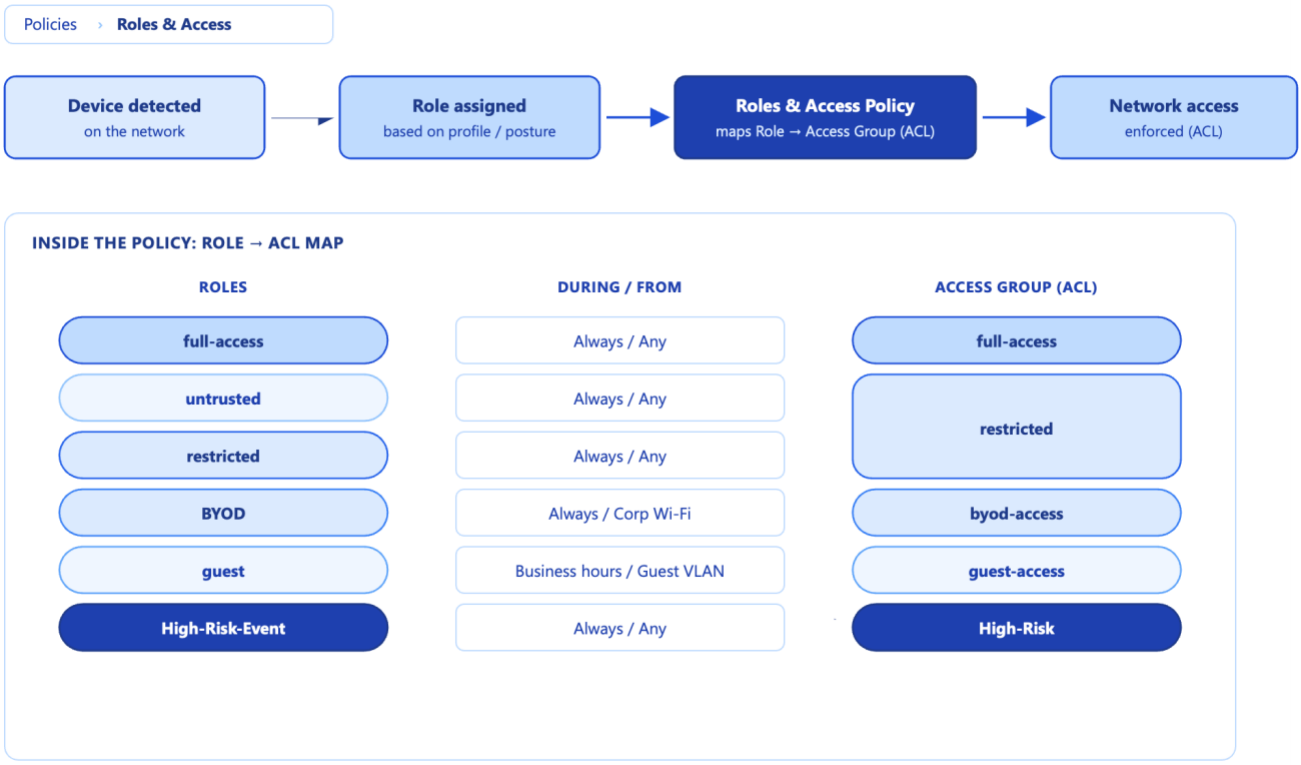
BEHAVIOR

— Each role is associated with an Access Group (ACL)

— Multiple roles can map to the same Access Group

— This allows for more granular classification while maintaining consistent enforcement

For example, both Untrusted and Restricted roles may be assigned the same restricted Access Group, while still being tracked separately for reporting purposes.



TIME AND LOCATION-BASED ASSIGNMENT

Access Groups can be assigned based on:

— Time (e.g. office hours)

— Location (e.g. specific subnets or IP range)

To configure time and location settings:

— Go to Policies → Time/Location/List

CONFIGURATION NOTES

— Ensure time and location profiles are defined before using them in policies

— After making changes, click Activate to apply

© 2026 InfoExpress, Inc.

ACCESS GROUPS (ACLS)

Each Access Group is associated with a configurable ACL that determines how traffic is handled for devices assigned to that group.

Navigation: Go to Control → Access Control Lists

MODIFYING AN ACL

— Select the Access Group to be modified

— Edit the ACL rules in the configuration dialog

— Save changes and activate the policy

DEFAULT RESTRICTED ACL BEHAVIOR

The default restricted ACL typically:

— Allows DHCP traffic

— Allows EasyNAC Compliance agent communication (TCP port 11698)

— Redirects DNS and/or HTTP traffic to the EasyNAC Captive Portal

— Blocks all other traffic

ACL RULE STRUCTURE

Each ACL rule follows the format:

<ACTION> WHEN <CONDITION>

SUPPORTED ACTIONS

— ALLOW – permits traffic when the condition matches

— DENY – blocks traffic when the condition matches

— HTTPREDIRECT – redirects HTTP/HTTPS traffic

— DNSREDIRECT / DNSREPLACE – modifies DNS responses

— DNSALLOW – allows DNS reply traffic

<ACTION> WHEN <CONDITION>

SUPPORTED CONDITIONS

ACL conditions are built using the following parameters:

— ETHTYPE – IP or ARP

— DIRECTION – IN or OUT

— PROTO – ICMP, TCP, UDP, IGMP

— PORT / LOCALPORT / REMOTEPORT – port matching

— LOCALADDR – IP of restricted device

— REMOTEADDR / ADDR – destination/source IP

— HOSTNAME – DNS hostname matching

— TRUE / FALSE – always true or false

© 2026 InfoExpress, Inc.

OPERATORS

— ==, != for comparisons

— >, <, >=, <= for numeric values

— ! to negate conditions

NOTES

Subnets and IP ranges are supported (e.g. '192.168.0.1-192.168.0.100')

All string values must be enclosed in single quotes

ACL EXAMPLES

The following examples illustrate common ACL rules used in EasyNAC. These can be adapted to meet specific deployment, onboarding, remediation, or restricted-access requirements.

Note:

1) ACL rules are processed in order, from top to bottom.
2) More specific allow rules should normally be placed above broader redirect or deny rules.

These ACLs ship as defaults but can be customized. As with all default ACLs, review and adjust the rules to match your environment before relying on them for enforcement.

1. Allow all traffic `ALLOW WHEN TRUE` Allows all traffic without restriction.	**2. Deny all traffic** `DENY WHEN TRUE` Blocks all traffic.
3. Allow HTTP traffic `ALLOW WHEN PROTO=='TCP' AND PORT==80` Allows HTTP traffic.	**4. Allow NAC agent traffic** `ALLOW WHEN PROTO=='TCP' AND PORT==11698` Allows communication for the NAC agent over TCP port 11698.
5. Allow HTTP traffic to a specific IP address `ALLOW WHEN PROTO=='TCP' AND PORT==80 AND ADDR=='192.168.100.200'` Allows HTTP traffic only to the specified IP address.	**6. Allow FTP traffic to a subnet** `ALLOW WHEN (PROTO=='UDP' OR PROTO=='TCP') AND PORT==21 AND ADDR=='192.168.0.0/24'` Allows FTP traffic to hosts within the specified subnet.
7. Redirect web traffic to a URL `HTTPREDIRECT http://company.com WHEN PROTO=='TCP' AND (PORT==80 OR PORT==443)` Redirects HTTP and HTTPS traffic to the specified URL.	**8. Redirect web traffic to the EasyNAC Captive Portal** `HTTPREDIRECT(CaptivePortal)` Uses the EasyNAC Captive Portal IP automatically for HTTP redirection.
9. Redirect DNS responses to the EasyNAC Captive Portal `DNSREDIRECT(CaptivePortal)` Modifies DNS reply packets so that requests resolve to the EasyNAC Captive Portal IP.	**10. Allow access to a specific website** `ALLOWSITE('microsoft.com')` Allows both DNS replies and traffic to the specified website.

© 2026 InfoExpress, Inc.

	This rule should be placed above any DNSREDIRECT rule.
11. Allow access to a website and all subdomains `ALLOWSUBSITE('microsoft.com')` Allows both DNS replies and traffic to the specified website and all its subdomains. This rule should be placed above any DNSREDIRECT rule.	**12. Replace DNS replies with the Captive Portal IP** `DNSREPLACE(CaptivePortal)` Useful in environments without DNS servers. DNS requests are answered directly with the EasyNAC Captive Portal IP.
13. Allow RDP access to a restricted endpoint `ALLOW WHEN (PROTO=='TCP' OR PROTO=='UDP') AND LOCALPORT==3389` Allows Remote Desktop access to a restricted endpoint. LOCALPORT refers to the port on the restricted device.	**14. Allow RDP access to one specific restricted endpoint** `ALLOW WHEN PROTO=='TCP' AND LOCALPORT==3389 AND LOCALADDR=='192.168.10.20'` Allows Remote Desktop access only to the restricted endpoint with IP address 192.168.10.20.
15. Allow RDP access from a specific subnet `ALLOW WHEN PROTO=='TCP' AND LOCALPORT==3389 AND REMOTEADDR=='192.168.10.0/24'` Allows Remote Desktop access to restricted devices only from the specified subnet.	**16. Allow FTP access to a specific server** `ALLOW WHEN PROTO=='TCP' AND (PORT==20 OR PORT==21) AND ADDR=='10.20.0.5'` Allows FTP traffic from restricted devices to the specified FTP server.

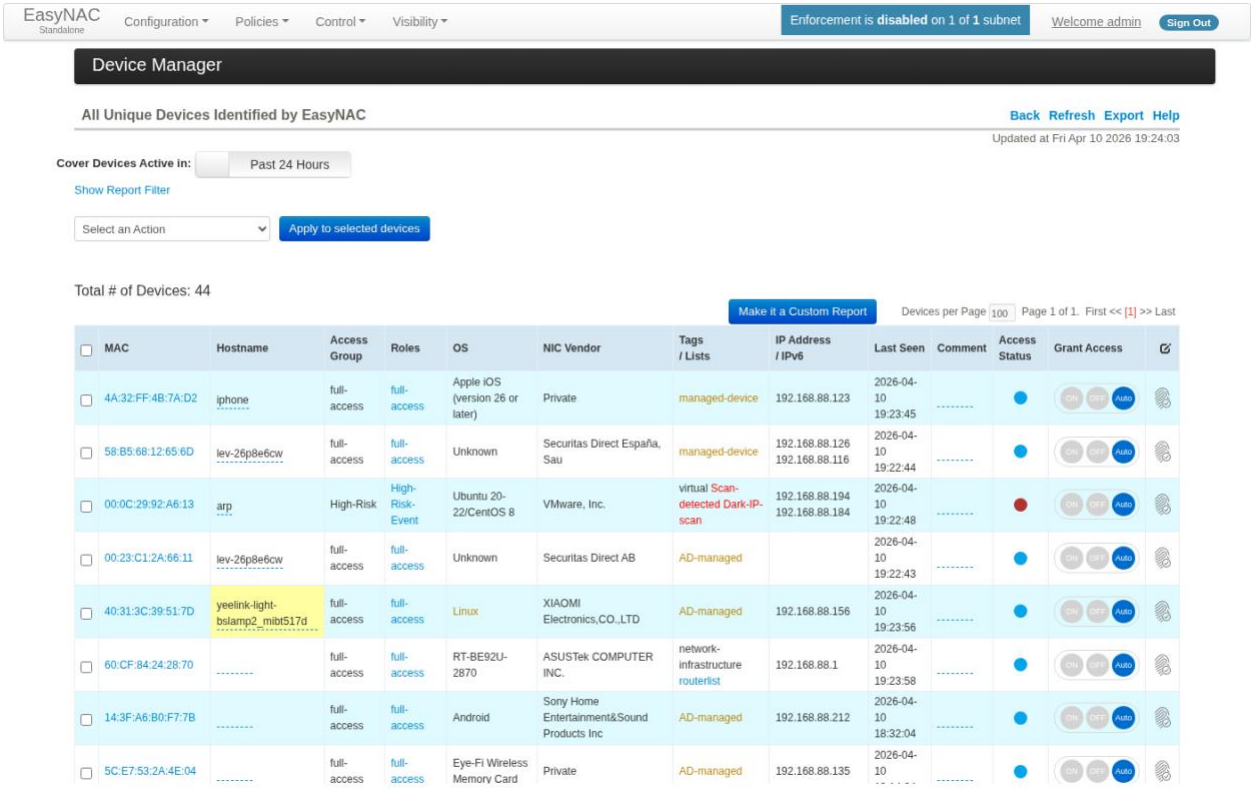
© 2026 InfoExpress, Inc.

TAGGING DEVICES AND ALLOWLISTING

In NAC deployments, it is a common requirement to grant access (Allowlist) specific devices that are not normally registered by end-users. Typical examples include printers, network infrastructure, VoIP phones and other types of devices.

An easy way to grant access is by using the concept of Tagging. The EasyNAC solution supports the ability for administrators to create and set tags on specific devices. Then using Auto Trust Policy, devices with specific tags can be granted full-access, restricted or assigned some other access.

By default, devices with any of these tags: AD-Managed, AV-Managed, managed-device, patch-managed, XDR-managed, enforcer, network-infrastructure, printer, router, switch, and VoIP, will automatically be granted full-access. This list can be modified to address unique. requirements.



Note: *The above policy order was changed for illustration purposes. Typically, these rules place lower in priority, so non-compliant devices or high-risk devices can be assigned a restrictive role.*

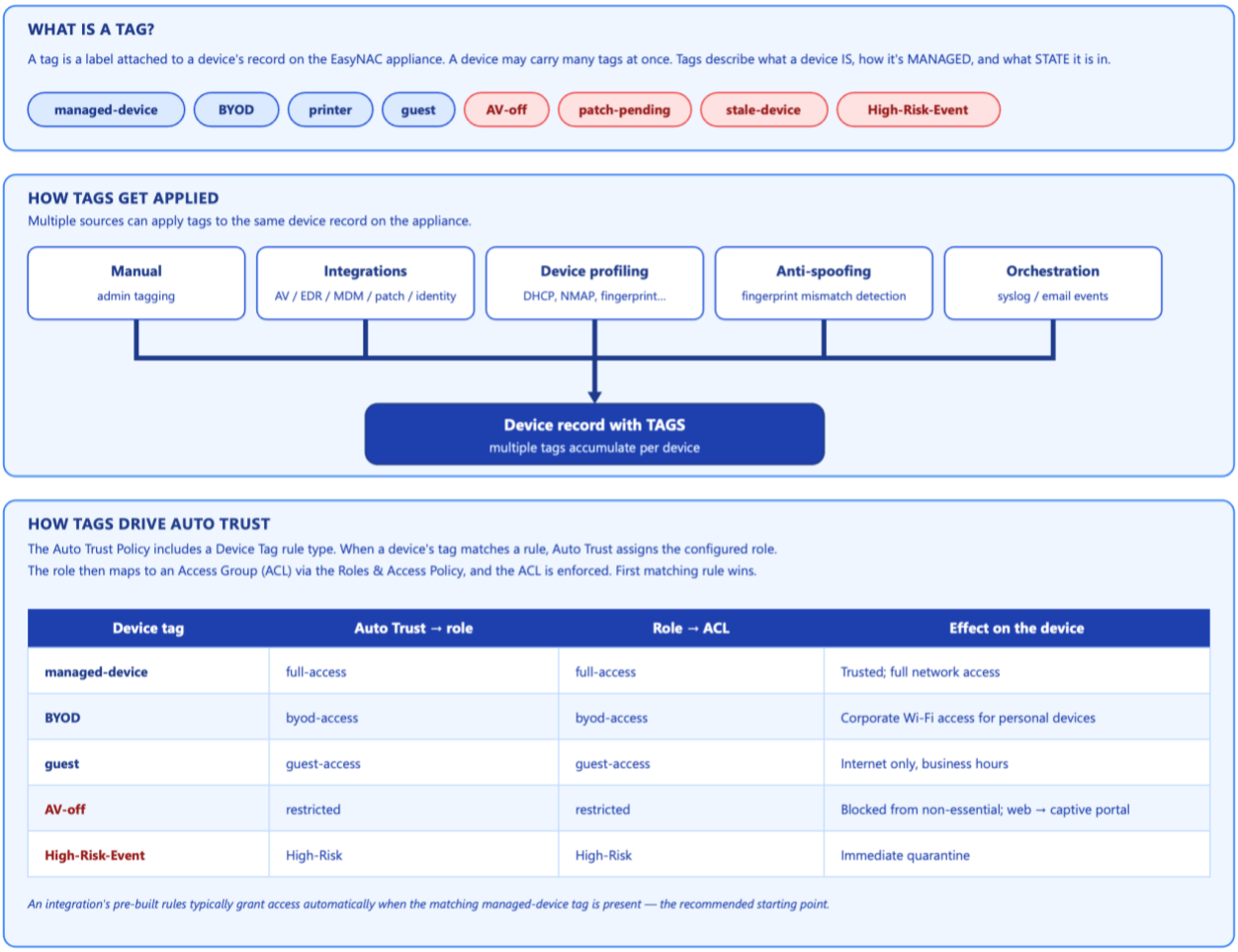
With the Device Profiler feature, EasyNAC automates the process of tagging. The EasyNAC solution can automatically tag a device based on the results of device profiling. If EasyNAC detects that a device is a printer, it will tag the device as a printer. If using the default Auto Trust Policy, the printer would then be granted full-access. The same is true for network infrastructure like routers.

TAGS

The EasyNAC Appliance supports pre-defined tags and custom tags. Pre-defined tags are organized into three separate groups: Compliance, Device Type and Event. Customers can also add their own custom groups and custom tags.

- Navigate to Configuration → General Settings - Click "**Tags and Groups Used by Policies**":

Tags can be leveraged to address many unique requirements. For example, if printers need to be physically checked before access is granted. Then a policy you can set to send an alert to the administrator when a device was automatically tagged as a printer shows up on the network. Once the printer has been verified, the administrator can then assign a custom tag, i.e., approved-printer, which allow it access to the network.



Setting Tags

To manually assign tags to devices via the Device Manager.

— Navigate to Visibility → Device Manager

If the list of devices is long, show the Report Filters at the top of the screen to narrow down the results.

Setting the tags manually can be done for one or more devices in a few steps.

— Select the device(s) where a tag is desired.

— Select an Action → Set tag and → Select Tag

— Confirm tag is Permanent or select an expiration period.

— Click “Apply to selected devices”

ALLOWLIST / BLOCKLIST / EXCLUDELIST / ROUTERLIST

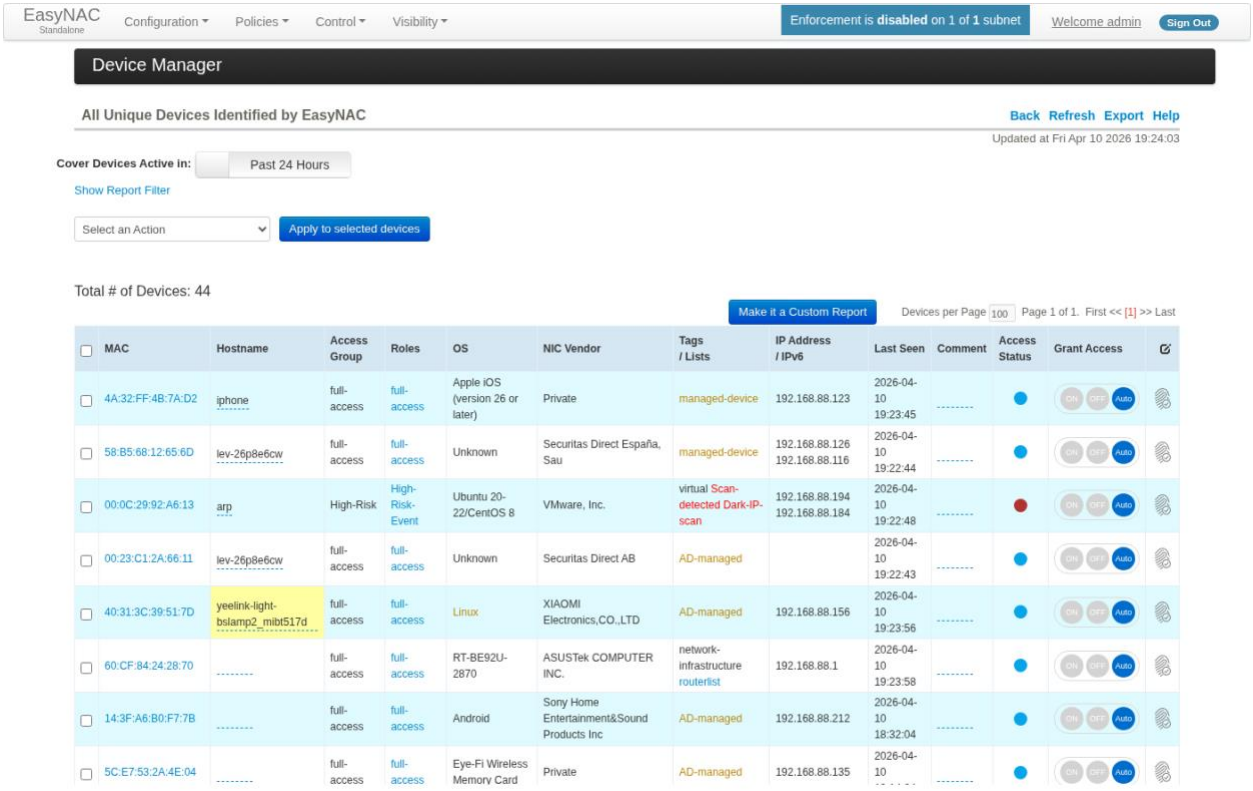
The EasyNAC Appliance also supports adding a device(s) to a manual Allowlist, Blocklist or Excludelist.

- **Allowlist** – Device will always have Full Access and be protected, regardless of policy.
- **Blocklist** – Device will always be Restricted, regardless of policy.
- **Excludelist** – Device is ignored by the EasyNAC Appliance. It will not be restricted or protected from rogue devices. Excluded devices do not consume a license.
- **Routerlist** – Default gateways will automatically have Full Access and be protected. For ARP enforcement to work as expected VRRP and HSRP routers would need to be add manually.

The examples below will assume Allowlist, but other lists will work the same way.

In the Network Map, add devices by MAC Address or IP Address to the Default Allowlist or a subnet-specific Allowlist. If entered the Default configuration, the Allowlist configure for all subnets. When adding devices to the Default configuration, it's best to use MAC addresses, so it can be relevant to all subnets.

- Navigate to Control → Network Map → Show Configuration



The Network Map can also be used to configure IP addresses or MAC addresses that should only be Allowlisted on a specific subnet(s).

- Navigate to Control → Network Map
- Find the desired subnet and click on the "Show Configuration." link

Once the "Show Configuration" link has been clicked, the view will expand to show the Allowlist box specific to this subnet. Both IP Addresses and MAC Addresses can be added.

© 2026 InfoExpress, Inc.

ADDING DEVICES TO THE ALLOWLIST OR BLOCKLIST

For quick additions to the Allowlist or Blocklist you can click the ON | OFF controls in the Device Manager. ON is the technical equivalent of being on the Allowlist, while OFF is the equivalent of being on the Blocklist. Auto means access is set automatically following the policies defined under Auto Trust Policy.

When you click the ON button you will be given the option to select an expiration period. Permanent is the default value.



When adding multiple devices to the Allowlist it can be convenient to add devices via the Device Manager.

- Select the device(s) to be added to Allowlist
- Select the action → Add to list → Select Allowlist
- Confirm the list is Permanent or select an expiration period.
- Click "Apply to selected devices"

Note: *Devices that are in the Allowlist display as ON. Blocklist devices display as OFF. Their respective list will also be shown in the Tags / Lists column.*

THE EXCLUDELIST

Excluded devices receive no EasyNAC Appliance protection.

It's typically used for handling a compatibility issue. Issues are rare, but one known example is with the Cisco wireless AP. If the AP is not excluded, it would cause DHCP to fail.

You can also use the Excludelist feature for short-term license management. Excluded devices do not consume licenses, which can help manage overcapacity temporarily. Use this carefully: excluded devices lack protection against rogue, non-compliant, or infected devices.

Note: *If the device license is exceeded by more than 10%, new devices joining the network automatically join to this Excludelist and would therefore not be enforced or protected.*

THE ROUTERLIST

The Routerlist is used to add non-default gateways to the settings. It commonly used if a customer is using VRRP or HSRP. With redundant gateways, it is required that router's virtual and actual MAC addresses be added in the "Routerlist" for enforcement to work properly.

© 2026 InfoExpress, Inc.

DEVICE DISCOVERY

The EasyNAC Appliance uses a combination of passive monitoring and active techniques to detect endpoints as they connect to the network. This hybrid approach ensures fast identification of new devices while maintaining full visibility of systems that may not generate regular network traffic.

DHCP-BASED DISCOVERY

When an endpoint configured for DHCP connects to the network, it broadcasts a DHCP DISCOVER request to obtain an IP address. This broadcast is visible to all devices within the same subnet, including the EasyNAC Appliance.

Once the DHCP server assigns an IP address, the endpoint begins normal network communication by sending ARP requests. EasyNAC observes both the DHCP exchange and subsequent ARP activity, allowing it to quickly identify and profile the new device.

STATIC IP DISCOVERY

Endpoints using static IP addresses do not generate DHCP traffic. Instead, they rely on Layer-2 ARP broadcasts to locate gateways and other devices on the network.

Because EasyNAC operates within the same broadcast domain, it passively listens for these ARP requests and can immediately detect newly connected devices, even in the absence of DHCP activity.

BROADCAST AND MULTICAST MONITORING

In addition to DHCP and ARP, EasyNAC passively monitors a range of broadcast and multicast traffic to improve device visibility. This includes protocols such as mDNS, NetBIOS, and other local discovery mechanisms commonly used by endpoints.

This capability is particularly useful for identifying unmanaged devices, IoT systems, and endpoints that may not follow standard network behavior.

ACTIVE NETWORK SCANNING

To complement passive detection, EasyNAC performs periodic network scans to identify devices that may not generate broadcast traffic. This includes:

* Quiet or idle devices
* Systems with long-lived connections
* Devices operating in tightly controlled or segmented environments

© 2026 InfoExpress, Inc.

This ensures that endpoints connected to the network are discovered even if they do not actively announce their presence.

SNMP-BASED DISCOVERY (OPTIONAL)

EasyNAC can optionally leverage SNMP to query network infrastructure such as switches, routers, and wireless controllers.

Through SNMP, EasyNAC can:

- Retrieve MAC address tables
- Map endpoints to specific switch ports
- Identify devices that may not be visible through broadcast traffic alone

This provides additional context and improves overall network visibility, particularly in larger or more complex environments.

SUMMARY

By combining passive monitoring, active scanning, and optional infrastructure integration, EasyNAC delivers comprehensive and near real-time device discovery without requiring agents or changes to existing network architecture.

© 2026 InfoExpress, Inc.

DEVICE PROFILING

When the EasyNAC Appliance detects a new endpoint, it profiles the device to identify its operating system.(OS) it is running, and which network ports are open by using both active and passive profiling techniques. Active Profiling includes network scanning such as NMAP, UPnP, NBTScan which detect an endpoint's OS, its open ports and grab the web server banner when it is detected on an endpoint.

Passive Profiling is accomplished by detecting the DHCP DISCOVER request broadcast packets and comparing them to the internal DHCP fingerprinting records to match up with the OS's unique identifier.

Note: *Device Profiling information is also obtained from optional agents or integration modules such as Active Directory or Endpoint Protection software.*

DHCP PROFILING

DHCP Profiling is enabled by default, and the EasyNAC Appliance maintains an internal database for common end-user operating systems such as Windows, macOS, iOS, Android, and Linux. For DHCP profiling of IoT devices, it's recommended to leverage Fingerbank, a cloud-based DHCP database of 35,000+ devices, which significantly improves profiling accuracy of IOT devices.

FINGERBANK

EasyNAC customers can leverage this cloud API for DHCP profiling of devices. Inverse allows companies to register for a free API license for up to 300 queries per hour. To register an account please visit:

https://api.fingerbank.org/users/register

To add this API to the EasyNAC Appliance:

- Navigate to Configuration → General Settings
- Click Device Profiler and select the Fingerbank tab.
- Paste the API key and click Test Connection.
- If the test succeeds, click Save.

Note: *It's recommended to use EasyNAC's built-in DHCP profiling for typical end-user computing devices. This would save the free API queries for IoT devices, where it's needed.*

Note: *The EasyNAC Appliance connects to api.fingerbank.org:443.*

NMAP PROFILING

NMAP Profiling is enabled by default. It profiles devices and detects open ports. NMAP scans run every 24 hours, the recommended frequency. You can disable NMAP scanning if needed. To review or change these default settings:

- Navigate to Configuration → General Settings
- Click Device Profiler and select NMAP Scan.

Note: *You can disable NMAP scanning entirely or on a per-subnet basis. To disable NMAP scanning on a specific subnet:*

- Navigate to Control → Network Map
- Find the desired subnet and click on the "Show Configuration" link
- Select Yes on the "Disable NMAP Scanning."", and it will be disabled on this subnet only.

© 2026 InfoExpress, Inc.

UPNP PROFILING

UPnP Profiling is enabled by default and retrieves Operating System and hostname information from UPnP-enabled IoT devices. UPnP scanning is lightweight and runs every 5 minutes. To review or modify these default settings:

- Navigate to Configuration → General Settings
- Click Device Profiler and select UPnP Scan.

SNMP SCAN

SNMP scanning is disabled by default. When enabled, SNMP queries network devices to identify the switch and port each device uses. This information enhances your ability to detect and prevent MAC spoofing.

Supported Brands: 3COM, Aruba, Cisco, F5, Fortinet, H3C, HP, Huawei, Juniper, Meraki, Mikrotik, PaloAlto, Sonicwall, TP-Link, and VMware.

To enable and configure SNMP Scan settings:

- Navigate to Configuration → General Settings
- Click Device Profiler and select SNMP Scan.

© 2026 InfoExpress, Inc.

CONFIGURING DEVICE PROFILER POLICIES

The EasyNAC Appliance collects detailed profiling information about devices. Use this information to create custom device profiling policies that automate device tagging.

DEVICE DETAIL DATA

To review the information collected about a device:

- Open Device Manager
- Click MAC address of the device

Tip: *Use the Device Detail Data to create custom Device Profiling Policies.*

DEVICE PROFILING POLICIES

In the EasyNAC Appliance GUI:

- — Navigate to Policies → Device Profiler

The EasyNAC Appliance has a few preconfigured Device Profiling Policies, these can be disabled or modified.

- Click Add Rule to create a custom profiling rule
- Click Add to create one or more Conditions
- Click Add to create one or more Actions
- — Click "Activate Policies"

Devices that match all three conditions receive the CCTV tag. After tagging, Auto Trust Policy, you can grant these devices full network access.

Note: *The above policy order was changed for illustration purposes. Typically, place these rules lower in priority to address non-compliant or high-risk devices can be assigned a restricted role.*

© 2026 InfoExpress, Inc.

Conditions you can test

- **Device profile attributes** — OS family, hostname pattern, MAC OUI / vendor, DHCP class identifier, open ports.
- **Network attributes** — IP range or Network Group membership, VLAN, switch port (when collected).
- Time-of-day / day-of-week qualifiers if you only want a profile to apply during specific hours.
- **All listed conditions in a rule are ANDed** — the device must satisfy every condition for the rule to fire.

Actions you can configure

- Apply one or more tags to the device (for example, CCTV, printer, VoIP-phone, IoT).
- Set or clear a fingerprint so anti-spoofing can detect later impersonation.
- Place the device into a specific Allowlist, Blocklist, or Excludelist.
- Trigger a notification (email / Slack / Teams / SMS / Syslog) when a new device first matches the rule.

Best practices

- Name rules with a numeric prefix (for example, 10-, 20-, 30-) so the priority order is obvious in the list.
- Make rule conditions as specific as possible so a device only matches one rule — generic catch-all rules belong at the bottom of the list.
- Use the Device Detail Data of a known good device to identify the most stable attributes to test (avoid attributes that change between firmware versions).
- Verify with a test device after activating: open Device Manager, confirm the expected tag has been applied, then confirm the Auto Trust Policy assigns the intended role.

Tip: *Profiling policies set device tags; Auto Trust then evaluates those tags through its Device Tag rule. Keep the two responsibilities separate — use Profiling to identify what the device IS, and use Auto Trust to decide what access that kind of device should get.*

© 2026 InfoExpress, Inc.

NETWORK MAP

The Network Map (Control / Network Map) is the page where the NAC parameters for every subnet seen by the EasyNAC Appliance are defined and managed. The page combines two layers of settings — a Default Configuration that applies to all subnets and per-subnet overrides that take precedence on individual subnets.

A global Enforcement Enable / Disable control sits at the top of the page. When Enforcement is set to Disabled here, EasyNAC control is completely stopped across the appliance — every subnet behaves as if enforcement were off, regardless of its individual mode.

Default Configuration (applied to all subnets)

The Default Configuration is opened with Show Configuration at the top of the page. Settings made here apply to every subnet unless overridden on the subnet itself.

- **Routerlist** — Routers on this list are granted full access. Traffic between enforced devices and a router is still captured and controlled per ACL.
- **Allowlist** — Devices on this list are granted full access and can optionally be protected.
- **Blocklist** — Devices on this list are treated as rogues.
- **Excludelist (Enforcement exclusion)** — Devices on this list are completely unprotected by NAC enforcement. Typical use is a Cisco AP in the subnet — if not excluded, it can cause DHCP to fail and devices on the subnet to exhaust the DHCP pool.
- **Devices to protect in addition to routers** — Routers are always protected; this option additionally protects devices on the Allowlist or those granted full access.
- **Allow duplicate subnets by location** — Allows the same subnet range to be configured across multiple locations.

Note: *Enable only where overlapping IP addressing is intentional. Confirm the design and implications with InfoExpress Support before use, as incorrect configuration may impact enforcement accuracy.*

- **Enable bidirectional capturing** — When enabled, EasyNAC performs ARP-based enforcement toward both ends of a communication flow, including the source device (for example, a rogue or non-compliant endpoint) and the destination device (for example, a protected resource). This improves enforcement coverage, particularly for east-west traffic and lateral-movement scenarios. If disabled, EasyNAC primarily directs ARP enforcement toward destination devices only, which may reduce visibility and control over source-side behavior.
- **Disable NMAP Scanning** – Only when it is disabled in the Global Settings, it can then be enabled on a per-subnet basis.
- **Send ARP request instead of response to** — Protected / Rogue.
- **Disable ARP Scanning** — Disables ARP-based discovery and scanning of devices within the subnet.
- **On-demand enforcement** — Enforcement is not applied pre-emptively; it is only triggered when actual traffic or a request is observed. This allows enforcement to occur reactively based on detected communication rather than proactively. Recommended for subnet with a /22 subnet.

Per-subnet rows

Below the Default Configuration each subnet appears as a row showing:

- **Network** — the subnet in CIDR notation.
- **Last seen** — when the subnet was last observed.
- **Location** — the Network Group the subnet belongs to.

© 2026 InfoExpress, Inc.

- **Mode** — three buttons: Enforce / Monitor / Disabled.
- **Show Configuration** — opens the subnet-specific settings; any setting changed here overrides the Default Configuration for this subnet only.

Per-subnet enforcement modes

- **Enforce** — Access control is applied. Non-compliant devices can be restricted, redirected to the captive / remediation portal, or quarantined per the Auto Trust Policy and the assigned ACL.
- **Monitor** — The appliance only observes the subnet. Devices are discovered, profiled, and tracked, but no enforcement is applied.
- **Disabled** — The appliance does nothing on this subnet. Use Disabled where the appliance is reachable but is intentionally not responsible for that subnet.

View types and bulk operations

The page can be viewed as Ungrouped, Grouped, or By Group (using Network Groups to organize the display).

The Apply to selected Subnets bar runs bulk operations on any selection:

- **Change Subnets group** — move the selected subnets into a different Network Group.
- Set mode value to Enforce.
- Set mode value to Monitor.

Other controls

- **Show timed-out subnets** — toggles whether subnets that have stopped reporting are shown.
- **Export** — downloads the current view.
- **Help** — opens the in-product help for this page in a new tab.

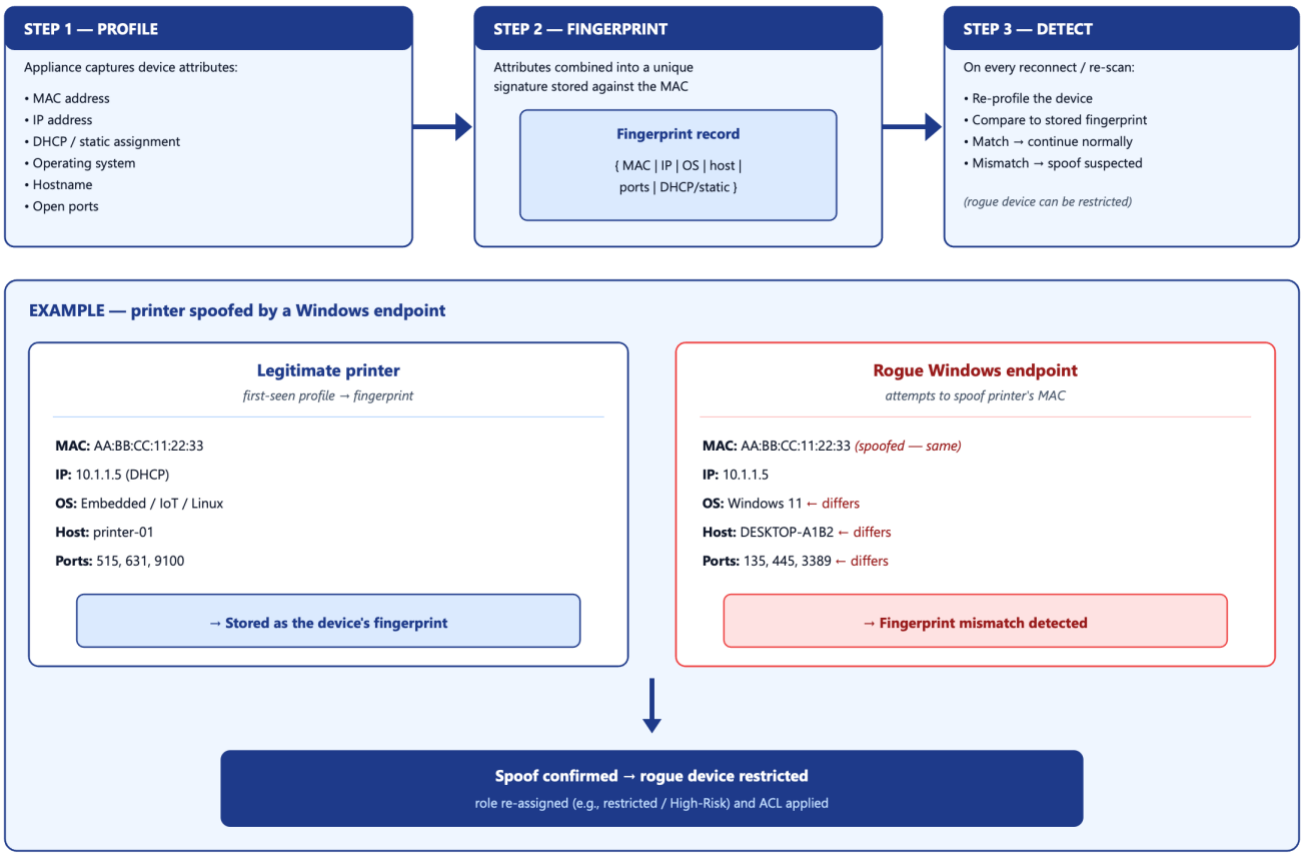
Assigning subnets to a Network Group

Use the Change Subnets group bulk operation (or the per-subnet equivalent) to place subnets into a Network Group. The group is a management container only — it lets configuration changes be applied to several subnets in one step and does not appear as a policy condition or filter.

