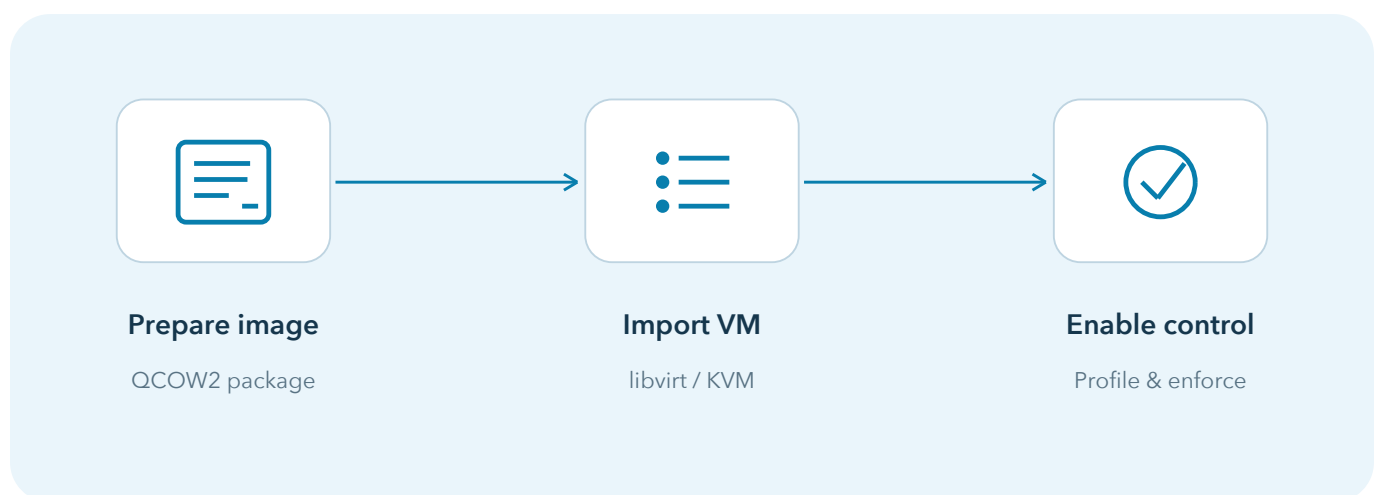


SIMPLE CONTROL, STRONG SECURITY

EasyNAC Quick Start Oracle Linux KVM

Virtual appliance deployment guide.

Import the EasyNAC QCOW2 image, connect management and protected VLANs, then verify visibility and enforcement.



IN THIS GUIDE

Pre-deployment / KVM import / 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

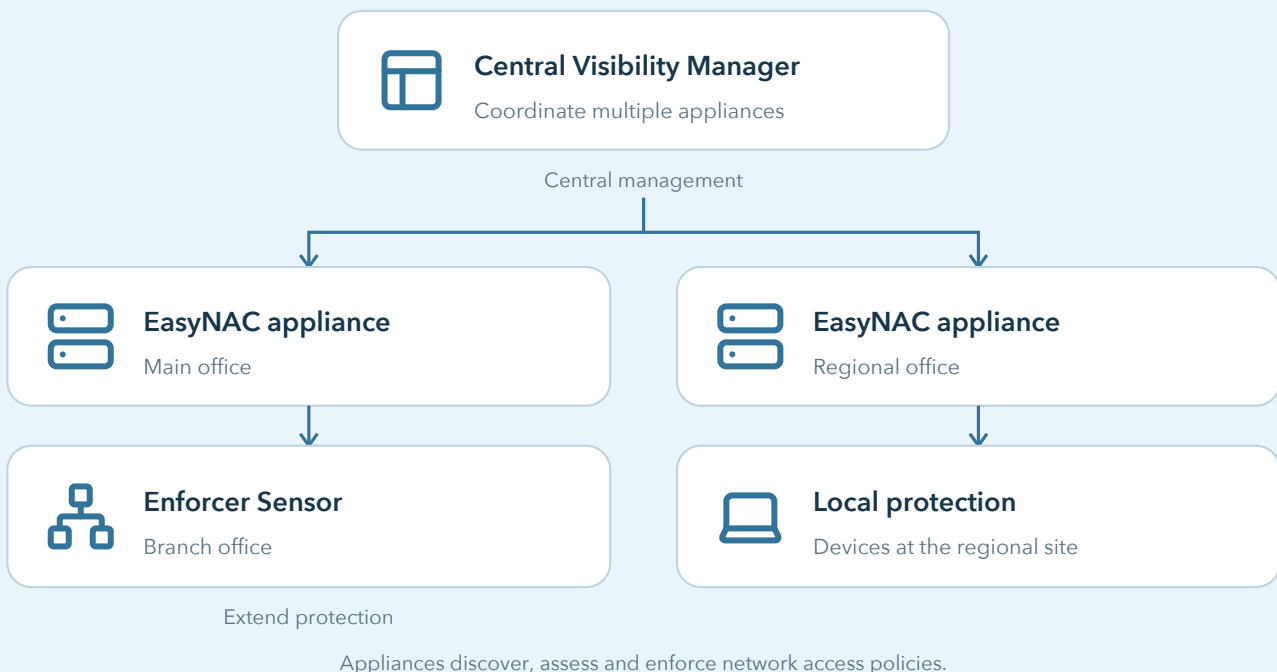
This quick start brings an EasyNAC virtual appliance from QCOW2 import to a healthy day-one state on Oracle Linux KVM. EasyNAC is an out-of-band NAC appliance: it enforces access by participating in the ARP layer of each protected subnet rather than sitting in the data path.

