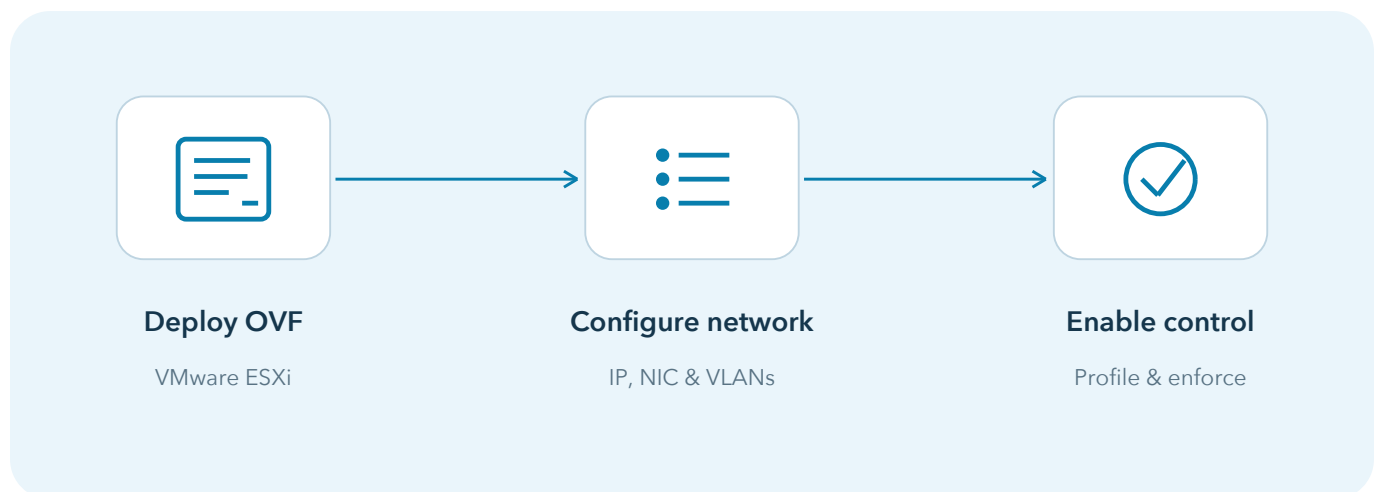


SIMPLE CONTROL, STRONG SECURITY

EasyNAC Quick Start VMware ESXi

Virtual appliance deployment guide.

Deploy the OVF, configure management and protected VLANs, then verify visibility and enforcement.



IN THIS GUIDE

Pre-deployment / VMware setup / Network configuration
Integrations / Device policy / Enforcement / Troubleshooting

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.