© 2026 InfoExpress, Inc.

ANTI-SPOOFING PROTECTION

EasyNAC's fingerprint feature protects against MAC address spoofing. The system automatically profiles each device, capturing its MAC address, IP address, DHCP or static assignment, Operating System, hostname, and open ports. Use this profiling data to create a unique fingerprint for each device. Once set, the fingerprint prevents spoofing attempts. Example: A printer fingerprint includes its hostname, IP address, open ports, and Embedded/IoT/Linux OS. If a Windows or Apple device attempts to spoof this printer's MAC address, the EasyNAC Appliance detects the spoof and can restrict the rogue device.



SETTING FINGERPRINTS

Use Device Manager to set fingerprints.

- Select the device(s) for which you want to set a fingerprint.
- Select the Action → Set fingerprint
- Click "Apply to selected devices"
- Confirm which device details to include in the fingerprint. → Save

Note: *To include Switch Port info in the fingerprint, SNMP scanning or the RADIUS Proxy feature requires configuration.*

Devices with set fingerprints will have a blue fingerprint icon displayed in the Device Manager. Clicking on the fingerprint will show the information included in its unique fingerprint.

© 2026 InfoExpress, Inc.

Tip: *Click the gray fingerprint icon to quickly set or change a fingerprint.*

MAC SPOOFING DETECTION

Once a fingerprint has been set, any changes in the fingerprint details will cause a mismatch and actions can be taken. In the example below, a Windows XP device had spoofed the MAC address of the printer. Since the Operating System and the hostname didn't match the fingerprint. The fingerprint icon was changed to red, and device was assigned a FP- mismatched tag so actions can be taken.

IP SPOOFING DETECTION

The fingerprint can also set and monitor the IP address allocation of the endpoints. Options include checks for:

1) Static IP 2)
2) DHCP assigned IP address or
3) DHCP assigned IP in a specific subnet scope.

Device changing how their IP address is assigned will be tagged as a FP-mismatched.

In the example below, the device's fingerprint was set for a DHCP assigned address in the 10.160.0.0/24 subnet.

When it's IP changed to a static IP address, even in the same subnet, it will be tagged FP-mismatched.

Using Policies → With Auto Trust rules, EasyNAC acts when a fingerprint mismatch is detected. Configure the policy so that a device is assigned the High-Risk-Event role and alerts are sent to the network administrator via email and Teams.

FINGERPRINT RESCAN INTERVAL

Some device profiling features, such as NMAP scanning, operate on a default 24-hour interval. To improve fingerprint mismatch detection, a shorter rescan interval can be configured. It is recommended to apply the increased scan frequency only to devices with configured fingerprints.

In the EasyNAC Appliance GUI:

- Navigate to Configuration → General Settings → Device Profiler
- Select Fingerprint tab

MULTI-FACTOR AUTHENTICATION

The Fingerprinting feature can also provide 2FA (Something you know (password) and something you have a (specific device). User accounts will be captured with the use of agents, WMI or 802.1X, and then associated with a specific device.

- Click "User Name" and then select the from a list of available accounts. Up to 5 accounts can be included in a Fingerprint.
- If using agents, click "Agent Serial number"; If it can't be selected then the device doesn't have and agent installed.
- Save Changes to Fingerprint

© 2026 InfoExpress, Inc.

Note: *If you are unable to select "User Name" then no user names have been detected for this device. User names are sourced from the use of Agents, WMI, or 802.1X authentication when using the RADIUS Proxy feature.*

MISMATCHED AUTHENTICATION

Once a fingerprint has been set, any changes in the fingerprint details will cause a mismatch and actions can be taken. If there is an authentication mismatch, the fingerprint icon was changed to red, and device was assigned a FP- mismatched tag so actions can be taken.

You can change the fingerprint to include more than one username to the fingerprint.

ROGUE DHCP SERVER DETECTION

With personal Wi-Fi routers and misconfigured virtual machines, it is not uncommon for rogue DHCP servers to show up on the network. EasyNAC can detect rogue DHCP servers. This allows you to quickly identify and remove unauthorized servers from your network.

- Navigate to Configuration → General Settings.
- Click "Other Servers"
- Under DHCP Servers, input the IP addresses of all the authorized DHCP servers on the network.
- Select "Detect Rogue DHCP Servers"

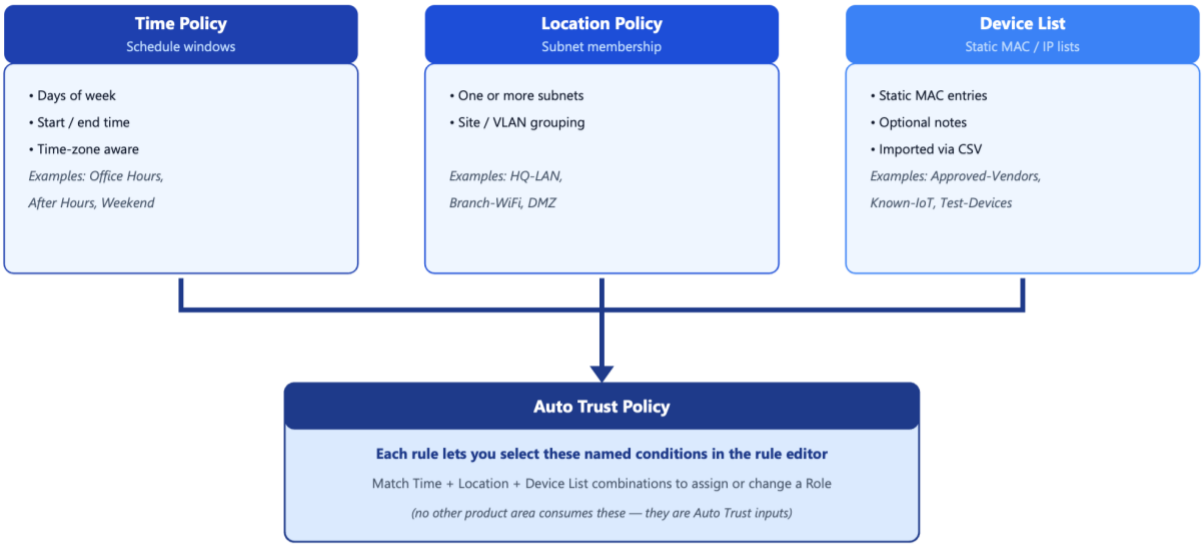
Note: *The EasyNAC Appliance tags any DHCP server not on your authorized IP list as DHCP-rogue.*

Using Policies → Auto Trust Policy, actions can be taken when DHCP-rogue is detected. Configure the policy to assign the device a restricted role and send alerts to the network administrators.

© 2026 InfoExpress, Inc.

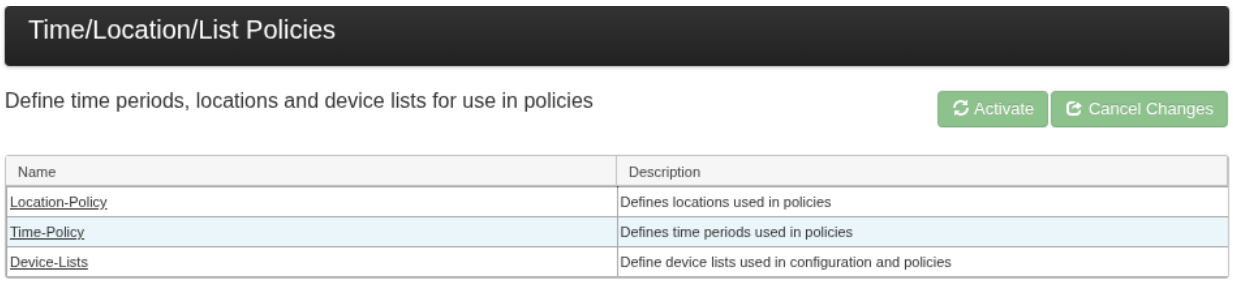
TIME / LOCATION / LIST POLICIES

It can be useful to use time, location, or lists of IP addresses to help determine what access should be granted. For example, the default settings will allow guests to access the internet at any time, and from any part of the network. If we wanted to limit where and when they can access the internet, we could use the Location and Time Policies.



LOCATION POLICY

Option 1: Set location names by adapter or VLAN in Configuration.→ Appliance settings



Option 2: Define location names by IP range.

- — Navigate to Policies → Time/Location/List and click on Location-policy.

  Location definitions can be based on IP address ranges. Once the Location name has been saved, it can now be added as a condition for Guest Access in the Roles & Access policy.

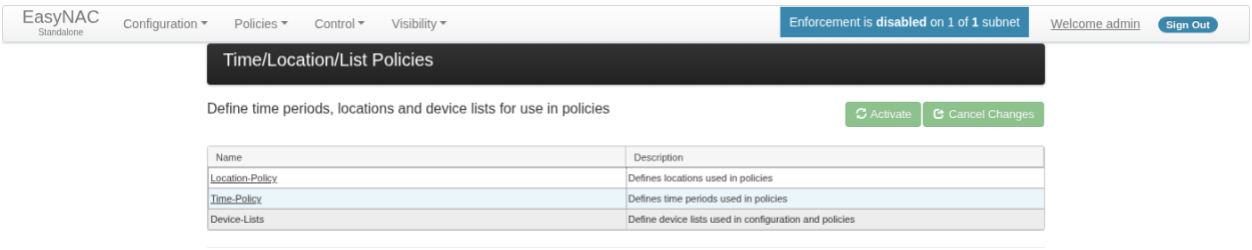
- Navigate to Policies → Roles & Access

This Roles & Access policy now provides two guest access groups. On the Guest WIFI, access is granted; at any other location, access is restricted. If we wanted to limited access to office hours, we could set a third condition based on time.

TIME POLICY

— Navigate to Policies → Time/Location/List and click on Time-policy.

Adjust existing time definitions or create new ones. Below is an example of how to define work hours:



After you save the Time Period name, you can use it as a condition in the Roles & Access policy.

— Navigate to Policies → Roles & Access

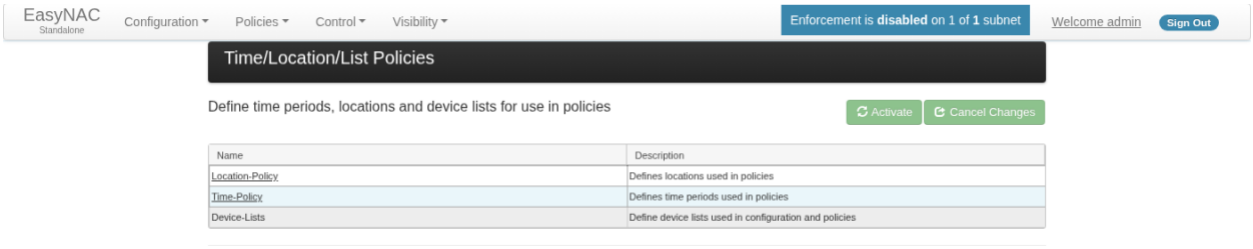
This Roles & Access policy now includes both time and location conditions. Guest access is granted only when both conditions are met.

DEVICE-LISTS POLICY

Device-Lists policies provide an easy method to define a list of IP addresses or MAC addresses to help determine what access should be granted. It is commonly used to define a group of IP addresses that need to be allowlisted.

— Navigate to Policies → Time/Location/List and click on Device-lists.

Device Lists can be adjusted, or new ones created. Below is an example of how to create a device list for a server farm using IP addresses.:



After you save the Device-List, you can use it as a condition in the Auto Trust Policy.

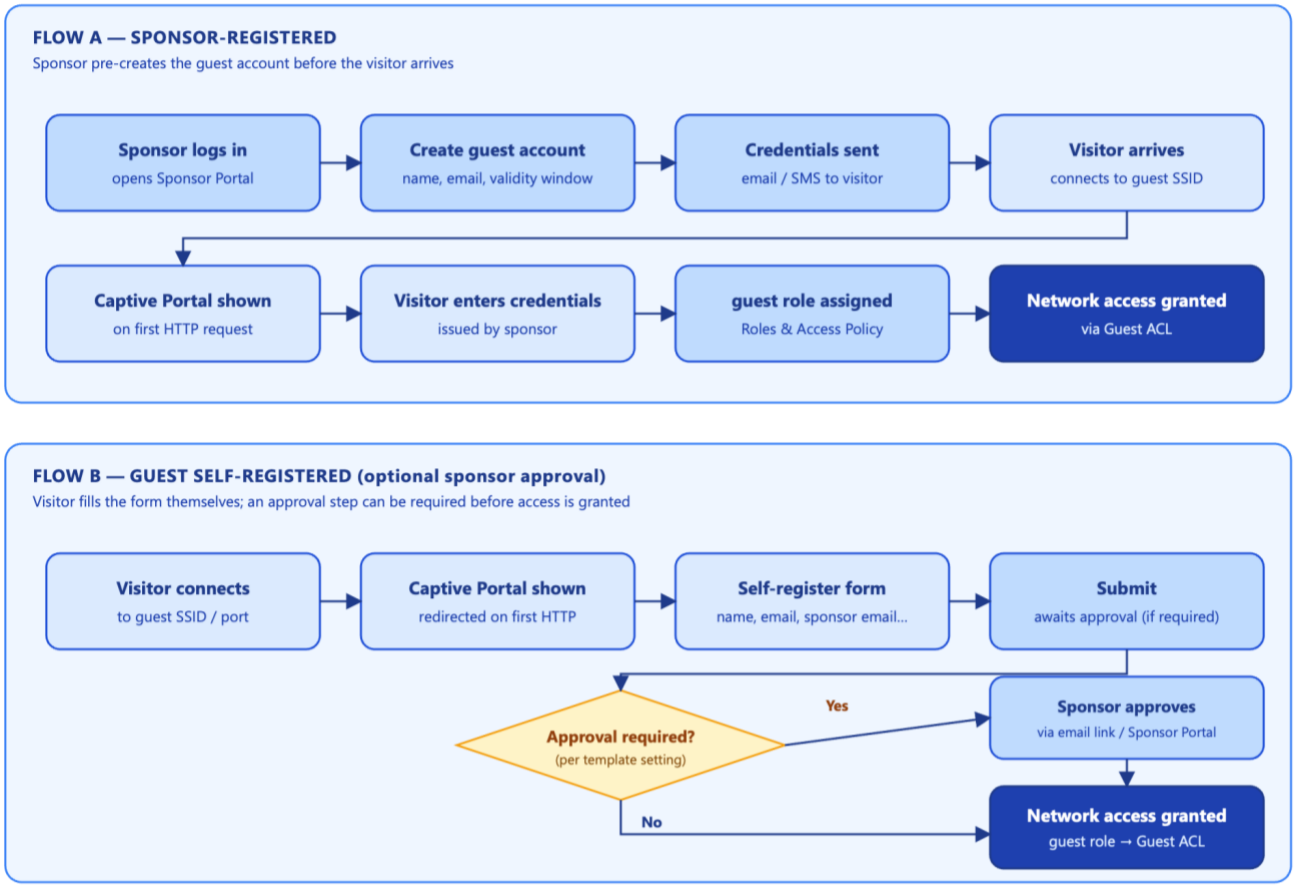
— Navigate to Policies → Auto Trust

The above Auto Trust policy will assign the Server Farm to have full-access

© 2026 InfoExpress, Inc.

CONFIGURING GUEST ACCESS

The EasyNAC Appliance supports multiple guest login methods: self-service registration, sponsor registration, and self-service registration with sponsor approval. You can enable all methods simultaneously to support different use cases. Guest Access is enabled by default. We recommend completing a few configuration steps to customize the guest experience.



CUSTOMIZE CAPTIVE PORTAL

Navigate to Configuration → General Settings and click on “Site Information”

Adjust the Company Title, Welcome Page Title, and any other details as desired.

Upload a corporate image and adjust the header and footer colors.

CUSTOMIZE GUEST PORTAL

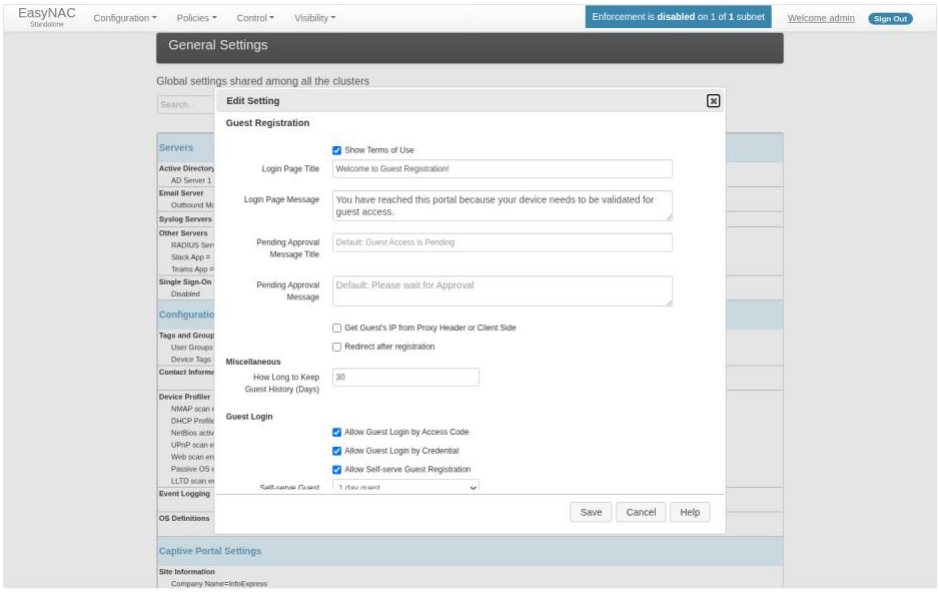
Navigate to Configuration → General Settings and click on “Guest Registration”:

— Edit the title and message boxes as desired.

— Enable or disable terms and conditions

— Set the number of days to keep guest history details

© 2026 InfoExpress, Inc.



Scroll down to enable your organization's preferred login methods.

Allow guest login by access code – This feature is enabled by default option allows for a guest to use a sponsor-provided access code to self-register a guest account. Based on Guest Templates, different access codes can require different registration information or grant different levels of access to guests (for example, a consultant access). Approval can also be required after the guest registers.

Allow guest login by credential – Enabled by default, this option allows for a guest to use their guest credentials to login. Guest Credentials can be provided by a sponsor or created by the guest as part of an earlier self-registration process.

Allow self-service guest registration – Enabled by default, this option allows a guest to provide their contact information required and get immediate guest access without requiring an access code. Based on the guest template used, approval can be required, and the information they must provide can be customized.

It is also possible to provide the guest with an option to provide their sponsor's email address for the approval process and on how long their registration should be active.

Automated Guest Registration – EasyNAC supports an optional automated guest account creation feature. Using syslog, third-party systems can send guest information to the appliance. For example: When a guest registers at reception, the front desk system sends guest details to EasyNAC. EasyNAC automatically creates a guest account for that user. Contact InfoExpress or your authorized partner for more information on this feature.

GUEST REGISTRATION TEMPLATES

The EasyNAC Appliance supports multiple registration methods for different guest experiences. Use templates to customize registration for different use cases. For example: One template might require basic guest information and grant internet access for one day. Another template might require detailed information, sponsor approval, and grant server access for three days.

The EasyNAC Appliance includes several pre-configured registration templates. You can modify these templates or create new ones. The default templates include:

Consultant Registers Themselves

- Consultant register themselves using an access code
- Account expiration set for 1 week, with authentication every 12 hours.

  - A consultant tag is assigned to give the guest consultant access.
  - Approval is optional; you can enable it if needed.
  - Limited to 1 device
- **1-day guest – no approval necessary**
  - The EasyNAC Appliance automatically generates a random password and username after the user provides their details.
  - Account is valid for 12 hours
  - Approval is optional; you can enable it if desired.
- **Automated Guest Registration**
  - Used only when the custom Automated Guest Registration Feature has been configured. This feature allows third-party servers to send guest accounts details to the EasyNAC Appliance.
  - Set the duration of guest access and how frequently users must re-authenticate.

CUSTOMIZING DEVICE REGISTRATION TEMPLATES FOR GUESTS

- Navigate to Configuration → Device Registration Templates → Guest Registration Templates
- Select an existing template or Click "Add template" to create a new one.
- Here administrators can adjust the user experience, required fields, and account validity, etc.

First, decide whether the template is for Self-Registration or Sponsor Registration. With Sponsor Registration, an approved employee creates the guest account and provides the credentials to the visitor. Sponsor Registration templates do not require access codes, so they have fewer configuration options.

Guest Template Options (for Self-Registration)

- **Method Name** – Use a meaningful name that sponsors will recognize.
- **Description** – Optional. Use this field to provide additional details about the template.
- **Username Created** – Decide whether the system automatically generates the account name or the guest specifies it.
- **Password Created** - Decide if the account name is auto generated by the system, or the guest.
- **Show guest credentials on registration** – After a guest completes the registration process their browser will show a successful web page. If selected, this checkbox will remind or inform the user of their credentials on this success page.
- **Select the information that the guest must enter** – Select the fields that guests see during registration. You can also add custom fields under Configuration.→ General Settings → Registration Fields.
- **Confirm Guest** – This dropdown box allows you to configure an additional verification check.
- **Sponsor Approval Required** – With this option a sponsor email is configured in the template. This sponsor will receive an email when a guest registers using this template. The Sponsor can 1-click a link in the email to approve the guest. If outside the office, the sponsor can also reply to the email with a keyword, like (approve, accept, OK, etc.) to also approve the guest. (email approval requires the email orchestration feature to be enabled.
- With Self-Service Registration, you can conveniently allow guests to specify their sponsor. A group of employees or the entire company can be given permission to sponsor a guest.

Note: *WhatsApp, Slack, and Teams can also approve guest accounts if the integration is enabled.*

- **Send Access code by Email** – With this method, EasyNAC sends a code to the email address the guest provides during registration. The guest then enters the code, which must be typed into the guest portal to complete the registration process. Note: the guest will need access to his email account.

© 2026 InfoExpress, Inc.

- **Send Access code by SMS** – With this method, EasyNAC sends a code to the phone number the guest provides during registration. The guest then uses code, that must be typed into the guest portal to complete the registration process. Note: an SMS gateway must be configured to use this feature.
- **Tag Guest** – When checked, you can select a Tag to assign to the guest's device. This tag is useful for assigning a specific type of access to this guest. For example, if assigned a consultant tag, they will be assigned consultant access. For more details on tags, see the section titled Tagging Devices and Allowlisting.
- **Access Code Type** – Access codes are useful for managing different templates for different guest types. This optional setting allows you to configure if the access codes created can be used more than once (Group use) or one-time only. Group use can be more convenient, while one-time use offers more security for when access is being provided to sensitive resources.
- **Code Expires after** – Set how long an access code remains valid after creation. For Group use codes, you may want to change them on a regular basis. You can provide a default value, but also choose to let sponsors change this value, when the Access code is first generated.
- **Access Code Prefix** – By default, EasyNAC randomly generates access codes with an optional prefix to help you identify what the code is for. For example, if you create a template designed for events, you may want to use a prefix EV. Then all access codes generated using this template will start with EV. A simpler approach is to check the box to allow the sponsors to create any code they prefer manually. With this approach, they can create an access code called Dec20-event. This is easier for both sponsors and guests to remember.
- **Account Expires After** – Sets the duration of the account once it has been created using this template. Once the account expires, the guest will need to complete the registration process again, if necessary. Using the checkboxes provided, the administrator can choose to allow sponsors or guests to adjust the length of time their account should last.
- **Max Devices per Guest** – Sets the maximum number of devices that a guest can use with their account.

© 2026 InfoExpress, Inc.

SETTING UP SPONSORS

The EasyNAC Appliance can query the Active Directory server to validate permissions for sponsors to access the management UI. Approved sponsors would only be given access to guest management functionality.

Using the "Active Directory Users and Computers" MMC:

Add the group "GRM-Sponsor"

> **Note:** *upper/lower case is significant when creating AD groups.*

After creating the GRM-Sponsor AD group, grant sponsor rights to staff by adding their user ID to the GRM-Sponsor group.

By default, sponsors can sponsor all types of guest accounts. To limit sponsors to only certain guest types (for example, if the reception staff is only permitted to create daily visitors), please follow these steps:

- Navigate to Configuration → Device Registration Methods
- Verify the types you want the sponsor to be able to administer.
- Navigate to Configuration → Permission Manager and select the GRM-Sponsor Role (or another role you may have created)
- Select the registration methods that sponsors are permitted to administer.

SPONSORING USERS

Creating a "consultant Registers Themselves" Access Code

- A user who has either GRM-Sponsor or CGX-Admin permissions can go to Visibility.→ Guest Registration Manager. If a user only has sponsor access, they can log in to the main EasyNAC web GUI and will have limited access to the Sponsor Guest pages.
- Choose "Consultant Registers Themselves" from the pick list and click on "Create a Sponsorship":
- Complete the fields as desired and click "Save":

  To create other types of access codes, follow the process outlined above. When additional information is needed, the web UI will request them.

© 2026 InfoExpress, Inc.

CONFIGURING DEVICE REGISTRATION

The EasyNAC Appliance supports device registration and is commonly used to support Bring Your Own Device (BYOD) initiatives. Employee's or student devices are checked by validating their credentials against Active Directory, Azure AD, or a RADIUS database. When a new device joins the network, it will be redirected to the Captive Portal. Staff would then be able to register the device, and this registration remains valid for days, weeks, or months. Several configuration options allow administrators to have access control of the BYOD devices. Administrative options include:

- Which AD groups are allowed to register BYOD device(s)
- Quantity of BYOD devices allowed per user (by group)
- Type of BYOD devices allowed

Role-based access granted

CUSTOMIZING THE DEVICE REGISTRATION PORTAL

- Navigate to Configuration → General Settings and click on "**Employee Device Registration**".
- Edit the title and message boxes as desired.
- Opt-in or Opt-out to show Terms of Use
- Click the Save button to accept any changes to the configuration.

CONFIRM ACTIVE DIRECTORY SETTINGS

To validate AD credentials, the AD server must be configured correctly. To verify settings, use the GUI.

- Navigate to Configuration → General Settings.
- Click Active Directory Servers
- Under Active Directory Server, confirm the host or IP address of the AD domain controller and the Account suffix in the "Account Suffix" field. **The.@ symbol should proceed the Account Suffix.**

By default, all domain users with valid credentials can register their BYOD devices. It is possible to limit which groups can register their devices, and to set different policies for different groups. To enable granular AD registration, the AD groups must be specified in the EasyNAC Appliance.

- Navigate to Configuration → General Settings.
- Click "Names Used by Policies"

Add the Active Directory groups that would need to register their devices. Groups that are added will be shown as a configurable option when customizing Device Registration methods.

CUSTOMIZING DEVICE REGISTRATION METHODS

- Navigate to Configuration → Device Registration Templates → Device Registration Templates

There are two default templates for employee device registration, one for customers who use cloud-based MS Azure AD, and another for traditional AD servers. To make changes to a typical registration…

- Click the "Employee Registers Personal Device" registration type:

© 2026 InfoExpress, Inc.

The above defines various parameters that can be customized for the device registration method. The default method is configured to apply to all users with valid credentials.

Additional device registration methods can be created for different AD groups to have different parameters. This can be useful in situations where different length of access, device quantity allowed, or different information needs to be gathered on the user.

To modify:

- Change the top pulldown box to 'Any of the groups checked'
- Select the Active Directory groups to which this template applies:
- Change the parameters for information gathered, access expiration, etc.
- Click 'Save' and Activate changes.

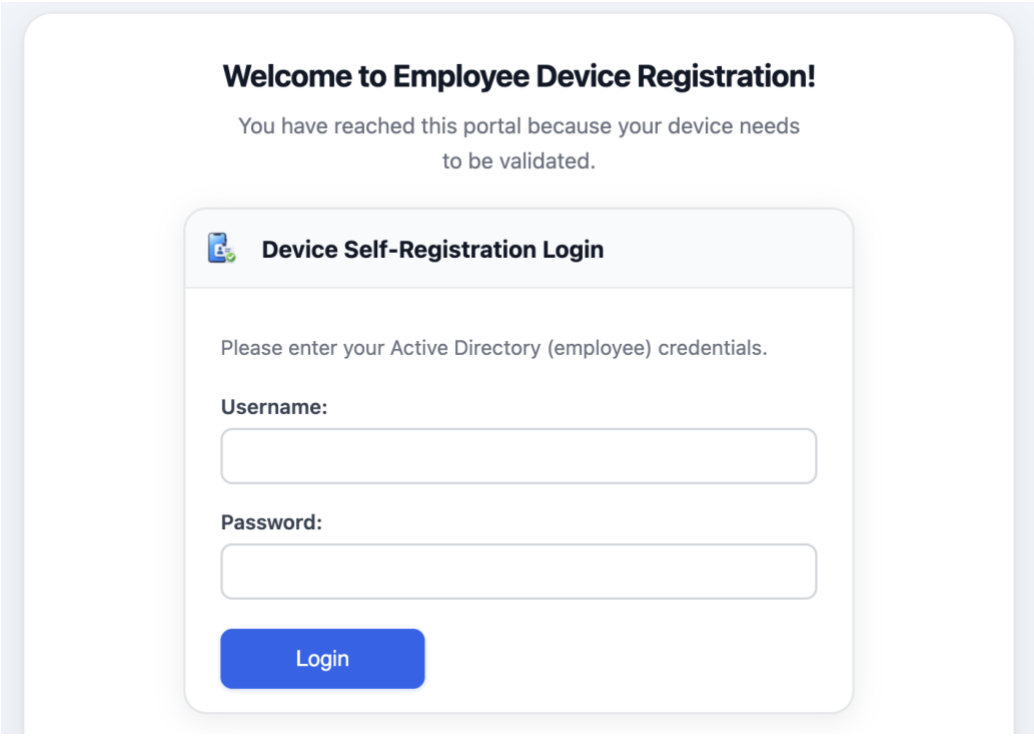
Note: *When you have multiple Device Registration Methods, they are evaluated from top to bottom. Methods can be re-arranged by dragging and dropping them in order they should be evaluated.*

USER EXPERIENCE

When a user is connected to the network, the browser will be redirected to a page like this:



Users can click on the Employee Device Registration link to be presented with a login screen:



At this point, the employee will enter their AD credentials. Depending on the configuration they may be prompted to complete an information form such as Full Name, Organization, Location, etc. After completion the appropriate access will be assigned.

This device will be remembered by the system based on the timeout specified in the device registration template. The user will not be asked for credentials until the device ages out of the database or the timer for login requests has expired.

> **Note:** *If a user exceeds the number of devices they are allowed to register, they will be shown their list of devices and can choose to deregister one or more devices.*

INTEGRATION MODULES

The EasyNAC Appliance integrates with leading enterprise antivirus, extended detection and response (XDR), and endpoint management platforms. By connecting directly to each vendor's management server, the EasyNAC Appliance can enforce compliance with security policies, without the use of agents. Devices out-of-compliance can be restricted, and an administrator(s) alerted.

Endpoint Security	Compatibility
Bitdefender GravityZone	Cloud and On-premises
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-premises – 6.5+ and Cloud
Trellix Endpoint Security HX (formerly FireEye HX)	Cloud
Kaspersky Antivirus	On-premises – 10.x+
Microsoft Defender	Cloud
Okta Verify	Cloud
SentinelOne	Cloud
Sophos Enterprise Console and Sophos Central	On-premises 5.x and Cloud
Symantec Endpoint Protection	On-premises 14.x and Cloud
Tenable Vulnerability Management	Cloud
Trellix ePO	On-premises – 5.x+
Trend Micro OfficeScan, Apex Central, and Vision One	On-premises XG+ and Cloud
Webroot	Cloud
Patch, Desktop & Mobile Management	**Compatibility**
HCL Big Fix	On-premises – 9.x+
Ivanti Security Controls	On-premises – 2019.3+
Kaseya VSA	On-premises or Cloud
ManageEngine Patch Manager	On-premises or Cloud - API v1.3 and v1.4
ManageEngine Endpoint Central	On-premises or Cloud - API v1.3 and v1.4
Microsoft SCCM / WSUS	On-premises – 4.x+ with SQL database
Moscii Starcat	On-premises -10.x
Microsoft Intune	Cloud
42Gears SureMDM	Cloud
Other Integrations	Compatibility
Microsoft Active Directory	On-premises

© 2026 InfoExpress, Inc.

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

INTEGRATION POLICIES PAGE STRUCTURE

The Integration Policies page in the EasyNAC management interface organizes integrations into four categories, with a panel of shared settings that apply to all integrations.

SETTINGS SHARED BY ALL THE INTEGRATIONS

- Alert if an integration server has been unreachable more than 2 times
- Ignore devices that have not updated in 30 days
- Not use DNS to resolve computer hostnames

VENDOR CATEGORIES

Each integration belongs to one of the following four categories. The categories are visual groupings on the Integration Policies page; they do not change how the integration is configured.

- **Network Infrastructure: Active Directory, Syslog** – Orchestration, E-mail – Orchestration, Malware Lateral Spread Protection (Zero Day), SolarWinds
- **Endpoint Security:** Bitdefender, Carbon Black, Cortex XDR, CrowdStrike, Cybereason, Elastic, ESET Antivirus, FireEye, Google Workspace, Jamf, Kaspersky Antivirus, Microsoft Defender, Okta, SentinelOne, Sophos, Symantec Endpoint Protection Manager, Tenable, Trellix ePolicy Orchestrator, Trend Micro, Webroot
- **Patch Management:** HCL BigFix, Ivanti Security Controls, Kaseya VSA, ManageEngine Patch Manager, Microsoft WSUS
- **Desktop & Mobile Management:** Headwind MDM, ManageEngine Endpoint Central (formerly Desktop Central), Moscii StarCat, Microsoft Intune, Microsoft WMI, Sure MDM

The per-vendor configuration sub-sections that follow in this chapter are presented alphabetically for ease of reference. The category labels are noted at the start of each vendor sub-section.

BITDEFENDER INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Bitdefender GravityZone to learn each managed device's protection status and enforce role-based access for endpoints that fall out of compliance.

Prerequisites:

- A Bitdefender GravityZone tenant reachable from the EasyNAC Appliance (cloud or on-premises Control Center)
- An API key generated under MyAccount / API in the GravityZone Control Center, with the Network API enabled for the key
- The Access URL exactly as shown in the GravityZone Control Center (must be entered in lower case)

© 2026 InfoExpress, Inc.

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Bitdefender.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the Access URL (lower case, matching the GravityZone Control Center).
- Enter the API Key obtained from MyAccount / API.
- Click Test connection to verify the appliance can reach GravityZone.
- Review the default query interval and tagging conditions, then click Save to apply.

Verification:

- Confirm a device managed by Bitdefender appears in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date) is applied within the configured query interval
- Review the integration log to confirm successful periodic queries against GravityZone

Note: *The Access URL is case-sensitive and must be lower case; the Network API must be enabled on the API key, otherwise authentication will fail. Use the AV-managed tag in the Auto Trust Policy to grant network access to any device protected by Bitdefender.*

CARBON BLACK CB RESPONSE INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Carbon Black Cb Response to identify endpoints under EDR coverage and to react to compliance events such as missing or stale sensors.

Prerequisites:

- A Cb Response server reachable from the EasyNAC Appliance over HTTPS
- An API token generated under Admin / My Profile / API Token in the Cb Response console
- Read access to device records on the Cb Response server

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Carbon Black.
- Enable the integration by selecting the Enable Integration checkbox, then choose Version: Cb Response.
- Enter the hostname or IP address and port number of the Cb Response server.
- In the Cb Response console go to Admin / My Profile / API Token, copy the token and paste it into the Token field.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by Cb Response appear in EasyNAC with a managed-device tag
- Take an endpoint offline from Cb Response for the configured stale interval and confirm a stale-device tag is applied
- Review the integration log to confirm successful periodic queries against the Cb Response server

© 2026 InfoExpress, Inc.

Note: *Use the managed-device tag in the Auto Trust Policy to grant access to endpoints under Cb Response coverage; tag stale endpoints (no check-in for x days) as stale-device and gate them to a non-compliant role.*

CARBON BLACK CLOUD INTEGRATION

Category: Endpoint Security

EasyNAC integrates with VMware Carbon Black Cloud (CBC) to learn endpoint protection status and apply role-based access for devices that fall out of compliance.

Prerequisites:

- A Carbon Black Cloud tenant reachable from the EasyNAC Appliance
- A custom Access Level configured under Settings / API Access with read access to Device General Information (only this scope is required — do not grant additional privileges)
- An API Key (API ID and API Secret Key) generated against that custom Access Level, plus the tenant Org Key

Configuration steps:

- In Carbon Black Cloud, navigate to Settings / API Access and define a new Access Level granting only read access to Device General Information.
- Add an API Key against that custom Access Level; copy the API ID and API Secret Key.
- In EasyNAC, navigate to Configuration / Integration and select Carbon Black; choose the Cloud version.
- Enable the integration and enter the Access URL, API ID, API Secret Key and Org Key.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm devices managed by CBC appear in the EasyNAC device list with a managed-device tag
- Disable the sensor on a test endpoint and confirm the corresponding tag (Sensor-out-of-date or stale-device) is applied
- Review the integration log to confirm successful periodic queries against CBC

Note: *Grant only read access to Device General Information for the custom Access Level — broader scopes are unnecessary and increase exposure if the API key is compromised.*

CROWDSTRIKE INTEGRATION

Category: Endpoint Security

EasyNAC integrates with CrowdStrike Falcon to identify endpoints with active sensor coverage and to react to compliance signals such as missing, stale, or quarantined hosts.

Prerequisites:

- A CrowdStrike Falcon tenant reachable from the EasyNAC Appliance

© 2026 InfoExpress, Inc.

- An API client created under Support and Resources / API Client and Keys, with read access to Hosts (this scope is required)
- The Client ID, Client Secret and the regional Falcon API Base URL

Configuration steps:

- In the CrowdStrike Falcon console, navigate to Support and Resources / API Client and Keys, then click Create API client.
- Grant the client read access to Hosts (required); add additional read scopes only if needed.
- Click Add and copy the Client ID, Client Secret and Base URL (these are shown only once).
- In EasyNAC, navigate to Configuration / Integration and select CrowdStrike; enable the integration.
- Enter the Access URL (regional Falcon Base URL), Client ID and Client Secret, then click Test connection.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm hosts with an active CrowdStrike sensor appear in EasyNAC with a managed-device tag
- Take a sensor offline on a test host and confirm a stale-device tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the Falcon API

Note: *Use the regional Base URL that matches your Falcon tenant (US-1, US-2, EU-1, US-GOV-1). Client Secret is shown only at creation time — record it securely. Grant only the Hosts read scope; broader scopes are not required.*

CYBEREASON INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Cybereason to identify protected endpoints and to react to sensor-state changes that affect compliance.

