

A group of four business professionals (three men and one woman) are gathered around a computer monitor in an office setting. They all have expressions of concern or urgency, looking intently at the screen. One man is holding a piece of paper, and another is holding a coffee cup. A woman in the foreground is holding a clipboard. The background shows a modern office with a grid-patterned wall and a window.

Who's Really on Your Network?

Why network access control is essential, why it so often stalls, and how to get it enforced without building it yourself



**OWN IT.
SECURE IT.
PROTECT IT.**

Contents

The Question Few Networks Can Answer	04
What Network Access Control Is	05
Why Your Network Needs It	06
Why Cisco ISE for NAC	07
The Implementation Pain: Why NAC Projects Stall	08
The Operating Pain: Day 2 Never Ends	11
Doing It Yourself vs. Managed ISE	13
Managed Cisco ISE as a Service	14
Is Your Network at Risk?	16

The Question Few Networks Can Answer

Right now, there are devices on your network that no one on your team can name. Think of a printer, a camera, a contractor's laptop, or a smart TV in a conference room. On a network without access control, each of them can reach far more than it should.



Organizations without network access control (NAC) live with that exposure every day. Organizations that have deployed NAC often face a quieter problem: the platform is in place, but it sits in monitor-only mode, watching traffic it was bought to control. Nobody made a bad decision. NAC is simply one of the hardest systems in IT to finish and keep running.

Either way, the risk compounds. Every unidentified device is a potential foothold. Every month without enforcement is a month an intruder can move freely once inside.

Whether you are evaluating NAC for the first time or own a deployment that never reached enforcement, this guide is for you. It explains what NAC is, why it matters, why Cisco ISE is the platform to run it on, and what it truly takes to implement and operate. It closes with how Padlock Technologies delivers **Managed Cisco ISE as a Service**: enforced, compliant, always-current access control as an outcome you buy, rather than a practice you have to build.



NAC is the gatekeeper that decides, every time something connects, whether it gets on the network and what it is allowed to reach. Instead of trusting any device that plugs into a wall jack or joins Wi-Fi, NAC asks four questions and enforces the answer.

Question	What NAC does	Common methods
Who are you?	Authenticates users and machines against your identity source	802.1X with certificates or credentials, tied to your directory
What are you?	Identifies devices that cannot log in, like printers, cameras, and medical gear	MAC address authentication plus device profiling from network traffic and attributes
Are you healthy?	Checks patch level, antivirus, and encryption before granting access	Posture assessment through an endpoint agent or integration with endpoint management
What may you reach?	Places the device in the right segment with the right permissions	Dynamic VLANs, access control lists, and identity-based segmentation tags

Mature NAC also covers guests and contractors through sponsored or self-registration portals, controls administrator access to network devices, and supports threat response. When a firewall or endpoint security tool flags a compromised host, NAC can quarantine it automatically.

Why Your Network Needs It

An open wall jack is an open door. Without NAC, anyone who can plug in a cable or learn a Wi-Fi password lands on your internal network with the same reach as an employee.



Device sprawl you cannot see

IP cameras, badge readers, printers, HVAC controllers, smart TVs, and medical devices now outnumber laptops in many environments. Most cannot run an agent, and many are rarely patched. NAC is how you discover them and fence them in.



Lateral movement is how breaches spread.

Ransomware rarely stays on the first device it lands on. Attackers move sideways across a flat network to reach servers and backups. NAC-driven segmentation limits that blast radius.



Zero Trust starts at the port.

"Never trust, always verify" is impossible if the network itself trusts every connection. NAC is the enforcement point that makes Zero Trust real on campus and branch networks.



Auditors and insurers are asking.

HIPAA requires access controls for systems holding patient data. PCI DSS relies on segmentation to limit the scope of the cardholder data environment. CMMC and NIST SP 800-171 include device and access control requirements. Cyber insurance applications increasingly ask how you control network access.



Contractors, guests, and BYOD are here to stay.

Visitors and personal devices need connectivity without touching production systems.

The question for most organizations is not whether to deploy NAC. It is whether they can run it well enough for it to actually protect them.

Why Cisco ISE for NAC

Whether you are choosing a NAC platform or already own one, Cisco Identity Services Engine (ISE) is the benchmark. It is the most complete NAC platform for enterprises running Cisco networks, and one of the most capable in any environment. It brings every NAC function, and much more, into a single policy engine.