1. Overview

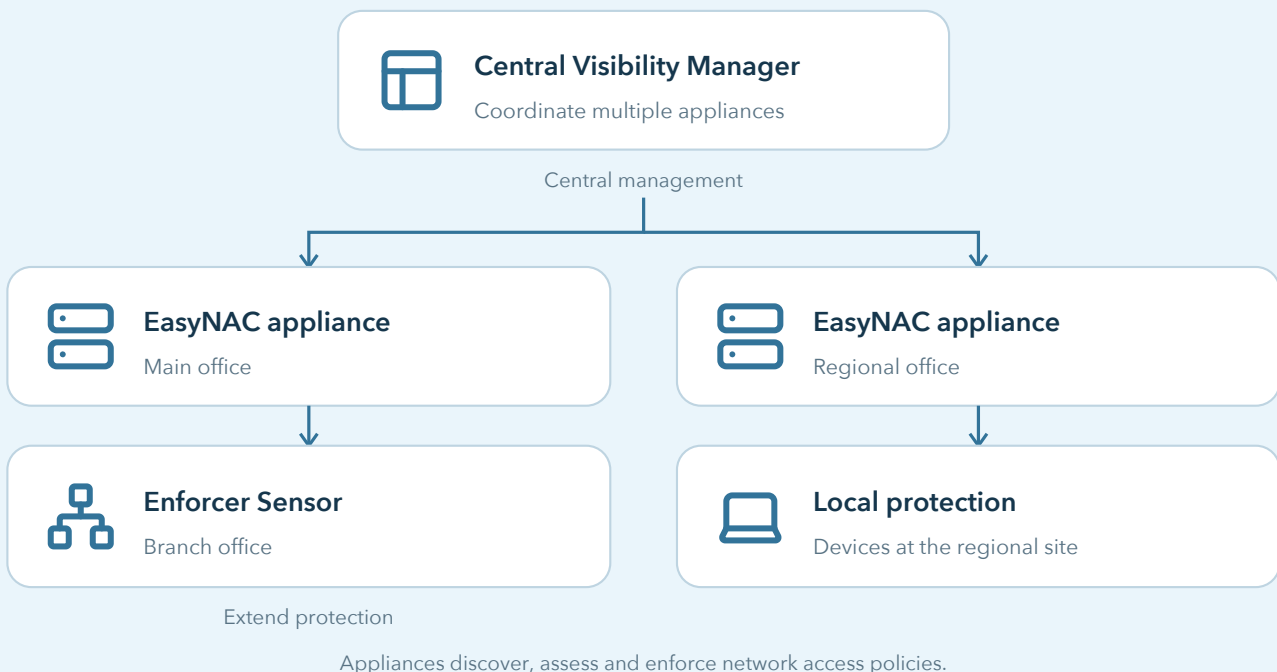
This quick start brings an EasyNAC virtual appliance from import to a healthy day-one state on VMware ESXi. EasyNAC is an out-of-band NAC appliance: it enforces access by participating in the ARP layer of each protected subnet rather than sitting in the data path.

Layer-2 visibility

Because enforcement uses ARP, EasyNAC must have Layer-2 reachability into every subnet it protects. At the main site, this is achieved through a direct adapter or an 802.1Q trunk. Subnets that are reachable only at Layer-3, across a router, MPLS link, or VPN, cannot be enforced from the central appliance. To extend protection to those subnets, deploy either a dedicated EasyNAC appliance at the remote site or an Enforcer Sensor (see Section 7).

HA pairs, Central Visibility Manager (CVM), profiling tuning, integrations beyond Active Directory, and the EasyNAC Compliance Agent are outside this quick start. Refer to the EasyNAC Installation and Configuration Guide for those topics.

One system. Three complementary roles.



2. Pre-deployment checklist and sizing

Prerequisites

- Hypervisor host: VMware ESXi with access to vCenter or the standalone Host Client, and permission to deploy an OVF template.
- Software: EasyNAC virtual-appliance image (.ovf, typically delivered inside a compressed .zip). Download from support.infoexpress.com. An authorized support account is required; contact InfoExpress or your business partner to request one.
- Network: management VLAN reachable from the host; for multiple protected VLANs, an 802.1Q trunk on the upstream switch allowing those VLANs; DNS, default gateway, and NTP reachable from the management subnet.
- Active Directory (optional, typical): domain-controller host/IP, a read-only AD service account, and an account suffix beginning with @, for example @corp.example.com.

- Optional: wildcard or SAN certificate covering Management, Captive Portal, and Remediation Portal FQDNs; SMTP, M365 OAuth2, or Google Workspace OAuth2 credentials for notifications.

IP addresses required

Three IPs minimum on the management subnet, plus one IP per additional protected VLAN.

IP	Purpose
Management IP	Web UI / SSH access; communication with AD.
Captive Portal IP	Landing page for unauthenticated devices. Must be reachable from every protected subnet.
Remediation Portal IP	Page shown to non-compliant devices. Hosted on its own IP, separate from the other two.
Per-VLAN IP (each)	Static or DHCP; one per additional protected VLAN.

VM capacity (ENAC-VM virtual appliance)

The ENAC-VM virtual appliance has the following supported capacities. Figures are approximate and depend on protected VLANs, endpoints, and enabled features. Plan production load at approximately 70% of these maxima to absorb spikes.