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).

This guide covers initial deployment and validation. For high availability, Central Visibility Manager (CVM), advanced profiling and compliance workflows, use the EasyNAC Installation and Configuration Guide.

One system. Three complementary roles.



2. Pre-deployment checklist and sizing

Prerequisites

- Hypervisor host: Oracle Linux 8 or 9 with libvirt/KVM, virsh and/or virt-manager, and a production Linux bridge attached to the physical network.
- Software: the EasyNAC QCOW2 appliance image, typically delivered in a .tar.gz package. Obtain it from support.infoexpress.com through an authorized support account, partner, or InfoExpress representative.
- Network: management VLAN reachable from the host; for multiple protected VLANs, an upstream 802.1Q trunk; DNS, 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 or supported OAuth2 mail 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 Oracle Linux KVM

The supplied Oracle Linux KVM package contains a QCOW2 virtual disk. Import it into a libvirt VM; the guest runs its bundled Linux OS and needs no additional guest installation. The examples below use EasyNAC-3.2 and bridge br0; substitute the delivered filename and your approved host network.

Prepare the image on the KVM host

Copy the supplied package to the host, extract it and check the image before import:

```
scp EasyNAC-3.2-Oracle-KVM.tar.gz root@kvmhost:/root/  
cd /root  
tar xzf EasyNAC-3.2-Oracle-KVM.tar.gz  
cd EasyNAC-3.2  
sha256sum -c ../EasyNAC-3.2-Oracle-KVM.tar.gz.sha256
```

Checksum: Run the final command when the matching .sha256 file was supplied beside the package. Resolve any mismatch before importing the disk.

Place the QCOW2 in the libvirt image store and give the qemu service account access:

```
cp EasyNAC-3.2.qcow2 /var/lib/libvirt/images/  
chown qemu:qemu /var/lib/libvirt/images/EasyNAC-3.2.qcow2  
chmod 640 /var/lib/libvirt/images/EasyNAC-3.2.qcow2
```

Identify the production bridge. Typical names include br0 and bridge0. The default NAT bridge virbr0 is unsuitable for production enforcement.

```
nmcli connection show  
bridge link show
```

Method A: virt-manager (GUI)

1. Select Create a New Virtual Machine, then Import existing disk image.
2. Choose /var/lib/libvirt/images/EasyNAC-3.2.qcow2; select Oracle Linux 9 as the OS type, or generic Linux if unavailable.
3. Assign CPU and RAM for the approved sizing tier. A typical starting point is 4 vCPU and 8 GB RAM.
4. Attach the VM NIC to the production bridge, for example br0. Do not select NAT/virbr0.
5. Name the VM, review the configuration and finish the import. Check the NIC and resource settings before continuing.

Method B: virt-install (CLI)

On a headless host, import the existing QCOW2 through libvirt. This example uses 4 vCPU, 8 GB RAM and br0:

```
virt-install \  
  --name EasyNAC-3.2 \  
  --memory 8192 --vcpus 4 --cpu host \  
  --disk path=/var/lib/libvirt/images/EasyNAC-3.2.qcow2,format=qcow2,bus=virtio \  
  --network bridge=br0,model=virtio \  
  --os-variant ol9 --import --graphics none --noautoconsole
```

If the VM is not already running, start it; then open the serial console. Exit the console with Ctrl + J.

```
virsh start EasyNAC-3.2
virsh console EasyNAC-3.2
```

SELinux: If the QCOW2 is stored outside the default libvirt image path, relabel that location with `restorecon -Rv /path/to/image`. An incorrect label can prevent the VM from starting.