Prerequisites:

- A Cybereason tenant reachable from the EasyNAC Appliance
- A user account that can sign in to the Cybereason management console (the same credentials are used for the integration)
- The Cybereason console URL

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Cybereason.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the Cybereason console URL.
- Enter the username and password (the same credentials used for the Cybereason management console).
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

© 2026 InfoExpress, Inc.

Verification:

- Confirm endpoints managed by Cybereason appear in the EasyNAC device list with a managed-device tag
- Disable a sensor on a test endpoint and confirm the corresponding tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Cybereason

Note: *Use a dedicated, read-only Cybereason account so credential rotation and audit are independent of administrative use.*

ELASTIC INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Elastic Stack (Elasticsearch, formerly the ELK stack) to forward events and to query indexed device data. Use this integration where Elastic is your primary SIEM or observability platform.

Prerequisites:

- An Elastic deployment reachable from the EasyNAC Appliance
- An API key or service-account token with the appropriate index privileges
- The target index or data stream pre-created with a compatible mapping

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Elastic.
- Provide the Elastic endpoint URL, including protocol and port.
- Enter the API key or token used for authentication.
- Specify the target index or data stream name.
- Configure which event categories should be forwarded (device events, policy events, agent events).
- Save and apply the integration.

Verification:

- Trigger a test event from EasyNAC and confirm it appears in the Elastic index within a few seconds
- Run a search in Elastic against the target index for an EasyNAC field (for example device.mac or event.action) and confirm results return
- Review the Elastic index size growth over 24 hours to confirm forwarding volume matches expectations

Note: *If your Elastic deployment uses a non-standard certificate authority, ensure the appliance trusts the CA before configuring the integration; otherwise, event forwarding will fail with TLS errors.*

ESET ANTIVIRUS INTEGRATION

Category: Endpoint Security

© 2026 InfoExpress, Inc.

EasyNAC integrates with ESET Security Management Center (SQL mode) or ESET PROTECT cloud to learn each device's AV state and to react to compliance signals such as out-of-date definitions or disabled protection.

Prerequisites:

- SQL mode: an ESMC server with MS SQL Server reachable on TCP 1433, a SQL account with read permission to the era_db database (default ESMC database name), and the ESMC server firewall opened to the EasyNAC Appliance
- Cloud mode: an ESET PROTECT cloud tenant in a supported region (USA, Europe, Canada, Japan or Other), the matching Authentication Domain and Device Management Domain (see help.eset.com/eset_connect for current values)
- Cloud mode: a user account that can sign in to ESET PROTECT cloud

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select ESET Antivirus.
- Enable the integration by selecting the Enable Integration checkbox.
- For SQL mode: enter the ESMC SQL server hostname or IP, database port (1433), database name (era_db) and the SQL account user name and password.
- For Cloud mode: select the region, then enter the Authentication Domain and Device Management Domain (e.g., us.business-account.iam.eset.systems and us.device-management.eset.systems), and the cloud account credentials.
- Optionally enable Use the hostname for finding and tagging devices to match endpoints by agent hostname.
- Click Test connection, then click Save to apply.

Verification:

- Confirm endpoints managed by ESET appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-out-of-date) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the ESMC database or cloud API

Note: *SQL mode requires TCP/IP enabled on the SQL Server, port 1433 reachable, and a SQL account with read access to era_db; the SQL account should be read-only. Cloud mode region values change occasionally — confirm Authentication and Device Management domains against ESET's documentation before saving.*

TRELLIX ENDPOINT SECURITY HX INTEGRATION (FORMERLY FIREEYE HX)

Category: Endpoint Security

EasyNAC integrates with Trellix Endpoint Security HX (formerly FireEye HX) to identify protected endpoints and to react to sensor compliance changes.

Prerequisites:

- An HX appliance reachable from the EasyNAC Appliance over HTTPS
- A user account on the HX appliance with the API Admin role assigned (this specific role is required)
- The HX appliance management URL (the same URL used for the HX management console)

Configuration steps:

- In the Trellix HX management console, navigate to Admin / Appliance Settings / User Accounts and create a new user account with the API Admin role.
- In EasyNAC, navigate to Configuration / Integration and select FireEye Integration (or Trellix HX in newer versions); enable the integration.
- Enter the Access URL (the same URL used for the HX management console).
- Enter the API Admin account user name and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm hosts under HX coverage appear in the EasyNAC device list with a managed-device tag
- Take a sensor offline on a test host and confirm a stale-device tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the HX appliance

Note: *The API Admin role is the specific role HX requires for read access to the host inventory; do not use a higher-privileged role for this integration.*

GOOGLE WORKSPACE INTEGRATION

Category: Identity Provider

EasyNAC integrates with Google Workspace as an identity source for guest registration and BYOD authentication. Users authenticate against Google Workspace via OAuth2, and EasyNAC consumes the resulting identity to apply policy. This is distinct from the Google Workspace email integration in the Notifications chapter.

Prerequisites:

- A Google Workspace tenant with an administrator account that can register OAuth clients
- A Google OAuth2 client (Client ID and Client Secret) configured with a redirect URI that points to the EasyNAC Appliance's Captive Portal address
- Domain ownership for the redirect URI used by EasyNAC
- **Minimum OAuth2 scopes for sign-in:** `openid email profile`. If Workspace group membership drives Auto Trust assignments, additionally request `https://www.googleapis.com/auth/admin.directory.user.readonly`. Domain-wide delegation is not required for the captive-portal flow.

Configuration steps:

- In Google Workspace Admin / Google Cloud, register a new OAuth2 client and capture the Client ID and Client Secret.
- Configure the OAuth client's redirect URI to point to the EasyNAC Captive Portal address.
- In EasyNAC, navigate to Configuration / Integration and select Google Workspace.
- Enter the Client ID and Client Secret.
- Specify the Workspace domain or domains permitted to authenticate; configure attribute mapping if required (for example, Workspace OU → EasyNAC tag).
- Save and test by visiting the Captive Portal as an unregistered user; the Google sign-in option should appear and authentication should succeed.

Verification:

- An end-to-end sign-in test from a guest device confirms authentication flows through Google and produces the expected EasyNAC role and tag assignment
- The EasyNAC audit log records the authentication event with the Google identity
- Sign-ins from disallowed Workspace domains are rejected at the Captive Portal

Note: *This integration is a captive-portal OAuth flow — it is not a directory query and does not require domain-wide delegation. Restrict allowed sign-in domains to those you intend to admit for guest / BYOD access.*

HEADWIND MDM INTEGRATION

Category: Mobile Device Management

EasyNAC integrates with Headwind MDM to identify enrolled mobile devices and to react to enrollment-state changes that affect access.

Prerequisites:

- A Headwind MDM server reachable from the EasyNAC Appliance
- A read-only API account on the Headwind MDM server
- The Headwind MDM server URL and account credentials

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Headwind MDM.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the Headwind MDM server URL.
- Enter the API account user name and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm enrolled mobile devices appear in the EasyNAC device list with a managed-device tag
- Unenroll a test device and confirm the tag is removed within the configured interval
- Review the integration log to confirm successful periodic queries against Headwind MDM

© 2026 InfoExpress, Inc.

Note: *Use the managed-device tag in the Auto Trust Policy to grant network access only to mobile devices currently enrolled in Headwind MDM.*

HCL BIGFIX INTEGRATION

Category: Patch Management

EasyNAC integrates with HCL BigFix by querying its SQL database to learn each endpoint's patch and compliance status.

Prerequisites:

- A BigFix server with MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the BFEnterprise database (default BigFix database name)
- The BigFix server firewall opened to allow the EasyNAC Appliance to reach SQL Server on port 1433

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select HCL BigFix.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and database name (BFEnterprise).
- Enter the SQL account user name and password.
- Click Test connection to verify connectivity to the BigFix database.
- Review the default query interval and patch-status tagging rules, then click Save.

Verification:

- Confirm endpoints managed by BigFix appear in the EasyNAC device list with a managed-device tag
- Cause a test endpoint to fall behind on patches and confirm a patch-pending or patch-failed tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the BigFix database

Note: *Confirm that MS SQL Server is enabled for TCP/IP and listening on a known port (typically 1433), and that the BigFix server firewall allows that port from the appliance. The SQL account should be granted read access to BFEnterprise only.*

IVANTI SECURITY CONTROLS

Category: Patch Management

EasyNAC integrates with Ivanti Security Controls (Protect) by querying its SQL database to learn each endpoint's patch status.

Prerequisites:

- An Ivanti Security Controls server with MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the Protect database (Ivanti uses Protect or SecurityControls as the default database name)
- The Ivanti server firewall opened to allow the EasyNAC Appliance to reach SQL Server on port 1433

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Ivanti Security Controls.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and database name (Protect).
- Enter the SQL account user name and password.
- Click Test connection to verify connectivity.
- Review the default query interval and patch-status tagging rules, then click Save.

Verification:

- Confirm managed endpoints appear in the EasyNAC device list with a managed-device tag
- Cause a test endpoint to fall behind on patches and confirm a patch-pending tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the Ivanti database

Note: *Verify that SQL Server is enabled for remote connections on TCP 1433 and that the Ivanti server firewall allows the appliance to reach it. The SQL account should be granted read access to Protect only.*

JAMF INTEGRATION

Category: Mobile Device Management

EasyNAC integrates with Jamf Pro to identify enrolled Apple devices and to use enrollment, inventory, and smart-group data in the Auto Trust Policy.

Prerequisites:

- A Jamf Pro tenant reachable from the EasyNAC Appliance
- A Jamf API role + API client (preferred), or a legacy read-only API account, configured under Settings / API Roles and Clients in Jamf Pro, with read access to the computer and mobile device inventory
- The Jamf Pro tenant URL and API credentials

Configuration steps:

- In Jamf Pro, navigate to Settings / API Roles and Clients, create an API role with read scopes on the computer and mobile device inventory, then create an API client bound to that role.
- In EasyNAC, navigate to Configuration / Integration and select Jamf; enable the integration.
- Enter the Jamf Pro tenant URL.

© 2026 InfoExpress, Inc.

- Enter the API client ID and Client Secret (or, for legacy installs, the API account user name and password).
- Click Test connection to verify connectivity.
- Review the default query interval and smart-group tagging rules, then click Save.

Verification:

- Confirm Apple devices enrolled in Jamf appear in the EasyNAC device list with a managed-device tag
- Move a test device into a tracked smart group and confirm the matching tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Jamf Pro

Note: *Prefer Jamf API roles + API clients over legacy account-based credentials; scope the role to read-only access on the inventory categories you need.*

KASEYA VSA INTEGRATION

Category: Endpoint Management

EasyNAC integrates with Kaseya VSA to identify endpoints under Kaseya management and to use agent state in the Auto Trust Policy.

Prerequisites:

- A Kaseya VSA server reachable from the EasyNAC Appliance
- A Kaseya user account whose privileges include System Role and System Scope (these are required for the integration to read the inventory)
- The Kaseya VSA server hostname or IP and port

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Kaseya VSA.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the Kaseya VSA server hostname or IP and port.
- Enter the user name and password for an account that holds the System Role and System Scope.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by Kaseya appear in the EasyNAC device list with a managed-device tag
- Cause a test endpoint to fall behind on patches and confirm a patch-pending or patch-stale tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Kaseya VSA

© 2026 InfoExpress, Inc.

> **Note:** *The integration account must have both the System Role and System Scope in Kaseya — accounts without these will fail to read the full inventory. Use a dedicated account so its privileges, audit and rotation are independent of administrative use.*

KASPERSKY ANTIVIRUS INTEGRATION

Category: Endpoint Security

EasyNAC integrates with the Kaspersky Administration Server by querying its SQL database to learn each endpoint's protection state.

Prerequisites:

- A Kaspersky Administration Server with MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the KAV database (default Kaspersky database name)
- The Kaspersky Administration Server firewall opened to allow the EasyNAC Appliance to reach SQL Server on port 1433

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Kaspersky Antivirus.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and database name (KAV).
- Enter the SQL account user name and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by Kaspersky appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the Kaspersky database

> **Note:** *Confirm that MS SQL Server is enabled for TCP/IP on port 1433 and that the Administration Server firewall allows the appliance to reach it. The SQL account should be granted read access to KAV only.*

MANAGEENGINE DESKTOP CENTRAL INTEGRATION

Category: Endpoint Management

EasyNAC integrates with ManageEngine Endpoint Central (formerly Desktop Central) to identify managed endpoints and to use agent state and patch status in the Auto Trust Policy. Both on-premises (Endpoint Central On-Premises) and cloud (Endpoint Central Cloud) deployments are supported.

© 2026 InfoExpress, Inc.

Prerequisites:

- On-premises mode: an Endpoint Central On-Premises server reachable from the EasyNAC Appliance, with a user account that can sign in to the management console (provide a QR code image if MFA is enabled on the account)
- Cloud mode: an Endpoint Central Cloud tenant under domain endpointcentral.manageengine.com (Zoho Accounts URL accounts.zoho.com) with a Self-Client OAuth application registered in the Zoho Developer Console
- Cloud mode: OAuth Client ID, Client Secret, Authorization code, and a derived OAuth Refresh Token, generated against scopes DesktopCentralCloud.Common.READ, DesktopCentralCloud.SOM.READ, DesktopCentralCloud.Inventory.READ, DesktopCentralCloud.PatchMgmt.READ and MDMOnDemand.MDMInventory.READ

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select ManageEngine Desktop Central; enable the integration.
- Choose ManageEngine Type: Endpoint Central On-Premises or Endpoint Central Cloud.
- On-Premises: enter Hostname or IP, port, and the management console username and password (upload a QR code image if MFA is enabled).
- Cloud (Self-Client): in the Zoho Developer Console add a Self-Client, generate the Client Secret, then generate an Authorization code (10-minute time duration) covering the read scopes above; enter the Domain (endpointcentral.manageengine.com), Zoho Accounts URL, OAuth Client ID and Secret in EasyNAC, then click Get OAuth Refresh Token to derive the long-lived refresh token from the Authorization code.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by Endpoint Central appear in the EasyNAC device list with a managed-device tag
- Cause a test endpoint to become non-compliant in Endpoint Central and confirm the corresponding tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Endpoint Central

Note: *Cloud mode uses an OAuth Access Token that expires after 1 hour; the Refresh Token is required to obtain new Access Tokens. The Authorization code is single-use — generate it only once per Self Client. Use the listed read-only scopes; do not request write scopes.*

MANAGEENGINE PATCH MANAGER INTEGRATION

Category: Patch Management

EasyNAC integrates with ManageEngine Patch Manager Plus to learn each endpoint's patch status. Both on-premises and cloud deployments are supported.

Prerequisites:

- On-premises mode: a Patch Manager Plus server reachable from the EasyNAC Appliance, with a user account that can sign in to the management console
- Cloud mode: a Patch Manager Plus Cloud tenant under domain patch.manageengine.com (Zoho Accounts URL accounts.zoho.com) with a Self-Client OAuth application registered in the Zoho Developer Console
- Cloud mode: OAuth Client ID, Client Secret, Authorization code, and a derived OAuth Refresh Token, generated against scopes PatchManagerPlusCloud.Common.READ and PatchManagerPlusCloud.PatchMgmt.READ

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select ManageEngine Patch Manager; enable the integration.
- Select the ManageEngine type: On-premises or Cloud.
- On-premises: enter Hostname or IP, port, and the management console username and password.
- Cloud (Self-Client): in the Zoho Developer Console add a Self-Client, generate the Client Secret, then generate an Authorization code (10-minute time duration) covering the read scopes above; enter the Domain (patch.manageengine.com), Zoho Accounts URL, OAuth Client ID and Secret in EasyNAC, then click Get OAuth Refresh Token to derive the long-lived refresh token from the Authorization code.
- Click Test connection to verify connectivity.
- Review the default query interval and patch-status tagging rules, then click Save.

Verification:

- Confirm managed endpoints appear in the EasyNAC device list with a managed-device tag
- Withhold a critical patch from a test endpoint and confirm a patch-pending or patch-stale tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Patch Manager

Note: *Cloud mode Access Tokens expire after 1 hour; the Refresh Token is required to obtain new ones. The Authorization code is single-use. Grant only the listed read scopes.*

MICROSOFT DEFENDER INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Microsoft Defender for Endpoint to consume threat detection signals and risk scores. When Defender flags a device, EasyNAC can automatically tag the device, change its role, or move it to the restricted ACL.

Prerequisites:

- A Microsoft Defender for Endpoint subscription, with API access enabled

- An Entra ID (Azure AD) app registration granting EasyNAC read access to the Defender API (delegated or application permissions, as required by your tenant policy)
- The Tenant ID, Application (client) ID and Client Secret from the Entra ID app registration
- Create the Entra ID app registration:
    - Go to https://portal.azure.com/, sign in, and select Manage Microsoft Entra ID.
    - Click App registrations / New registration, enter an app name, then click Register.
    - Copy the Directory (tenant) ID and Application (client) ID for later use.
    - Click API permissions / Add a permission / APIs my organization uses, click WindowsDefenderATP, choose Application permissions / Machine / Machine.Read.All, then click Add permissions.
    - Grant admin consent for the permission.
    - Click Certificates & secrets / New client secret, enter a name, then copy the Value of the client secret immediately (the value is shown only once).

Configuration steps:

- Register an Entra ID (Azure AD) application as documented by Microsoft, granting the appropriate Defender API permissions and obtaining admin consent.
- In EasyNAC, navigate to Configuration / Integration and select Microsoft Defender; enable the integration.
- Enter the Tenant ID, Application (client) ID and Client Secret.
- Configure the polling interval and the Defender risk-score threshold above which an EasyNAC action should fire.
- Map Defender alert categories to EasyNAC tags or actions (for example, an Active Threat alert may map to the High-Risk-Event role).
- Click Test connection to verify the appliance can call the Defender API, then click Save to apply.

Verification:

- Trigger a benign test alert in Defender (for example using the Microsoft Defender for Endpoint test detection script) and confirm the alert reaches EasyNAC and produces the configured action
- Review the integration log to confirm successful periodic queries against the Defender API

Note: *Defender integrations are sensitive to Entra ID permission scopes — if integration calls fail, review the app registration's permission grants and confirm an administrator has consented to the required scopes. Rotate the Client Secret on the schedule defined by your credential policy.*

MICROSOFT INTUNE INTEGRATION

Category: Mobile Device Management

EasyNAC integrates with Microsoft Intune to identify enrolled devices, learn their compliance state, and use that state in the Auto Trust Policy.

Prerequisites:

- A Microsoft Intune tenant

- **Required Microsoft Graph application permissions:** `DeviceManagementManagedDevices.Read.All` and `DeviceManagementConfiguration.Read.All` (admin consent required). Read-only scopes are sufficient — write scopes are not used by this integration.
- An app registration in Microsoft Entra ID (formerly Azure Active Directory) with the required Intune Graph API permissions and admin consent granted
- The Tenant ID, Application (client) ID and Client Secret from the Entra ID app registration; an EasyNAC sign-in account holding the Intune Administrator role

Configuration steps:

- In Microsoft Entra admin center, navigate to App registrations / New registration and register a new application for EasyNAC.
- Generate a Client Secret for the registration; copy the Client ID, Tenant ID and Client Secret immediately (the secret is shown only once).
- Set API permissions on the registration as required by Intune Graph API access; ensure each permission's name and type are correct, and grant Admin consent.
- In EasyNAC, navigate to Configuration / Integration / Microsoft Intune and paste the Tenant ID, Client ID and Client Secret copied in step 2.
- Sign in with the EasyNAC Intune account (this account must hold the Intune Administrator role).
- Click Test connection, then click Save to apply.

Verification:

- Confirm devices enrolled in Intune appear in the EasyNAC device list with a managed-device tag
- Take a test device out of compliance in Intune and confirm a non-compliant tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Microsoft Graph

Note: *The AD-Managed tag applies to both Azure AD-joined and AD-registered devices; the managed-device tag applies only to Azure AD-joined devices. The Client Secret is shown only once at creation — store it securely. Rotate the Client Secret on the schedule defined by your credential policy.*

MICROSOFT SCCM / WSUS INTEGRATION

Category: Patch Management

EasyNAC integrates with the WSUS SQL database (and SCCM where present) to learn each endpoint's patch and compliance status.

Prerequisites:

- A WSUS server using MS SQL Server (not the Windows Internal Database — WSUS uses WID by default and must be migrated to SQL for this integration)
- MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the WSUS database, and the WSUS server firewall opened to TCP 1433

© 2026 InfoExpress, Inc.

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Microsoft WSUS.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and database name.
- Enter the SQL account username and password.
- Click Test connection to verify connectivity.
- Review the default query interval and patch-status tagging rules, then click Save.

Verification:

- Confirm endpoints reported by WSUS appear in the EasyNAC device list with a managed-device tag
- Cause a test endpoint to fall behind on patches and confirm a patch-pending or patch-failed tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against WSUS

Note: *WSUS uses the Windows Internal Database by default — you must migrate it to a full SQL Server before this integration will work. Confirm SQL Server is enabled for TCP/IP on port 1433 and that the WSUS server firewall allows the appliance to reach it.*

MICROSOFT WINDOWS MANAGEMENT INSTRUMENTATION (WMI)

Category: Endpoint Management

EasyNAC integrates with Microsoft Windows Management Instrumentation (WMI) to query Windows endpoints directly for installed software, services, hotfixes, and other inventory used in the Auto Trust Policy.

Prerequisites:

- Network reachability from the appliance to each target Windows endpoint over WMI / RPC ports
- A Domain Administrator account (or equivalent with rights to perform WMI queries on the target endpoints) — an underprivileged account is unlikely to succeed
- Windows Firewall and DCOM on the target endpoints configured to allow remote WMI queries from the appliance (see Microsoft's WMI Remote Connection guidance)

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Microsoft WMI.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the username in the form domain\username, plus the password.
- Click Test connection against a known-reachable Windows endpoint to confirm WMI succeeds.
- Review the default query interval and tagging conditions, then click Save.
- If WMI queries fail, review Windows Firewall, DCOM and Active Directory settings on the targets — Microsoft's documentation at docs.microsoft.com/en-us/windows/win32/wmisdk covers remote WMI prerequisites.

Verification:

- Confirm a target Windows endpoint appears in the EasyNAC device list with WMI-derived attributes populated
- Stop a tracked service on a test endpoint and confirm the corresponding tag is applied within the configured interval
- Review the integration log to confirm successful periodic WMI queries against managed endpoints

Note: *WMI requires a privileged account; in most environments a Domain Administrator is required because lower-privileged accounts cannot run remote WMI queries. When endpoints are restricted (for example by Captive / Remediation Portal redirect), the assigned ACL must still allow them to reach AD / WMI for the integration to function — sample ACLs that retain WMI/AD reachability for non-compliant endpoints are provided in the Configuring ACLs for WMI access section.*

MOSCII STARCAT INTEGRATION

Category: Asset Management

EasyNAC integrates with Moscii StarCat by querying its SQL database to learn each endpoint's asset and software-inventory state.

Prerequisites:

- A StarCat server with MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the StarCat database (StarCat 2013 does not use a default database name — verify the actual name on the SQL server)
- The StarCat server firewall opened to allow the EasyNAC Appliance to reach SQL Server on port 1433

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Moscii StarCat.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and the StarCat database name as configured on your SQL server.
- Enter the SQL account username and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm assets known to StarCat appear in the EasyNAC device list with a managed-device tag
- Take an endpoint offline so it stops checking in to StarCat for x days and confirm a stale-device tag is applied
- Review the integration log to confirm successful periodic queries against the StarCat database

Note: *StarCat 2013 has no default database name; check the SQL server for the correct database name before configuring. The SQL account should be granted read access to that database only.*

© 2026 InfoExpress, Inc.

OKTA INTEGRATION

Category: Identity Provider

EasyNAC integrates with Okta to learn the user identity associated with each device and to use Okta group membership in the Auto Trust Policy.

Prerequisites:

- An Okta tenant reachable from the EasyNAC Appliance
- An Okta API token created under Security / API / Tokens with read access to users and groups
- The Okta organization URL (Access URL)
- **Required Okta administrator role for token creation:** Read-Only Administrator. Higher-privileged roles (Super Admin, Org Admin) are not required for this integration. Generate the token under a dedicated service-account user so its rotation and audit are independent of interactive admins.

Configuration steps:

- In Okta, log in with administrator privileges and navigate to Security / API / Tokens, then click Create Token.
- Copy the API token to your clipboard immediately (it is shown only once).
- In EasyNAC, navigate to Configuration / Integration and select Okta; enable the integration.
- Enter the Access URL (your Okta organization URL).
- Paste the API token into the API Key field, then click Test connection.
- Review the default query interval and group-tagging rules, then click Save.

Verification:

- Confirm a known Okta user appears against the expected device record
- Add a test user to a tracked Okta group and confirm the matching tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Okta

Note: *Okta API tokens expire after 30 days. This expiration period cannot be modified, but each use of the token resets the timer — a token that is in active use therefore remains valid. If the integration goes idle for more than 30 days the token will need to be re-issued.*

PALO ALTO CORTEX XDR INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Palo Alto Cortex XDR to identify endpoints with active agent coverage and to react to compliance signals from the XDR platform.

Prerequisites:

- A Cortex XDR tenant reachable from the EasyNAC Appliance

© 2026 InfoExpress, Inc.

- An API key created under Settings / Configurations / Integrations / API Keys with security level Standard and role Viewer
- The API URL, API ID and API Key from the Cortex XDR console

Configuration steps:

- In the Cortex XDR management console, navigate to Settings / Configurations / Integrations / API Keys and click + New Key.
- Select Standard as the security level and Viewer as the role; click Save to generate the API key, then copy it.
- Note the API URL and API ID from the same page (both are required for EasyNAC).
- In EasyNAC, navigate to Configuration / Integration and select Cortex XDR; enable the integration and paste the API key.
- Enter the API URL and API ID values from Cortex XDR.
- Click Test connection to verify connectivity, then click Save.

Verification:

- Confirm endpoints with an active Cortex XDR agent appear in EasyNAC with a managed-device tag
- Take an agent offline on a test endpoint and confirm a sensor-offline or sensor-stale tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Cortex XDR

Note: *Use the Viewer role with Standard security level — broader roles are not required for the read-only signals EasyNAC consumes. The Sensor-offline tag may not be set on first network join (the device may be starting up); use a recent DHCP request as a corroborating signal to avoid an initial restriction.*

SENTINELONE INTEGRATION

Category: Endpoint Security

EasyNAC integrates with SentinelOne to identify endpoints with active agent coverage and to react to compliance and threat signals from the SentinelOne console.

Prerequisites:

- A SentinelOne tenant reachable from the EasyNAC Appliance
- A service user created under Settings / Users / Service Users with the appropriate access level (read access to agents)
- **Minimum service-user role:** Viewer (read-only). Restrict the service user to the specific Site or Account scopes that EasyNAC needs to monitor.
- **The SentinelOne management URL (Access URL** — same as the management console URL)

Configuration steps:

- In the SentinelOne management console, navigate to Settings / Users / Service Users and create a new service user with the access level required to read agent data.
- Copy the API token issued for the service user (shown only once).

© 2026 InfoExpress, Inc.

- In EasyNAC, navigate to Configuration / Integration and select SentinelOne Integration; enable the integration and paste the API token.
- Enter the Access URL (same URL used by the SentinelOne management console).
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints with an active SentinelOne agent appear in EasyNAC with a managed-device tag
- Disable an agent on a test endpoint and confirm an AV-offline or AV-out-of-date tag is applied within the configured interval
- Review the integration log to confirm successful periodic queries against SentinelOne

Note: *Use a service user (Settings / Users / Service Users) for the API token rather than an interactive admin's token, so the integration's access can be audited and rotated independently.*

SOLARWINDS INTEGRATION

Category: Network Infrastructure

EasyNAC integrates with SolarWinds (typically Network Performance Monitor / Orion) via the SolarWinds Information Service (SWIS) API to share device inventory and to enrich SolarWinds-monitored elements with EasyNAC role and tag context.

Prerequisites:

- A SolarWinds installation with the SWIS API reachable from the EasyNAC Appliance
- A SolarWinds account with read access to the relevant entities (orion.Nodes, orion.NodesCustomProperties and similar)
- The SolarWinds server URL and SWIS API port

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select SolarWinds.
- Enable the integration by selecting the Enable Integration checkbox.
- Provide the SolarWinds server URL and SWIS API port.
- Enter the SolarWinds account credentials (username and password, or a token if your SolarWinds version supports it).
- Configure the synchronization direction: push EasyNAC tags to SolarWinds custom properties, pull SolarWinds inventory into EasyNAC, or both.
- Click Test connection, then click Save to apply.

Verification:

- Open the SolarWinds Node Details page for a known device and confirm the EasyNAC-driven custom properties are populated

© 2026 InfoExpress, Inc.

- Confirm any pulled SolarWinds nodes appear in EasyNAC's Device Manager with the appropriate location and tag
- Review the integration log to confirm successful periodic queries against SWIS

Note: *The SolarWinds account needs read access on orion.Nodes and orion.NodesCustomProperties at minimum; grant additional entities only as required by your synchronization direction.*

SOPHOS INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Sophos in two ways: against the on-premises Sophos Enterprise Console (SQL Server) and / or against Sophos Central (cloud API). Both can be enabled to support migration to the cloud.

Prerequisites:

- Enterprise Console mode: a Sophos Enterprise Console with MS SQL Server reachable on TCP 1433, a SQL account with read permission to the Sophos database, and the Sophos server firewall opened to TCP 1433. Sophos uses different database schemas (e.g., SOPHOS540 for EP 5.4, SOPHOS521 for EP 5.2) — verify which schema your installation uses.
- Sophos Central mode: a Sophos Central tenant with a Client ID and Client Secret created under System Settings / API Credentials Management.
- In your Sophos Central, go to the General Settings page.
- Click API Credentials Management.
- Click Add Credentials.
- Enter your credential name and choose one of the four roles below for your credential. Click Add.
    - **Recommended minimum role:** Service Principal ReadOnly
- Click 'Copy' to note down the client ID. Also show the client secret.
- Click 'Copy' to note down the client secret.
- Sophos Central mode: outbound internet access from the EasyNAC Appliance to Sophos Cloud

Configuration steps:

- Enterprise Console: in EasyNAC, navigate to Configuration / Integration, select Sophos, enable the integration and select Enterprise Console (SQL Server). Enter the SQL server hostname or IP, database port (1433), database name, and SQL account username and password. Click Test connection, then Save.
- Sophos Central: in Sophos Central, navigate to System Settings / API Credentials Management and create a Client ID for the EasyNAC Appliance.
- Copy the Client ID and Client Secret from Sophos Central.
- In EasyNAC, navigate to Configuration / Integration, select Sophos, enable the integration and select Sophos Central.
- Right-click in the Client ID and choose Paste to enter the Client Secret.
- Click Test Connection to verify; on success click Save. If the test fails, confirm the appliance has internet access to reach Sophos Cloud.

Verification:

© 2026 InfoExpress, Inc.

- Confirm endpoints managed by Sophos appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against Enterprise Console SQL or Sophos Central

Note: *Both modes can be enabled simultaneously to support a phased migration to Sophos Central. For Enterprise Console mode, confirm the actual database schema name (SOPHOS540, SOPHOS521 etc.) before configuring; for Sophos Central mode, the appliance must have outbound internet access to Sophos Cloud endpoints.*

SURE MDM INTEGRATION

Category: Mobile Device Management

EasyNAC integrates with 42Gears SureMDM to identify enrolled mobile and rugged devices and to react to enrollment-state changes that affect access.

Prerequisites:

- A SureMDM cloud or on-premises tenant reachable from the EasyNAC Appliance
- A SureMDM API key with read access to enrolled devices
- The SureMDM tenant URL

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Sure MDM.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SureMDM tenant URL.
- Enter the API key.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm enrolled devices appear in the EasyNAC device list with a managed-device tag
- Unenroll a test device from SureMDM and confirm the tag is removed within the configured interval
- Review the integration log to confirm successful periodic queries against SureMDM

Note: *Use the managed-device tag in the Auto Trust Policy to grant network access only to devices currently enrolled in SureMDM.*

© 2026 InfoExpress, Inc.

SYMANTEC ENDPOINT PROTECTION MANAGER - 14.X

Category: Endpoint Security

EasyNAC integrates with Symantec Endpoint Protection Manager (SEPM) 14.x to learn each endpoint's AV state and to react to compliance signals such as out-of-date definitions or disabled protection.

Prerequisites:

- A SEPM server reachable from the EasyNAC Appliance over HTTPS
- A read-only SEPM administrator account with access to the relevant groups
- The SEPM server URL and account credentials

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Symantec SEPM.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SEPM server URL.
- Enter the API account username and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by SEPM appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against SEPM

Note: *Use a read-only administrator account so credential rotation and audit are tracked independently of interactive administrators.*

TENABLE INTEGRATION

Category: Vulnerability Management

EasyNAC integrates with Tenable (Tenable.io / Tenable.sc, formerly Nessus / SecurityCenter) to consume vulnerability scan results and apply NAC policy based on host vulnerability state. Vulnerable hosts can be tagged automatically and routed through restricted ACLs until remediated.

Prerequisites:

- A Tenable.io or Tenable.sc deployment reachable from the EasyNAC Appliance
- Tenable API access keys (Access Key and Secret Key) with read permission for the relevant scans and assets
- The Tenable endpoint URL

© 2026 InfoExpress, Inc.

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Tenable; enable the integration.
- Enter the Tenable endpoint URL.
- Enter the Access Key and Secret Key.
- Configure the asset import scope (all scans, named scans, or specific tag-based filters in Tenable).
- Map Tenable severity levels to EasyNAC tags or actions (for example, Critical findings → High-Risk-Event role; High findings → non-compliant role).
- Configure the polling interval, then click Test connection and Save.

Verification:

- Confirm scanned hosts appear in EasyNAC with vulnerability-derived tags
- Re-scan a previously vulnerable host that has now been remediated and confirm the tag is removed at the next polling cycle
- Review the Auto Trust Policy to confirm Tenable-driven tags lead to the intended access outcomes

Note: *Restrict the API user to read-only scopes on the relevant scans and assets. Map Tenable severity levels to roles deliberately — auto-quarantining on every High finding can be operationally disruptive.*

TREND MICRO INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Trend Micro in two ways: against the on-premises Apex One / OfficeScan Enterprise Console (SQL Server) and / or against Apex Central / Vision One cloud. Both can be enabled to support migration to the cloud.

Prerequisites:

- On-premises Enterprise Console mode: an Apex One server with MS SQL Server reachable on TCP 1433, a SQL account with read permission to the Apex One database, and the Apex One server firewall opened to TCP 1433 (if Apex One is not yet on SQL, Trend Micro provides a migration tool — see success.trendmicro.com/solution/1059973)
- Apex Central mode: an Apex Central tenant with an Application ID and API Key generated under Automation / API Access Settings; the API Key role must be Endpoint Administrator
- Vision One mode: a Vision One tenant with the regional API URL (https://api.<region>.xdr.trendmicro.com — see automation.trendmicro.com/xdr/Guides/Regional-Domains) and an API Key created against Endpoint Administrator role

Configuration steps:

- Enterprise Console: in EasyNAC, navigate to Configuration / Integration, select Trend Micro, enable the integration and select On-premises. Enter SQL hostname or IP, database port (1433), database name and the SQL account username and password. Click Test connection, then Save.

- Apex Central: in Apex Central, navigate to Automation / API Access Settings and generate an Application ID and API Key.
- In EasyNAC, select Trend Micro / APEX Central, enter the Apex Central host or IP, then paste the Application ID and API Key.
- Vision One: select the Vision One checkbox, enter the regional API URL (e.g., https://api.sg.xdr.trendmicro.com) and the API Key.
- Optionally enable Use the hostname for finding and flagging devices and enable Show Query Result Data to inspect the test response.
- Click Test connection, then click Save to apply.

Verification:

- Confirm endpoints managed by Trend Micro appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date, AV-offline) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the Trend Micro server

Note: *When using Apex Central there may be fewer monitoring options than the on-premises mode, due to Trend Micro API limitations. The API Key role must be Endpoint Administrator. For Vision One, the regional API URL changes by region — confirm yours against Trend Micro's Regional Domains documentation.*

TRELLIX EPOLICY ORCHESTRATOR INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Trellix ePolicy Orchestrator (ePO, formerly McAfee ePO) by querying its SQL database to learn each endpoint's protection state.

Prerequisites:

- An ePO server with MS SQL Server reachable from the EasyNAC Appliance on TCP 1433
- A SQL account with read permission to the ePO database
- The ePO server firewall opened to allow the EasyNAC Appliance to reach SQL Server on port 1433

Configuration steps:

- In EasyNAC, navigate to Configuration / Integration and select Trellix ePolicy Orchestrator.
- Enable the integration by selecting the Enable Integration checkbox.
- Enter the SQL server hostname or IP, database port (1433) and database name.
- Enter the SQL account username and password.
- Click Test connection to verify connectivity.
- Review the default query interval and tagging conditions, then click Save.

Verification:

- Confirm endpoints managed by ePO appear in the EasyNAC device list with a managed-device tag

- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the ePO database

Note: *Confirm that MS SQL Server on the ePO server is enabled for TCP/IP on port 1433 and that the ePO server firewall allows the appliance to reach it. The SQL account should be granted read access to the ePO database only.*

WEBROOT INTEGRATION

Category: Endpoint Security

EasyNAC integrates with Webroot Business Endpoint Protection via the Unity API to learn each endpoint's protection state.

Prerequisites:

- A Webroot Console tenant reachable from the EasyNAC Appliance
- Unity API credentials (Client ID and Client Secret) created under Settings / Unity API Access / New (the Event notification API is not used)
- A Webroot Management Console username and password (used for API authentication) plus the site Key Code from Settings / Downloads — do NOT use the Parent Keycode (the connection will succeed but no results will be returned)

Configuration steps:

- In Webroot Console, navigate to Settings / Unity API Access / New and create a new client credential; copy the Client ID and Client Secret.
- In EasyNAC, navigate to Configuration / Integration and select Webroot; enable the integration.
- Paste the Client ID and Client Secret.
- Enter Access URL: https://unityapi.webrootcloudav.com
- Enter the Webroot Management Console username and password, plus the site Key Code (from Settings / Downloads — not the Parent Keycode).
- Click Test connection to verify connectivity, then click Save.