Capacity / capability	ENAC-VM
Maximum devices	10,000
Maximum protected subnets	400
Virtual NICs (pre-provisioned)	10
Out-of-band ARP enforcement	Yes
Inline (VPN) enforcement	Yes
802.1Q VLAN trunking	Yes
High Availability (paired)	Yes

VM resource allocation

Pick the row matching your expected device count. The 1,000+ and 5,000+ tiers carry additional vCPU headroom to support dense integrations and active NMAP profiling. Provision at the next tier up if you expect rapid growth.

Tier	vCPU	RAM	Storage
100+ devices	2 vCPU	4 GB	40 GB - 512 GB
500+ devices	4 vCPU	8 GB	40 GB - 512 GB
1,000+ devices	8 vCPU	16 GB	40 GB - 512 GB
5,000+ devices	16 vCPU	32 GB	40 GB - 512 GB

Note: A minimum of 8 GB RAM is recommended for optimal performance. Confirm allocation with InfoExpress or your authorized business partner for High Availability, multiple integrations, or sustained operation above 70% of the device-count maximum.

3. Deploy the appliance on VMware ESXi

EasyNAC for VMware ships as an OVF template inside a compressed .zip. Once deployed, the appliance runs on its bundled Linux OS; no additional software installation is required.

Choose the OVF deployment path

- Host managed by vCenter: sign in to the vSphere Client through vCenter. Right-click the target host or cluster and select Deploy OVF Template.
- Standalone host with the older Host Client (ESXi 7/8 or ESX 9.0): open Virtual Machines, select New Virtual Machine, then choose the option to deploy from an OVF or OVA file.
- Standalone ESX 9.1 host: in the Host Client, select Host > Actions > Deploy OVF Template. The OVF option is no longer under New Virtual Machine.

Complete the deployment wizard

1. Extract the .zip locally and sign in to the applicable client in a browser. Open Deploy OVF Template using the path above.
2. Choose Local file, browse to the OVF, and click Next. Review template details; an “unsigned template” warning is expected. Continue.
3. Enter a VM name, for example EasyNAC-3.2; select the compute resource and datastore; choose thin or thick provisioning.
4. Configure network mappings for each EasyNAC interface. Select the correct port groups or distributed switches. Click Next, review, and Finish.
5. When the deploy task completes, power on the VM and open the console. The appliance boots into the EasyNAC console menu in a minute or two.

Note: Verify CPU, memory, and disk before powering on. Confirm the sizing tier with InfoExpress if unsure.

4. First-boot console setup

Open the VM console from the hypervisor and let the system finish booting. The Management IP must be set with the setup wizard before the web UI is reachable. SSH access becomes available once that IP is configured.

Default accounts: admin for web UI, SSH, and console maintenance; cguser for SFTP uploads only. Default passwords match the usernames. Change both during setup.

Important: Store the new admin password securely. If it is lost and no alternate administrative account is available, recovery may not be possible.

Run the setup wizard

1. At the console prompt, log in as admin / admin.
2. From the main menu, enter 1 (Run Setup Wizard) and press Enter.
3. Step through Time zone, Date and Time, Management IP, Subnet Mask, Default Gateway, DNS, and Hostname.
4. Verify connectivity by pinging the Management IP from the same subnet and from a different subnet.

5. Web UI initial configuration

Open <https://<Management-IP>/> in a recent browser (Edge, Chrome, Firefox, or Safari) and log in as admin. The default self-signed certificate produces a browser warning at this stage.

Captive and Remediation Portal IPs

The Captive Portal is shown to unauthenticated devices; the Remediation Portal is shown to non-compliant devices. Each is hosted on its own IP, separate from Management and from each other, and must be reachable by every protected subnet.

1. Navigate to Configuration > Appliance Settings > Networking.
2. Enter the Captive Portal IP / Subnet Mask, for example 10.0.0.251 / 255.255.255.0, and click Submit Landing Pages.
3. Repeat for the Remediation Portal IP using the same path.