4. First-boot console setup

Open the VM console in virt-manager, or use `virsh console EasyNAC-3.2`, and let the system finish booting. Set the Management IP with the setup wizard before opening the web UI; SSH access becomes available after 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.

Server Maintenance Services Site Settings Static Routes Support Tools AGENT LOGGING SERVER INLINE ENFORCEMENT RADIUS PROXY	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. Connect protected VLANs on Oracle Linux KVM

To protect multiple subnets, attach EasyNAC to a Linux bridge connected to an upstream 802.1Q trunk, then add each VLAN inside EasyNAC. With bridge VLAN filtering disabled, tagged frames pass transparently to the guest; EasyNAC handles its 802.1Q sub-interfaces internally.

Prepare the upstream switch and host bridge

The physical switch port must allow every protected VLAN. Adapt this Cisco IOS example to your interface and VLAN IDs:

```
interface fastEthernet 0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 2,3,5,100
 switchport trunk native vlan 1
```

Option A: bridge VLAN filtering off

1. Confirm the physical uplink, for example enp1s0, is enslaved to the production bridge br0: bridge link show.
2. Check /sys/class/net/br0/bridge/vlan_filtering. A value of 0 means the bridge passes tagged frames without VLAN filtering.
3. Attach the EasyNAC trunk NIC to br0 and confirm the upstream switch trunk allows the intended VLANs.

```
cat /sys/class/net/br0/bridge/vlan_filtering
```

Option B: bridge VLAN filtering on

Use host-side filtering when you need to restrict VLANs on the bridge. Permit required VLANs on both the physical uplink and the VM tap interface; replace the example interfaces and VLAN range:

```
ip link set br0 type bridge vlan_filtering 1
bridge vlan add vid 2-100 dev enp1s0
bridge vlan add vid 2-100 dev vnet0
bridge vlan show
```

Why bridge mode matters: EasyNAC enforcement sends ARP responses on the protected Layer-2 network. Do not attach its protected interface through NAT/virbr0 or macvtap private, VEPA or passthrough modes; those paths can prevent the

appliance from reaching peer devices.

Add each VLAN in EasyNAC

1. Open Configuration > Appliance Settings > Networking and select + on the trunk adapter.
2. Enter the VLAN ID and a static IP address and mask, or use DHCP. Add a Location label if useful.
3. Submit Network Changes. Leave Metric at its automatically assigned value, then verify the VLAN appears in Network Map.

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](#)

Check: Before broad enforcement, test visibility and ARP behavior on a non-production device. If the appliance is healthy but devices on a tagged VLAN are absent, inspect the upstream trunk, bridge membership and bridge vlan show output.