Capability	What Cisco ISE provides	Why it matters
Unified access policy	One policy engine for wired, wireless, and VPN users and devices	Consistent rules everywhere people connect
Deep network integration	Native 802.1X, MAB, Change of Authorization and downloadable ACLs on Cisco switches, wireless controllers, and firewalls	Enforcement at the port, not just the perimeter
Device visibility	Profiling from DHCP, RADIUS, SNMP, HTTP, NetFlow, NMAP, and other probes	Identifies IoT, OT, and medical devices that cannot authenticate
Posture compliance	Endpoint checks through the Cisco Secure Client posture module	Unhealthy devices are remediated before they get full access
Segmentation	Cisco TrustSec Security Group Tags	Policy follows identity instead of IP addresses and VLANs
Guest and BYOD	Sponsored, self-registration, and device onboarding portals	Visitors and personal devices stay off production systems
Device administration	TACACS+ for network device logins and command authorization	Audit-ready control of who changes your network
Ecosystem sharing	pxGrid integration with firewalls, SIEM, EDR, and MDM platforms	Security tools can see context and trigger quarantine

The platform is not the problem. The operating model is. Every capability above is another set of policies, certificates, integrations, and upgrades that someone has to own, every day. The next sections show what that really involves.

The Implementation Pain: Why NAC Projects Stall

Most NAC projects do not fail at installation. They fail at enforcement. Getting ISE running takes days; getting to a closed, enforced network without breaking the business can take a year or more, and many organizations never get there.

1. Design decisions that are expensive to undo

Before a single port is enforced, someone must decide node personas (Policy Administration, Monitoring, Policy Service), sizing, high availability across sites, and where each Policy Service Node sits relative to the switches and WLCs it serves. Licensing tier choices (Essentials, Advantage, Premier, plus Device Admin) determine which features you can even use. Get these wrong, and you will redeploy later under production load.

What it costs you: rework under production load, or features you paid for and cannot use.



2. Certificates and PKI are the silent prerequisite

Certificate-based 802.1X is the right answer, and it means building or fixing an internal PKI. Every managed laptop needs a machine certificate auto-enrolled through Group Policy or Intune. ISE needs its own EAP, admin, portal, and pxGrid certificates, trusted by every endpoint. A single misconfigured trust chain means a building full of users who cannot connect.

What it costs you: one expired or untrusted certificate can lock an entire building out of the network.

3. Supplicants are inconsistent across your fleet

Windows, macOS, Linux, iOS, and Android all handle 802.1X differently. Native supplicants must be configured through Group Policy, an MDM profile, or an onboarding portal. Machine versus user authentication, and how they chain, decides whether a laptop gets on the network before anyone logs in. Edge cases are endless.

What it costs you: your executives and frontline staff become the test group, one help desk ticket at a time.

4. The devices that cannot authenticate

Printers, cameras, phones, badge readers, lab equipment, and medical devices fall back to MAB, which is only as safe as your profiling. Building accurate profiling policies requires tuning probes (DHCP, RADIUS, SNMP, HTTP, NMAP, NetFlow) and validating thousands of devices. Many organizations discover hundreds of devices no one can identify, owned by departments no one can find.

What it costs you: unknown devices either get blanket exceptions, which defeat the purpose, or enforcement never happens.

5. Switch and wireless configuration at scale

Every access switch needs consistent AAA, RADIUS, CoA, device tracking, and per-port 802.1X configuration. Different platforms and IOS versions behave differently. Hundreds of switches and thousands of ports must be touched, tested, and kept consistent.

What it costs you: a single inconsistent port becomes an outage or a security hole, and you find out at the worst possible moment.