The screenshot shows the 'Server Maintenance' section on the left sidebar. The main content area is divided into two sections: 'DNS & Domain Name' and 'Landing Pages'.

DNS & Domain Name:

DNS Servers	8.8.8.8
Hostname	eznac
Domain Name	

Submit DNS & Domain Name

Landing Pages:

Support NAT'd	☐	
Host Name for Captive Portal		
Captive Portal's IP Address	192.168.88.35/255.255.255.0	Adapter #1 ▼
Host Name for Remediation Portal		
Remediation Portal's IP Address	192.168.88.36/255.255.255.0	Adapter #1 ▼

Submit Landing Pages

Replace the self-signed certificate (optional)

Go to Configuration > Appliance Settings > Server Maintenance > SSL Certificate Manager > Manage. Generate a Private Key and CSR, have your CA sign it, and upload the signed certificate; or upload a certificate and private key directly. A wildcard or SAN certificate covering all three FQDNs is recommended. Reboot the appliance for the new certificate to take effect.

Connect to Active Directory

1. Configuration > General Settings > Active Directory Servers. Enter DC host/IP and Account Suffix (for example @corp.example.com; @ is mandatory). Use a read-only service account.
2. Click Test LDAP Connection; resolve errors before saving.
3. Configuration > Integration > Active Directory Integration. Tick Enable Integration and Tag devices that are domain computers.

Tip: AD integration auto-identifies domain-joined devices as AD-managed and grants them full network access. Up to 20 AD servers per appliance.

6. Add additional VLANs via 802.1Q

To protect more than one subnet, attach EasyNAC to an 802.1Q trunk port group, then add VLANs inside the EasyNAC web UI. Standard vSwitch and Distributed Switch (VDS) configure trunking differently. Use the path that matches your environment.

Upstream switch trunk (Cisco IOS example)

```
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
```

Option A - Standard vSwitch

1. vSphere Client > Host > Configure > Networking > Virtual switches.
2. Edit or add the port group used by the EasyNAC trunk interface.
3. Set VLAN ID = 4095. On a Standard vSwitch, this special value trunks all VLANs (0-4094).
4. On the port group Security policy, set Promiscuous mode = Accept and Forged transmits = Accept. Save.
5. Assign the EasyNAC virtual appliance interface to this port group.

Option B - vSphere Distributed Switch (VDS)

VDS does not use VLAN ID 4095. The Distributed Port Group has a VLAN type selector with a separate VLAN trunking mode.

1. vSphere Client > Networking > select the Distributed Switch > New Distributed Port Group, or edit an existing one.
2. On the VLAN page, set VLAN type = VLAN trunking.
3. Set the VLAN trunk range to the VLANs to allow, for example 2,3,5,100, or 0-4094 for all VLANs.
4. On the Security policy, set Promiscuous mode = Accept and Forged transmits = Accept. MAC address changes = Accept is also recommended. Save.
5. Assign the EasyNAC trunk interface to this Distributed Port Group.

Note: Choose VLAN type "VLAN" only if a single VLAN is needed on that adapter. For trunking multiple VLANs from EasyNAC, "VLAN trunking" is required.

Why these security settings: Promiscuous mode lets the EasyNAC adapter receive every frame on the port group, which is required to see all VLAN traffic. Forged transmits lets the adapter send ARP responses with non-original MACs, which is how ARP-based enforcement quarantines untrusted endpoints. Without both settings, ARP enforcement can silently fail: the appliance appears healthy but cannot block.

Add the VLAN in EasyNAC

1. Configuration > Appliance Settings > Networking > click + on the trunk adapter.
2. Enter the VLAN ID and a static IP / mask, or DHCP. Optionally set a Location label.
3. Click Submit Network Changes. Do not modify Metric; it is set automatically.