Verification:

- Confirm endpoints managed by Webroot appear in the EasyNAC device list with a managed-device tag
- Disable AV on a test endpoint and confirm the corresponding tag (e.g., AV-off, AV-out-of-date) is applied within the configured interval
- Review the integration log to confirm successful periodic queries against the Unity API

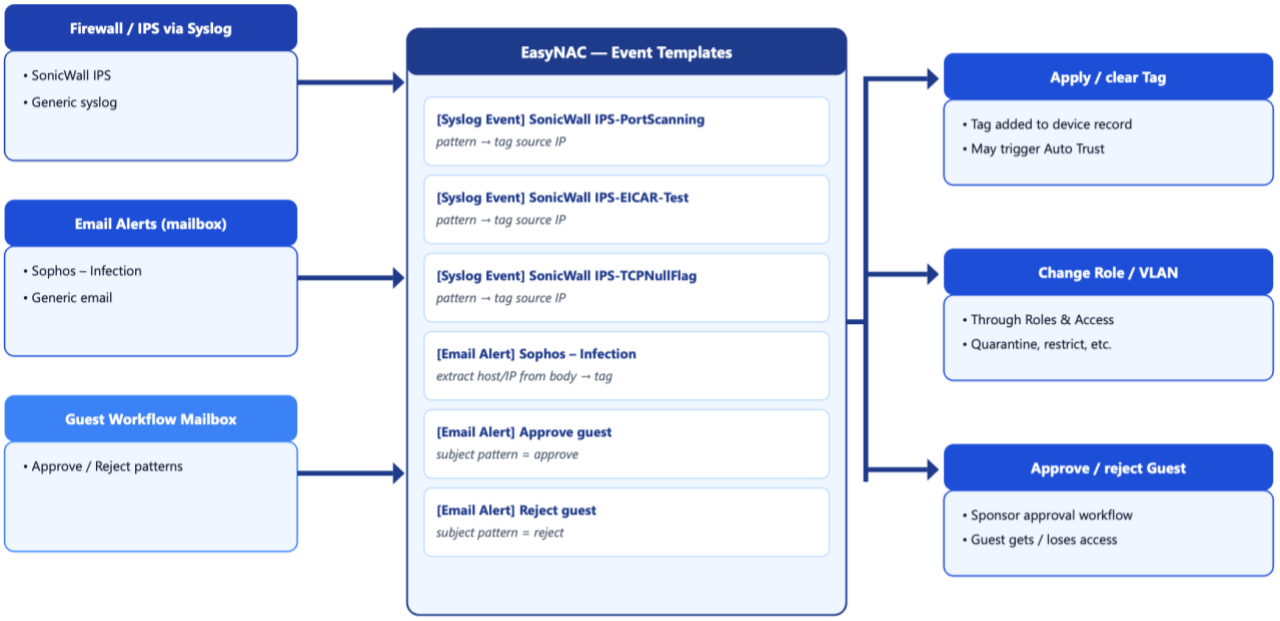
Note: *Use the site Key Code (Settings / Downloads) — the Parent Keycode is accepted by the API but returns no results, which can mask configuration mistakes. The Event notification API is not consumed by EasyNAC.*

© 2026 InfoExpress, Inc.

ORCHESTRATION EVENTS

Orchestration Events define how EasyNAC interacts with external systems to automate response and enforcement actions. These events are triggered based on specific conditions such as device state changes, compliance status, or detected security events.

Through Orchestration Events, EasyNAC can integrate with third-party systems (e.g. SIEM, firewalls, endpoint security platforms) to initiate automated actions such as restricting access, updating policies, or generating alerts. This enables a coordinated and real-time security response across the network environment.



ORCHESTRATION WITH SYSLOG

Firewalls, APT solutions, and other security solutions designed to monitor devices and network traffic can send event-based alerts for administrative action. The EasyNAC Appliance can receive event-based syslog messages from a wide range of security devices and take immediate action when necessary. If the EasyNAC Appliance receives an alert that a device has malware or is misbehaving, it can restrict the device immediately.

Any solution that can send event-based syslog messages can be configured to work with the EasyNAC Appliance.

- In the EasyNAC management interface, navigate to Configuration → Integration
- **Click "Syslog** - Orchestration"

On the Syslog – Orchestration page, events can be enabled and configured. The Event Source IP field specifies the IP address of the security appliance that sends syslog messages to the EasyNAC Appliance. Multiple IP addresses or IP ranges can be entered.

© 2026 InfoExpress, Inc.

SYSLOG EVENT CREATION

The EasyNAC Appliance can work with any solution (Firewall, APT, IPS, SIEM, etc.) that can send event-driven syslog messages. To create new events, follow these steps:

- In the EasyNAC management interface, navigate to Policies → Orchestration Events
- Click "New Event"
- Select "Device event from syslog"

This dialog defines the conditions under which a syslog message triggers a device event. When the specified search pattern matches an incoming syslog message, the event is triggered for the corresponding IP address. Each event requires configuration of four sections:

- **Event Name**
  - Assign a descriptive name that identifies the source device and the condition being monitored.
- **Search syslog for**
  - The EasyNAC Appliance searches incoming syslog messages for the keywords specified here. For example: "ID=attack detected". Regular expressions are supported; however, do not include "/" at the beginning and the end.
- **Type of Information Extracted**
  - Specify whether the EasyNAC Appliance should extract an IP address or hostname from the syslog message.
  - If using IP: The EasyNAC Appliance extracts the IP address of the offending endpoint using the predefined macro: (%IP) for the IP address's position. For example, we will specify: "SRC=(%IP)" if the IP value can be found after SRC:=..."
  - If using Hostname: The EasyNAC Appliance extracts the hostname of the offending endpoint based on a keyword. For example, hostname:
- **Tag the Device as**
  - Select the tag to assign to the offending device when the event is triggered. The Device Classification policy can then automatically quarantine the tagged device.
  - Custom tags names can be created under Configuration → General Settings → Names Used by Policies

© 2026 InfoExpress, Inc.

ORCHESTRATION EMAIL ALERT

The EasyNAC Appliance can receive email messages from a wide range of security devices and take immediate action when necessary. If the EasyNAC Appliance receives an email alert that a device has malware or is misbehaving, it can restrict the device immediately.

Any solution that can send email messages can be configured to work with the EasyNAC Appliance.

- Verify that an inbound email server has been configured
- In the EasyNAC management interface, navigate to Configuration → Integration
- **Click "Email** - Orchestration"
- On the Email – Orchestration page, events can be enabled and configured.
- To limit which email addresses are allowed to send an email alert to the EasyNAC Appliance, specify the approved emails in the Sender's Address section. When blank all addresses are allowed.
- The Query interval specifies how often the EasyNAC Appliance checks the mail server for new email alerts.

EMAIL EVENT CREATION

The EasyNAC Appliance can work with any solution (Firewall, APT, IPS, SIEM, etc.) that can send email messages. To create new events, follow these steps:

- In the EasyNAC management interface, navigate to Policies → Orchestration Events
- Click "New Event"
- Select "Device event from an email alert"

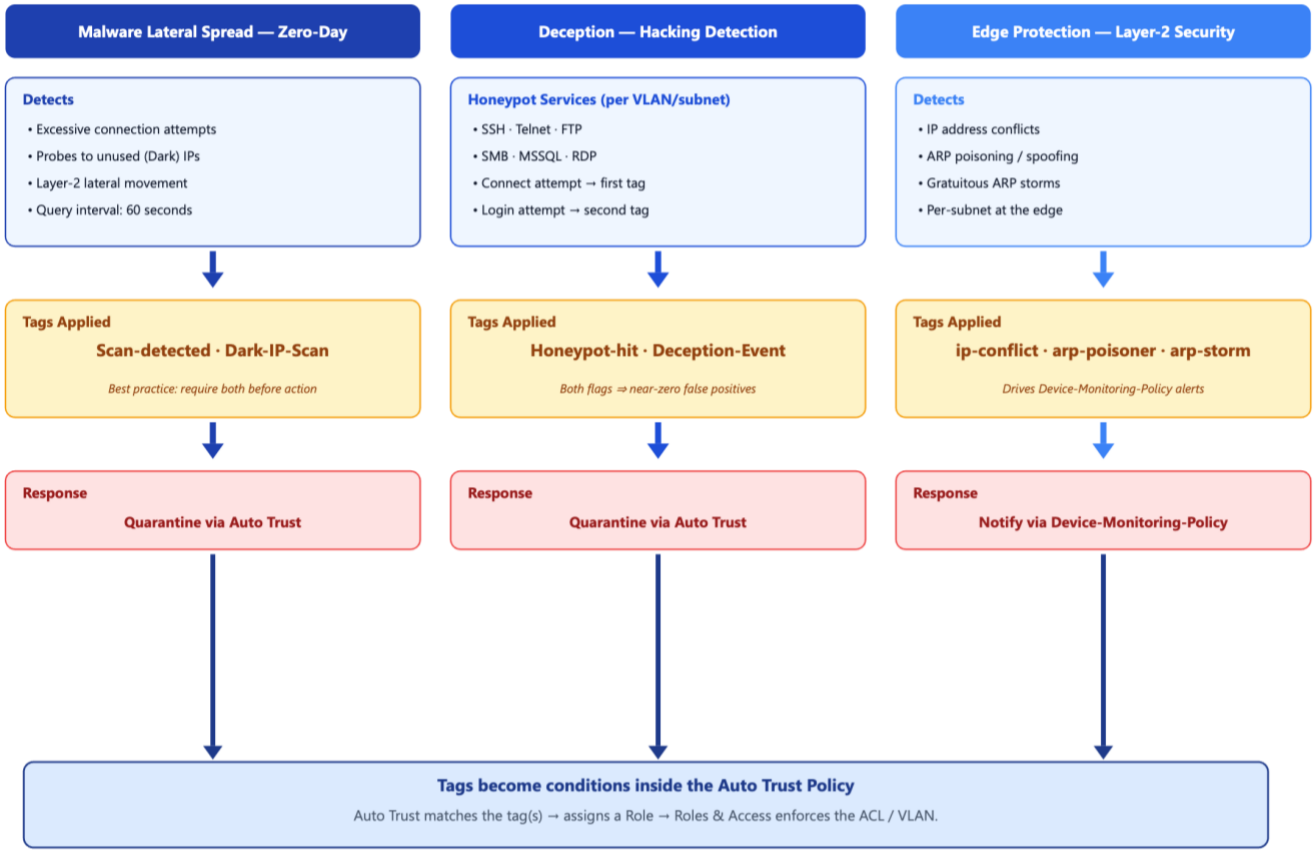
This dialog defines the conditions under which an email alert triggers a device event. When the specified search pattern matches an incoming email, the event is triggered for the corresponding IP address or hostname. Each event requires configuration of four sections:

- **Event Name**
  - Assign a descriptive name that identifies the email source and the alert condition.
- **Search email alerts for**
  - The EasyNAC Appliance searches incoming email messages for the keywords specified here. For example: "Virus/Spyware". Regular expressions are supported; however, do not include "/" at the beginning and the end.
- **Type of Information Extracted**
  - Specify whether the EasyNAC Appliance should extract an IP address or hostname from the email message.
  - If using Hostname: The EasyNAC Appliance extracts the hostname based on the specified keyword. For example, if Machine: is specified as the keyword, any name following it will be assumed as the hostname.
  - If using IP: The EasyNAC Appliance extracts the IP address of the offending endpoint using the predefined macro: (%IP) for the IP address's position. For example, we will specify: "SRC=(%IP)" if the IP value follows after SRC:=.
- **Tag the Device as**
  - Select the tag to assign to the offending device when the event is triggered. The Device Classification policy can then automatically quarantine the tagged device.

© 2026 InfoExpress, Inc.

- Custom tags names can be created under Configuration → General Settings → Names Used by Policies

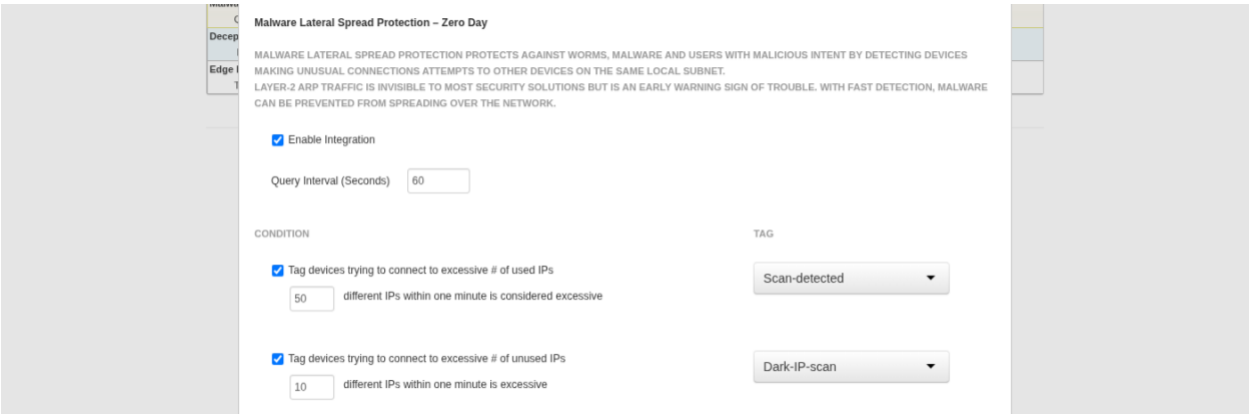
ADVANCED SECURITY



MALWARE LATERAL SPREAD PROTECTION - ZERO-DAY

With its Layer-2 visibility, EasyNAC can detect devices making 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 tries to connect to Dark IPs that are not active on the network, this is suspicious behavior. This behavior is indicative of a network scan being performed or malware trying to probe the network in an attempt to spread. EasyNAC can detect this behavior and immediately quarantine this device so it can't spread malware laterally on the network.

- In the EasyNAC management interface, navigate to Policies → Advanced Security
- **Click "Malware Lateral Spread Protection** – Zero-Day"



When enabled, any device that attempts connections to an excessive number of hosts is tagged as "Scan-detected". Devices attempting to connect to unused IP addresses are tagged as "Dark-IP-Scan"

POLICY-BASED RESPONSE

When the "Scan-detected" and "Dark-IP-Scan" tags are assigned to a device, the EasyNAC Appliance can automatically quarantine the device through the Auto Trust Policy.

- In the EasyNAC management interface, navigate to Policies → Auto Trust
- Add a rule to act when a device is tagged "Scan-detected" and "Dark-IP-Scan"
- Drag the new rule near the top of the list to give it higher priority over other conditions.

Tip: *By specifying "All tags" both the "Scan-detected" tag and "Dark-IP-Scan" tag needs to be present. Requiring both tags to be present can reduce false positives.*

CLEARING ZERO-DAY EVENTS

After a device has been restricted, the event must be cleared before the device can regain network access.

- In the EasyNAC management interface, navigate to Visibility → Alerts and Notifications
- Click "Devices with Events"
- Select the affected device(s), choose the "Clear event" option and Apply

HANDLING EXCEPTIONS

Some devices may require exceptions from network monitoring. To exclude devices from zero-day behavioral detection, apply the following tags to the allowed devices as "arp-scan-ignoring" and "darkip-scan-ignoring". These tags can be set using the Device Manager or Device with Events report.

- In the EasyNAC management interface, navigate to Visibility → Alerts and Notifications
- Click "Devices with Events"
- Select the device(s) to exempt, choose the "Ignore Zero-Day Behavioral Detection" option and Apply

Note: *By default, devices tagged as Network Infrastructure are exempt from scanning checks.*

DECEPTION – HACKING DETECTION

With its Layer-2 protection, the EasyNAC solution will host fake services such as SSH, Telnet, FTP, SMB, MSSQL and RDP on every VLAN or subnet it's protecting, creating a distributed honeypot network. Since these services serve no legitimate business purpose, any user or bot that attempts to log in to these fake services is 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.

- In the EasyNAC management interface, navigate to Policies → Advanced Security

- **Click "Deception** – Hacking Detection"

The "Honeypot-hit" tag will be assigned to any device that attempts to connect to any of the fake services. To minimize false positives, exclude IP addresses of authorized network scanners.

The "Deception-Event" tag is assigned after the user attempts to log in to the fake services. For near-zero false positives, it's best practice to quarantine a device only when both flags are present.

POLICY-BASED RESPONSE

When the "Honeypot-hit" tag and "Deception-Event" tags are assigned to a device, the EasyNAC Appliance can automatically quarantine the device through the Auto Trust Policy.

- In the EasyNAC management interface, navigate to Policies → Auto Trust
- Add a rule to act when a device is tagged "Honeypot-hit" and "Deception-Event"

CREDENTIALS USED

The Deception feature will record the credentials used in the detected hacking attempt. To view:

- Click the MAC address of the restricted device
- Click the Honeypot Tab

EDGE PROTECTION – LAYER-2 SECURITY

With its Layer-2 visibility, the EasyNAC solution can help detect configuration issues (IP conflicts and ARP storms) or security risks (ARP spoofing) occurring at the edge of the network.

POLICY-BASED NOTIFICATIONS

When an "ip-conflict", "arp-poisoner" or "arp-storm" tag is assigned to a device, the EasyNAC solution can send notifications based on Device Monitoring Policy.

- In the EasyNAC management interface, navigate to Policies → Monitoring → Device-Monitoring-Policy
- Add Rule to send alert when a device is tagged "ip-conflict", "arp-poisoner" or "arp-storm"

© 2026 InfoExpress, Inc.

AGENT SUPPORT

The EasyNAC Appliance is fundamentally an agentless solution. However, optional agent licenses enable more in-depth compliance checks, automatic remediation, and additional capabilities. Agents are required only for VPN protection. When using agents, you can also consider a hybrid deployment model, where laptops needing stronger security checks use the agents, while desktops use the agentless approach. The table below summarizes the differences in these approaches.

	EasyNAC - Agent	EasyNAC – Agentless
Detection	Agent would detect changes within 10 seconds	Compliance check with integration module depends on the re-check interval
Supported OS	• Microsoft Windows • Apple MacOS • Linux	The Operating Systems supported by Integration solution(s)
Compliance checks	Compliance check can be customized to Include but not limited to the followings: • Running Process • Registry values • Files and locations • Ini files and contents • Machine names and OS check • Authentication	Agentless solution – Integrations with AD, third-party AV, Patch, and WMI
End-user compliance communication	Pop-up Message	HTTP Redirection
Real-time Wi-Fi adapters control	When connected to any wired network that has connectivity to EasyNAC (i.e., Corporate Network). The wireless network adapter can be disabled automatically. It is re-enabled once a wired NIC is disconnected	N/A Can use Windows Connection Manager as a substitute
Automatic Remediation	When a compliance check fails, a remediation action can be kicked in. It includes running scripts or binary in the host that has the agent installed. With or without administrative rights.	N/A

WORKING WITH AGENTS

EasyNAC Appliances include default agents and compliance policies that serve as a starting point for testing or as a baseline for building custom compliance policies.

By default, the Auto Trust Policy grants full access to devices that pass an agent audit and assigns a failed-agent-audit role to devices that fail. Because policy order determines evaluation priority, some environments may require to drag and drop these policies up for higher priority.

- In the EasyNAC management interface, navigate to Policies → Auto Trust

© 2026 InfoExpress, Inc.

Devices assigned the "failed-agent-audit" role receive the "restrict-agent" ACL, which by default blocks all traffic except DNS, DHCP, and agent communication over TCP port 11698.

It is recommended to edit the default "restrict-agent" ACL to allow access to approved remediation resources, such as the antivirus server, patch server, and any other systems required for remediation.

HOSTING AGENTS

EasyNAC Appliances include default agents that meet most deployment requirements. To make these agents available for download:

- In the EasyNAC management interface, navigate to Configuration → General Settings → EasyNAC Agents
- Adjust the Captive Portal settings to allow agent downloads:

To host agents on the appliance, use the Remediation IP address. Once the above settings are configured, determine when the agent installers should be presented to end users.

The timing of agent installer display can be configured based on requirements. This is particularly useful in environments where guest, consultant, or BYOD devices must install agents to obtain network access.

The appliance automatically presents only the agent type appropriate for the detected operating system. For example, a macOS user sees only the macOS agent. To display all available agent options, select "Show all configured agent links".

INSTALLING AGENTS

EasyNAC Compliance agents (Also known as CyberGateKeeper agents) are designed for silent installation. Once launched, the installer completes in the background without requiring any configuration options or system reboots. The Windows installers are approximately 8–10 MB in size. The MAC OSX agent installer is approximately 4 MB. These sizes make it quick to download and install. Once running, agents consume approximately 4–6 MB of RAM and utilize roughly 1% CPU every 30 seconds.

Most organizations deploy the agent automatically using a software deployment tool or Active Directory Group Policy with a computer startup script. Contact InfoExpress support to obtain a sample deployment script.

For manual deployment, local administrative rights are required on the target device.

- Right-click the installer file and select "Open With Windows Installer," or double-click the installer to begin.
- When prompted, click "Yes." Allow 30–60 seconds for the installation to complete in the background.
- Upon completion, an icon appears in the system tray. Double-clicking this icon opens the agent viewer, which displays the current compliance status.

ON-DEMAND AGENTS (RECOMMENDED FOR CONSULTANTS)

© 2026 InfoExpress, Inc.

Standard EasyNAC Compliance agents are designed for managed devices and require administrative rights to install. Once installed, the agent runs in the background, providing transparent and continuous compliance checks. However, it may be desirable to perform similar compliance checks on unmanaged computers used by consultants. For this requirement, you can the on-demand agents.

The key difference with the on-demand agent is that it does not require administrative rights, because it is not permanently installed. The on-demand agent is a 2–3 MB executable that runs in memory until the agent viewer is closed. Once the agent viewer is closed, the agent checks are stopped, and the consultant will need to run the executable again if she needs to reconnect to the network. By default, a device passing audit will continue to be passing audit for 5 minutes, after this agent has been closed.

Requirements / Limitations:

- Supported on 64-bit Windows Operating Systems (Windows 10 and later)
- Supports Windows Security Center and Windows Update plug-ins
- Nic Manager Plug-in or any plug-in requiring admin rights is not supported
- Automatic Remediation is not supported

AGENT COMPLIANCE POLICIES

EasyNAC virtual appliances ship with default agent compliance policies preloaded on the appliance. These default policies include checks for common antivirus solutions:

- Anti-Virus Installed
- Anti-Virus Running
- AV Up-to-date
- Real-time scanning enabled
- Windows Updated Enabled
- Recent Microsoft updates

While these policies provide a solid starting point, it is recommended that each organization customize them to align with specific security requirements. For example, if your organization's endpoint security is TrendMicro, then it may only be necessary to check for this brand.

To customize policies, install the CyberGateKeeper Policy Manager (CGPM). Contact InfoExpress support or your authorized partner to obtain the CGPM installer and the EasyNAC Appliance Default Settings installer.

Setup procedure:

- Install the CGPM (CyberGateKeeper Policy Manager) software on a 64-bit Windows machine.
- Keep Policy Manager closed (do not launch it yet).
- Run the EasyNAC Appliance Default Settings installer to seed the appliance with the default policies and synchronize them with the agents.

Note: *If using the default agents, run the EasyNAC Appliance Default Settings installer to ensure proper synchronization between the agents and Policy Manager.*

© 2026 InfoExpress, Inc.

POLICY MANAGER

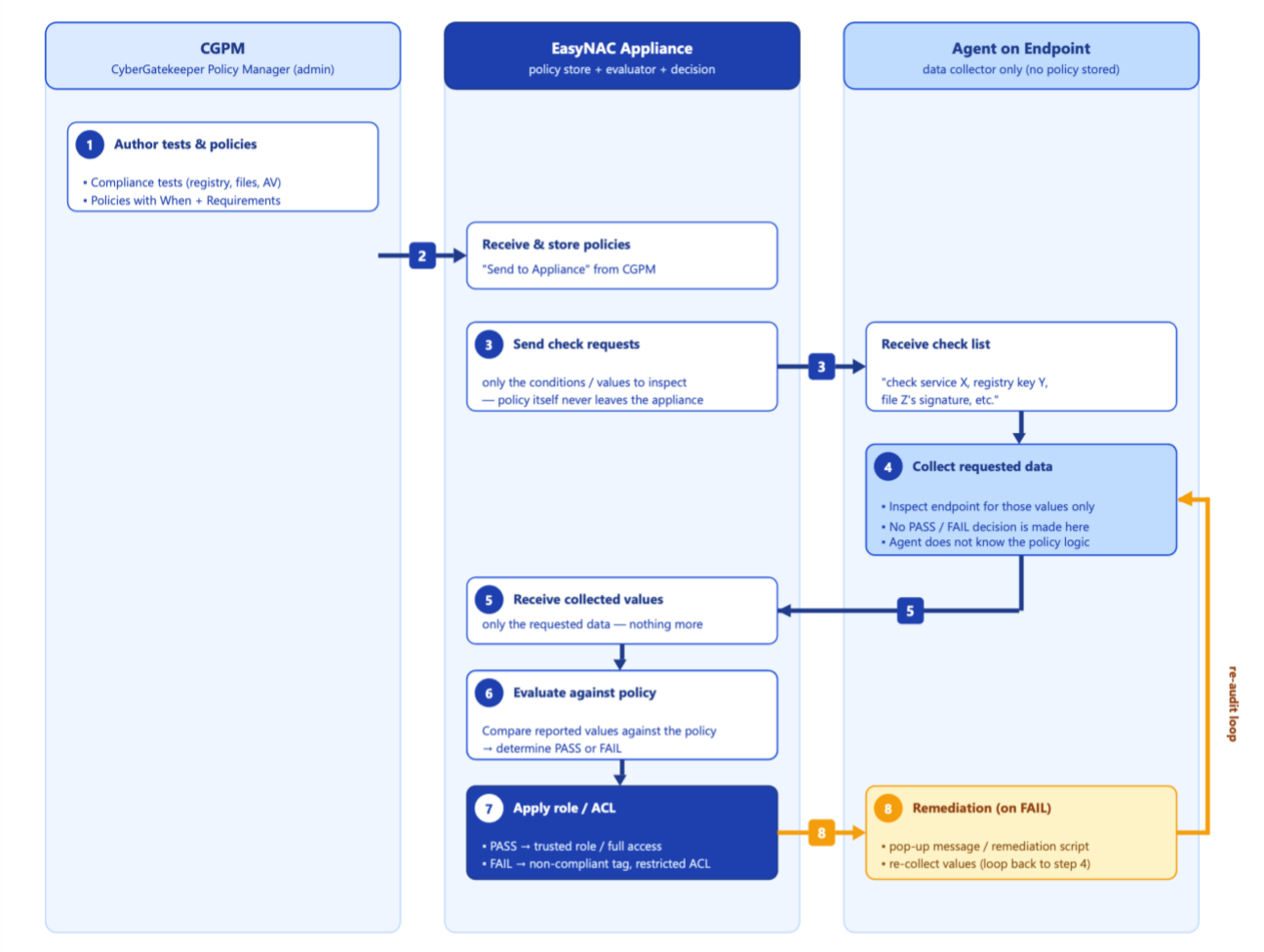
The Policy Manager (CGPM — CyberGateKeeper Policy Manager) is a Windows-based application that can be installed on any 64-bit Microsoft Windows operating system.

The Policy Manager application is used for:

- Creating compliance tests
- Creating compliance policies
- Uploading Compliance Policies to the EasyNAC Appliance
- Building agents for different operating systems

The following sections provide a quick-start guide and best practices for using the Policy Manager to create agent compliance checks.

Tip: *For comprehensive details, refer to the CyberGateKeeper Policy Manager Reference Manual.*



POLICIES

The **Policies** creates and edits audit policies. Audit policies enable administrators to define which applications, configurations, and system states are required for corporate network access.

Each policy consists of a When Section and a Requirements Section. The When Section defines which remote systems the policy applies to, and each Requirements Section can include its own remediation instructions.

If this policy's When Section does not match the audit information from the remote system, the next policy will be checked. If the When Section matches the audit information from the remote system, the Requirements Section is checked to see whether the remote system should be given access to the corporate network.

When Section structure:

The When Section contains conditions consisting of **WHEN** or **WHENNOT** commands followed by test conditions. The **WHEN** command passes if the test condition is true. The **WHENNOT** command passes if the test condition is not true. All of the When Conditions in the policy must match the audit information for the policy to be valid (All conditions are ANDed).

© 2026 InfoExpress, Inc.

Ordered policies use a numbered prefix in their names and are evaluated in alphanumerical order. The order in which policies will be evaluated can be seen in the list of policies on CGPM. An agent matches only one ordered policy at a time. Once a match is found in the When Section, the policy is taken by this agent and no other policies are checked.

POLICIES BEST PRACTICES

- As a best practice, use a numbered prefix when naming policies. This approach allows easy prioritization by changing the prefix number.

  For example, an ordered policy named **80-Windows.def** is evaluated before another policy named **90-Windows.def** because the system would evaluate the policies in alphanumeric order.

- Policies with more specific When Section conditions should be evaluated first. Adjust the policy name prefix to ensure the correct evaluation order.

  For example, if your **90-Windows.def** has two When conditions defined (When Any Windows and When in IP range 192.168.0.0/24) and your **80-Windows.def** has 1 When condition defined (When Any Windows).

  In this case, all your agents would be getting the **80-Windows.def** because it has a more generic When condition (only 1).

  The correct way to do it, is to rename the **90-Windows.def** to, for example, **70-Windows.def**. This would make the policy list higher alphanumerically and hence be evaluated first.

- For environments with both 32-bit and 64-bit Windows operating systems, create separate policy sets for each architecture to ensure accurate compliance checks.

- Policies are stored in the Policy Manager installation folder. It is recommended to maintain a backup of the entire Policy Manager folder located at C:\Program Files\InfoExpress\CyberGateKeeper Policy Manager.

REQUIREMENTS TO PASS A POLICY

The Requirements Section contains requirements consisting of **REQUIRE**, **PROHIBIT**, **DESIRE** or **NOTDESIRE** commands followed by test conditions.

- The **REQUIRE** command is used to ensure certain conditions are present and passes if the test condition(s) are true. If any REQUIRE command is not satisfied, the agent fails the policy and the overall audit.
- The **PROHIBIT** command is used to prevent certain conditions and passes if the test condition is not true. If any PROHIBIT command is not satisfied, the agent fails the policy and the overall audit.
- The **DESIRE** command is used to check if certain conditions are present. If the test condition(s) are true, it would pass the policy. However, even in the case the DESIRE command is not satisfied, the overall audit still passes. This is useful when compliance data is needed for reporting purposes, but quarantine action is not required.
- The **NOTDESIRE** command is used to check if certain conditions are not present and passes if the test condition is not true. However, even in the case the NOTDESIRE command fails, the audit still passes. This is helpful if compliance information is desired, but no quarantine action should be performed.

REQUIREMENTS PRIORITY

All tests added to a policy constitute its requirements. Requirements are evaluated sequentially from top to bottom.

© 2026 InfoExpress, Inc.

For example, if a policy lists DESIRE "Windows Automatic Updates Enabled" first, followed by REQUIRE Anti-Virus Installed and REQUIRE Anti-Virus Running, the DESIRE check is evaluated first, then each REQUIRE in order.

When a REQUIRE or PROHIBIT test fails, the audit is immediately marked as FAIL, and any remaining tests below are not evaluated.

However, because DESIRE and NOTDESIRE commands are informational, the audit continues even if these tests fail, and the next requirement is still evaluated.

For example, if REQUIRE Antivirus Running fails, the agent stops evaluation at that point. Subsequent tests such as REQUIRE Virus Definitions Current and REQUIRE Real-Time Scanning Enabled are not checked.

REQUIREMENT BEST PRACTICES

It is recommended to place the DESIRE and NOTDESIRE commands at the top of the requirements list by promoting them with the up-arrow control in the requirements list. This ensures all informational tests are evaluated before REQUIRE and PROHIBIT commands.

- To change a command type, right-click on the command and select the desired type (for example, changing from DESIRE to REQUIRE).
- Review the prerequisites for each test and arrange the test order accordingly.

For example, a test for Antivirus Running should precede a test for Antivirus Signature Age, because the antivirus program cannot update its signatures if it is not running.

REMEDIATION

When an agent fails a policy requirement, the administrator can run a remediation action, display a remediation message to the user, or both.

- Remediation actions can be configured to automatically bring the device back into compliance, enabling it to pass subsequent audit checks.
- The remediation message displays a dialog box with information or instructions to the user.
- A unique remediation action and pop-up message can be configured for each requirement within a policy.

To configure remediation, select the corresponding test in the Requirements section and click Edit. The Edit Remediation Option dialog opens, where the remediation message, the remediation link, and the script execution behavior can all be configured (each is described in the sub-sections below).

POP-UP MESSAGES

- In the Edit Remediation Option dialog, enter an appropriate remediation message in the Remediation Message field. For example, "No authorized antivirus software is found".
- Remediation messages are not displayed by default. To show a message when a requirement fails, select the "Pop up Message on User's System" checkbox in the same dialog.
- A URL can be embedded in the remediation message to direct the user to additional resources, or entered in the Remediation Link field.

© 2026 InfoExpress, Inc.

REMEDIATION ACTIONS

- In the Edit Remediation Option dialog, the remediation action must be entered under the Remediation Link field. Enter either a URL tag or a UNC (Universal Naming Convention) tag — the tag points to the file that runs on the end-user system when the endpoint fails the requirement.
- The file can be any executable file type, such as executables (.exe) or Windows scripts (.vbs, .bat, .cmd). If the remediation script or executable requires parameters (arguments) they can be entered under "Command Arguments". Multiple parameters should be separated by spaces.
- For example:
    - URL Tag: http://192.168.253.128/fix/ResShieldOn.vbs
    - Even when a remediation script URL is defined in the Remediation Link, the user may still need to click the link to download and run the script manually.

AUTO-REMEDIATION

To improve the end-user experience, configure the remediation action to run automatically without user intervention. The privilege level at which the remediation script runs is also configured in the Edit Remediation Option dialog:

- To run the remediation script automatically with the currently logged-on user's privileges, select the **Run remediation for Desktop Agent**.
- To allow the remediation script to run automatically but with local administrative rights, select both the **Run remediation for Desktop Agent** and **Run Remediation with Admin Rights**.

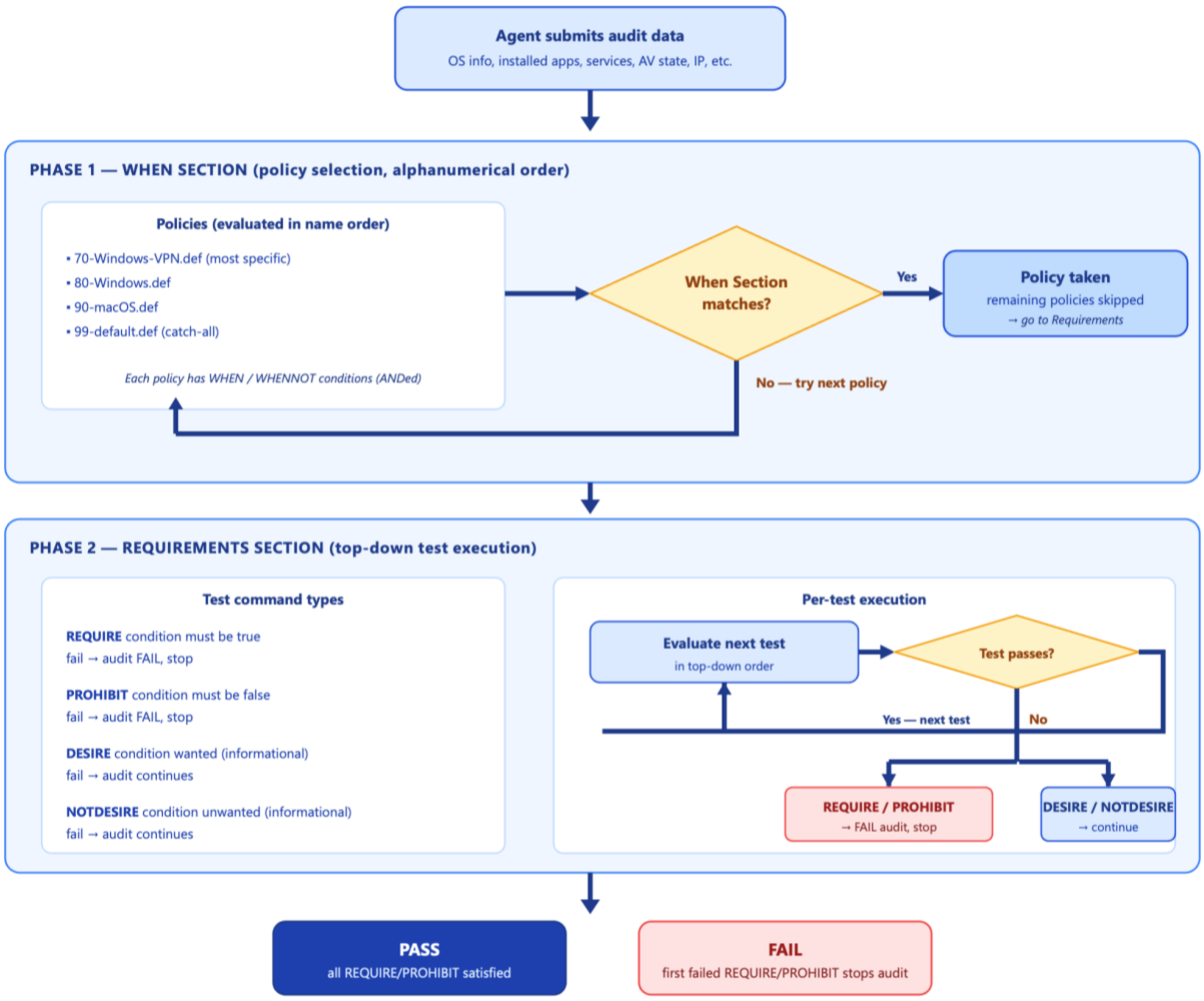
Note: *Only the Persistence Windows Agent and macOS Agent support remediation actions.*

REMEDIATION BEST PRACTICES

- Configure the remediation action using a URL instead of a UNC path. The agent runs with the local system account on the endpoint, so network resources may lack sufficient privileges. Host remediation scripts on the EasyNAC Appliance or Central Visibility Manager.
- Configure the remediation action to run without user intervention.

  For example, running a batch file (.bat) as a remediation script is supported but it might trigger a command prompt to be shown on the user's endpoint. It would look malicious to users. However, when running it with a VB Script, it can do the same remediation action but can be configured in the script to hide any user feedback (more transparent user experience).
- Configure the appropriate privilege level for the remediation script based on its requirements. For example, if the script requires administrative privilege to restart a service, running it with user-level privileges alone may fail.

© 2026 InfoExpress, Inc.



USING ACTIVE DIRECTORY USER GROUP IN AUTO TRUST POLICY

The Active Directory User Group of the currently logged-on user can be used as a condition in the Auto Trust Policy, enabling role-based network access.

PREREQUISITES

- DNS server and Domain Settings for the EasyNAC Appliance
- Configure Active Directory User Group
- EasyNAC to be joined as a Domain Member
- Additional “Authentication Plugin” in CyberGateKeeper Agent

DNS SERVER AND DOMAIN SETTINGS FOR THE EASYNAC APPLIANCE

Configure the DNS server, hostname, and domain name of the EasyNAC Appliance so that Active Directory can resolve the appliance. The DNS server should point to the Active Directory Server. The EasyNAC Appliance must be joined as a Domain Member.

© 2026 InfoExpress, Inc.

In the example above, the EasyNAC's hostname is configured as cgx-access and the Domain Name of the Active Directory is configured as "easynac.demo". The DNS server is pointing to the Active Directory Server's IP address.

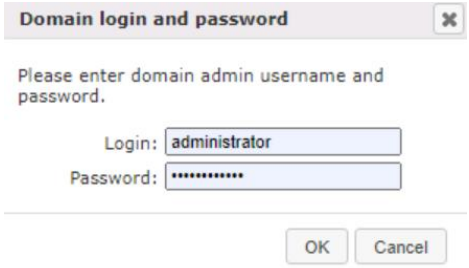
CONFIGURE ACTIVE DIRECTORY USER GROUP

To configure Active Directory User Group integration, complete the following steps:

- The following example uses a User Group named "Tech" to be used in the EasyNAC Appliance. Add Active Directory Users to the corresponding Active Directory Group.
- Add the Active Directory Group name that the EasyNAC Appliance should recognize.
    1. In the EasyNAC management interface, navigate to Configuration → General Settings
    2. Click the "Name used by Policy" of Configuration Settings
    3. Add the Active Directory User Group to be used as follow
    4. Click Save to confirm

JOINING THE EASYNAC APPLIANCE TO ACTIVE DIRECTORY

- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- Click Configure under the "Active Directory Domain Settings" and configure the Domain NETBIOS name and Doman Controller.
- Click Join Domain and type the Domain Administrator credential into the dialog box.