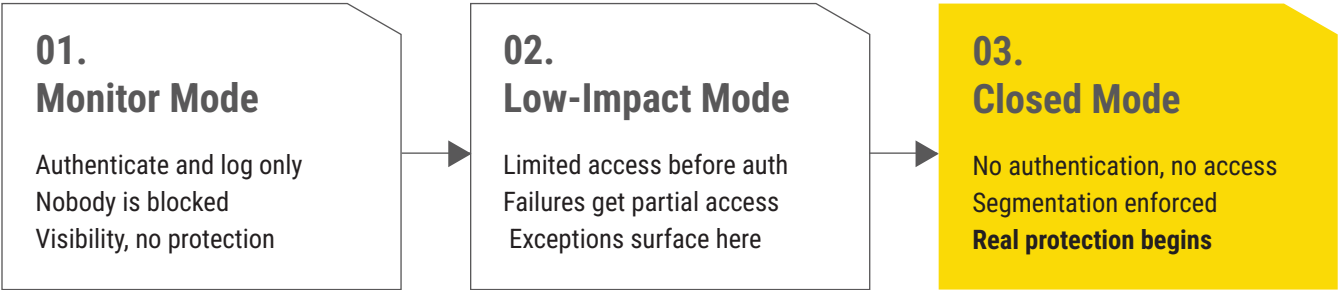


6. The phased rollout that never finishes

The safe path to enforcement runs through three modes, each with its own exit criteria. Moving from one to the next demands weeks of log review, exception handling, and coordination with every business unit.

Protection only begins in the last of three phases

Each step demands log review, exception handling, and business sign-off



NAC enforcement rollout · 3 phases

Many in-house deployments stall at phase one, where the network is watched but nothing is actually blocked.

The Operating Pain: Day 2 Never Ends

Once enforcement is on, ISE becomes part of the critical path for every connection in the company. If it breaks, people cannot work. That changes the operating burden from “a security project” to “a tier-zero service that needs constant care.”

A scenario every NAC team fears

It is Monday, 7:45 a.m. The help desk takes its first “I can’t connect” call. By 8:15 a.m., the queue is full. Over the weekend, the certificate ISE presents during authentication expired, and every laptop now refuses to trust it. The fix takes minutes once someone who knows ISE finds the cause. Until then, the business waits.

Nothing about that morning was unpredictable. The expiration date was printed on the certificate from the day it was issued. What was missing was someone whose job was to watch it.

Patches and upgrades are high-stakes.

ISE receives regular patches and periodic major releases, some driven by security advisories. Upgrades touch every node in a distributed deployment, require careful sequencing and backups, and can change behavior that policies depend on. Many teams fall several versions behind because the risk of upgrading feels larger than the risk of waiting.

Certificate expiration is an outage on a timer.

When an ISE EAP certificate or the CA chain behind it expires, authentication fails across the board. The same is true for machine certificates that stop auto-renewing on endpoints. These events are predictable and still catch teams off guard.

The help desk becomes NAC support.

“My laptop won’t connect” tickets require someone who can read ISE live logs, RADIUS failure reasons, and switch port state, and decide whether the cause is the user, the device, the certificate, the directory, or the policy.

Policy drift and exception creep.

Every urgent request adds a one-off rule or a MAC address to an allow list. Over time, the policy set becomes hard to read, easy to break, and quietly less secure.

Directory and identity dependencies.

ISE relies on healthy Active Directory joins, domain controller reachability, and clock synchronization. Changes made by other teams can break authentication without anyone touching ISE.

Profiling and posture never stand still.

New device models arrive, feed updates change classifications, operating systems ship new versions, and posture requirements must be revised. The Secure Client posture module itself needs its own deployment and update cycle.

Logs and evidence for auditors.

Proving who connected, when, and with what access means retaining and reporting on monitoring data, often beyond what the MnT nodes keep by default.

Integrations multiply the moving parts. Each pxGrid link to a firewall, SIEM, EDR, or MDM platform brings its own certificates, versions, and failure modes.

The people problem

Underneath all of this sits the hardest constraint: expertise. Engineers who can design, troubleshoot, and upgrade ISE confidently are scarce and in demand. Organizations often rely on the one person who built the deployment. When that person leaves, takes a vacation, or is pulled onto another project, the NAC program freezes or quietly degrades.



Doing It Yourself vs. Managed ISE

The license is the smallest line item. The true cost of in-house NAC is the people, time, and risk required to keep it enforced and healthy.

Cost area	Running ISE in-house	Managed ISE with Us
Expertise	Senior engineers with deep ISE, 802.1X, PKI, and switching skills, plus backup so one person is never the only one who knows it	A CCIE-led team, with no single point of failure on your payroll
Time to value	Months of design, piloting, and phased rollout before enforcement delivers any protection	A defined plan to enforcement, with agreed exit criteria at each phase
Ongoing operations	Patching, upgrades, certificate renewals, profiling, posture, and policy hygiene, every month	Planned, tested, and executed by Padlock under change control
Support load	Tier 2 and Tier 3 troubleshooting your help desk cannot resolve	Your help desk escalates; we resolve
Training	Continuous skill-building as ISE and its integrations evolve	Our responsibility, not your budget line
Outage risk	Downtime when a certificate expires, an upgrade fails, or a policy change blocks users	Certificates and upgrades tracked and scheduled before they become incidents
Security gap	Paying for NAC while getting visibility, not protection	Enforcement is the goal of the engagement, not a someday phase

The most expensive NAC deployment is the one that is fully licensed and never enforced.