System Configuration > Networking 

Networking

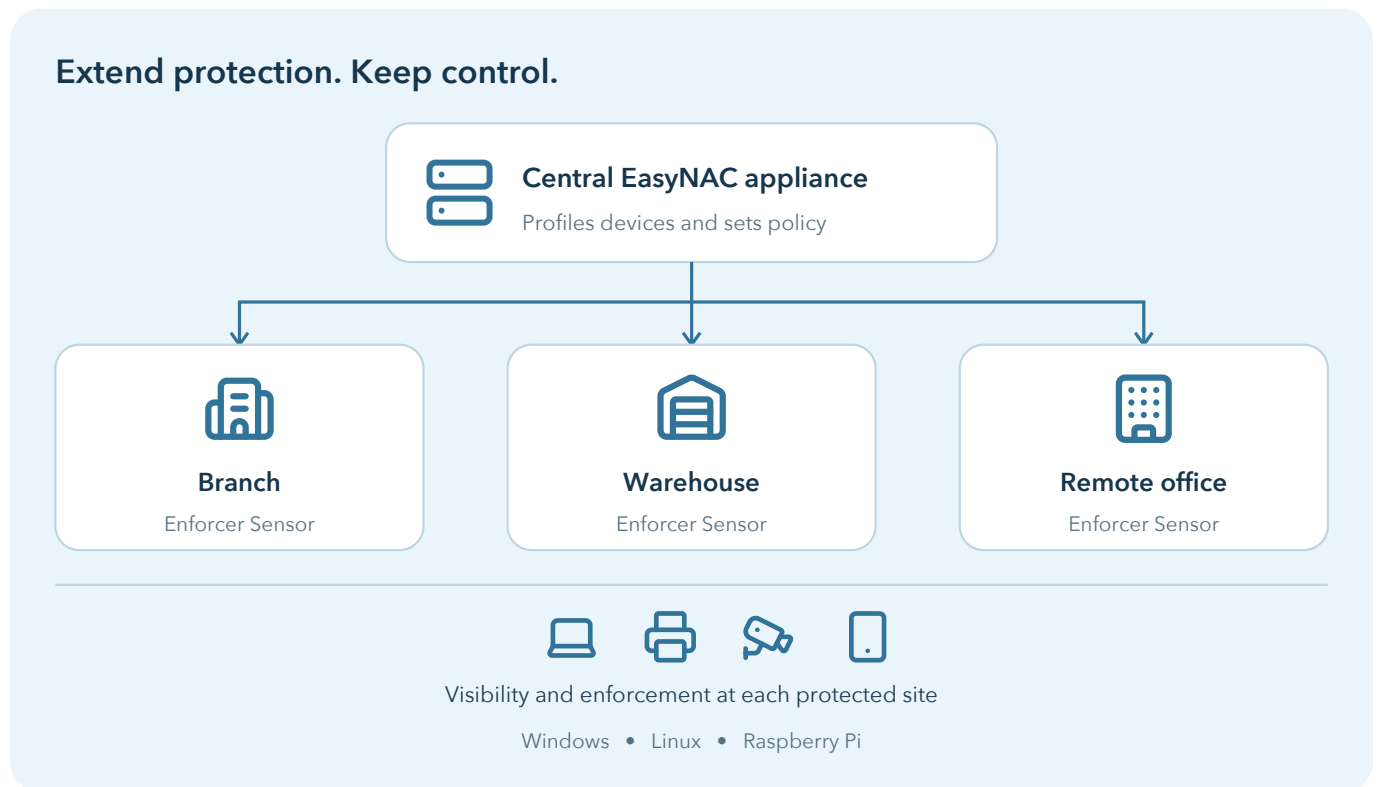
Adapters	IP / Netmask	Gateway	Metric	VLAN ID	Location	Configuration	State	VLAN
Adapter #1 MAC: 00:0c:29:87:c4:52 Speed: 1 Gb/s	192.168.88.34/255.255.255.0	192.168.88.1	100			Managed IP		
Adapter #2 MAC: 00:0c:29:87:c4:5c Speed: 1 Gb/s	/		500			Off		
	192.168.200.10/255.255.255.0	192.168.200.1	5200	200		Static IP		
Submit Network Changes Show Additional Adapters								

7. Extend protection to remote branches

When VLANs do not span back to the main site, deploying a full appliance at every branch is rarely cost-effective. The Enforcer Sensor extends EasyNAC visibility and enforcement to remote subnets without requiring a full appliance per site.