- Click OK to confirm.

CYBERGATEKEEPER AGENT AUTHENTICATION PLUGIN

When building the CyberGateKeeper agent installer in Policy Manager, include the "Authentication Plugin" before building the agent installer.

To confirm the Authentication Plugin has been included, open the CyberGateKeeper agent GUI and click Help → About to ensure the AuthPlugin has been added.

ADD THE USER GROUP AS A CONDITION IN AUTO TRUST POLICY

To create an Auto Trust Policy rule using the "User Group" added as a condition. Select the User Group that you would like to check and assign it to the corresponding device role.

The Auto Trust Policy rules demonstrate how User Groups can assign different network roles based on the currently logged-on user.

TROUBLESHOOTING AGENTS

INSTALLATION ISSUES

Agent installation on Windows PCs may encounter issues specific to the target environment. The following command-line options assist with troubleshooting installation problems.

From the admin command prompt type:

cgamsi32.exe or cgamsi64.exe and use any of the options below:

-debug	Generates installation log at %tmp%\cgainstall.log. *You can send this log to support when requiring assistance for installation issues*
-log	Enables agent debug logging in agent install dir [filenames=IEXCGAxxxxx.log]
-manual	Interactive install. Shows install window and progress.

For Example:

```
> cgamsi64.exe –manual –debug
```

This will start a manual installation with install progress & enable installation debug logging file at %tmp%\cgainstall.log

After installation, verify the agent service is running:

```
> tasklist | find /i "cga"
```

Note: *For problems installing Linux agents, please contact support for the Linux agent install guide.*

CONNECTION ISSUES

Outbound Ports use by CyberGateKeeper Agent:

— TCP 11698: Agent Connections to EasyNAC Appliance

— TCP 11697: Agent (NIC Manager) to EasyNAC Appliance

After successful installation, the agent may encounter connectivity issues with the EasyNAC Appliance. To diagnose connectivity issues, open the agent window and review any displayed messages or warnings. By default, the CyberGateKeeper agents are configured to talk with hostnames cgx-access and cgx-access.local. These values can be changed when building agents. Take note of the EasyNAC IP-address and/or Hostname configured in the agent. (Henceforth referred to as CGXA]

Error/warning seen on EasyNAC Compliance Agent window	Command to execute on endpoint CLI/Shell	Objective	Resolution
Failed. Cannot resolve hostname <CGXA>	`> nslookup <CGXA>`	To check if DNS is correctly resolving CGXA hostname. [*if hostname is used while agent building*]	Check is your DNS is configured to resolve CGXA hostname
Failed. Unable to connect to CyberGateKeeper <CGXA>	`> Ping <CGXA>`	to check CGXA reachability *(if your firewall allows ICMP)*	Check if agent or that network segment can reach CGXA appliance
Failed. Unable to connect to CyberGateKeeper <CGXA>	`> telnet CGXA 11698`	To check if agent can connect to audit port TCP 11698 on CGXA	Check if Anti-Virus or firewall is blocking TCP port 11698
Cannot establish session with a server from a different administrative domain or server is disabled.			See "different administrative domain error" below.
Failed. CyberGateKeeper indicated failure in audit session.			Agent has failed compliance. Check rules that agent

			should pass. Checking Device Manager - Reports would help identify why this agent failed compliance.

Different Administrative Domain error: This error occurs when the agent and the policy on the EasyNAC Appliance were built from different Policy Manager instances, or when no policy has been uploaded to the appliance. The agent and the appliance must share the same secret key, which is key is generated and provided by the Policy Manager. It is included when the agent is built, and when the policy is uploaded to the appliance. If the keys do not match, the client cannot connect to the appliance.

This can be fixed by any of the following:

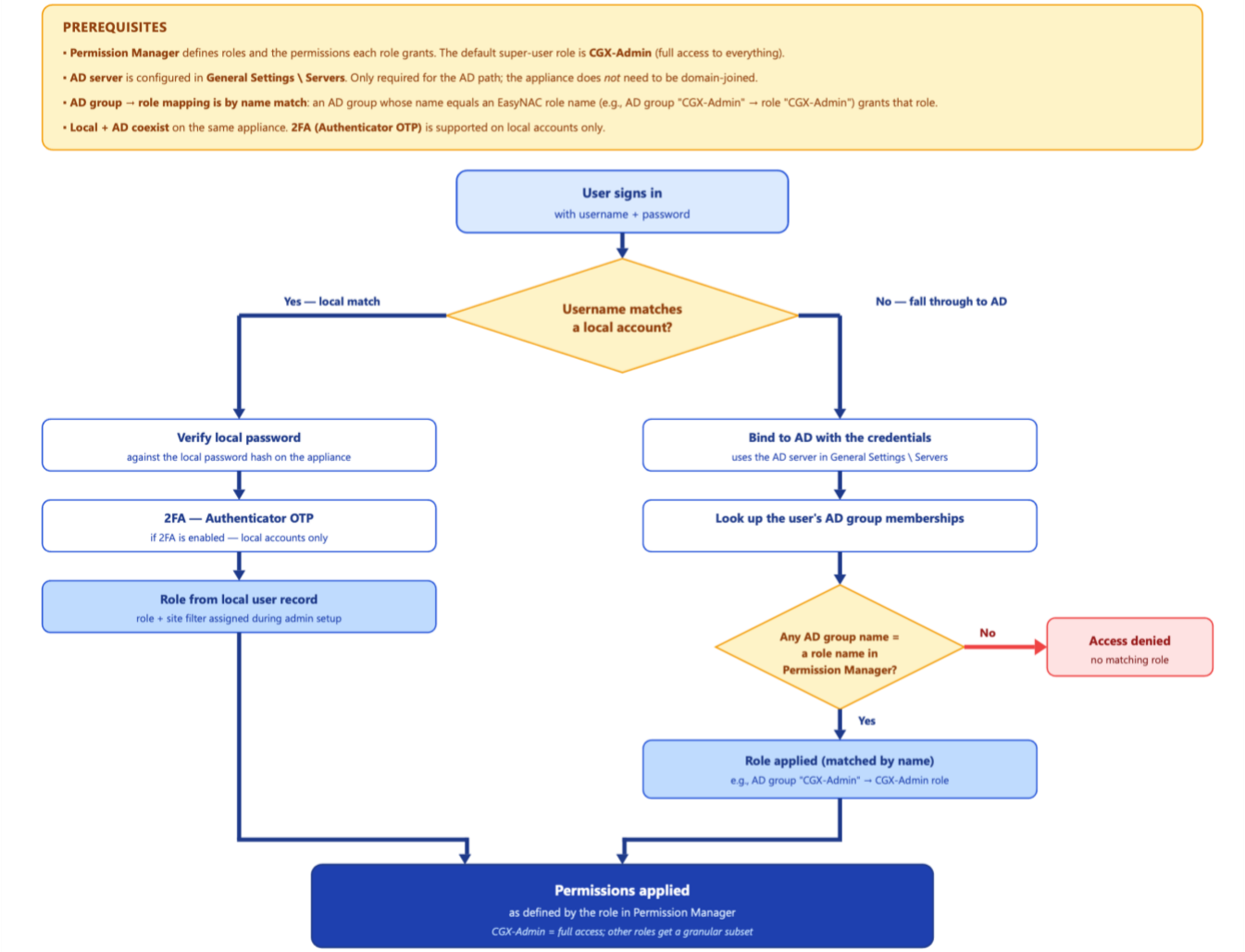
- Uploading the policy to the appliance, from the same Policy Manager that built the agent.
- Import the correct Shared Settings into the Policy Manager and re-upload the policies to the EasyNAC Appliance. (If using default agents, contact support for the default EasyNAC shared settings).
- Re-building and re-distributing the agent from the same system that uploaded the current policy.

Once the agent connects to the EasyNAC Appliance successfully, the agent window displays a “successful” message in agent window.

- When passing audit (compliant)
- When failing audit (non-compliant)

ADVANCED CONFIGURATION OPTIONS

PERMISSION MANAGER - ADMINISTRATION PERMISSIONS



Local Administrator Accounts

The EasyNAC Appliance can also authenticate administrators using local accounts stored on the appliance itself. Local accounts do not require Active Directory and can be used in standalone deployments, alongside AD authentication, or as break-glass accounts for environments that depend on AD.

Local accounts use the same role model as AD authentication. Each local user is assigned one of the predefined administrator roles (CGX-Admin, CGX-AdminRO, GRM-Sponsor) or any custom role created in Permission Manager. The role determines the level of access; a site filter and an optional account expiration date can also be set per user.

© 2026 InfoExpress, Inc.

When a user signs in, the appliance checks the local account table first. If the username matches a local account, authentication proceeds against the locally stored password hash. If there is no local match, the appliance falls through to AD authentication, provided an AD server is configured under General Settings → Servers. Local and AD authentication therefore coexist on the same appliance.

Two-factor authentication using an authenticator application (Authenticator OTP) can be enabled per local account. When enabled, the user is prompted for a one-time code after the password is verified. 2FA is supported for local accounts only — AD-authenticated sign-ins rely on whatever multi-factor protection AD itself enforces.

- Navigate to Configuration → Appliance Settings → Server Maintenance → Account Manager

The EasyNAC Appliance can also query the Active Directory server to validate permissions for administrators to access the management GUI. The EasyNAC Appliance uses management accounts stored in Active Directory. Different levels of access are given to admin users based on their AD group membership.

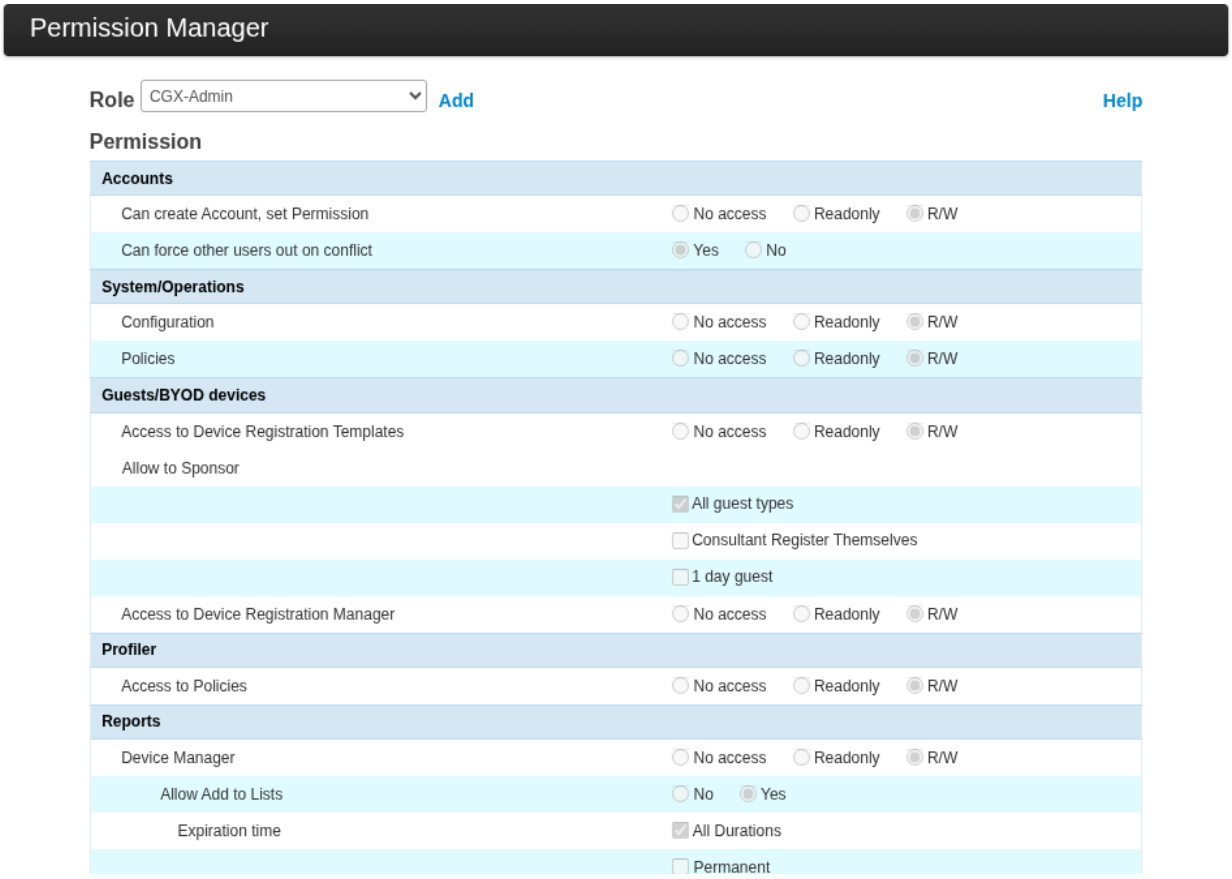
Administrator roles

The EasyNAC Appliance includes three preconfigured administrator roles: CGX-Admin, CGX-AdminRO and GRM-Sponsor. “CGX-Admin” is a default role that cannot be modified. It has full privileges. “CGX-AdminRO” can be used for limited administrative privileges. GRM-Sponsor is a group allowed to sponsor guest access. Each permission role can be configured with different access rights. Permission roles may be deleted or added. These roles correspond to groups in Active Directory.

Each role maps to a group defined in Active Directory. Administrators authenticate using their Active Directory credentials and receive access based on their group membership. For an Active Directory user to be placed into the CGX-Admin role on the EasyNAC, the user must be member of an AD group of the same name.

- Navigate to Configuration → Permission Manager

© 2026 InfoExpress, Inc.



Create the EasyNAC Appliance Admin Groups in Active Directory

Using the "Active Directory Users and Computers" MMC:

- Add the groups CGX-Admin, CGX-AdminRO and GRM-Sponsor. Note: Group names are case-sensitive.
- At minimum, add one account (typically your own) to the CGX-Admin group.

If you create a new account, make sure it's not set with "User must change password at next logon" as this prevents the account from authenticating to the EasyNAC Appliance until the password has been changed.

Test AD Connection

- Log out of the EasyNAC Appliance admin GUI
- Log in with your AD domain account

If authentication with AD credentials succeeds, the EasyNAC Appliance is communicating correctly with the Active Directory domain. If authentication fails, verify that the address of the LDAP server and the account suffix was entered correctly. Also, double check that the changes/additions you made to AD groups have been synchronized to the DC that the EasyNAC is connecting to (i.e. the host or IP entered).

© 2026 InfoExpress, Inc.

PRE-DEFINED ADMINISTRATOR ROLES

EasyNAC ships with four pre-defined administrator roles. Most deployments can map their operational personas onto these roles directly; custom roles are supported for environments with finer-grained separation-of-duties requirements.

Role	Intended persona	Capability summary
CGX-Admin	Senior administrator	Full read-write access to configuration, policies, device manager and reports.
CGX-AdminRO	Auditor or operations reviewer	Read-only access across the full appliance. Can view configuration and policies but cannot change them.
GRM-Sponsor	Reception, HR or business sponsor of guest visitors	Limited to the Guest Registration Manager. Can create and approve guest registrations on behalf of visitors.
CGX-CVMAdmin	Central Visibility Manager administrator	Full administrative scope for the CVM and its centrally-managed appliances. Used in CVM and MSP Manager deployments.

GRANULAR PERMISSION GRID

When creating a custom role, permissions are configured across the following permission groups. Each group can be set to No access, Readonly, or R/W (read and write) independently.

Permission group	Controls
System / Operations	Appliance system pages: About, Networking, Services, Logging, Backup and Restore, Server Maintenance
Configuration	General Settings, Integration, Permission Manager, License Manager
Policies	Auto Trust, Roles & Access, Time / Location / List, Orchestration Events, Monitoring, Device Profiler, Advanced Security
Guests / BYOD devices	Access to Device Registration Templates, the Allow to Sponsor permission, access to Device Registration Manager • All guest types • Consultant Register Themselves • 1 day guest
Profiler	Access to Device Profiler policies
Reports	Access to Reports Manager, Network Inventory, Alerts and Notifications
Device Manager	Per-action sub-permissions: • Allow Add to Lists (Yes / No) • Allow Remove from Lists (Yes / No) • Allow Set Tag (Yes / No), with Tag type filter: All Types / Manually Set • Allow Remove Tag (Yes / No), with Tag type filter: All Types / Manually Set

© 2026 InfoExpress, Inc.

	• Allow Manage Fingerprint (Yes / No), with Fingerprint Action filter: All Actions / Set Fingerprint / Change Fingerprint / Remove Fingerprint

SITE FILTER AND EXPIRATION

Two further controls apply to every role:

- **Site filter** — limits the role's scope to All Sites or to a specific named site. In CVM and MSP Manager deployments, this allows a role to be used by personnel responsible only for a subset of the managed estate.
- **Expiration time** — optionally sets a date and time at which the role assignment expires. Useful for time-bound access such as consultants or short-term contractors.

RECOMMENDED ROLE DESIGN

When designing your role set, prefer least-privilege over reuse. Several typical operational personas and their suggested role mapping are set out below. Adapt these to your environment.

Persona	Recommended starting point
Network Operations Center (NOC) — first-line	Custom role: Readonly on Configuration and Policies; R/W on Device Manager (Allow Add to Lists, Allow Remove from Lists). No access to Permission Manager or License Manager.
Help Desk	Custom role: Readonly across the appliance; R/W on Device Manager (Allow Set Tag for byod and consultant tags only). No access to Configuration or Policies.
Compliance / Auditor	CGX-AdminRO.
Guest reception	GRM-Sponsor.
Senior administrator	CGX-Admin.
Partner or external auditor (time-limited)	CGX-AdminRO with Expiration time set to the engagement end date.
MSP technician (multi-tenant)	CGX-CVMAdmin with Site filter set to the customer's site.

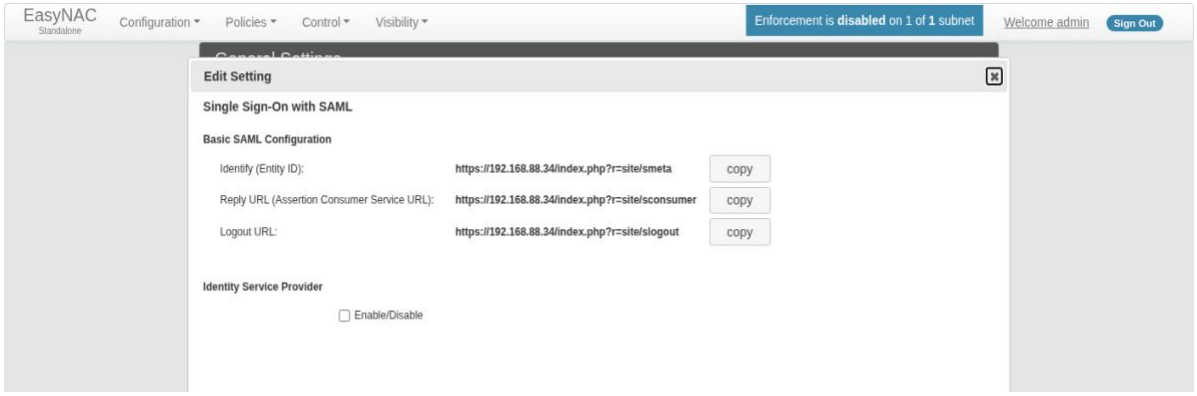
© 2026 InfoExpress, Inc.

SINGLE SIGN-ON WITH SAML

The EasyNAC Appliance supports SAML for single sign-on to the management GUI.

To configure Single Sign-On:

- Navigate to Configuration → General Settings
- Select "Single Sign-on with SAML"
- Check Enable/Disable to configure



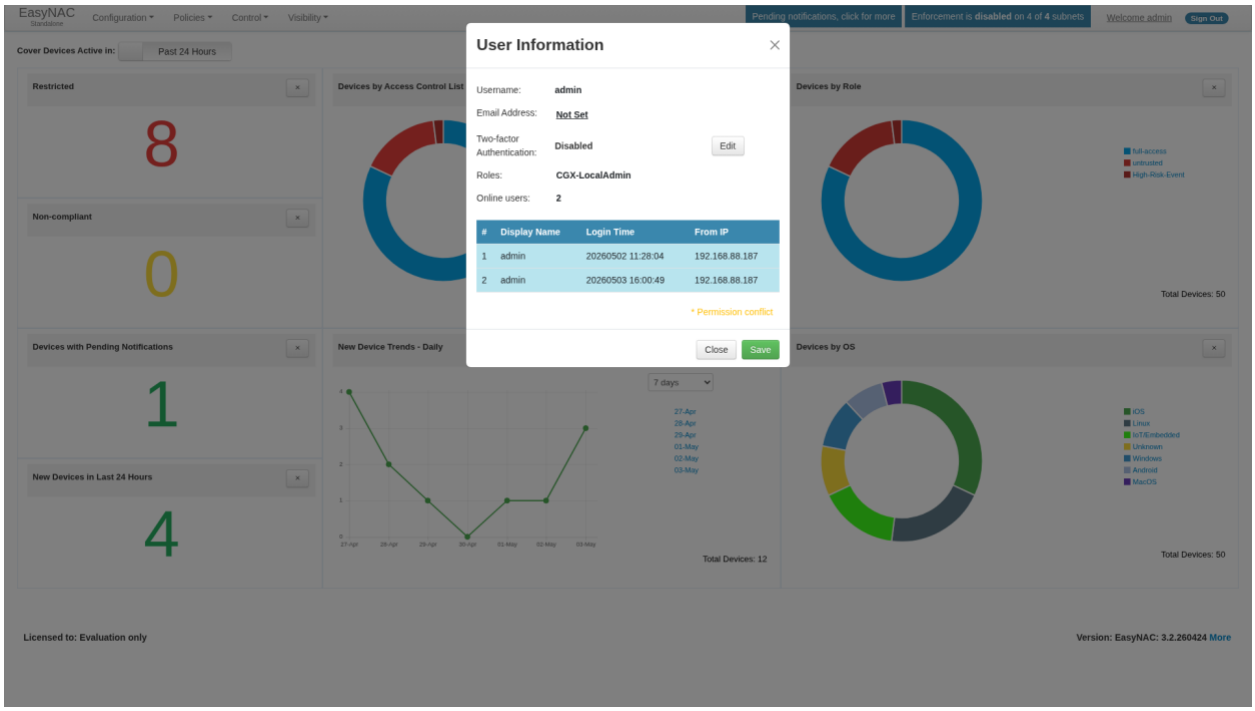
Note: *Click the Help button for provider-specific setup instructions for:*

- Azure AD
- OKTA
- Google

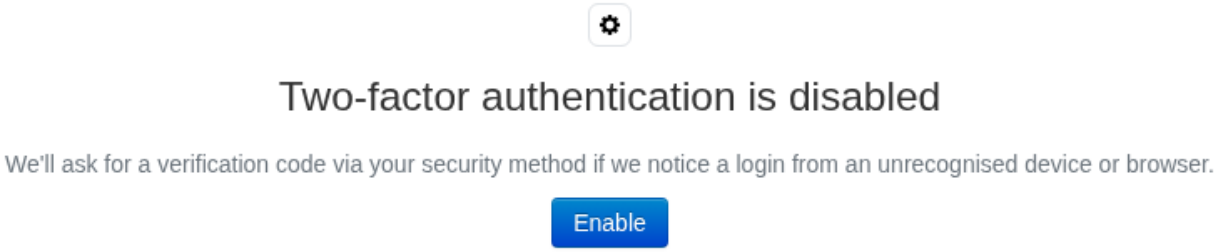
CONFIGURING 2FA FOR THE EASYNAC APPLIANCE ADMIN LOGIN

Enable two-factor authentication on the EasyNAC Appliance accounts using Time-based One-Time Password (TOTP) apps. **To enable:**

- After logging in to the EasyNAC management interface, click on your username.



- Click Edit button



- Reconfirm your password
- Select preferred Authentication App and complete the process
- Upon completion, a list of backup codes is generated. Store these codes in a secure location in case the TOTP application becomes unavailable.

CONFIGURING RADIUS FOR EASYNAC ADMIN LOGIN OR BYOD AUTHENTICATION

RADIUS SERVER CONFIGURATION

Note: *Free RADIUS server is used in this guide. For specific instructions for Microsoft NPS RADIUS server please see Appendix C*

- On the RADIUS server, register the EasyNAC Appliance as an authorized client:
- Add VSA id 2939 in dictionary with following attributes

- Add the user and assign the appropriate group. Group-level permissions are detailed later in this guide.

EASYNAC CONFIGURATION

- Navigate to Configuration → General → Servers → RADIUS Server
- Configure your RADIUS Server details (PAP or MSCHAPv2)

For group-level permissions, use the predefined groups or create custom groups with specific permissions.

- Navigate to Configuration → Permission Manager

Note: *Assign the same group and return it with RADIUS VSA 2939 as discussed above.*

- Save changes and log out
- Log in with the user defined on RADIUS server
- Verify the permissions granted to the user

When mapped to the read-only role, the user can view but cannot change these settings.

CUSTOMIZING LANDING PAGES

The EasyNAC Appliance offers two customization methods: edit text fields through the main configuration interface (see Configuration → General Settings). Modify the styles of landing pages by editing the CSS (Cascading Style Sheet). Steps to create such a CSS can be found below.

CSS files govern the look and feel of the landing pages only. The file should be called main.css

Upload CSS and images to EasyNAC

When complete, upload the main.css file and the images directory to the EasyNAC Appliance through SFTP using the cguser account. Below is the directory structure that should be present on the EasyNAC

Path			Contents
/updates	/grm-theme	/css	contains the main.css file
		/images	contains the images referenced by the css file

Only the main.css file and images are needed on the EasyNAC.

After uploading the files, the EasyNAC Appliance automatically detects and applies the changes to the landing pages. No additional commands are required. Allow a few seconds for the update to complete.

© 2026 InfoExpress, Inc.

EASYNAC API

OVERVIEW

EasyNAC includes a programmable API that allows external applications to query device information, manage tags and lists, and integrate with custom workflows. Access is granted via registered applications, each of which receives a Display Name, an Application (client) ID, and credentials suitable for OAuth-style token issuance.

The Application Registration screen is the management surface for these registrations. From this screen an administrator can create new registrations, view existing registrations, and revoke or disable applications.

WHAT THE API DOES AND DOES NOT DO

The scope of the EasyNAC API includes:

- Device queries: retrieve devices by MAC, IP, hostname, role, tag or list membership
- Tag and list management: add or remove devices from Allowlist, Blocklist, Excludelist or Routerlist; set or clear device tags
- Read access to policy and ACL definitions
- Read access to recent events for use by external SIEMs and orchestration platforms

The following are not in scope for the Early Release:

- Modifying Auto Trust policy rules programmatically
- Creating or modifying ACL rule structures programmatically
- Triggering software updates or appliance restarts
- Backup and restore operations

Note: *Capabilities marked as out of scope above may become available in subsequent releases. Confirm the current capability set with InfoExpress support before designing an integration that depends on a specific feature.*

AUTHENTICATION MODEL

The EasyNAC API uses an OAuth-style application registration model. Each external application is registered separately and receives its own credentials. The application uses those credentials to obtain a token, and the token is presented with each subsequent API call.

Registering separate applications for separate integrations enables fine-grained revocation: if one integration is compromised or retired, that application can be disabled without affecting any other integration.

REGISTERING AN APPLICATION

- Navigate to Configuration → Appliance Settings → EasyNAC API.
- Click New registration in the upper-right of the Application Registration panel.
- Enter a Display Name. Choose a name that clearly identifies the consuming application — for example, “SIEM Integration — Splunk” or “Asset Inventory Sync”.

© 2026 InfoExpress, Inc.

- Complete any additional fields presented on the registration form. Field-level details are documented in the Application Registration screen's Help dialog, accessible via the Help link in the upper-right of the panel.
- Save the registration. EasyNAC issues an Application (client) ID and the credentials needed to obtain access tokens.
- Record the Application (client) ID and credentials in your secrets manager. Treat them as sensitive — anyone with these credentials can call the API as your registered application.

Important: *The exact fields on the New registration form, and the precise format of the credentials issued, are documented in the screen's Help dialog. Refer to that dialog at the time of registration to confirm the current behavior, as details may evolve between builds.*

TOKEN ISSUANCE AND LIFECYCLE

The application uses its credentials to request an access token from the appliance. The token is then passed in the Authorization header of subsequent API calls, following the OAuth2 Bearer token convention.

Token lifetime, refresh-token semantics and revocation procedures are documented in the EasyNAC API Help dialog available from the Application Registration screen. Confirm these details against the running build before designing your integration.

SAMPLE API CALL STRUCTURE

API calls follow a REST convention over HTTPS. A typical call structure is:

— 1. Obtain an access token by POSTing the Application (client) ID and secret to the token endpoint.

— 2. Send a GET, POST, PUT or DELETE request to the relevant API endpoint, with the access token in the Authorization header.

— 3. Parse the JSON response, handling HTTP status codes per the API documentation.

Note: *Specific endpoint paths, request schemas and response formats are documented in the EasyNAC API Help dialog and in the developer documentation supplied. Refer to those sources for the authoritative reference. This guide does not reproduce them because they are subject to change during the Early Release period.*

RATE LIMITS AND ERROR CODES

The EasyNAC API enforces rate limits to protect appliance performance. The current limits and the standard error codes used by the API are documented in the EasyNAC API Help dialog. Integrations should implement exponential back-off on rate-limit responses and should log error codes verbatim to aid troubleshooting.

DISABLING OR REVOKING AN APPLICATION

© 2026 InfoExpress, Inc.

When an integration is retired, or if credentials are suspected of compromise, disable or revoke the corresponding application:

- Navigate to Configuration / Appliance Settings / EasyNAC API.
- **Locate the application in the registration list** — search by Display Name or by Application (client) ID.
- Open the application's detail view and choose the disable or revoke action.
- Confirm the change. From this point forward the application's existing tokens are no longer accepted, and new tokens cannot be issued under the revoked credentials.

Tip: *After revoking credentials, monitor your audit logs for several hours for failed API calls. Any continued failures indicate an integration that has not been notified of the revocation and may need to be updated or retired.*

API VERSIONING AND DEPRECATION POLICY

The EasyNAC API follows a major / minor versioning model. The major version is included in the request path (for example, /api/v1/devices). Within a major version the API is additive — new fields and endpoints are introduced without breaking existing callers. Breaking changes are deferred to a new major version.

DEPRECATION TIMELINE

- When a major version is superseded, the prior major version remains supported in parallel for a minimum of 18 months from the release date of the new major version.
- Endpoints scheduled for removal are marked in the API reference and emit a `Deprecation` header on each response for at least 6 months before removal.
- Field-level deprecations follow the same 6-month minimum and are documented in release notes.

COMMUNICATIONS

Deprecations and breaking changes are announced through the EasyNAC release notes, the customer portal, and the integration logs on the appliance. Customers running production integrations should subscribe to release-note updates so deprecation timelines are visible to engineering teams before the deprecation window closes.

ERROR CODES

HTTP code	Meaning	Suggested handling
200 / 201	Success	Process the response body normally.
400	Bad request	Caller error. Inspect the response body for the validation message; do not retry without a code change.
401	Unauthorized	Token missing, invalid or expired. Refresh the token and retry once. Repeated 401s indicate the application has been disabled or revoked.
403	Forbidden	Token is valid but the application does not have permission for this resource. Review the application's assigned scopes.
404	Not found	The requested resource (device, tag, list) does not exist on this appliance.
409	Conflict	A write request conflicts with current state (for example, attempting to add a device that is already on the list). Treat as success or fetch current state and adjust.
429	Too many requests	Rate limit exceeded. Honour the Retry-After header.

© 2026 InfoExpress, Inc.

500 / 502 / 503	Server-side error	Retry with back-off. Persistent 5xx indicates an appliance-side issue; contact InfoExpress Support if the condition persists more than five minutes.

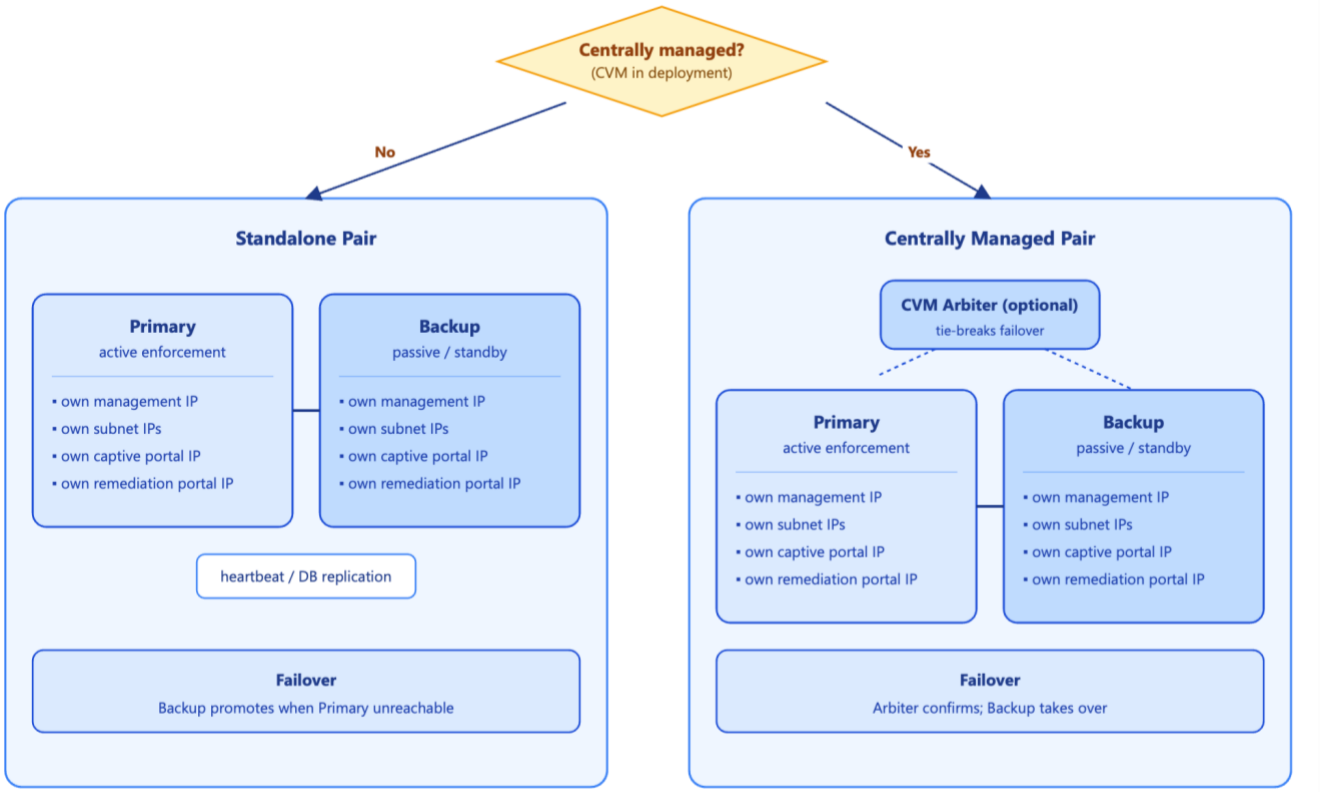
HIGH AVAILABILITY

Overview

The High Availability option provides redundancy in the event that an appliance or virtual appliance fails or goes offline. HA uses 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 returns online, the Backup appliance synchronizes the configuration and database back to the Primary, which then resumes active operation.

In centrally managed environments, configure the Central Visibility Manager as an arbiter to participate in determining which appliance should be active.



REQUIREMENTS

- An HA license is required
- The Backup appliance must use the same physical appliance type or hypervisor as the Primary. Mixing physical and virtual appliances within an HA pair is not supported.
- Configure the Backup appliance trunk port settings to mirror the Primary, using unique IP addresses.
- Deploy the primary and backup appliances on the same VLAN.
- Appliances must be able to ping their default gateway.

© 2026 InfoExpress, Inc.

- HA appliances may not be suitable for inline deployments. Contact InfoExpress to discuss VPN HA design requirements.
- When the CVM is configured as an arbiter, each appliance pair requires a unique arbiter port.

CONFIGURATION – STANDALONE APPLIANCES

These high availability configuration steps must be completed in the correct order.

1. Disable Enforcement (Use monitor mode on each VLAN)
2. Re-enable enforcement (as desired)

Tip: *Before configuring HA, create a current backup of the Primary appliance.*

Configure the Primary Unit

The Primary unit is the main appliance where all configuration changes are made.

Note: *If the primary appliance is already in production, place enforcement in monitor mode until the HA setup is complete.*

1. In the EasyNAC management interface, navigate to Configuration → Appliance Settings
2. Scroll down to Site Settings and change "EasyNAC Server Mode" from Standalone Appliance to Standalone Appliance - HA mode
3. Check box to make the Primary EasyNAC Server
4. Configure the IP address of the backup appliance (Peer EasyNAC Address)
5. Click Submit Server Mode. You will be warned that the Backup should not already be configured. It's OK for the backup unit to be on the network, but it should not yet be configured for HA.
6. You will be logged out of the EasyNAC Appliance while the changes take effect. Wait 2-5 minutes before logging back in.
7. Within 2-5 minutes, the primary appliance enters high availability mode.

Note: *The Backup will not be reachable until it has also been configured for HA*

Configure the Backup Unit

The backup appliance pulls its configuration from the primary appliance, so only IP addresses and network configurations need to be pre-configured. Except for the appliance's IP addresses, other network settings should be identical.

Note: *Before configuring the Backup unit, the Primary unit must first be configured for HA, as instructed above.*

8. In the EasyNAC management interface, navigate to Configuration → Appliance Settings
9. Scroll down to Site Settings and change "EasyNAC Server Mode" from Standalone Appliance to Standalone Appliance - HA mode
10. In the "Peer EasyNAC Address" configure the IP address of the Primary appliance
11. Click Submit. You will receive a warning that the primary appliance should be in high availability mode and working.
12. You will be logged out of the EasyNAC Appliance and the changes will take effect. The configuration and database will be synced from the Primary. This will take some time, Allow 5 to 10 minutes for synchronization to complete before logging back in.
13. Within 5-10 minutes, the appliance enters high availability mode and displays the primary as active.

Note: *When in Backup mode, only the Configuration menu will be available.*

© 2026 InfoExpress, Inc.

CONFIGURATION – CENTRALLY MANAGED APPLIANCES

These high availability configuration steps for centrally managed appliances are straightforward but must be done in the correct order.

CONFIGURE THE CVM TO BE AN ARBITER (OPTIONAL)

In environments that have Centrally Managed Appliances, the Central Visibility Manager can be configured to be an arbiter to participate in the decision of which appliance should be active.

Note: *In environments with reliable network connectivity to the CVM, enabling independent arbiter functionality on the CVM is recommended. However, if connectivity is inconsistent, this could prevent the failover to the backup unit from occurring. Therefore, in environments with inconsistent connectivity, it is best not to use the CVM as an arbiter.*

14. In CVM go to Configuration → Appliance Settings
15. Scroll down to Site Settings and click "Configure"
16. Select "New Arbiter Instance(s)"
17. Configure a unique port for each appliance pair. If you have three high availability appliance sets, configure three unique ports, starting from port 27019.
18. Click "Submit Server Mode" to save changes

Configure the Primary Unit

The Primary unit is the main appliance where all configuration changes are made.

