# Network Access Control: One Step Before Your First Line of Defence

Soliton®

# *01.*

## Introduction
NAC has never been more essential

IT managers today face a great challenge. The new reality is that not everyone is accessing a network from the same controlled ecosystem. Increasing employee mobility, a rising number of BYOD devices, and the need to support hybrid work environments has greatly increased our reliance on network security in order to prevent cyber- attacks. IT admins are forced to review the security perimeter.

Network Access Control is moving up the agenda for many organisations because of its unique ability to address these challenges. The main aim for any NAC solution is to protect the whole perimeter. Naturally, NAC incurs an initial cost, but demonstrates it value after that initial investment.

This guide will examine what NAC is, what it does, and how it helps you monitor and regulate your network while creating an optimal working experience for both your internal and external users.

# #01

## Access without proper authentication doesn't make sense

Strengthening the security of networks, systems and data is one of the most pressing challenges IT managers face. It requires a comprehensive approach to security, and it starts with managing who has access to your company's most valuable asset: data.

The task of IT is to provide secure access to IT sanctioned networks and applications while keeping unauthorised users at bay, this is why providing robust network security is more important than ever.

The paramount responsibility of a secure system is to ensure that only authorised users have access to the network. Legitimate users should be allowed in, and cybercriminals kept out. This is done by authenticating the identity of the user seeking access, and then checking that the user is authorised to enter.

Authentication enables organisations to keep their networks secure by permitting only authenticated users to gain access to their protected resources. NAC is a building block in deploying a strategy to protect users fully, endpoints, and the network infrastructure from threats to data confidentiality, integrity and availability.

The ultimate goal is an environment where users can access resources with a frictionless experience that does not compromise IT efficiency, security or compliance.

# #02

## Key tasks of Network Access Control

Network Access Control, or NAC, provides the mechanism for ensuring only authenticated users can access the private company network.

It is primarily a security solution designed to identify, assess, and enforce access control on all devices before connecting. It ensures that only users with authenticated and reliable devices (whether they belong to the company or the individual) can log on to the network.

Once granted access, NAC enforces policies to regulate the areas of the network users can access while continuously monitoring and logging their activity.

NAC allows for a complete centralised security approach of your network and follows the follow the principle of the 3 A's:

**Authentication**
User is prompted for credentials and identity verification (Who are you? Can you prove you are who you say you are?)

**Authorisation**
System confirms or denies based on the access policies (What are you allowed to do on the network?)

**Accounting**
System tracks user activities (What are you doing, and for how long?)

NAC ensures that users who access networks, data, devices, and software resources are properly authorised. In many cases, this is fundamentally a security concern, making sure that sensitive data and functions do not fall in the hands of people who might purposefully or inadvertently use them.

# #03

## Taking the end user out of the equation

It's a given fact that the user is the weakest link in the security chain, the cost of human errors adds up. For IT administrators, an ideal system does not require knowledge from an end-user, as end-users are more likely to make mistakes than an automated process. The person should not be there; they need to be verified correctly but not by themselves. This is why you should try to eliminate the user as maximum as possible.

Using digital certificates, you remove the user as part of the authentication process. Digital certificates provides credentials that identify a user (and often their device or devices) known to the network.

With certificate-based authentication, a business can verify that all devices connected to its network are authorised. Digital certificate authentication provides a unified way of authenticating users before authorising access to appropriate data and applications. It gives you full control, knowing that different elements are checked before granting access by providing authentication through a certificate instead of a username and a password or biometric identification.

Meanwhile, your employees will appreciate they do not need to think about security matters.

# #04

## Take the Pain out of Employee Onboarding & Offboarding

For IT professionals, onboarding and offboarding employees are complex and manual. Onboarding is how unmanaged devices, guests, third parties, and company-owned devices initially connect to your network. The onboarding process for authorised users and devices needs to be efficient and easy to implement and manage—ideally without any hands-on involvement by IT (once deployed and configured).

However, many organisations still rely on rudimentary methods built into their network infrastructure (such as pre-shared keys and MAC authentication) that can impact user experience and create security risks. By deploying digital certificates to authenticate users' (internal and external) devices, organisations can significantly improve visibility, mitigate risk, and improve productivity.

Managing digital certificates, especially expirations and renewals, continues to be a challenging process for businesses of all sizes, and such occurrences can create costly service disruptions. A purpose-built system for secure automated network onboarding is a critical tool that enables IT to manage certificates better. Automation greatly reduces or eliminates certificate expiration, alleviating compliance concerns and freeing up IT resources. Users can provide their devices for network access with intuitive self-service workflows without IT intervention. They get online quickly and securely—with only the appropriate level of access to network resources.