How it works

An Enforcer Sensor installed on the remote subnet reports devices it sees to the central EasyNAC Appliance over TCP/8889. The central appliance profiles those devices and computes policy decisions; the sensor enforces those decisions locally using ARP. The central appliance remains the policy source of truth.



Supported platforms

Platform	Hardware	Recommended scope
Windows 10+ (64-bit)	Dual-core CPU / 4 GB RAM	10 subnets / 300 devices
Linux (Ubuntu 24.04+, AlmaLinux, Debian, Rocky; x86_64)	Dual-core CPU / 4 GB RAM	25 subnets / 500 devices
Raspberry Pi (4 or 5)	EasyNAC Raspberry Pi OS / 4 GB RAM / 64 GB SD	10 subnets / 300 devices

Network and licensing requirements

- TCP port 8889 must be open and reachable from the Enforcer Sensor to the central EasyNAC Appliance.
- Sensors are compatible with EasyNAC Appliance versions 3.1.220317 and above.
- Both MPLS and NAT environments are supported. In NAT environments, profiling depth is reduced because the central appliance cannot fully profile devices behind NAT, and a Restricted ACL entry must permit traffic to the Captive Portal via the sensor.
- Enforcer Sensors are licensed separately from the central appliance.

Deployment flow

1. Obtain the Enforcer Sensor installer from your InfoExpress partner, representative, or support.infoexpress.com.
2. Install on the chosen Windows or Linux host, or write the Raspberry Pi image to an SD card and boot the device on the remote subnet.
3. On the central appliance, navigate to Control > Enforcer Sensors. The new sensor appears as a pending connection identified by its IP address.
4. Click Accept; optionally enter a Location label to identify the site or subnet.
5. After approval, the sensor status changes to Active and the monitored subnet appears under Control > Network Map flagged as an Enforcer.

Note: If the central appliance uses a customized shared-settings configuration with the EasyNAC Compliance Agent, generate a compatible Enforcer Sensor package using the EasyNAC (CyberGateKeeper) Policy Manager rather than the default installer.

8. Notifications and alerting

Configure SMTP and at least one notification contact so EasyNAC can send alerts when policies trigger or guests register. Without these, e-mail alerts and scheduled reports will not be delivered.

SMTP server

1. Configuration > General Settings > E-mail Server.
2. Enter the SMTP host, port, and authentication credentials. Set the sender address; optionally set BCC recipients to copy on guest-registration emails.
3. Click Save and use the test option to confirm delivery.

Microsoft 365 OAuth2 mail is also supported under the same menu if SMTP is unavailable in your environment.

Notification contacts

1. Configuration > General Settings > Contact Information for Notifications.
2. Add at least one administrative contact. This contact receives event alerts (Auto Trust, Roles & Access, Monitoring policies, Device Profiling) and scheduled reports.

Note: The sender address must use a valid and trusted domain configured on your mail server. Mismatched or unrecognized sender domains may be silently dropped by upstream mail relays.

9. Integrate with endpoint security

EasyNAC integrates with endpoint platforms to identify managed devices, validate posture (signature age, real-time protection state, missing patches), and quarantine non-compliant endpoints. Each integration is configured under Configuration > Integration.

Source scope: The 33 supported integrations listed below are reproduced from the supplied EasyNAC Installation and Configuration Guide (Integration Modules chapter). Refer to that guide for per-vendor prerequisites and procedures.