Note: *If the primary appliance is already in production, place enforcement in monitor mode until the HA setup is complete.*

19. In the EasyNAC management interface, navigate to Configuration → Appliance Settings
20. Scroll down to Site Settings and change "EasyNAC Server Mode" to Centrally Managed Appliance - HA mode
21. Input a Site Name (often a location name)
22. Input the correct CVM IP address
23. Check box to make the Primary EasyNAC Server
24. Configure the IP address of the Backup appliance (Peer EasyNAC Address)
25. If using CVM as an Arbiter than specify one unique port that had been configured on the CVM. (optional)
26. Click Submit Server Mode. You will be warned that the Backup should not be configured. It's OK for the backup unit to be on the network, but it should not yet be configured for HA.
27. You will be logged out of the EasyNAC Appliance while the changes take effect. Wait 2-3 minutes before logging back in.
28. Within 2-3 minutes, the primary appliance enters high availability mode.
29. Confirm the Arbiter is reachable.

Note: *The Backup will not be reachable until it has also been configured for HA.*

Configure the Backup Unit

The Backup unit will pull its configuration from the Primary unit, so only IP Addresses and network configurations need to be pre-configured. Except for the appliance's IP addresses, other network settings should be identical.

Note: *Before configuring the Backup unit, the Primary unit must first be configured for HA.*

30. In the EasyNAC management interface, navigate to Configuration → Appliance Settings
31. Scroll down to Site Settings and change "EasyNAC Server Mode" to Centrally Managed Appliance - HA mode
32. In the "Peer EasyNAC Address" configure the IP address of the Primary appliance
33. Click Submit Server Mode. You will be warned that the Primary unit should be in HA mode and in working state.

© 2026 InfoExpress, Inc.

34. You will be logged out of the EasyNAC Appliance and the changes will take effect. The configuration and database will be synced from the Primary, Allow 5 to 10 minutes for synchronization to complete before logging back in.
35. Within 5 to 10 minutes, the appliance transitions to HA mode and displays the Primary as Active.

    Note: *When in Backup mode, only the Configuration menu will be available.*

36. Log in to the Central Visibility Manager and navigate to the Appliance tab to confirm that the HA status is displayed correctly.

MAKING HA CONFIGURATION CHANGES

If it's necessary to make changes to a working HA setup, please be sure to follow the steps outlined below:

REPLACE A PRIMARY

- Make sure the original Primary is offline or off HA (i.e., standalone)
- If new Primary has a different IP than the original one, change peer on Backup to the new IP
- Configure the new Primary (check "Replacement for existing Primary")
- No need to change arbiter configuration

REPLACE A BACKUP

- Make sure the original Backup is offline or off HA (i.e., standalone)
- If new Backup has a different IP than the original one, change peer on Primary to the new IP
- Configure the new Backup
- No need to change arbiter configuration

RESTORE FROM A BACKUP IMAGE

- Disable Enforcement
- Change Backup to Standalone mode
- Restore Primary
- Rejoin Backup to HA
- Re-enabled Enforcement

UPGRADE TO A NEW VERSION

- Disable Enforcement
- Change Backup to Standalone mode
- Update Primary, Backup
- Rejoin Backup to HA
- Re-enabled Enforcement

OTHER RECONFIGURATION CHANGES

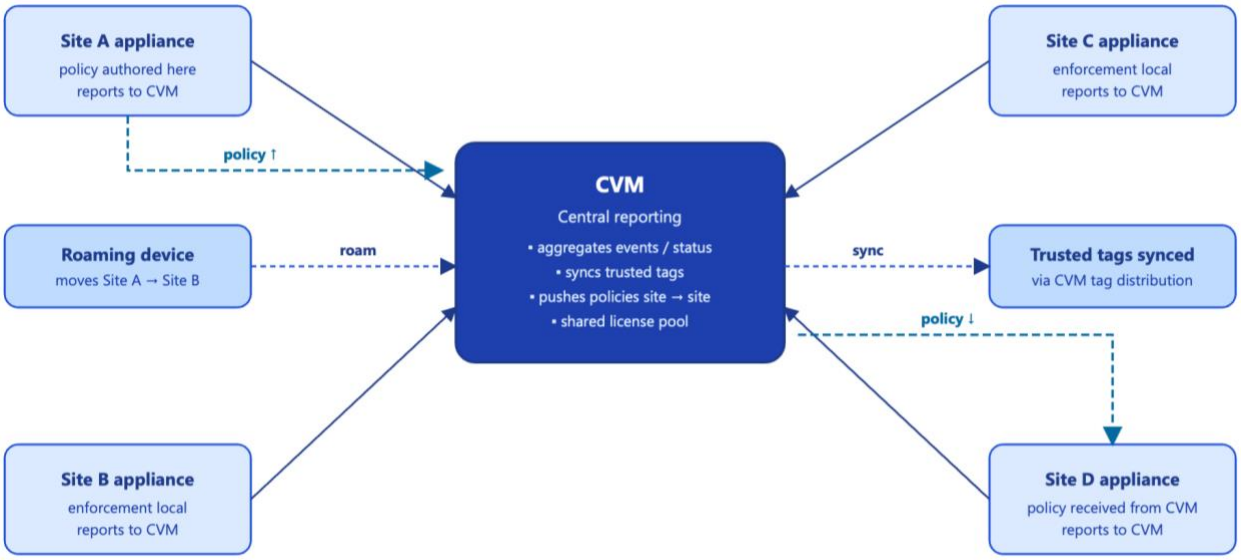
- Convert both members of the HA to standalone
- Remove the arbiter port if using CVM arbiter
- Create HA from scratch

© 2026 InfoExpress, Inc.

CENTRAL VISIBILITY MANAGER

CVM OVERVIEW

It's common to deploy multiple EasyNAC Appliances in multiple offices. In these scenarios where more than one EasyNAC Appliance is deployed it is beneficial to use the Central Visibility Manager (CVM) for an organization-wide visibility and management of these appliances.



The Central Visibility Manager doesn't perform monitoring and enforcement actions itself. It's used for consolidated reporting and management of multiple appliances.

REQUIRED PORTS

For normal operation, allow the following ports between centrally managed appliances and the CVM:

- **TCP 443** – Administrative GUI and Synchronization
- **TCP 10101** – for Synchronization

You may also need to allow TCP 21 from a management subnet to the centrally managed appliances, so agent policies and software updates can be uploaded to the distributed appliances. See the table below:

	Traffic Direction	Central Visibility Manager (CVM)	Centrally Managed Appliance (Primary)	Centrally Managed Appliance (Backup)
Central Visibility Manager (CVM)				
Centrally Managed Appliance (Primary)	g	TCP 10101 TCP 443 TCP xxxx (arbiter)*		TCP 10120
Centrally Managed Appliance (Backup)	g	TCP 10101 TCP 443 TCP xxxx (arbiter)*	TCP 10120	

© 2026 InfoExpress, Inc.

Jump Server / Policy Manager PC	g	TCP 443 TCP 21	TCP 443 TCP 21	TCP 443 TCP 21

*If CVM is configured as the arbiter in HA setups.

CONFIGURING A CENTRAL VISIBILITY MANAGER

The Central Visibility Manager uses the same appliance image as the normal EasyNAC Appliance, so the initial setup will be like setting up an EasyNAC Appliance.

Note: *The CVM is licensed separately and has a unique CVM license required to operate.*

Basic IP Configuration

  - For physical appliances, use a direct connect ethernet cable for SSH access to the default IP Address 10.0.0.250/24. Alternatively, plug-in a keyboard and HDMI monitor.
  - For virtual appliances open a console window and power on the VM.
- After the boot cycle completes, you will be prompted to log in.
  - Login as admin/admin.
  - From the main menu choose 1 (Run setup wizard) and follow the prompts to set the Managed IP address and netmask, the default gateway, DNS servers, system name, time zone and date/time.

Note: *Keep the admin password in a safe place. If it is lost, without having access to an alternate admin level account, there will be no way to recover the password.*

- Default user accounts are:
  - **admin** - used for initial setup and configuration as well as SSH access for maintenance tasks
  - **cguser** - used for uploading files through ftp
- The default passwords are the same as the username
- After the setup wizard completes, the system is accessible on the network.
  - Confirm that you can ping the management IP from another system on the same subnet and also from a system on another subnet. If connectivity tests fail double check the physical or virtual connections and the basic IP configuration
  - Connect to the EasyNAC Appliance web GUI by opening https://<Managed IP> (that was configured previously)
- Log in as user admin (default password admin). A modern browser such as Chrome is strongly recommended. Older versions of IE or Firefox may not display the pages correctly.
- Using the web GUI, configure additional settings:
  - (Optional) Active Directory server settings (used for Permission Management)
  - (Optional) E-mail & SMS server settings (used for alerting)
  - (Required) Add license for Central Visibility Manager
  - In the EasyNAC management interface, navigate to Configuration → License Manager
  - Click “New License”
  - Paste the key into the space provided and apply
- The License Manager will show the maximum number of GX Access appliances that CVM can manage. If using a Distributed license, you will also see the number of devices that can be managed, and the current allocation of the license. With the distributed license, customers can allocate the license across different appliances.
- After completing the initial configuration, switch the new server to a Central Visibility Server mode.
- In the EasyNAC Appliance GUI go to Configuration → Appliance Settings
- Scroll down to Site Settings and change “EasyNAC Server Mode” from Standalone Appliance to Central Visibility Manager

© 2026 InfoExpress, Inc.

- Set both the Site name.
- If left blank, the site name defaults to Central Visibility Manager.
- The site name must contain only A-Z, a-z, 0-9, and underscore (_) characters.
- Click Submit Server Mode. You will be logged out of the EasyNAC Appliance and the changes will take effect.

CONFIGURING AN APPLIANCE TO BE CENTRALLY MANAGED

After configuring a Central Visibility Manager, you can convert new or existing standalone EasyNAC Appliances to be centrally managed by the CVM.

- If the EasyNAC Appliance is a new deployment and not a conversion of an existing standalone appliance, first perform the Initial Configuration as covered on Page 14. At a minimum, the appliance should have:
- Have a primary IP address assigned
- Have a Host name
- Have a DNS server
- After the server has basic configuration, switch it to a Centrally Managed Appliance mode:
- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- Scroll down to Site Settings and change “EasyNAC Server Mode” from Standalone Appliance to Centrally Managed Appliance
- Set the Site name and Central Visibility Manager IP Address.
- Site Name should only consist of the characters A-Z, a-z, 0-9, and _
- Click Submit Server Mode. You will be logged out of the EasyNAC Appliance and the changes will take effect.
- Within two minutes, device data replicates to the Central Visibility Manager.

Note: *If the CVM is configured for High Availability, input both IP addresses separated with a comma, no space.*

© 2026 InfoExpress, Inc.

DEPLOYMENT MANAGER

The Central Visibility Manager includes a Deployment Manager that is used to accelerate deployments or configuration changes among different EasyNAC Appliances.

- In CVM GUI go to Configuration → Deployment Manager

Create a Deployment Set

1. Specify a name
2. Select the Source appliance to copy the settings from
3. Choose which settings to include in the Deployment set
4. Click Save

Push a Deployment Set

- Select a Deployment Set
- Select the location(s) to push to
- Click Push
- Confirm the Push

SOFTWARE UPDATES

- Deployment Manager can also be used to update software across multiple appliances at the same time.
- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- Scroll down to Server Maintenance → Software Update
- Browse to location of file and upload the image
- Once uploaded, go to Configuration → Deployment Manager → Software Update tab
- Choose the correct image, complete checksum: and file size:
- Select the appliances to be upgraded and click **Upgrade**
- Images download to the appliances. If the checksum and file size are accurate, each appliance will be upgraded. Allow 15-30 minutes for upgrades to occur. The appliances will be rebooted after the upgrade is complete.

© 2026 InfoExpress, Inc.

CENTRAL VISIBILITY MANAGER – DEVICE ROAMING

The Central Visibility Manager maintains a list of all devices connected to the extended enterprise. This list can be used to facilitate device roaming between locations. There is no setup required on the CVM itself. Each EasyNAC Remote can be configured to control which type of devices and from what locations are allowed to connect.

- In the EasyNAC management interface, navigate to Configuration → Integration → Central Visibility Manager – Roaming Integration
- **Select Sites** - devices can roam from these sites
- Select types of devices that can from the selected sites
- For example, you can configure only "BYOD" registered devices and devices tagged as "AD-Managed" will be allowed to roam from either of the sites. These roaming devices will be tagged "Roaming", so using this "Roaming" tag, the devices can be assigned limited access to the network, as desired.

CENTRAL VISIBILITY MANAGER – INTEGRATION PROXY

When integrating with third-party security solutions, the CVM can act as an integration proxy. With this feature, the Central Visibility Manager integrates directly with the 3rd-party servers. The CVM would then share this integration data with the Centrally Managed Appliances. This architecture would aid deployments and minimize the load on the third-party servers.

Central Visibility Manager Configuration

- In CVM, go to Configuration → Integration Proxy
- Configure the desired integration (See Integration section for specific vendor info)

Centrally Managed Appliance Configuration

- In the managed appliances, go to Configuration → Integration
- Select the desired integration
- Select the "via Central Visibility Manager"

Note: *Each Centrally Managed Appliance would still be able to set their own policies.*

© 2026 InfoExpress, Inc.

MIGRATING FROM OTHER NAC SOLUTIONS

EasyNAC includes built-in tooling to ease migration from two source platforms: Dynamic NAC (DNAC), the previous-generation NAC product from InfoExpress, and Forescout. The tooling is accessible from Configuration → Appliance Settings / Support Tools, under the NAC Migration Tool section.

This chapter describes the pre-migration discovery work that should be completed regardless of the source platform, and then provides specific procedures for each of the two supported sources.

PRE-MIGRATION DISCOVERY CHECKLIST

Before importing data from any source NAC, gather the following information about the existing environment. This work pays for itself by exposing assumptions in the source platform that may not translate cleanly into EasyNAC's model.

- Inventory of all enforcement points: switches, wireless controllers, VPN concentrators, firewalls. Capture model, software version, current authentication mode (802.1X, MAB, Captive Portal) and current dynamic VLAN scheme.
- Inventory of all known endpoints: counts by OS, by location, by criticality. Identify any endpoints that are exempt from NAC enforcement and the reasons (medical devices, OT systems, legacy printers and so on).
- Existing policies: which devices are placed in which VLAN, which roles, which posture states. Capture the rules in human-readable form, not just configuration export.
- Identity sources: Active Directory domains and forests in use, RADIUS servers, certificate authorities issuing endpoint certs.
- External integrations: SIEM, EDR, MDM, vulnerability scanner, ticketing. Note which of these the existing NAC writes to, reads from, or both.
- Compliance constraints: data retention windows, audit logging requirements, separation-of-duties rules. EasyNAC's defaults may need adjusting to match.
- Cutover plan: parallel run window, rollback procedure, communications plan to affected users.

MIGRATING FROM DYNAMIC NAC (LEGACY INFOEXPRESS PRODUCT)

Dynamic NAC (DNAC) is the previous-generation NAC product from InfoExpress. EasyNAC includes a built-in migration tool that imports the legacy Dynamic NAC whitelist into the EasyNAC Allowlist, preserving the trust posture of devices that were already approved on the legacy system. This chapter is for existing InfoExpress customers who are upgrading from a Dynamic NAC deployment to EasyNAC.

PRE-MIGRATION CHECKLIST

Before running the import, gather the following from the legacy Dynamic NAC system:

- The current bvalues.xml whitelist file from the legacy Dynamic NAC server
- A note of any per-device comments held in Dynamic NAC's comments field that you want to preserve
- A list of any Dynamic NAC operational policies (subnet exemptions, exclusions) that need to be reproduced in EasyNAC's policy framework
- A migration window during which the legacy Dynamic NAC and the EasyNAC Appliance can run in parallel

© 2026 InfoExpress, Inc.

IMPORT PROCEDURE

- In EasyNAC navigate to Configuration → Appliance Settings → Support Tools.
- In the NAC Migration Tool section, click the Use link next to "Tool to import whitelist from DNAC solution". The DNAC Migration Tool screen opens.
- The tool's Current State is Disabled by default. Click the Enable button to activate the tool.
- Click Choose File next to "Select bvalues.xml file to upload" and choose the bvalues.xml file you obtained from the legacy Dynamic NAC server.
- Optionally tick "Tag DNAC White-listed devices" and select a tag from the dropdown. The default tag is DNAC-WL. Tagging the imported devices makes it easy to identify which records originated from the legacy system and to filter on them later.
- Optionally tick "Copy DNAC comments field to EasyNAC" if you want the legacy comments preserved as device comments in EasyNAC.
- Click Submit. The tool reports the number of records imported.

POST-IMPORT VALIDATION

- In Visibility / Device Manager, filter on the DNAC-WL tag (if you used it) and confirm the imported device count matches the count of whitelisted devices in the legacy system.
- Spot-check several devices to confirm MAC, IP and any imported comments are populated as expected.
- Confirm imported entries appear under Tagging Devices and Allowlisting.
- Run Auto Trust in observe-only mode for a representative sample of subnets and confirm access decisions match expectations.
- Resolve any rejected records flagged by the import report before enabling enforcement.

The DNAC Migration Tool imports the legacy Dynamic NAC whitelist (bvalues.xml). It is not used for migrating from Cisco DNA Center or Cisco Catalyst Center. There is no built-in tool for that scenario.

MIGRATING FROM FORESCOUT

Forescout (formerly known as CounterACT) maintains rich device-property data and policy state that is similarly valuable to migrate. The EasyNAC Forescout migration tool imports device data so that visibility is preserved across the cutover.

SOURCE DATA MAPPING

Forescout concept	EasyNAC equivalent
Host (MAC + IP)	Device record in Device Manager
Host group / segment	Device tag and / or role
Host property (operating system, vendor, etc.)	Device record fields, populated by Device Profiler
Policy match	EasyNAC role and ACL combination
Compliance status	Tag (managed-device, non-compliant and similar)
Endpoint Module device classification	Device Profiler classification

EXPORTING DATA FROM FORESCOUT

Export the device dataset from Forescout in a format the EasyNAC tool can consume. As with DNAC, confirm the specific format with the version of the EasyNAC migration tool and the Forescout release in use; export options have changed across Forescout releases.

© 2026 InfoExpress, Inc.

IMPORTING INTO EASYNAC

- In EasyNAC navigate to Configuration → Appliance Settings → Support Tools.
- In the NAC Migration Tool section, click the Use link next to "Tool to import device data from Forescout". The Forescout Migration Tool screen opens.
- The tool's Current State is Disabled by default. Click the Enable button.
- Click Choose Files next to "Select CSV file to upload" and choose one or more CSV files exported from Forescout. The tool accepts multiple files in a single import.
- Under "Existing files", choose either "Replace existing files" (if this is a fresh import) or "Keep old files" (if you are adding to an earlier import).
- Optionally tick "Tag devices" and select a tag. The default tag is "Forescout".
- Under "Copy comments from", choose either "Display Name" or "Comment" depending on which Forescout field you want preserved as the EasyNAC device comment.
- Click Submit.

POST-IMPORT VALIDATION

Apply the same validation steps as for the DNAC migration:

- Compare device counts between the source export and the EasyNAC Device Manager
- Spot-check device records for completeness and correctness
- Confirm tag assignments correspond to Forescout host group memberships
- Run Auto Trust in observe-only mode and verify outcomes against the existing Forescout policy decisions for a representative sample
- Resolve any rejected records before enabling enforcement

GENERAL POST-MIGRATION CHECKLIST

Whichever source platform you migrate from, complete these steps before decommissioning the source NAC:

- Run the source NAC and EasyNAC in parallel for at least one full business cycle (typically two to four weeks). EasyNAC enforces, the source NAC observes and alerts only.
- Compare access decisions made by EasyNAC against decisions the source NAC would have made for the same endpoints. Investigate divergences.
- Migrate any external integrations (SIEM, EDR, MDM) that previously talked to the source NAC so they now talk to EasyNAC. Use Configuration → Integration to add the EasyNAC side.
- Update operational runbooks: where help-desk staff used to look up devices in Forescout or DNAC, point them to Visibility →Device Manager.
- Communicate the cutover date and rollback plan to operations, security and the help desk.
- Take a full backup of EasyNAC immediately before the cutover so a rollback to the parallel-run state is possible if needed.
- Decommission the source NAC only after a successful production cycle on EasyNAC alone, and after the source NAC's data retention obligations have been transferred to EasyNAC, your SIEM, or another long-term store.

© 2026 InfoExpress, Inc.

HARDENING CHECKLIST

Before exposing the EasyNAC Appliance to production traffic, complete the items in this chapter. These steps reduce the risk of unauthorized access to the appliance, ensure that audit data is retained, and confirm that recovery procedures are in place. The items are presented in the recommended Day-1 sequence.

Each item is summarized in the table below and explained in detail in the subsections that follow. Cross-references are provided where the procedure is documented in another chapter.

#	Item	Why it matters	UI path
1	Change default admin / admin credentials	The factory default credentials are publicly known	Server Maintenance → Account Manager
2	Replace default self-signed SSL certificate	Browsers warn on self-signed certs and trust is broken	Server Maintenance → SSL Certificate Manager
3	Restrict SSH service access with a need to know basis.	SSH is enabled by default and it should only be allowed by authorized subnet or IP.	Firewall settings
4	Configure AD, RADIUS, 2FA or SAML for admin authentication	Local password is a single point of failure for compromise	See “Advanced Configuration Options”
5	Set audit and device-record log retention	Review the default retention period	Logging
6	Configure backup destination and Automatic Backup	Without scheduled backups, configuration loss is unrecoverable	Backup and Restore
7	Verify NTP servers are reachable	Correct system time and time zone are required for accurate audit logs and AD/Kerberos authentication.	Services → NTP Servers
8	Apply latest software update	Production traffic should never be the first run of an unpatched build	Server Maintenance →Software Update
9	Review default Auto Trust policy	Default rules may be too permissive or too strict for your environment	Policies → Auto Trust
10	Review Permission Manager roles	Shared admin login defeats audit and accountability	Configuration → Permission Manager
11	Document recovery procedures	Recovery in a crisis depends on knowing where backups are, who holds the license, and the appliance role	Maintained outside the appliance

1. CHANGE DEFAULT ADMIN / ADMIN CREDENTIALS

Newly installed EasyNAC Appliances ship with the user name admin and the password admin. These credentials grant full administrative access and must be changed before the appliance is reachable from any untrusted network.

To change the password:

- Navigate to Configuration → Appliance Settings → Server Maintenance.
- In the Server Maintenance panel click the Manage link next to Account Manager.
- Select the admin account and choose Change Password.
- Enter a strong password (minimum 12 characters, mixed case, numbers and symbols recommended).
- Save and log out. Log back in with the new password to confirm it works.

Tip: *If your organization uses a password manager, store the new admin password there before logging out, not after.*

© 2026 InfoExpress, Inc.

2. REPLACE DEFAULT SELF-SIGNED SSL CERTIFICATE

The EasyNAC management interface, the Captive Portal and the Remediation Portal are all served over HTTPS. By default they use a self-signed certificate. Replace it with a certificate issued by a CA your endpoints already trust, otherwise users will see browser warnings whenever the Captive Portal redirects them, and your own administrators will become accustomed to clicking through certificate warnings.

To replace the certificate:

- Navigate to Configuration → Appliance Settings → Server Maintenance.
- Click the Manage link next to SSL Certificate Manager.
- Choose either Generate Certificate Signing Request (CSR), or Upload certificate and private key. The two options are documented in the "Configuring the EasyNAC Appliance" chapter earlier in this guide.
- Apply the certificate and verify by reloading the management interface in a fresh browser session.

Note: *If the appliance hosts the Captive Portal under a different hostname or IP from the management interface, ensure the certificate covers all hostnames in use, or upload separate certificates as appropriate.*

3. RESTRICT SSH SERVICE ACCESS WITH A NEED TO KNOW BASIS.

SSH is enabled by default on the EasyNAC Appliance to support troubleshooting by InfoExpress support engineers. As a security best practice, SSH access should be restricted to authorized subnets or specific management IP addresses rather than left broadly accessible.

If required, restrict access via network controls (e.g. firewall rules) to approved IP ranges, or click Disable if SSH is not needed.

4. CONFIGURE RADIUS, 2FA OR SAML FOR ADMIN AUTHENTICATION

Local password authentication is acceptable for evaluation purposes but is not recommended for production deployments. EasyNAC supports more secure alternatives for administrator authentication, including integration with Active Directory (via LDAP/RADIUS), two-factor authentication (TOTP), and SAML single sign-on. These options are documented in the "Advanced Configuration Options" chapter and relevant appendix sections.

Before exposing the appliance to production, it is recommended to implement at least one of the following:

- **Active Directory (LDAP/RADIUS)** — integrate with Microsoft Active Directory (e.g. via NPS) to centrally manage administrator authentication and access control.
- **Two-factor authentication (TOTP)** — add an additional layer of security for admin logins where required.
- **SAML SSO** — integrate with identity providers for single sign-on and centralized identity management.

5. SET AUDIT AND DEVICE-RECORD LOG RETENTION

EasyNAC retains two main classes of historical data: audit logs (administrative and policy events) and device records (per-endpoint history). The defaults are 30 days for audit logs and 90 days for device records. Adjust these to match your compliance window.

- Navigate to Configuration → Appliance Settings → Logging.
- Set Max Days To Keep Audit Logs (range 1 to 200, default 30) and click Submit.

© 2026 InfoExpress, Inc.

- Set Max Days To Keep Device Records (default 90) and click Submit.

Tip: *If your appliance is forwarding events to an external SIEM via Syslog, you can keep the on-appliance retention shorter than the SIEM retention.*

6. CONFIGURE BACKUP DESTINATION AND AUTOMATIC BACKUP

The EasyNAC Appliance supports backups to a Local destination (on the appliance itself) and to a Remote destination (a CVM or a remote server). For production, configure both, and enable Automatic Backup so a current copy always exists.

- Navigate to Configuration → Appliance Settings → Backup and Restore.
- Select the Local checkbox so the appliance keeps a local copy.
- Select the Remote checkbox and choose CVM or Server. Provide the remote target's address.
- Click Submit Destination Changes.
- In the Automatic backup row, click Enable. The default schedule is daily.
- Verify by clicking Backup Now and confirming the backup file appears at the configured destination.

Warning: *Local-only backups will not survive a hardware failure or VM corruption. Always configure a Remote destination for production deployments.*

7. VERIFY NTP SERVERS ARE REACHABLE

Accurate time is essential for Active Directory authentication, certificate validation, Kerberos tickets, log correlation, and any time-based access policy. Confirm the appliance can reach an NTP server before relying on it in production.

- Navigate to Configuration → Appliance Settings → Services.
- Click the Configure link next to NTP Servers.
- Add at least two NTP servers (an internal time source and a public fallback such as pool.ntp.org if your network allows it).
- Save the configuration.
- Return to Configuration → Appliance Settings → Date and Time and confirm the displayed time matches an external trusted source within a few seconds.

8. APPLY LATEST SOFTWARE UPDATE

Production traffic should never be the first run of an unpatched build. Always check for and apply the latest update before going live.

- Navigate to Configuration → Appliance Settings → Server Maintenance.
- Click Update next to Software Update.
- Follow the prompts to install the latest available build.
- After the update, return to the About page (Configuration → Appliance Settings → About) and confirm the System Release version matches the expected build number.

Tip: *Take a backup before applying any update. If the update behavior is unexpected, the backup is your fastest path to a known-good state.*

9. REVIEW DEFAULT AUTO TRUST POLICY

EasyNAC ships with a default Auto Trust policy that includes rules driven by Allowlist, Blocklist, Routerlist, agent audit results, and several customer-tunable rules. Before allowing the appliance to enforce against your production network, review every rule and confirm it behaves as expected for your environment.

© 2026 InfoExpress, Inc.

Pay particular attention to the Orchestration Event rule (which restricts on tags including SIEM-Event, IPS-Event, infected, FW-Event and APT-Event), the Fingerprint Mismatch rule (which restricts on FP-mismatched), the Trusted Managed Device rule (which grants full access to AD-managed, AV-managed, managed-device, patch-managed and XDR-managed tags) and the Trusted IOT Device rule (which grants full access to enforcer, network-infrastructure, printer, switch and VoIP tags). A misconfigured tag source can cause a production outage if those rules are wrong for your environment.

Review procedure: see the "Auto Trust Policy" section in the "Enforcement Overview" chapter.

10. REVIEW PERMISSION MANAGER ROLES

A single shared admin login defeats audit and accountability. Before opening the appliance to your operations team, create individual administrator accounts and assign each one to the least-privilege role appropriate for that person's responsibilities.

EasyNAC ships with four pre-defined roles:

- **CGX-Admin** — full administrative access
- **CGX-AdminRO** — read-only access to all configuration and policies
- **GRM-Sponsor** — limited to sponsoring guest registrations via the Guest Registration Manager
- **CGX-CVMAdmin** — Central Visibility Manager administrator role

Custom roles can be created with granular permissions. See "Administration Permissions" in the "Advanced Configuration Options" chapter for the full procedure.

11. DOCUMENT RECOVERY PROCEDURES

Recovery in a crisis depends on knowing where backups are stored, who holds the license file, and what role the appliance plays. Document the following information and store it outside the appliance, ideally in your IT operations runbook or wiki:

- Local and remote backup destinations, including credentials needed to retrieve a backup
- EasyNAC License
- Server Mode (Standalone, Centrally Managed, Central Visibility Manager, MSP Manager, with or without HA) and the IP addresses and roles of any peer appliances
- Hostnames, IPs and VLAN IDs of all configured network adapters
- Active Directory domain, NETBIOS name and Domain Controller details if joined
- AD/RADIUS, SAML or 2FA configuration sufficient to log in if the local admin account is unavailable
- Vendor and serial information for any integration that holds shared credentials with EasyNAC

© 2026 InfoExpress, Inc.

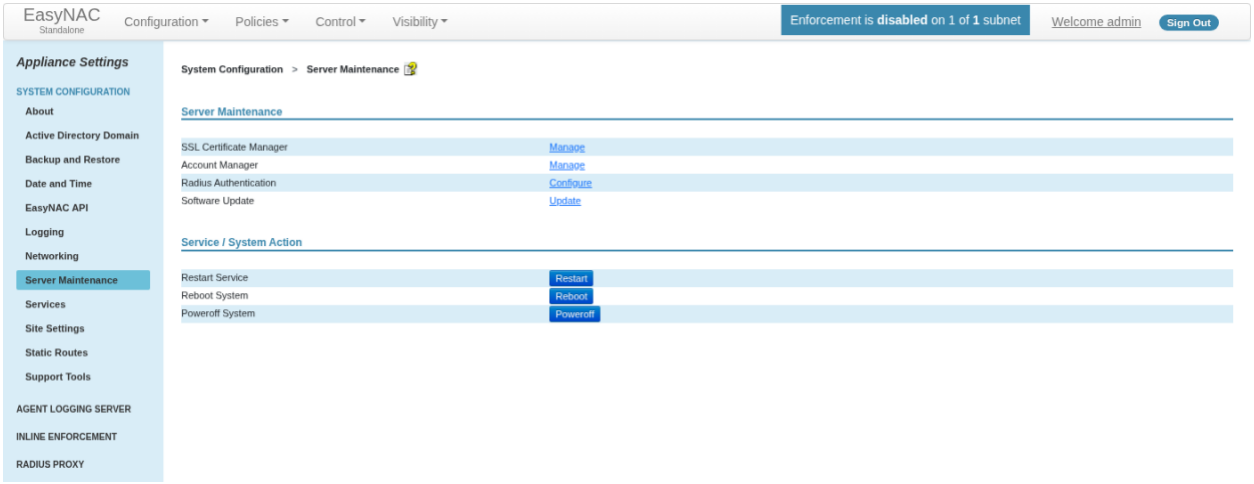
MAINTENANCE AND SUPPORT

UPGRADING FIRMWARE

InfoExpress may provide firmware updates to upgrade EasyNAC with new features or fix issues. A binary update file (BIN file) will be provided with a checksum and file size.

Upgrade the EasyNAC firmware through the web interface.

- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- Select Server Maintenance → Software Update
- Browse to location of file and upload the image



- Once uploaded, select file, complete checksum: and file size: then click **Submit**

The EasyNAC may reboot. Allow 5-15 minutes for upgrade to occur.

Note: *The "Force" checkbox should only be used when explicitly instructed by InfoExpress support. Performing a downgrade without guidance may result in system instability or corruption of the EasyNAC Appliance.*

© 2026 InfoExpress, Inc.

COLLECTING LOGS (DUMP2)

For troubleshooting purposes, InfoExpress support may ask administrators to collect Dump2 Logs.

Note: *Before collecting dump2 logs, please check with Support if you need to enable debug logging and the duration of logging required.*

Collecting Logs (Web GUI method)

- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- On left menu, Select → Support Tools → Debug Logging → Click **Configure**
- Cleanup Logs
- Enable Logging and reproduce the problem

- After reproducing problem, click the DUMP button
- **Wait for Dump process to complete** – It may take 5 to 15 minutes depending on number of endpoints. Longer if the system has had core dumps.
- Once complete, download the file and send to support.

Note: *If the web interface is unavailable, use the SSH CLI method to collect logs.*

Collecting Logs (SSH CLI method)

- In the EasyNAC Appliance SSH Console, use Option 91 - Server Maintenance
- Type "DUMP2"
- Type "y" to confirm
- **Wait for dump process to complete** – It may take 5 to 15 minutes depending on number of endpoints. Longer if the system has had core dumps.
- FTP to EasyNAC Appliance with Admin account to download the logs and send to support.

© 2026 InfoExpress, Inc.

SSL CERTIFICATE MANAGER

EasyNAC's HTTPS endpoints — the management interface, the Captive Portal and the Remediation Portal — are served using a certificate held in the appliance's certificate store. Manage certificates from Configuration / Appliance Settings / Server Maintenance, then click the Manage link next to SSL Certificate Manager.

Two paths are supported:

- Generate a Certificate Signing Request (CSR) on the appliance and send it to your CA. The procedure is documented under "Configuring the EasyNAC Appliance" earlier in this guide.
- Upload a certificate and private key obtained out-of-band. Useful when the same wildcard certificate is used across multiple internal services.

Tip: *Replace the default self-signed certificate as part of Day-1 hardening (see the Hardening Checklist chapter). Browsers warn on self-signed certificates and users will become accustomed to clicking through the warnings, which weakens overall security culture.*

ACCOUNT MANAGER

Local administrator accounts are managed at Configuration → Appliance Settings → Server Maintenance → Account Manager. Use this page to:

- Change the default admin account password during initial setup
- Create additional local administrator accounts (avoid sharing the default admin login)
- Disable accounts that are no longer needed, rather than deleting them, to preserve audit trail integrity

Note: *Where RADIUS, SAML or 2FA admin authentication is configured, local accounts remain useful as a break-glass mechanism for the event that the external authentication path is unavailable. Document any such break-glass accounts and rotate their credentials regularly.*

SOFTWARE UPDATE PROCEDURE

EasyNAC software updates are delivered through Configuration → Appliance Settings → Server Maintenance → Software Update. The update procedure follows these steps:

- Take a backup. Always. See Configuration → Appliance Settings → Backup and Restore.
- Review the release notes for the target build. Look for behavioral changes that may affect your existing policies.
- Schedule the update during a maintenance window. Updates may require a service restart and, in some cases, a full system reboot.
- From the Software Update page, click Update.
- Wait for the update to complete. Do not interrupt the appliance during the update.
- After the update, navigate to Configuration → Appliance Settings → About and confirm the System Release version matches the expected build.
- Log into the management interface from a fresh browser session and confirm normal operation.

Warning: *If the update applies to multiple appliances in an HA pair or in a CVM-managed estate, follow the staged update procedure described in the High Availability and Central Visibility Manager chapters. Do not update all appliances simultaneously.*

© 2026 InfoExpress, Inc.

SITE SETTINGS AND SERVER MODE

The EasyNAC Appliance can operate in eight Server Modes, configured at Configuration → Appliance Settings → Site Settings. The mode determines whether the appliance is standalone, part of a Centrally Managed pair, a Central Visibility Manager, or an MSP Manager (and whether HA is enabled in each case).

Mode	Use case
Standalone Appliance	Single-site deployment without HA. Suitable for evaluation, small offices, and proofs of concept.
Standalone Appliance — HA mode	Single-site deployment with primary / backup HA pairing.
Centrally Managed Appliance	Site appliance managed by a Central Visibility Manager. Used in multi-site deployments where central reporting and coordinated policy are required.
Centrally Managed Appliance — HA mode	As above, with HA pairing at the site.
Central Visibility Manager	Top-level appliance providing visibility, reporting, software updates and integration proxy across multiple Centrally Managed appliances.
Central Visibility Manager — HA mode	CVM with HA pairing.
MSP Manager	Managed Service Provider mode for partners managing many customer estates. Adds multi-tenant scoping above the CVM model.
MSP Manager — HA mode	MSP Manager with HA pairing.

Important: *Changing the Server Mode is a significant operation. It typically requires a service restart, may invalidate existing CVM relationships, and may require re-licensing. Plan the change during a maintenance window and take a backup beforehand.*

BACKUP DESTINATIONS AND AUTOMATIC BACKUP

Backups are configured at Configuration → Appliance Settings → Backup and Restore. Two destinations are supported and can be combined:

- **Local** — the backup is stored on the appliance itself. Useful for fast restore in the event of a configuration mistake but does not protect against hardware or VM corruption.
- **Remote** — the backup is sent to a remote target. Two remote target types are supported: a CVM (the Central Visibility Manager itself stores the site appliances' backups) or a Server (a generic remote backup server reachable from the appliance).