Managed Cisco ISE as a Service

Padlock Technologies takes ownership of your ISE deployment so you get enforced access control as an outcome, not a project. The service is led by Donald C. Heslop Jr., a dual CCIE (#61970) in Enterprise Infrastructure and Security, the two disciplines NAC depends on most.

What we deliver

01.Assessment and design.

Discovery of your users, devices, switches, and wireless network, followed by a deployment architecture sized for your sites and growth.

02.Deployment and phased enforcement.

We build ISE, integrate it with your directory and PKI, configure your network devices, and drive the rollout from Monitor Mode to Closed Mode against agreed exit criteria.

03.Lifecycle management.

We plan, test, and execute patching, version upgrades, backups, and certificate renewals.

04.Policy and profiling management.

Ongoing tuning of authorization policy, profiling, and posture, with disciplined change control instead of exception creep.

05.Escalation support.

Your help desk handles the first call; we handle the ISE troubleshooting behind it.



06.Reporting and audit evidence.

Regular reporting on access activity, endpoint inventory, and policy changes to support HIPAA, PCI DSS, CMMC, and cyber insurance reviews.

07.Integration management.

pxGrid and related integrations with your firewalls, SIEM, EDR, and MDM platforms, maintained as part of the service.

Who does what

Activity	Your team	Us
Business access requirements and approvals	Owns	Advises
ISE architecture, build, and upgrades	Informed	Owns
ISE certificates and the NAC trust chain	Informed	Owns
Network device NAC configuration	Approves changes	Owns
Policy, profiling, and posture tuning	Approves changes	Owns
First-line user tickets	Owns	Supports
ISE troubleshooting and escalation	Escalates	Owns
Compliance reporting	Reviews	Produces

Service levels, coverage hours, and scope boundaries are defined in your Managed Security Services agreement, so responsibilities are clear from day one.

Getting started is low-risk

Already own ISE? We start from your existing deployment, licenses, and policies. There is no rip-and-replace.

Starting fresh? We design and build your deployment with you, with enforcement as the planned destination from day one.

Either way, your team keeps control of business decisions about who gets access. We handle everything it takes to make those decisions work.



Is Your Network at Risk?

Take two minutes and check every statement in your group that is true today. If you check two or more, your access control is likely costing more than it protects.



If you do not have NAC today

- ☐ We could not produce a complete list of every device on our network right now
- ☐ Anyone who plugs into an open wall jack can reach internal systems
- ☐ Guests, contractors, and personal devices share the network with production systems
- ☐ An auditor or cyber insurer has asked how we control network access, and we struggled to answer

If you already run Cisco ISE

- ☐ Our deployment has been in Monitor Mode for more than six months
- ☐ We are more than one major release behind, or unsure which patch we run
- ☐ We do not have a documented calendar of ISE and CA certificate expiration dates
- ☐ Only one or two people can troubleshoot an 802.1X failure
- ☐ We have devices on the network we cannot identify or assign an owner to
- ☐ Our policy set has grown through exceptions nobody fully understands



Your next step

Already running Cisco ISE?

Padlock Technologies offers an ISE health and readiness review: a paid engagement that gives you an expert, independent look at your deployment and a clear path to full enforcement. You come away with:

- Your current enforcement status, stated plainly
- Your most pressing operating risks, such as certificate expiration, version currency, and single points of failure
- A practical path from where you are to an enforced, segmented network
- The findings are yours to keep, whether or not you engage Padlock to run ISE for you.

Don't have NAC yet?

Start with a conversation about your network, your compliance obligations, and your goals. We will scope a Managed Cisco ISE deployment built to reach enforcement from day one, so you never get stuck in monitor-only mode.

Every month without enforcement is risk you are already carrying. Contact Padlock Technologies, LLC today.

Phone: (833) 879-7274

Email: info@padlocktech.com

Web: padlocktech.com



PADLOCK
TECHNOLOGIES

WWW.PADLOCKTECH.COM