Supported integrations

Category	Platforms
EDR / XDR (9)	Carbon Black Cb Response, Carbon Black Cloud, CrowdStrike, Cybereason, Elastic, Microsoft Defender, Palo Alto Cortex XDR, SentinelOne, Trellix Endpoint Security HX (formerly FireEye HX)
EPP / Antivirus (8)	Bitdefender, ESET Antivirus, Kaspersky Antivirus, Sophos (Enterprise Console and Sophos Central), Symantec Endpoint Protection Manager 14.x, Trellix ePolicy Orchestrator, Trend Micro (OfficeScan, Apex Central, Vision One), Webroot
Endpoint management / patching (8)	HCL BigFix, Ivanti Security Controls, Kaseya VSA, ManageEngine Desktop Central, ManageEngine Patch Manager, Microsoft SCCM / WSUS, Microsoft Windows Management Instrumentation (WMI), SolarWinds Observability
Mobile device management (5)	Headwind MDM, Jamf, Microsoft Intune, Moscii StarCat, Sure MDM (42Gears)
Identity / IAM (2)	Google Workspace, Okta
Vulnerability (1)	Tenable Vulnerability Management

Configuration pattern

1. Configuration > Integration > select the platform.
2. Provide connection details (URL, API key, or service-account credentials). Click Test.
3. Once verified, EasyNAC begins polling and tags devices accordingly. Tags become available as conditions in Auto Trust Policy and Roles & Access.

Tip: Start with a single integration that already covers most of your endpoint estate, for example CrowdStrike, Defender, or Sophos Central. Confirm tag synchronization before adding another.

10. Profile, tag, and allow-list devices

Visibility is the foundation of every other control in EasyNAC. Before a device can be trusted, restricted, or grouped into a policy, the appliance must know what it is. This section covers profiling, Device Profiler rules, and per-device Allowlist / Blocklist overrides.

How profiling works

When EasyNAC detects a new endpoint on a protected subnet, it builds a profile by combining agentless techniques. Each runs without modification to the endpoint.

Technique	Default	What it contributes
Passive DHCP	On	OS family from DHCP DISCOVER fingerprint (Windows, macOS, iOS, Android, Linux). Built-in database covers typical end-user devices.
Fingerbank	Optional	Cloud DHCP database of 35,000+ devices (free tier: 300 queries/hour). Recommended for IoT classification of printers, cameras, sensors, and other non-standard devices.
NMAP	On (every 24h)	Active scan: OS detection, open ports, and web-server banner grab. Can be disabled per subnet under Control > Network Map.
UPnP	On (every 5 min)	Lightweight active scan: OS and hostname from UPnP-enabled IoT devices.
SNMP	Off	Active query against switches and access points to identify each device's switch and port. Strengthens MAC-spoofing detection. Supported on 3COM, Aruba, Cisco, F5, Fortinet, H3C, HP, Huawei, Juniper, Meraki, Mikrotik, Palo Alto, Sonicwall, TP-Link, VMware.

Active Directory and integrated endpoint security platforms (configured in Sections 5 and 9) feed additional attributes into the same device record, including domain-joined state, AV coverage, EDR sensor health, and patch level. These become available as policy conditions.

From profile to policy

Profile data drives policy in three stages:

1. Profiling: EasyNAC fingerprints each device and stores attributes such as OS, hostname, MAC OUI, open ports, AD state, and AV state.
2. Tagging: Device Profiler rules evaluate those attributes and apply tags, for example printer, ip-camera, byod-laptop, or AV-managed.
3. Policy: Auto Trust Policy and Roles & Access reference the tags to grant access, apply an ACL, or assign a VLAN.

This separation matters: a tag survives changes in low-level profile detail. A device tagged “printer” stays printer-class even if its IP or hostname changes; policy only needs to read the tag.

Custom Device Profiler rules (typical for IoT classes)

1. Policies > Device Profiler.
2. Click Add Rule.
3. Add Conditions on profile attributes. Multiple conditions use AND logic. Examples: OS contains “printer”; DHCP fingerprint matches a known camera vendor; MAC OUI belongs to a known device family.
4. Add Actions, typically Set Tag (for example tag = printer or ip-camera).
5. Click Activate Policies.