Additional controls on this page:

- **Backup Now** — performs an immediate one-off backup to the configured destination(s)
- **Upload Backup** — restores the appliance from a backup file uploaded from your local system
- **Download Backup** — downloads the latest backup file to your local system
- **Automatic backup** — when enabled, the appliance runs scheduled backups according to the configured cadence

Tip: *For production deployments, configure both Local and Remote destinations and enable Automatic Backup. The local copy supports rapid configuration recovery; the remote copy supports recovery after a hardware or VM failure.*

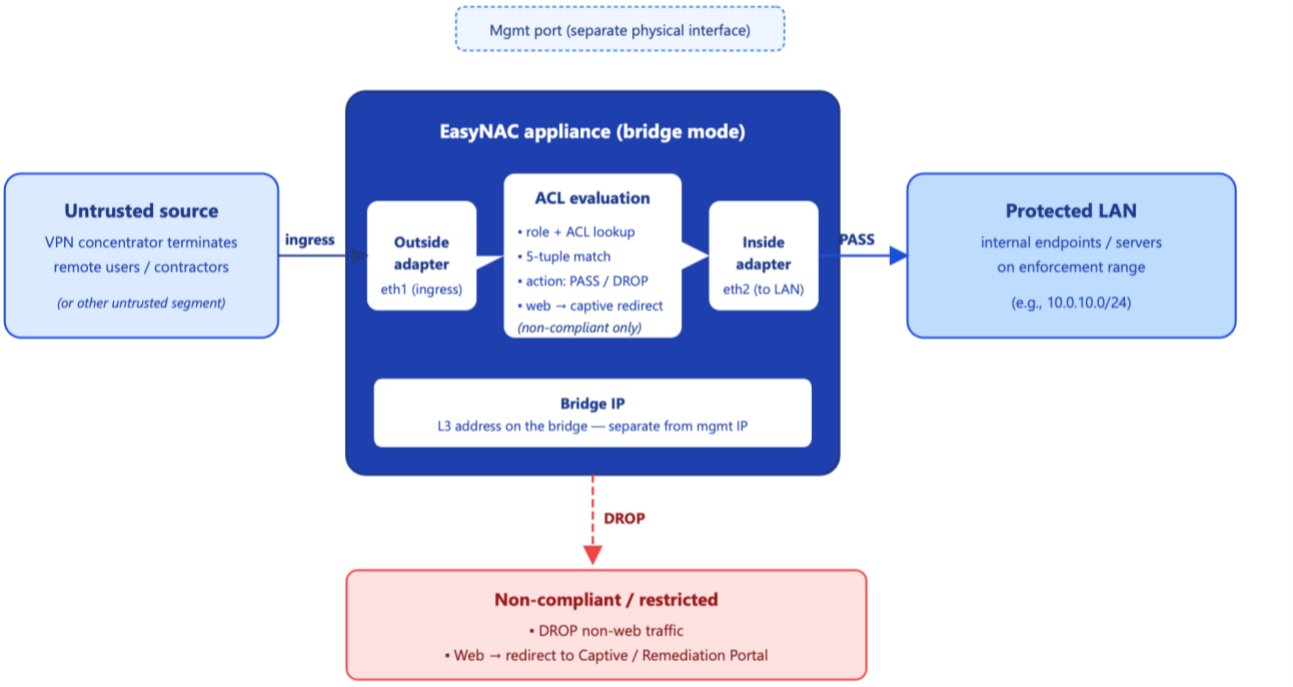
© 2026 InfoExpress, Inc.

APPENDIX A – INLINE ENFORCEMENT

INLINE ENFORCEMENT OVERVIEW

The Inline Enforcement Module (Inline EM) controls access to the network through an Access Control List associated with the outside NIC. This module can be used to control access for remote access servers, remote access VPNs, and site to site VPNs.

The Inline EM is available in the EasyNAC product family with EasyNAC Appliances. When using the Inline EM, the EasyNAC Appliance is placed in between the network and the network access device, such as a remote access VPN server.



FEATURES

The Inline EM supports the following features:

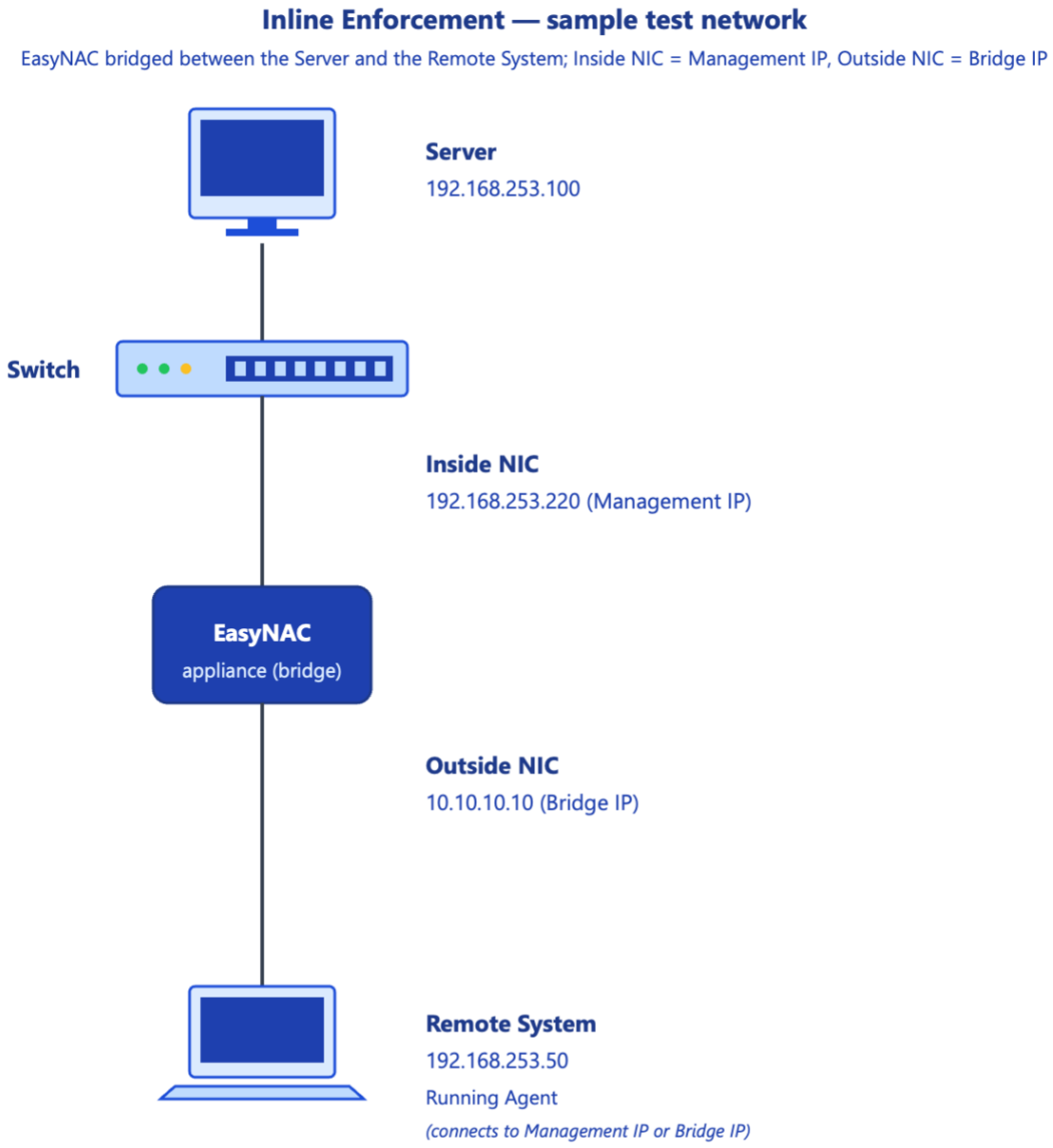
- Bridges traffic to avoid network topology changes.
- Optimized to handle continuous high traffic loads.
- Option for automatic failover through STP or KSTP if a redundant server is present.

REQUIREMENTS

- The EasyNAC Appliance must be physically placed between the inside (trusted) network and the remote access gateways such as VPN concentrators.
- Physical Appliance or virtual appliance with a least two network interfaces
- Endpoint Systems must use agents to pass a compliance check.
- VPN must pass TCP 11698 into the network (Agent uses TCP 11698)
- VPN Server must use an IP Pool, so every connected device has a unique IP address.

© 2026 InfoExpress, Inc.

SAMPLE TEST NETWORK



This is a minimal configuration to test and evaluate the Inline EM. Although company networks are not this simple, it can be used to test the features in a controlled test environment. All systems in this configuration are connected to the same subnet.

The EasyNAC Appliance is placed between a single PC which simulates the remote system, and the rest of the LAN which represents the inside network. The inside NIC is connected to the switch closest to the internal network, and the outside NIC is connected to the remote system.

The agent communicates with the Managed IP or the bridge virtual IP address.

Note: *If the remote PC is connected directly to the EasyNAC Appliance, a crossover cable may be required.*

© 2026 InfoExpress, Inc.

CONFIGURATION

This Configuration steps for the Inline EM consist of:

- Choose the proper location to connect the inline appliance
- Configure the network interfaces
- Set Bridge IP (This is another IP the agent can audit with)
- Set Access Control List (ACL) rules
- Set the Enforcement Ranges
- Enable Enforcement Mode

LOCATION

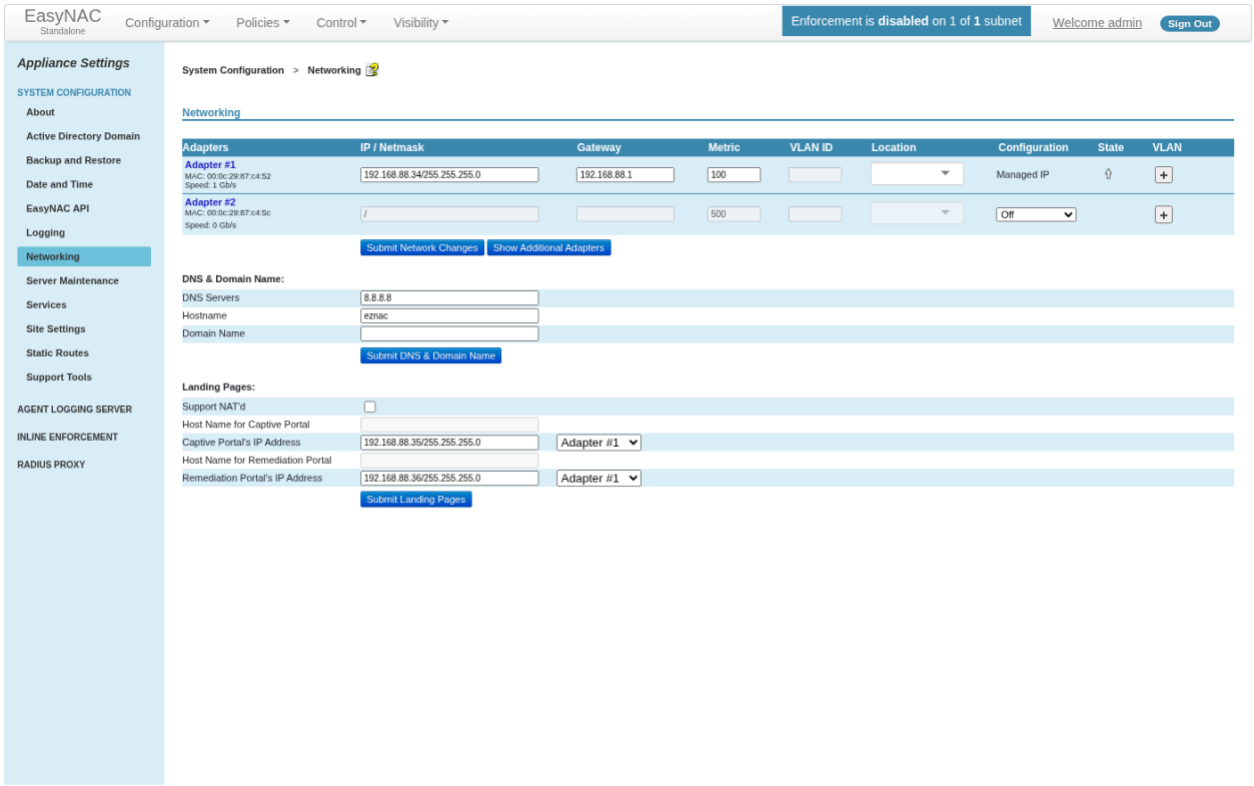
The Inline EM restricts traffic from remote systems, so the outside NIC must face the remote access servers and the inside NIC must face the internal network. When using the Inline EM, the EasyNAC Appliance is usually placed between the VPN and the default router on the network. The Inline EM bridges traffic so network routing tables do not need to be changed.

With this configuration, remote agents communicate to EasyNAC Management IP or bridge IP address. The bridge IP is virtual and is recommended for deployments where multiple inline appliances have been deployed to ensure scalability and compatibility with other addresses.

NETWORK INTERFACES

To set up the Inline Enforcement

- In the EasyNAC management interface, navigate to Configuration → Appliance Settings
- Click Inline Enforcement:
- Enable Bridge Mode



- Use STP to protect against network loops from misconfigured networks
- Select the Inside Network Adapter
- Select the Outside Network Adapter
- Set a Bridge IP address or maintain the default value (See below for more details)
- Submit Changes (reboot will be performed)

Note: *Inline enforcement is disabled by default to prevent unintended enforcement.*

Note: *A Secondary bridge could be useful in environments with VPN concentrators configured in an Active / Passive configuration.*

BRIDGE IP

When the inline enforcement controls endpoint access, agents should audit with either the EasyNAC Manager management IP or the Bridge IP address.

The Bridge IP allows for optimal scalability. Traffic to the bridge IP address is transparently intercepted when received on the EasyNAC Appliance through the outside NIC. Using the same bridge IP address is important when there are multiple EasyNAC servers deployed in Inline mode. Larger organizations may have dozens or even hundreds of remote access points. Keeping track of all the corresponding EasyNAC addresses for each entry point becomes a management burden.

By using the same bridge IP address for all audits, EasyNAC avoids this problem.

The bridge IP address can be any IP address that the VPN will route to the inside (trusted) network through the bridge interface on the EasyNAC server. This ensures connections from agents can audit with the EasyNAC Appliances. The default bridge IP address is 198.151.234.241/255.255.255.255

Note: *It's not typically required to change the default Bridge IP.*

© 2026 InfoExpress, Inc.

ACCESS CONTROL LIST

Inline Enforcement has its own ACL that is optimized for wire speed through-put. To edit the ACL click the Configure button.

For ease of setup, the ACLs are pre-configured with settings that should address most organization requirements.

Global ACL - Devices without agents or not yet auditing is assigned the "global acl".

- DNS and DHCP traffic are also allowed to pass through the appliance, even when restricted.
- Agent audit traffic (TCP 11698) will be redirected to the Bridge IP, so agents can audit with the inline appliance, even if the agents are configured to audit with a different IP address.
- The Global ACL will also redirect web browsers to the Remediation portal to allow for the download of agents or end-user communications.

Full-Access ACL - When a device is passing an agent audit, it will be assigned the "full-access" ACL.

- The full-access ACL will allow Any IP traffic. This will override the Global ACL.
- The Agent audit traffic (TCP 11698) will continue to be redirected to the Bridge IP for continuous compliance checks.

Restrict-agent ACL - When a device is failing an agent audit, it will be assigned the "restrict-agent" ACL.

You can customize the "restrict-agent" ACL to allow remediation resources. In the example above, a restricted devices can still access the remediation portal over port 80 and 443. This portal can be used to host automatic remediation scripts. The default "restrict-agent" doesn't conflict with the "global-acl" so the global-acl will also be applied.

Restricted ACL - When a device is Blocklisted, it will be assigned the "restricted" ACL.

This default "restricted" acl is blank. No lines override the "global-acl" so the global-acl will also be applied.

For additional help with the ACL, you can click the Help button.

ENFORCEMENT RANGES

When working with Inline enforcement it's common to need to limit the range of IP addresses that are subject to enforcement. For example, if deployed behind a Firewall / VPN, you would want to set the enforcement range to only include the IP ranges of the VPN IP pool. When this is setup, only remote VPN users are required to pass an agent audit. Note: For Testing purpose, you may want to limit the range to just one IP.

To set up the Enforcement Ranges

- Click Configure
- Choose the Add Action
- Complete the Start IP and End IP of the range and Click Submit
- **When all ranges have been specified** – Click "Upload to Server" button
- Once Enforcement range is set, turn on Enforcement to test.

Agent requirement

Inline Enforcement requires agents on remote endpoints. EasyNAC Appliances include default agents and default polices that can be used for testing or as a baseline to start building your custom compliance policies.

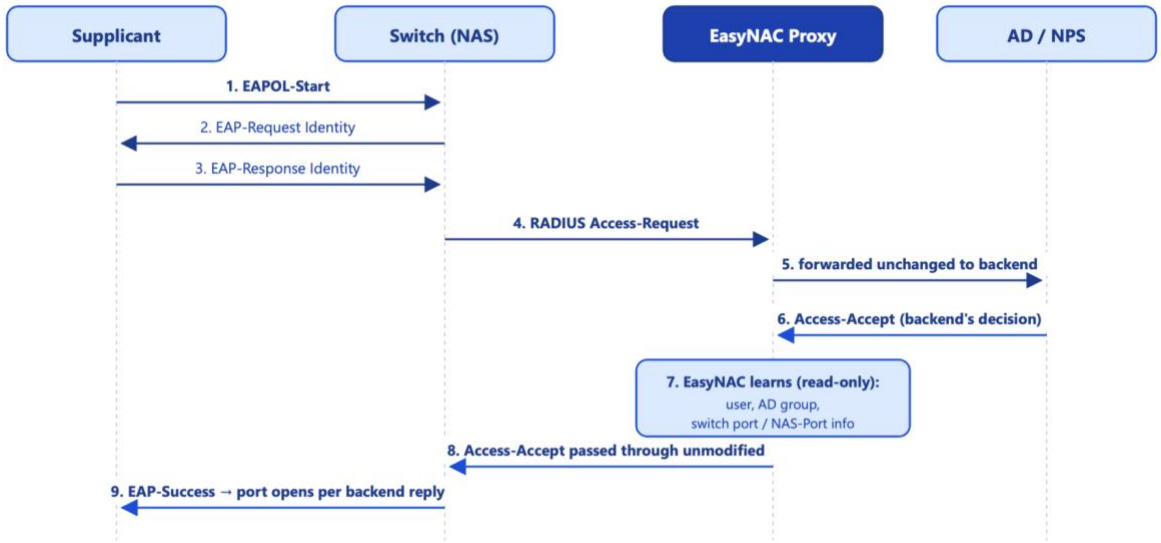
- An agent license is required to use the agents.
- To customize the policies or agent, it is necessary to install the CyberGateKeeper Policy Manager (CGPM). Contact InfoExpress or your partner for the CGPM installer.

© 2026 InfoExpress, Inc.

APPENDIX B – 802.1X RADIUS PROXY

RADIUS PROXY OVERVIEW

The EasyNAC Appliance can act as a RADIUS proxy for customers using 802.1X authentication. With this setup, end-user's 802.1X username can be captured at login time. In addition, the switch and port the device is connecting from is also monitored for reporting purposes. This information can then be used to enhance our ability to detect and prevent MAC spoofing real-time, and can also be used for Multi-factor Authentication.



REQUIREMENTS

- A third-party RADIUS Server
- A working 802.1X environment. Before adding the EasyNAC Appliance as a RADIUS Proxy, first have your wireless controller or switches configured and working with 802.1X and/or MAB.
- After 802.1X is working correctly, add the EasyNAC Appliance to the RADIUS stream. On the switches, EasyNAC Management IP should be configured as the primary RADIUS server, and the real RADIUS server as the secondary server, for fail-open purposes.

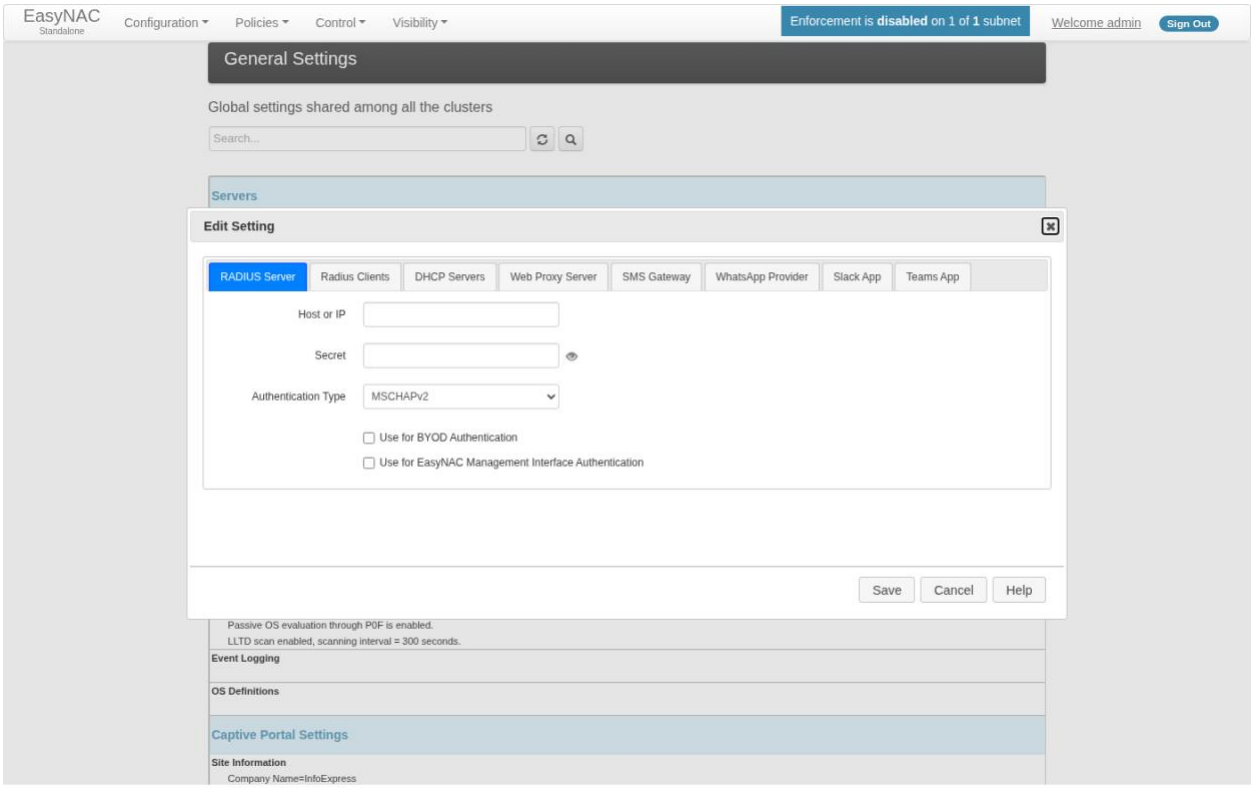
FEATURES

- Captures the end-user's name which can be used for Multi-Factor Authentication
- Captures the switch IP and switch port information to include in a Fingerprint. When enabled a trusted MAC address must be attached to the correct switch and port.

CONFIGURING RADIUS PROXY SETTINGS ON THE EASYNAC APPLIANCE

- In the EasyNAC management interface, navigate to Configuration → General Settings.
- Click Servers

© 2026 InfoExpress, Inc.



Under “RADIUS Server” tab, enter the Hostname or IP address of the RADIUS server

Enter the shared secret. It should be the same as configured for this EasyNAC Management IP under “RADIUS clients” on the RADIUS server.

Next, click on “RADIUS Clients” tab

Enter RADIUS client (WIFI controller/Switch controller) hostname or IP.

Enter the RADIUS password configured on the RADIUS client.

In the EasyNAC management interface, navigate to Configuration → Appliance Settings → RADIUS Proxy

Enable RADIUS Proxy Module

- Configure your WIFI Controller or Switch with EasyNAC Management IP as the RADIUS server
- Configure the same shared secret as configured in “RADIUS clients” on CGXA earlier.

Connect a wireless endpoint and enter user credentials configured on RADIUS Server.

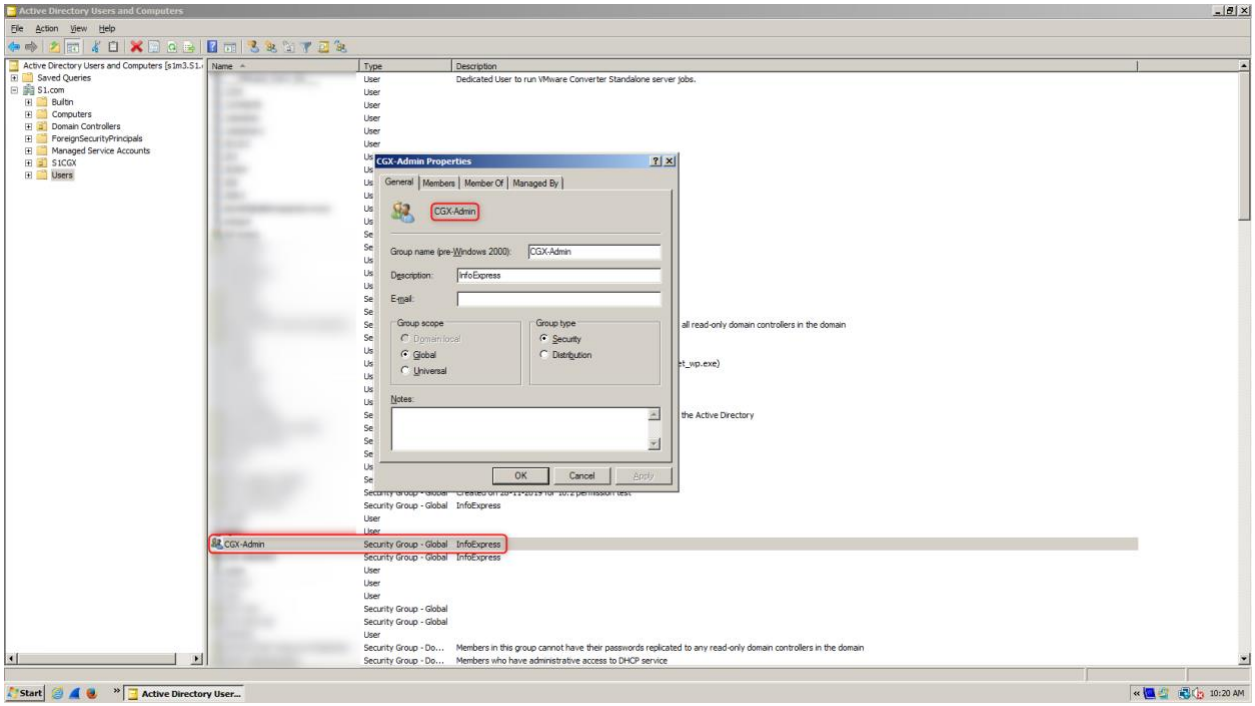
Confirm details on Device manager page on CGXA

APPENDIX C – USING NPS TO AUTHENTICATE EASYNAC USERS

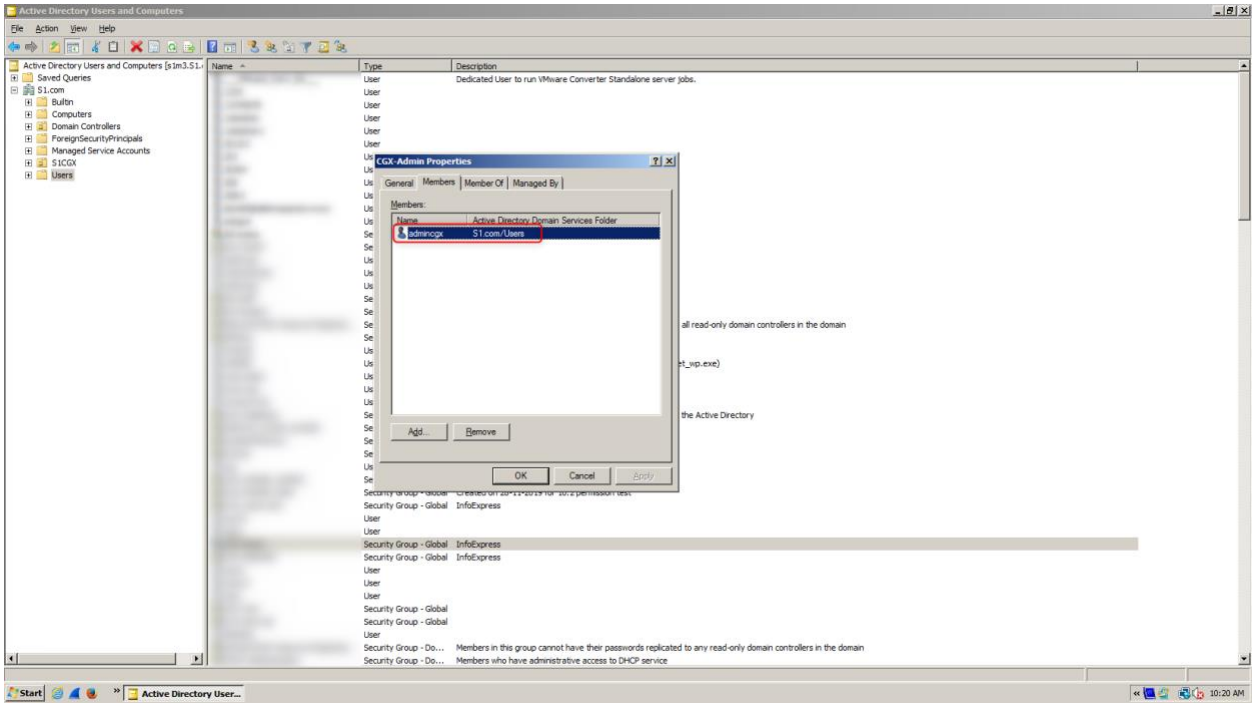
The EasyNAC Appliance can leverage Microsoft Network Policy Server (NPS) and other RADIUS servers for Management and/or BYOD authentication. The steps below are specific to NPS.

ADD ADMIN GROUP / USERS TO ACTIVE DIRECTORY

1. Create a security user group in Active Directory named “CGX-Admin”

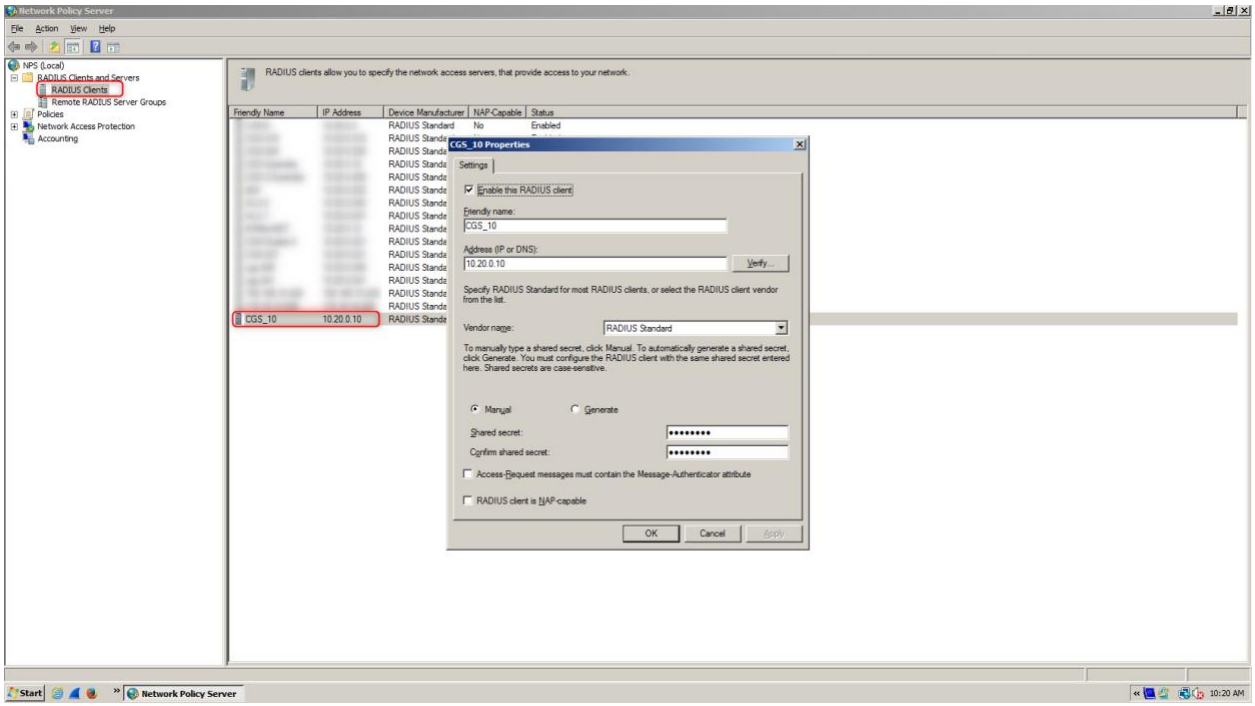


2. Add members to this group who need administrative read-write access to CGX-Access.

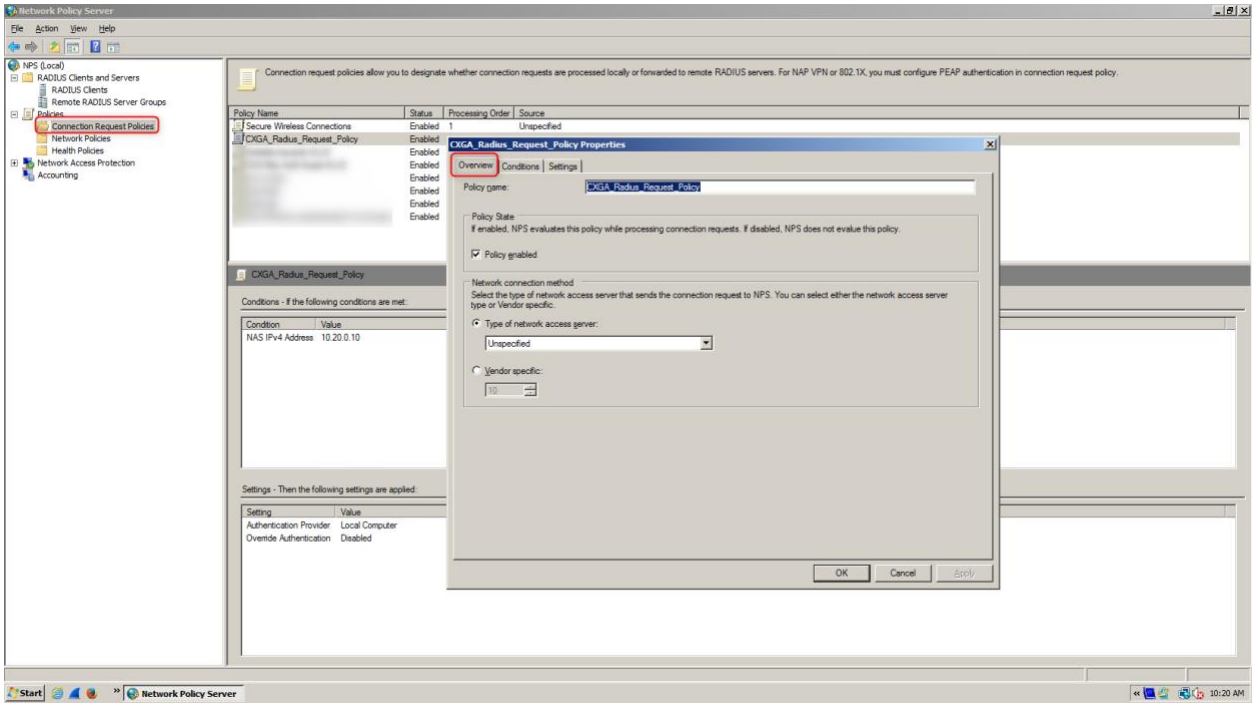


CONFIGURE NETWORK POLICY SERVER

1. Open “Network Policy Server” and add CGX-Access as a RADIUS client.

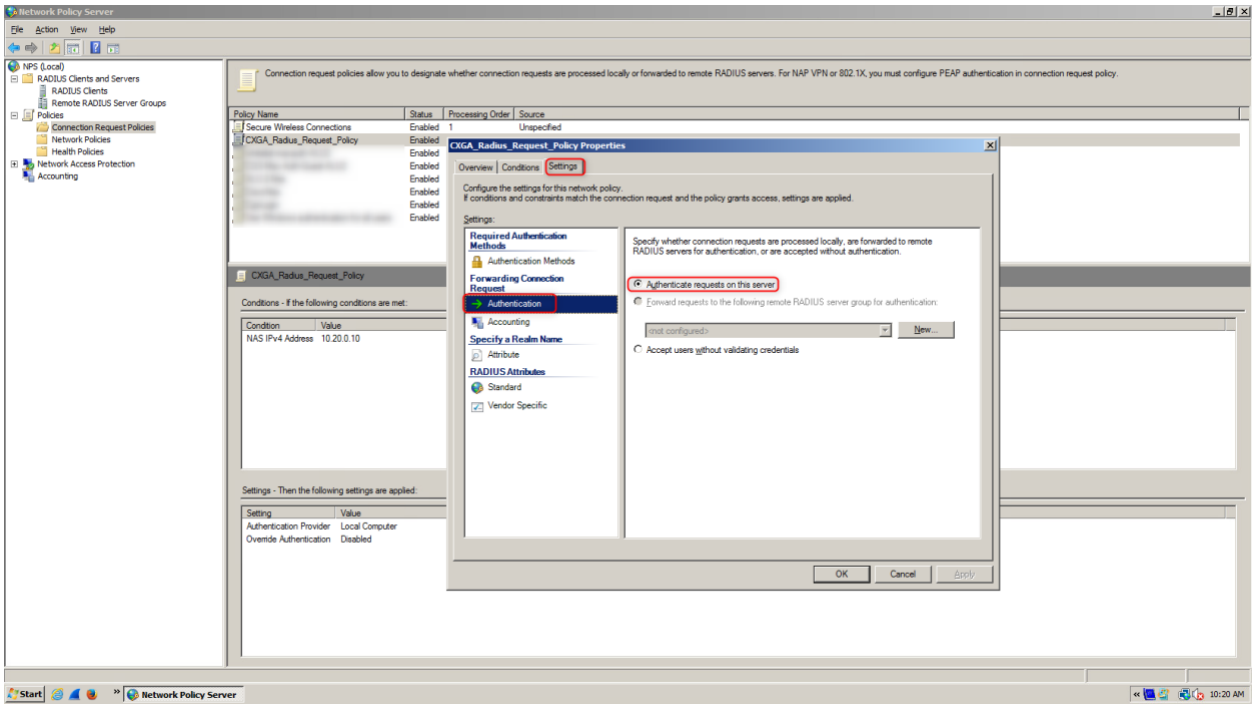


2. Create a new Connection request policy with parameters as listed below.



3. Add CGX-Access IP address in “Conditions” tab as “NAS IPv4 address”

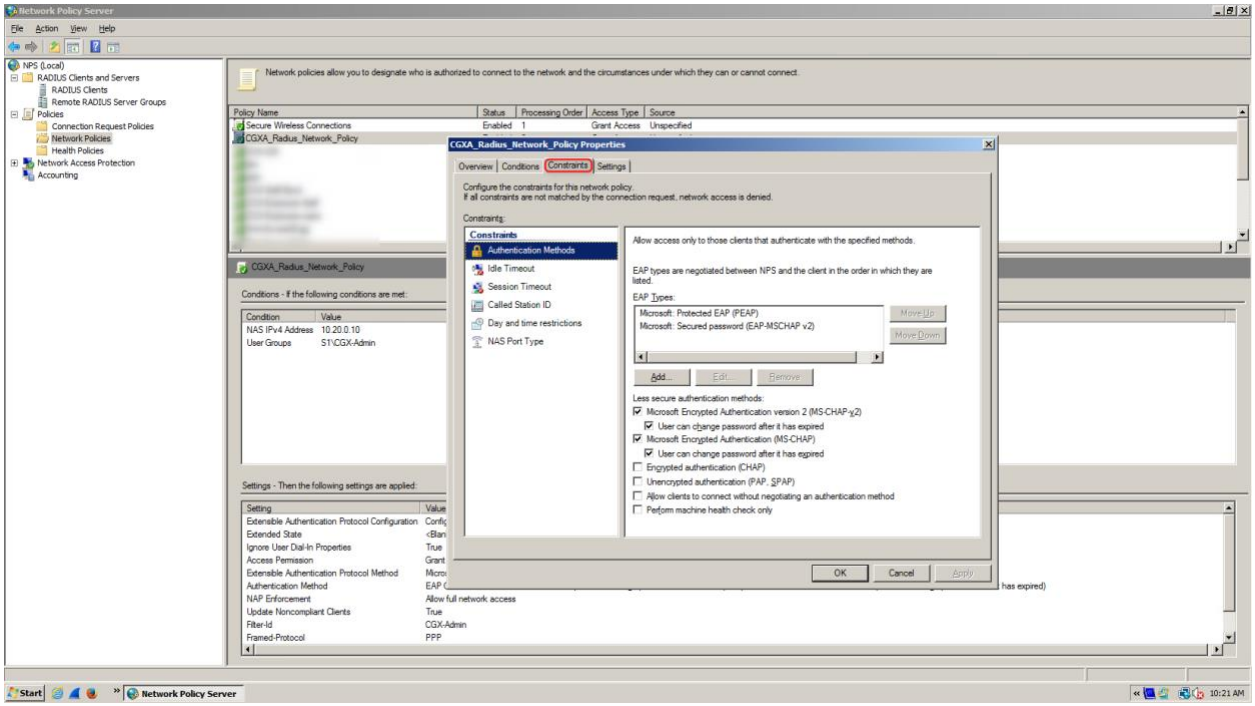
4. Under “Settings” tab select “Authenticate requests on this server”



5. Add a new Network policy for CGX-Access

6. Under “Conditions” Tab add “NAS IPv4 address” and “User Groups” (Domain\CGX-Admin)

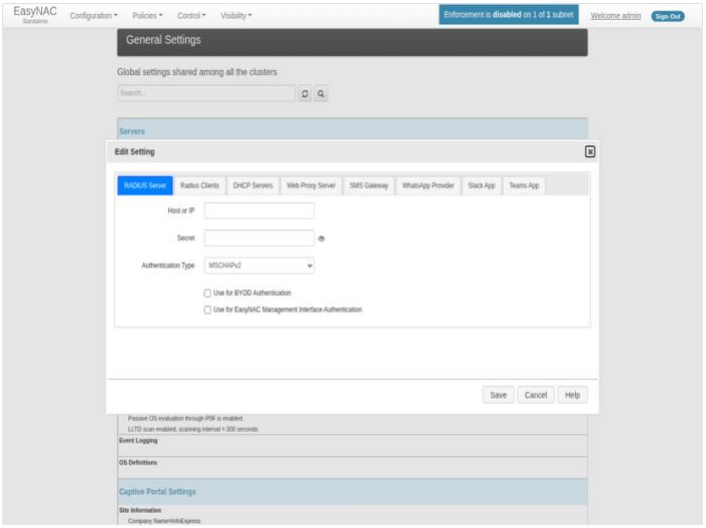
7. Under “Constraints” select the “Authentication Methods”



8. Under “Settings” tab Select “Standard” and add “Filter-id” as CGX-Admin

CONFIGURE THE EASYNAC APPLIANCE TO ALLOW LOG IN USING RADIUS

1. Navigate to the EasyNAC Appliance > Configuration > General Settings > Servers > RADIUS Server
2. Add the NPS server IP and configure same secret as configured on NPS server.
3. Select “Use for EasyNAC Management Interface Authentication”



4. Save
5. Log out of CGX and log in using the username that was added to AD group CGX-Admin.

TO AUTHENTICATE BYOD USERS VIA NETWORK POLICY SERVER

Follow the same procedure with the following changes:

In the “Add admin group/users to Active Directory” steps, you can use existing groups or create a new one and add users to that group.