**Certificates are the only complete authentication method for a fully automated, hands-off approach.**

On the other hand, offboarding has a significant risk to the business if done improperly. Failing to completely offboard means ex-employees could still access important company data and information, creating unnecessary risks.

Offboarding is usually the responsibility of the employee's line manager and the Human Resource department. IT security teams are an afterthought, and employees could have access to passwords and other access points to a company's network.

During offboarding processes, the IT security team should ensure the proper removal of an employee's access to the network. When someone leaves the organisation, it's quick for admins to remove access early. But, even if they forget, the certificate will still expire on its end date and prevent unauthorised access.

**Automate certificate life cycle management.** The multiplatform certificate management app (Soliton KeyManager) makes it easy for network administrators to use short-life certificates for enhanced security. Users can self-service on any device, automatically requesting and installing user- and device certificates in just 3 steps.

Soliton KeyManager app sends users a warning when certificates are due to expire. Users can click the link to renew the certificate which delivers four significant benefits to businesses:

- Reduces the time the IT team spend on certificate management
- Adds a new layer of security to the Simple Certificate Enrolment Protocol (SCEP) via a unique secret per request
- Enables public and private key pairs to be generated
- Thanks to the way it's created, it never leaves the device during the issuing process

# 02.

## How digital certificates give you the edge

Certificate-based authentication is very secure and very user-friendly. It is completely transparent to the user and it runs all the time but requires no user input. Users don't have to authenticate themselves repeatedly, as most authentication occurs without the user noticing. Digital certificates provide the best workflow for the end-user and the highest level of security for the administrator.

Digital certificates allow users to access the correct areas of the network the first time and every time, which reduces queries to IT support teams. For businesses, digital certificates are scalable - it's never been simpler to add devices to the network, essential when there are more devices than ever and more employers checking in from random office locations.

With certificate-based authentication, a business can verify that all devices connected to its network are authorised.

# #01

## Let's take the fear out of unmanaged devices

Regardless of your preferred authentication solution, it needs to be mobile and flexible. Whether it's your employee, a guest or a contractor, they all should be able to use their preferred device.

For authentication, it should be completely irrelevant whether a device is managed or unmanaged. The great thing about using digital certificates for authentication (as opposed to usernames and passwords) is that you can issue them to devices your company does not manage without troubling the IT team. It is fully independent towards the endpoint. As long as you can provide a certificate to identify who you are, it's all good.

Using a unified deployment process to issue, distributing and install digital certificates on endpoints, means there is no need to install an agent, only a client application which is easily downloaded from the app stores. Not having to install an agent has some great benefits for IT and end-users.

Adhering to security protocols, software incompatibility issues, ensuring the latest version of an agent is installed, and the overhead of updating agents on thousands of devices are just some of the barriers IT departments face when it comes to deploying software. For users working with the personal devices the advantage of agentless technology is it removes the barriers associated with installing additional software which potentially could lead to IT peeking into private apps and data.

Soliton's NAC solution enables distribution of certificates (and profiles) to unmanaged external systems, such as privately-owned devices or the devices of partners and contractors.

The Soliton KeyManager app removes the need for specific mobile device management to deploy these certificates, making it easy and secure for users to install digital certificates on their preferred systems.

# #02

## Flexible and seamless integration - supporting your business

A particular weakness of many NAC solutions is their hardware dependence caused by the use of proprietary protocols and applications. Such vendor lock-ins are tedious: they stop you from getting the optimum solution you want.

When it comes to managing user access, you should first focus on tools that offer native integration with your enterprise's existing software. You don't want to have to change your infrastructure or network design in order to bring the NAC solution online.

NAC should address the many dimensions of scale and help future-proof your business, not only support growth by adding more licences. The ideal NAC solution:

- scales for increased usage and spikes
- scales for more sophisticated use cases
- the technology is enterprise-ready on a global scale
- the technology scales to help ease other common growing pains

Soliton delivers authentication solution that addresses the many dimensions of scale and help future-proof your business. Our solutions easily adapt to different workflows and evolves to offer features you need now and those you'd like to introduce in the future.

The built-in RADIUS conforms to the RFC standard allowing Soliton's NAC solution NetAttest EPS to integrate and communicate with any network infrastructure component, such as switches and access points. It provides for certificate-based and mutual authentication of the client and the network.