Adjust Auto Trust Policy to grant the appropriate access level to devices carrying the new tags.

Allowlist / Blocklist (per-device override)

Custom rules and tags suit classes of devices. For individual exceptions, such as a vendor laptop on a short engagement, a known-bad rogue endpoint, or a temporarily tolerated test machine, use the per-device controls in Device Manager. These bypass Auto Trust Policy entirely.

In the Device Manager row, the ON / OFF / Auto control sets per-device behavior:

- ON - Allowlist. Full Access regardless of policy.
- OFF - Blocklist. Restricted regardless of policy.
- Auto - access follows Auto Trust Policy (the default and recommended setting).

Bulk allow / block

1. Device Manager > select the target devices.
2. Action > Add to list > Allowlist (or Blocklist).
3. Choose Permanent or set an expiration period. Expiration is recommended for temporary access.
4. Click Apply to selected devices.

11. Enable enforcement

New subnets default to monitoring mode. EasyNAC observes and profiles devices but does not block. Once integrations are connected and IoT devices are tagged, enable enforcement subnet by subnet. A status banner across the top of the management console flags any subnet still in monitoring mode.

Switch from monitoring to enforcement

1. Control > Network Map.
2. Identify the subnet to enforce.
3. Toggle the subnet to Enforcement mode.

4. Allow a few minutes for enforcement to take effect after first enabling it.

Verify enforcement

- In Device Manager, confirm the access role assigned to managed devices is Full Access, typical for AD-managed and tagged devices.
- From a Full Access device, test connectivity to the resources it should reach.
- From a Blocklisted or untrusted device, confirm it is quarantined. If a Captive Portal is configured, opening a browser should redirect to the EasyNAC landing page.
- Optionally bring an unmanaged device onto a protected subnet and confirm classification and enforcement behavior.

Recommended: Enable enforcement on a small set of test VLANs first. Monitor for false positives over a day or two before broadening to the rest of the estate.

12. Troubleshoot and go further

Common issues

Symptom	Likely cause / fix
Cannot reach Management IP	Wrong virtual switch or port group, or upstream port not on management VLAN. Recheck both; rerun the setup wizard if IP must change.
Severe certificate warning	Default self-signed certificate. Replace via Configuration > Appliance Settings > Server Maintenance > SSL Certificate Manager; reboot to apply.
Test LDAP Connection fails	Account suffix missing @, expired service-account password, AD server unreachable from management subnet, or firewall blocking LDAP/LDAPS.
Captive Portal does not redirect	Portal IP is not within the protected subnet, or is blocked by an upstream ACL. Each protected subnet must have Layer-2 reachability to the portal IPs.
Devices on tagged VLAN not seen	Verify the VMware port group has VLAN ID 4095 (or correct distributed port-group VLAN range), and the upstream switch port allows the VLAN.
Enforcement appears active in UI but devices are not blocked	Verify the VMware port group has Promiscuous mode = Accept and Forged transmits = Accept. Without these, ARP enforcement silently fails.
Profiling slow or incomplete	Active NMAP profiling adds load. Stay within approximately 70% of supported maxima; engage InfoExpress Support for sizing review if combined with many integrations.

What to do next

Typical next steps once the appliance is healthy. Refer to the EasyNAC Installation and Configuration Guide for full procedures.

- Design the Auto Trust Policy and Roles & Access mapping; move from monitoring to enforcement on a small set of test VLANs first.
- Tune Device Profiling Policies (DHCP, Fingerbank, NMAP, UPnP, SNMP) and add notifications (SMTP, M365, Google Workspace, Teams, Slack, or WhatsApp).
- Add integrations (EDR, MDM, vulnerability scanner) and confirm tag synchronization.
- For resilience, plan an HA pair; for multi-site, add Enforcer Sensors at Layer-2-isolated subnets or a Central Visibility Manager.
- Deploy the EasyNAC Compliance Agent if you need faster posture assessment, pop-up messaging, or auto-remediation on endpoints.