In the “Configure Network Policy Server” steps, create a new policy to authenticate BYOD users and add the BYOD user group as the User Group condition.

In the same procedure, skip the step that adds “Filter-id” as CGX-Admin.

In the “Configure the EasyNAC Appliance to allow log in using RADIUS” steps, select “Use for BYOD Authentication” instead of “Use for EasyNAC Management Interface Authentication.”

> **Tip:** *For any troubleshooting logs on NPS server*

Start Event Viewer > Custom Views > Server Roles > Network Policy and Access Services

APPENDIX D – VLINKS OVERVIEW

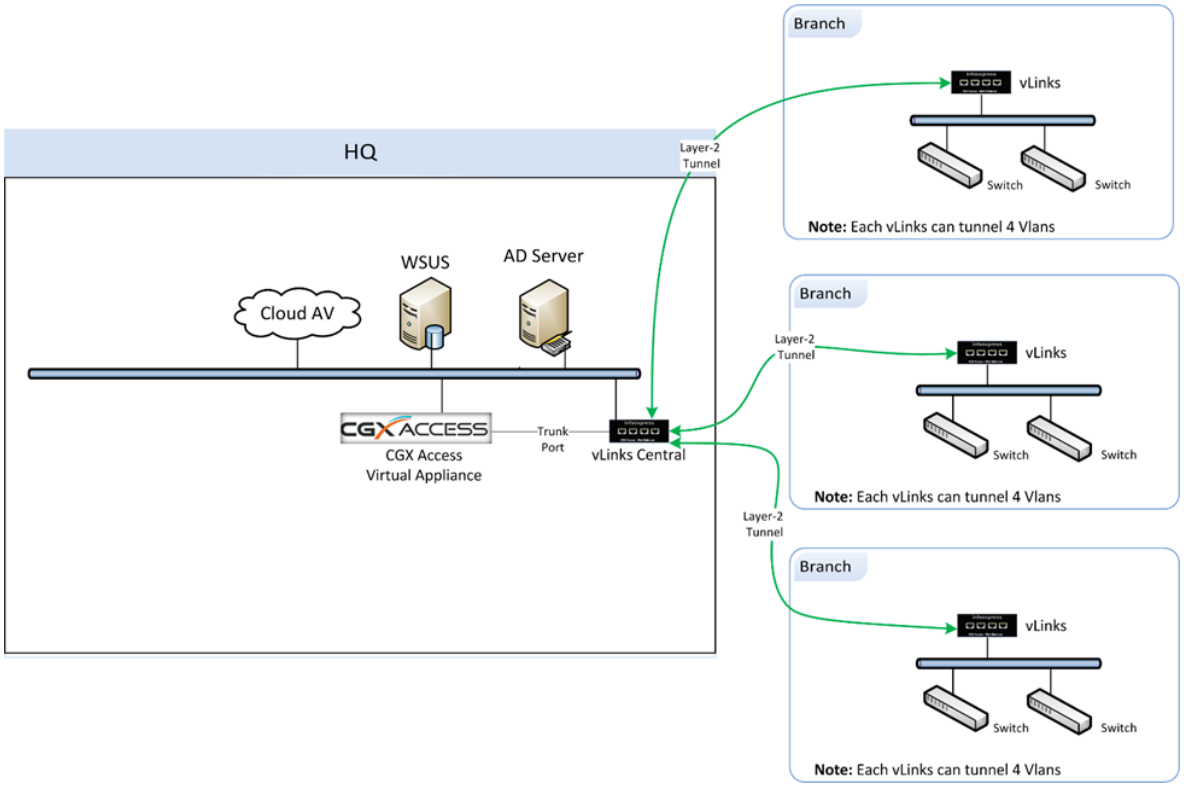
To deliver full visibility and protection, the EasyNAC Appliance requires Layer-2 visibility into the subnets it monitors. At the main site, this is typically straightforward to achieve using trunk or standard access ports. However, extending this same Layer-2 visibility to remote sites can be more complex.

The vLinks solution addresses this challenge by extending the reach of EasyNAC, enabling it to protect smaller remote locations using cost-effective hardware.

In this architecture, a vLinks appliance is deployed at each remote site to capture local Layer-2 traffic. This traffic is then encapsulated and tunneled over the existing corporate WAN to a central vLinks appliance. Because the solution leverages the existing WAN infrastructure, a pre-existing network—such as MPLS or NAT-based connectivity—is required.

At the main site, the vLinks Central appliance aggregates Layer-2 traffic from multiple remote vLinks devices and forwards it directly to the EasyNAC Appliance via a dedicated connection. With this setup, EasyNAC gains visibility into remote environments, allowing it to detect and quarantine rogue devices in real-time.

All core EasyNAC capabilities are fully supported, including compliance checks, captive portals, and Automated Threat Response.



Extending EasyNAC protection to remote sites using vLinks is a two-stage process. The first stage involves configuring the vLinks Central appliance. Once the vLinks Central is set up, the vLinks Remote appliances can then be deployed and configured to connect to EasyNAC and automatically retrieve their configurations.

© 2026 InfoExpress, Inc.

VLINKS CENTRAL SETUP

The vLinks Central appliance is built on MikroTik hardware.

To configure the device

- Download the WinBox application from https://mikrotik.com/download.
- Connect the vLinks Central appliance (adapter 1) to your PC using an RJ45 cable
- Access it via WinBox using either its MAC address or the IP address assigned through DHCP.
- The default account is admin. The default password is blank.

Perform the following steps to assign a static IP, default gateway, and admin password:

- **Configure a Static IP address** - Navigate to: IP →Addresses → Click + to Add IP address to the ether1 Interface.
- **Configure a default route** - Navigate to: IP → Routes → Click + to Add a Gateway for Dist Address 0.0.0.0/0
- **Configure a password** - Navigate to: System → Password.
- Shutdown the vLinks Central appliance and place on the network: System > Shutdown

Note: *Configurations changes made on vLinks Central take effect immediately, there are no added steps required to save the configurations.*

- **Physical Placement** - Place the vLinks Central Appliance on the production network using Adapter 1.

Model: VLC-5SM

- **Test connectivity** – Using WinBox, log in to the IP address of the EasyNAC Appliance. Navigate to: Tools → Ping to verify connectivity to the default gateway as well as any off-subnet resources.
- **Connect to EasyNAC Appliance** - Connect a second cable using Adapter 2 directly into any open port on the EasyNAC Appliance. Take note of the port used on the EasyNAC Appliance for later configuration. This is a direct connection between the vLinks Central and EasyNAC Appliance.
- Once connected to the EasyNAC Appliance, log in to the EasyNAC Appliance web interface.
- Navigate to: Configuration → vLinks Manager
- Select Add New vLinks Central and complete the registration process
- **Name** – Use any name to help you distinguish this vLinks Central from other vLinks Central you may deploy.
- **IP Address** – Use the Static IP address that was set in Step 1 above
- **Port** – Port 1194 is the recommended default port.
- **VLAN ID Range** – A 5 port vLinks Central can support 50 remote subnets, so you can configure a range of 50 VLAN IDs. You can use any VLAN range desired. To avoid confusion, we recommend these VLAN ranges be outside the range of other VLAN IDs used on your corporate network. The 12-port vLinks Central can support 200 remote subnets, and can be configured with a range of 200 VLAN IDs.
- **Username** – The default username is admin.
- **Password** – The default password in blank. It recommended you create a secure admin password.

Once saved, the above settings will be pushed to the vLinks Central server and the vLinks Central will be ready to accept connections from vLinks Remote network extenders.

VLINKS REMOTE SETUP

The vLinks Remote boxes have minimal configuration requirements. The recommended deployment technique is to leverage the Auto Configuration feature to pull the necessary configuration details from the EasyNAC server. This section will detail the steps to use the Auto Configuration method.

© 2026 InfoExpress, Inc.

- To allow Auto Configuration a Config Key must be set within the vLinks Manager.
- vLinks Remotes are configured to support DHCP by default. You can attach the vLinks Remote to any DHCP enabled network and then use the web interface to configure the Auto Configuration.
- The default account is **root.** The default password is **GlassDoor2020**.
- Configure the basic information required to sync with the EasyNAC Appliance → Navigate to: System → Auto Configuration
- Click Save & Apply
- Configure **all** auto configuration settings including the EasyNAC Appliance address and configuration key with the Static IP and prefix (the netmask).

  vLinks Name – Any name to help you distinguish this vLinks Remote from other sites

  EasyNAC – Provide the Management IP address of the EasyNAC that the vLinks Central is attached to. It will use this IP to download the auto configuration.

  Config Key – This key must match the key configured in the EasyNAC Appliance to allow the automated configuration downloads.

  IP Proto – Use this field to change to a Static IP if required. For simplified deployment, DHCP is recommended as each vLinks Remote will have the same configuration and can then be used on any network.

  NTP Server – A NTP server is critical to maintain time-sensitive tunnels with the vLinks Central.

Caution: *If time is out of sync, the connection to the vLinks Central will fail.*

  Auto DNS – It's recommended to use DNS server where available

  Static IP - When assigning a Static IP address, it will take a few extra steps to set the configuration.

- Save and Apply Changes. A message will be shown that it Failed to confirm. This is expected if the IP address has changed.



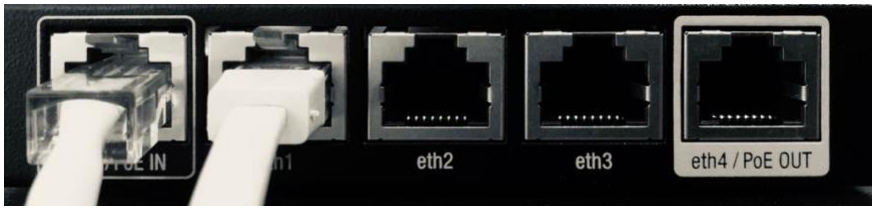
- Move the vLinks Remote to a network you can access the new IP address and login again. Verify all the Auto Configuration settings are correct. If not, set all the Auto-configuration settings, and Save and Apply again. This time a confirmation should be shown that the Configuration has been applied.

Tip: *To perform the verification, it may be useful to set a static IP on your laptop and connect directly to the vLinks remote.*

- **Physical Placement** - Place the vLinks Remote box on the remote network using Adapter 1 (eth0). Adapter 1 is used for tunneling Layer-2 traffic from the remaining 4 ports (eth1-eth4) back to the EasyNAC Appliance.



  Adapter 1 is not protected, so if this subnet needs protection, a second cable should be attached to Adapter 2 (eth1). Each vLinks Remote can protect 4 subnets.



- **Accept vLinks Remotes** - Once placed on the remote networks the vLinks Remotes will connect to the EasyNAC Appliance to request configurations.

  Configuration > vLinks Manager Click the Accept button. Once Accepted the vLinks Remote will be shown in your vLinks list.

- The last step is to configure the EasyNAC Adapter settings to protect the remote segments. On the EasyNAC Appliance take note of which adapter the vLinks Central was plugged into, during Step 7 of the vLinks Central setup.

  On the web GUI - Navigate to: Configuration > Appliance. Click the + button next to the appropriate adapter to add a VLAN

  VLAN ID – Specify any unique VLAN ID that was defined during the vLinks Central. Normally 1-50 by default. On vLinks Remote each Adapter(eth1-eth4) that is active will use a VLAN ID.

  DHCP / Static – Each adapter(eth1-eth4) will use an IP address if the port is active. If using DHCP this address will be auto assigned. If using a Static environment, the Static IP is configured in this step.

  vLinks – Use the dropdown box to select the appropriate vLinks for this remote network. If the vLinks box is not shown, confirm it has been accepted during the Auto Configuration stage.

Note: *This process repeats for each remote subnet that is be to protected. Up to 4 subnets per vLinks.*

Once network additions have been made, click the Submit button to activate changes. There will be a delay as each subnet using DHCP will requests an IP assignment.

If successful the interface displays an IP address has been obtain, and device monitoring will be active.

Navigate to: NAC > Network Map

Deployment is complete and devices from the remote sites will now be shown in the System Overview and the Device Manager, just as other devices are.

Caution: *A NTP server is critical to maintain time-sensitive tunnels with the vLinks Central. If time is out of sync, the connection to the vLinks Central will fail.*

APPENDIX E – FAILURE MODES

This appendix lists the operational behavior of EasyNAC under common failure conditions. Use it during incident response and during architecture reviews.

Failure scenario	Behavior	Operator action
Appliance unreachable from a protected subnet	Devices already trusted continue to function on the existing access. New devices on that subnet may fail to be profiled or enforced until reachability is restored.	Verify network adapter / 802.1Q trunk health; check upstream switch port; confirm the Enforcer Sensor (if used) is online.
Active Directory unreachable	Existing AD-derived tags continue to apply (cached). New AD lookups (group membership, hostname-to-user mapping) fail until AD is reachable again.	Verify DNS, AD service status, network path. Auto Trust rules that depend on AD groups are paused.
HA primary failure	The backup unit takes over within the configured failover window. Active enforcement state is preserved; in-flight traffic is not disrupted for already-trusted devices.	Verify the backup is now primary; investigate the failed unit; restore HA per the High Availability chapter.
Integration API unreachable	Tags derived from that integration become stale. Existing policy continues to enforce based on cached tag state.	Verify third-party API health; check credentials and rate-limit status; review the integration log.
CVM unreachable from a managed appliance	Local enforcement continues. Centralized policy push, roaming-device synchronization, and integration-proxy data are paused.	Verify CVM service status; check network path between appliance and CVM; review CVM logs.
Power outage at the appliance	Without HA: ARP enforcement stops; the network would be fail-open (no NAC). Existing TCP sessions continue using switch / router state. With HA: the surviving unit takes over.	For HA deployments, confirm the backup unit is operational.

© 2026 InfoExpress, Inc.

APPENDIX F – CONFIGURING THE CAPTIVE PORTAL API

This appendix describes how to configure the EasyNAC Captive Portal API together with a Microsoft Windows DHCP server, using DHCP Option 114 (IETF RFC 8910), so that modern operating system automatically detect EasyNAC captive-portal redirection and respond appropriately.

When an endpoint joins a network, DHCP Option 114 supplies the captive-portal URI. The endpoint queries the URI to determine its captive state and, if captive, presents the EasyNAC Captive Portal to the user.

PREREQUISITES

- A DHCP Server that is capable to configure DHCP Option 114
- A valid Captive Portal hostname configured on the EasyNAC Appliance, with corresponding DNS A records resolvable from client subnets.
- A trusted digital certificate installed on both the EasyNAC Appliance for the FQDN of the Captive Portal
- The device must trust the certificate authority that signed the Captive Portal certificate.

CONFIGURATION ON THE EASYNAC APPLIANCE

- Sign in to the EasyNAC management interface.
- Navigate to Configuration → Appliance Settings → Networking and configure a valid domain name and Captive Portal hostname for the appliance.
- Confirm that the Captive Portal hostname has a corresponding DNS A record published in the DNS zone used by client subnets.
- Click Save to apply the configuration.
- Navigate to Configuration → General Settings →Captive Portal Settings → Site Information
- Configure the Portal Page URL with the FQDN of the Captive Portal page over https.

> **Note:** *the URI used in the DHCP option must match the Captive Portal hostname exactly, including the path component. The default path is /ss/grm/captive-portal/api.*

CONFIGURATION ON THE WINDOWS DHCP SERVER

Define DHCP Option 114 as a predefined option on the DHCP server, then assign the option value to each scope that should advertise the Captive Portal URI.

DEFINE THE PREDEFINED OPTION

- On the server running the DHCP Server role, open the DHCP Server console (`dhcpmgmt.msc`).
- Expand the DHCP tree and select the DHCP server name.
- Right-click **IPv4** and select **Set Predefined Options**.
- In the **Predefined Options and Values** window, click **Add**.
- In the **Option Type** window, enter the following values:
    1. **Name:** Captive Portal URL
    2. **Data Type:** String
    3. **Code:** 114
    4. **Description: optional** — for example, *IETF RFC 8910 captive-portal URI*.

© 2026 InfoExpress, Inc.

- Click **OK**. The option is now defined on the DHCP server and can be applied to a specific scope.

APPLY THE OPTION VALUE TO A DHCP SCOPE

- Expand the DHCP server in the console tree and select the scope that serves the target client subnet.
- Right-click **Scope Options** under that scope and choose **Configure Options**.
- Locate **114 Captive Portal URL** in the list and select its checkbox.
- In the **String value** field, enter the full Captive Portal URI. For example:

https://portal.easynac.com/ss/grm/captive-portal/api

- Click **OK** to apply the value to the scope.
- Repeat for each additional scope that should advertise the Captive Portal URI.

VERIFICATION

- From a Windows client on the configured scope, run `ipconfig /all` or `Get-DhcpServerv4OptionValue` to confirm DHCP Option 114 is being delivered with the expected URI.
- From an Apple device on the configured scope, connect to the network. Devices that support RFC 8910 (iOS 14, iPadOS 14, macOS 11 Big Sur, and later) consume DHCP Option 114 automatically. The device probes the supplied URI and either presents the Captive Portal or proceeds to full network access depending on the response.
- Open the URI manually in a web browser to confirm the appliance returns the expected response. If the requesting device is restricted, the response payload contains:

captive: true

- If the requesting device is unrestricted, the response payload contains:

captive: false

NOTES

- A trusted server certificate must be installed on the EasyNAC Appliance, and the issuing certificate authority must be trusted by the Apple device. If the certificate chain is not trusted, the device fails the captive-portal probe and may either fall back to legacy NCSI behavior or display a certificate warning.
- DHCP Option 114 is also honored by recent Android, Windows 11, and other modern operating systems that implement RFC 8910. The procedure above therefore benefits all RFC 8910-aware clients on the affected scopes, not only Apple devices.
- For environments that do not use the Microsoft Windows DHCP Server, define the equivalent option on the third-party DHCP server (most modern DHCP implementations support custom option codes; refer to the vendor documentation for the syntax).
- The Captive Portal URI must be reachable from each client subnet and must resolve to the EasyNAC Captive Portal IP address.

© 2026 InfoExpress, Inc.

APPENDIX G – DEPLOYMENT CHECKLIST

This appendix is a phased deployment checklist for use by customer engineers and InfoExpress partners during a new EasyNAC deployment. Work through the phases in order. Each phase ends with a verification step; do not proceed to the next phase until the current phase verifies successfully. Items marked with ☐ are checkbox actions; complete and tick each one in your project records as it is performed.

Section references in this checklist point to the body chapters and other appendices of this guide. Where an item references the Hardening Checklist, complete the Hardening Checklist tasks individually rather than treating the reference as a single tick.

PHASE 1 — PRE-DEPLOYMENT PLANNING

Confirm the design before any infrastructure work begins. Capture the answers in your runbook so the deployment team can reference them throughout the engagement.

☐	Confirm the EasyNAC Appliance model based on expected device count, subnet count, and integration density (refer to the Sizing & Capacity Planning section).
☐	Document the list of subnets to be protected, including VLAN IDs and CIDR ranges.
☐	Allocate three IP addresses on the management subnet: Management IP, Captive Portal IP, Remediation Portal IP.
☐	Confirm DNS server addresses (primary and secondary) reachable from the appliance. If you use internal DNS name, please make sure it is the DNS server that can resolve internal FQDN.
☐	Confirm NTP server addresses (primary and secondary) reachable from the appliance. Time synchronization is a hard requirement.
☐	Identify the Active Directory domain controllers that will be queried, and the AD service account to be created.
☐	Identify the third-party integrations to be enabled in this phase of the deployment (full list available in the Integration Modules chapter).
☐	Confirm the licensing model and that licenses have been issued or staged.
☐	Choose one existing access port per protected VLAN or an optional 802.1Q trunk. Arrange switch administration access if a trunk must be created or adjusted.
☐	Identify the change-management window and rollback owner.

Verification: the deployment team holds a written record of each item above before any deployment work begins.

PHASE 2 — VIRTUAL MACHINE PREPARATION

Applicable to virtual-appliance deployments. Skip this phase for hardware appliances and proceed to Phase 3.

☐	Confirm the target hypervisor (VMware ESXi, Microsoft Hyper-V, Nutanix AHV/Prism, or Proxmox VE) is supported and at a release level documented in this guide.
☐	Allocate the recommended vCPU, RAM, and storage for the chosen ENAC-VM size (refer to the Appliance System Specifications table).

© 2026 InfoExpress, Inc.

☐	Obtain the EasyNAC virtual-appliance image (.ovf for VMware, .vhdx for Hyper-V, .qcow2 for Nutanix/Proxmox) from your authorised InfoExpress source.
☐	Verify the image checksum against the checksum published with the release.
☐	Access ports: map a separate virtual NIC to each protected VLAN's port group.
☐	Trunk option: configure the virtual switch or port group for VLAN tagging. Allow only the VLANs the appliance will protect.
☐	Import the virtual-appliance image into the hypervisor and create the virtual machine using the supplied template.
☐	Attach virtual NICs in the order documented for your hypervisor. Follow its 802.1Q instructions if using a trunk.
☐	Power on the virtual machine and confirm it reaches the console login prompt.

Verification: the appliance reaches the SSH/console prompt and the virtual NICs report link state Up on the hypervisor.

PHASE 3 — NETWORK PREPARATION

Verify Layer-2 access to each protected subnet and the required firewall paths.
Choose the access-port or trunk steps below for each connection.

☐	Access ports: connect a separate EasyNAC interface to each protected VLAN. Existing ports assigned to the required VLANs need no switch changes.
☐	Trunk option: use one 802.1Q port for multiple VLANs. Create or adjust the trunk only as needed and allow only the VLANs to be protected.
☐	Trunk option: use the management VLAN as the native VLAN on the Management/Trunk port. Keep untagged traffic from other VLANs off this port.
☐	Open firewall paths from the appliance to: DNS servers (UDP/TCP 53), NTP servers (UDP 123), Active Directory domain controllers (TCP 88, 389, 445, 636, 3268, 3269 as applicable), and the Captive/Remediation Portal IPs from each protected subnet.
☐	For deployments with remote Enforcer Sensors: open TCP 8889 between the appliance and each remote sensor location.
☐	For HA pairs: open the inter-appliance heartbeat ports between the primary and backup appliances per the High Availability chapter.
☐	For CVM-managed deployments: open the documented ports between each managed appliance and the CVM (refer to "Required Ports" under Central Visibility Manager).
☐	Confirm Layer-2 reachability from the appliance to each protected subnet by issuing an ARP request from the appliance console once it is configured (Phase 4).

Verification: the appliance can resolve DNS, sync NTP, and ARP-resolve a known endpoint on every protected VLAN.

PHASE 4 — INITIAL APPLIANCE CONFIGURATION

Console-driven first-boot configuration. The default IP address on factory reset is 10.0.0.250/24; connect via SSH or HDMI/keyboard to begin.

© 2026 InfoExpress, Inc.

☐	Connect to the appliance console via SSH (default IP 10.0.0.250/24) or via HDMI/keyboard.
☐	Run the setup wizard: configure timezone, hostname, and Management IP / subnet mask / default gateway.
☐	Configure DNS server addresses.
☐	Configure NTP server addresses; confirm the appliance clock synchronises within 5 minutes of starting NTP.
☐	Apply the configuration and reach the appliance management UI on its Management IP over HTTPS.
☐	Sign in to the management UI as admin/admin and immediately change the default admin password (Hardening Checklist item 1).
☐	Replace the default self-signed SSL certificate with one issued by your trusted CA (Hardening Checklist item 2).
☐	Configure the Captive Portal IP and Remediation Portal IP under Configuration → Appliance Settings → Networking.
☐	Apply the appliance license under Configuration → Appliance Settings → License Manager (or via the CVM in centrally-managed deployments).
☐	Apply the latest software update under Configuration → Appliance Settings → Server Maintenance → Software Update (Hardening Checklist item 8).

Verification: the appliance management UI is reachable over HTTPS using the new certificate, the admin password has been changed, and the version shown in About matches the latest released build.

PHASE 5 — ACTIVE DIRECTORY INTEGRATION

Configure the appliance to query Active Directory for user / group lookups, hostname-to-user mapping, and AD-joined-device tagging.

☐	In Active Directory, create a dedicated EasyNAC service account with read-only access; do not use a domain administrator account.
☐	Configure the service-account password to never expire (or document the password-rotation procedure if your policy mandates rotation).
☐	Confirm the EasyNAC service account can resolve DNS for the AD domain and reach each domain controller on the required ports (Phase 3).
☐	In EasyNAC, navigate to Configuration → General Settings → Active Directory Server.
☐	Add the AD server entry with: Hostname or IP of each domain controller, the service-account Username and Password, and the Account Suffix (UPN or pre-Win2000 form, prefixed with @).
☐	Click Test Connection and confirm a successful response.
☐	Configure the Computer-Object OUs to query if your AD environment uses non-default OUs for computer objects.
☐	Confirm a known AD-joined endpoint appears in the EasyNAC device list with an AD-joined or AD-Managed tag once the appliance is on the network (Phase 9).

Verification: the AD Test Connection returns success, and a known AD-joined test endpoint appears with the expected AD-derived tag at the next polling interval.

© 2026 InfoExpress, Inc.

PHASE 6 — NOTIFICATIONS

Configure email and (optional) Slack/Teams/WhatsApp notifications so that administrators receive alerts during and after the deployment.

☐	Configure the SMTP relay or OAuth2 mailbox under Configuration → General Settings → E-mail Server (refer to the Notifications chapter).
☐	Add notification contacts (administrator email addresses, distribution lists) under Configuration → General Settings → Contact Information for Notifications.
☐	Send a test alert and confirm delivery to each configured recipient.
☐	Configure Slack, Microsoft Teams, or WhatsApp integration if required by your operations runbook.
☐	Configure syslog forwarding to your SIEM (refer to the Orchestration with Syslog).

Verification: a test alert reaches every configured channel within 60 seconds.

PHASE 7 — POLICY CONFIGURATION

Configure the policy primitives that will govern device access. Begin in Monitor mode on every protected subnet; move to Enforce only after Phase 9 verification.

☐	Review the Default Auto Trust Policy under Policies → Auto Trust and adjust rules to match the customer environment (refer to the Enforcement Overview chapter).
☐	Define Roles & Access ACLs for each role to be assigned (Restricted, Trusted, Guest, BYOD, IoT, etc.).
☐	Define Tags for any vendor / device-class / compliance signals that will drive Auto Trust matches.
☐	Configure Time / Location / List policies if access is to be restricted by schedule, subnet, or static device list.
☐	Configure the Captive Portal site information under Configuration → General Settings → Site Information.
☐	Configure the Guest Registration template(s) under Configuration → Device Registration Templates → Guest Registration Templates.
☐	Configure the Device Registration template(s) for BYOD if required.
☐	Set every protected subnet to Monitor mode under Control → Network Map; do not enable Enforce yet.

Verification: policy rules are saved without errors, and devices on protected subnets are visible in the EasyNAC device list with profiling attributes populated.

PHASE 8 — INTEGRATION SETUP

Enable the third-party integrations identified in Phase 1. Refer to the Integration Modules chapter for vendor-specific configuration steps. The order below is the recommended deployment sequence.

☐	Active Directory: confirmed in Phase 5.

© 2026 InfoExpress, Inc.

☐	Endpoint protection / EDR (Microsoft Defender, CrowdStrike, SentinelOne, etc.): collect API credentials and configure the integration; verify managed-device tags appear on a test endpoint within the polling interval.
☐	Patch management (SCCM/WSUS, BigFix, Ivanti, Kaseya, ManageEngine): collect SQL or API credentials; verify patch-status tags on a test endpoint.
☐	MDM (Intune, Jamf, SureMDM, Headwind, Moscii): collect API or Graph credentials; verify mdm-enrolled tags on a test mobile device.
☐	Identity providers (Okta, Google Workspace): configure OAuth client; verify guest-portal sign-in flow.
☐	Vulnerability management (Tenable, SolarWinds): configure API credentials; verify vulnerability-tagged hosts appear.
☐	SIEM / log analytics (Elastic, syslog forwarders): confirm event volume in the destination matches expectations.
☐	For each enabled integration, run Test Connection and confirm the integration log records successful periodic queries.
☐	Document each integration's API credential location, owner, rotation schedule, and last-rotation date in the customer runbook.

Verification: every enabled integration shows a successful Test Connection, and at least one tag derived from each integration is visible on a test device.

PHASE 9 — PRE-CUTOVER TESTING

Validate enforcement behavior on a controlled test subnet or test VLAN before changing the production network.

☐	Identify a test subnet (a small VLAN with a known set of test devices) and switch it from Monitor to Enforce under Control → Network Map.
☐	Connect a known-compliant test device and confirm it receives full access per the Auto Trust Policy.
☐	Connect a known-non-compliant test device (for example, a device without the AV agent installed) and confirm it is restricted to the captive / remediation portal.
☐	Connect a guest device and complete the Captive Portal registration end-to-end; confirm the guest receives the expected Guest role.
☐	Connect a BYOD device and complete the Device Registration end-to-end; confirm the device receives the expected BYOD role.
☐	Trigger an integration-driven event (for example, disable AV on a test endpoint) and confirm the corresponding tag and Auto Trust action fire within the configured polling interval.
☐	For HA deployments: fail over to the backup unit and confirm enforcement continues without interruption (refer to the High Availability chapter).
☐	Capture the audit log entries for each test action and confirm they are forwarded to the SIEM.

Verification: every test scenario produces the expected outcome, and the audit log records each event correctly.

PHASE 10 — PRODUCTION CUTOVER

Move from test to production. Pace the cutover according to the customer's change-management practice; consider enforcing one subnet at a time.

© 2026 InfoExpress, Inc.

☐	Confirm the change window with the customer; obtain the rollback owner's sign-off.
☐	In Control → Network Map, switch each production subnet from Monitor to Enforce on the agreed schedule.
☐	After each subnet transitions to Enforce, monitor the EasyNAC device list and the helpdesk channel for unexpected restrictions for at least 30 minutes.
☐	If unexpected restrictions occur, switch the affected subnet back to Monitor, investigate, then re-attempt.
☐	Once all production subnets are in Enforce, confirm Auto Trust still produces the expected outcomes for guest, BYOD, contractor, and AD-joined classifications.
☐	Notify the customer's service desk that EasyNAC is now in production and provide the escalation contact for InfoExpress Support.

Verification: all production subnets are in Enforce mode, and the device count, role distribution, and audit-log volume match the projections from Phase 1.

PHASE 11 — POST-DEPLOYMENT HARDENING

Complete the Hardening Checklist (separate chapter) and capture the customer-facing operational handover.

☐	Complete each Hardening Checklist item that has not already been addressed in earlier phases (default credentials, SSH access restriction, RADIUS/SAML/2FA admin authentication, log retention, backup destinations, NTP, software update, default Auto Trust review, Permission Manager review, recovery procedures).
☐	Configure local and remote backup destinations under Configuration → Appliance Settings → Backup and Restore; enable Automatic Backup.
☐	Trigger a manual backup and confirm a successful copy lands in both destinations.
☐	Confirm log retention is configured to the customer's compliance window (default 30 days for audit logs and 90 days for device records, increase if required).
☐	Document the operational runbook: backup location, license owner, escalation contacts, integration-credential rotation schedule, and recovery procedure.
☐	Hand the runbook to the customer's operations team; archive a copy with InfoExpress.

Verification: the Hardening Checklist is fully signed off, an automatic backup has succeeded to both destinations, and the customer's operations team holds a copy of the runbook.

At completion of Phase 11, the deployment is in production and ready for routine operation. Schedule a 30-day post-deployment review with the customer to confirm tag accuracy, integration health, and any policy adjustments uncovered during the first month of production.

© 2026 InfoExpress, Inc.

APPENDIX H – GLOSSARY

Acronyms and product-specific terms used in this guide. Where a term has a generic industry meaning and an EasyNAC-specific use, both are noted.

- **ACL** — Access Control List — a rule set that defines permitted and denied traffic by source, destination, port, and protocol. EasyNAC applies ACLs through the Roles & Access policy.
- **AD** — Active Directory — Microsoft's directory service. EasyNAC integrates with AD for user / group lookups, hostname-to-user mapping, and authenticated-device tagging.
- **ARP** — Address Resolution Protocol — the IPv4 protocol that maps IP addresses to MAC addresses. EasyNAC enforces network access by injecting ARP traffic onto the protected subnet.
- **Auto Trust Policy** — EasyNAC's primary device-to-role mapping policy. Each rule matches device conditions (tags, OS, IP, etc.) and assigns or changes the device's role.
- **BYOD** — Bring Your Own Device — employee- or student-owned devices that connect to a corporate or institutional network.
- **Captive Portal** — A web page presented to a device before it is granted full network access. EasyNAC uses captive portals for guest registration and for device remediation.
- **CGPM** — CyberGateKeeper Policy Manager — the Windows-side editor for compliance policies executed by EasyNAC agents.
- **CGX / CGX-Access** — Legacy product name for the EasyNAC Appliance. May appear in older documentation, in the appliance UI, and in network-side configuration. Use the canonical name "EasyNAC Appliance" in new deployments.
- **CVM** — Central Visibility Manager — a separate EasyNAC component that provides cross-appliance reporting, tag synchronization, and centralized integration proxy for multi-site deployments.
- **DHCP** — Dynamic Host Configuration Protocol — the protocol used to allocate IP addresses to network devices. EasyNAC uses DHCP traffic for passive device profiling.
- **Enforcer Sensor** — A lightweight EasyNAC component deployed at a remote site that extends ARP enforcement to a subnet not directly reachable at Layer-2 from the central appliance.
- **HA** — High Availability — a deployment pattern where two appliances are paired; one is primary, the other is standby. Failover is automatic.
- **IPS** — Intrusion Prevention System.
- **MAB** — MAC Authentication Bypass — a fallback authentication mechanism on switches and wireless controllers where the device's MAC address is treated as its identity.
- **MDM** — Mobile Device Management — a class of tools that manage mobile and (often) endpoint devices. EasyNAC integrates with several MDM products.
- **MFA** — Multi-Factor Authentication — any combination of two or more authentication factors. TOTP and SAML SSO are supported for the EasyNAC management interface.
- **NAC** — Network Access Control — the product category to which EasyNAC belongs. NAC products determine which devices may connect to a network and at what level of access.
- **NPS** — Network Policy Server — Microsoft's RADIUS implementation. EasyNAC supports NPS for management-interface authentication and for BYOD authentication scenarios.
- **OAuth2** — An authorization framework. Used by EasyNAC for Microsoft Graph and Google Workspace integrations.
- **OIDC** — OpenID Connect — an identity layer on top of OAuth2. Not directly supported as a management-interface SSO mechanism; use SAML 2.0 instead.
- **RADIUS** — Remote Authentication Dial-In User Service — a network authentication protocol. EasyNAC can act as a RADIUS proxy (Appendix B) and as a RADIUS client for management-interface authentication.

© 2026 InfoExpress, Inc.

- **RBAC** — Role-Based Access Control — a model where users are assigned roles that grant specific permissions. The EasyNAC Permission Manager implements RBAC for the management interface.
- **Roles & Access Policy** — EasyNAC's ACL- and VLAN-application policy. Each role defined here has an associated ACL or VLAN that is applied when Auto Trust assigns the role to a device.
- **SAML** — Security Assertion Markup Language — a single sign-on protocol. Supported for EasyNAC management-interface authentication.
- **SIEM** — Security Information and Event Management — a centralized log-collection and analysis platform.
- **SOAR** — Security Orchestration, Automation and Response — a platform that automates security playbooks. EasyNAC integrates with SOAR via its API and orchestration events.
- **SSO** — Single Sign-On.
- **SSL/TLS** — The encryption protocols used for HTTPS. The EasyNAC management interface, Captive Portal, and remediation portal are served over HTTPS.
- **TOTP** — Time-based One-Time Password — the authentication-app token format (RFC 6238).
- **VLAN** — Virtual Local Area Network — a Layer-2 segmentation primitive on Ethernet networks.
- **vLinks** — A separately-licensed EasyNAC component that extends Layer-2 visibility to remote sites over a corporate WAN. See Appendix D.
- **VPN** — Virtual Private Network.
- **WMI** — Windows Management Instrumentation — Microsoft's management API. EasyNAC uses WMI for AD-joined Windows endpoint information.
- **XDR** — Extended Detection and Response — a class of security products that correlate signals across endpoint, network, and other sources.

© 2026 InfoExpress, Inc.