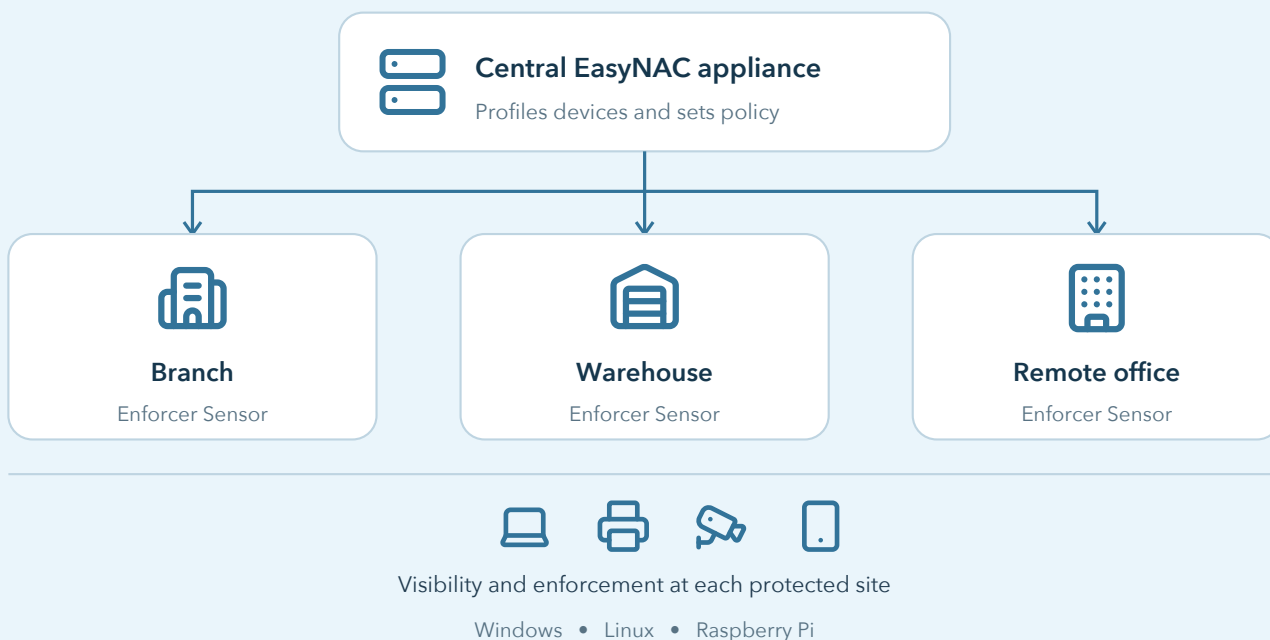
7. Extend protection to remote branches

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.

Extend protection. Keep control.



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 intelligence sources

EasyNAC combines directory, endpoint-security, patch-management and device-management evidence to identify managed devices, assess posture and drive access policy. Configure each source under Configuration > Integration. Use the EasyNAC Compatibility & Integrations guide for module-specific policy signals, product editions and deployment references.

Integration modules

Category	Modules
Network infrastructure (4)	Active Directory, AWS, Azure, SolarWinds
Endpoint security (17)	Bitdefender, Carbon Black, Cortex XDR, CrowdStrike, Cybereason, Elastic, ESET Antivirus, FireEye, Kaspersky Antivirus, Microsoft Defender, SentinelOne, Sophos, Symantec Endpoint Protection Manager, Tenable, Trellix ePolicy Orchestrator, Trend Micro, Webroot
Patch management (5)	HCL BigFix, Ivanti Security Controls, Kaseya VSA, ManageEngine Patch Manager, Microsoft WSUS
Desktop & mobile management (9)	Google Workspace, Headwind MDM, Jamf, ManageEngine Endpoint Central, Moscii StarCat, Microsoft Intune, Microsoft WMI, Okta, SureMDM

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	Check the VM NIC bridge and upstream management VLAN. Confirm binding with <code>virsh domiflist EasyNAC-3.2</code> ; rerun the console wizard if the IP needs correction.
Severe certificate warning	The default certificate is self-signed. Replace it in SSL Certificate Manager and reboot to apply the new certificate.
Test LDAP Connection fails	Check that the account suffix begins with @, the service-account password is current, and the AD server is reachable from management.
Captive Portal does not redirect	Check each portal IP and upstream ACL. The portal service must be reachable from every protected subnet.
Devices on a tagged VLAN are absent	Check the switch trunk, physical uplink bridge membership and, if filtering is enabled, bridge vlan show for both uplink and VM tap.
Enforcement active but devices not blocked	Check for NAT/virbr0 or macvtap private, VEPA or passthrough mode. Attach the protected NIC to a real Linux bridge and retest Layer-2 ARP reachability.
VM will not start; SELinux denial	A QCOW2 outside the default libvirt path may have the wrong SELinux context. Run <code>restorecon -Rv /path/to/image</code> and retry.
Profiling slow or incomplete	Active NMAP profiling adds load. Review VM sizing and integration load with InfoExpress Support if the appliance approaches supported limits.

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.

Deployment verification checklist

Record the outcome of these checks before moving a protected subnet beyond its initial pilot:

Check	Evidence to record
VM and management	Approved vCPU/RAM/disk; production bridge attached; Management IP responds from the intended admin network.
Portal services	Captive and Remediation Portal IPs are distinct and reachable from protected networks; certificate status is known.
Protected VLANs	Upstream trunk and Linux bridge carry the intended tags; each VLAN appears in EasyNAC Network Map.
Identity and signals	AD test succeeds where configured; selected intelligence-source connection tests pass and device tags synchronize.
Pilot policy	A known managed device retains expected access; an untrusted test device receives the intended restriction.
Operations	Notification test is delivered; admin credentials are stored; a recovery owner and next review date are assigned.

Deployment reference

For the full EasyNAC deployment workflow, see www.easynac.com/agentless-nac-deployment-guide.