By default, RADIUS eliminates the need for an agent. Agentless means that there are no endpoint agents to deploy, update, and maintain for the NAC to discover, classify, assess, and control all network-connected devices. It does not require anyone to install software on their devices, avoiding complex life cycle management due to software updates and agents with security holes.

Unlike other NAC solutions, NetAttest EPS is not built on proprietary features in the RADIUS protocol, offering flexibility and seamless integration into any existing infrastructures avoiding vendor lock-in.

# 03.

## A seamless experience for guests, contractors and external partners - orchestrating workforce ecosystems

Organisations are increasingly outsourcing internal functions and operations and external services. Contractors, partners, or temporary workers need to access the company network.

But network security problems can arise when you bring in third parties to access corporate resources. Third-party users access needs to be managed separately and without clients.

When a user requests remote access to NAC portals, the system immediately checks their credentials. NAC regulates the areas of the network users can access - while monitoring and logging their activity - and enforce these policies, limiting an individual to just those systems.

Sensitive resources like client databases can be kept off-limits to unauthorized users. Malicious actors will also struggle to move laterally throughout networks, limiting the dangers posed by malware attacks.

NAC can drastically improve an organization's network security posture by allowing for greater control over what devices are accessing the network, and what they are granted access to. NAC also allows companies to admit guest users securely. Secure guest access makes it possible to collaborate with partners and contractors while keeping security threats low.

Soliton

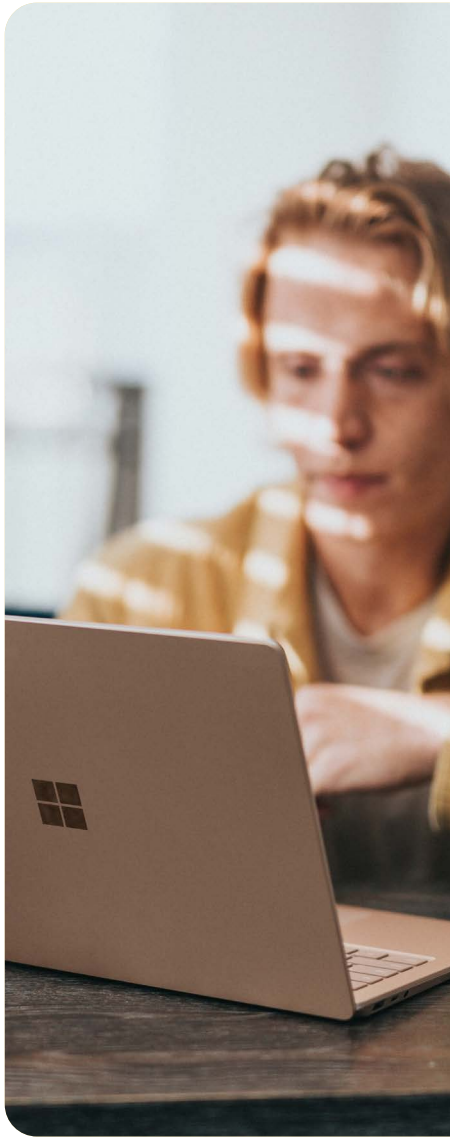
# #01

## The modern proof alternative to Mac address filtering

The MAC address authentication method grants access to a secure network by authenticating devices for access to the network. It is well-suited for clients not capable of providing interactive logons, such as wireless access points and machinery.

In local networks, companies can use MAC addresses to make access whitelists or blacklists. This is called MAC address filtering. Basically, one or more network access servers, like switches or Wi-Fi access points, are configured with a whitelist only used to allow or deny a device accessing the network. This is why MAC address filtering is sometimes called MAC address authentication, as if it were an authentication method. However, MAC address filtering is easy for hackers to spoof and evade restrictions. As MAC addresses are not encrypted on the network, outsiders can clearly identify them by capturing packets from the wireless LAN. Tools to change MAC addresses are distributed on the Internet and easily available. In other words, malicious attackers can effortlessly get past the security system and get unwanted access to your network just by using these tools to “spoof” (falsify) the MAC address.

Instead of purely focusing on a device feature, make your identification and authentication method waterproof by working with a stronger identification factor. Digital certificates are very powerful because a different certificate can be installed on each client. Certificates have expiration dates but can also be revoked before they expire in case this is needed.



In some situations it's impossible to entirely avoid dealing with machines that only come with MAC addresses (especially in areas such as healthcare and automotive) as an identity. At Soliton, we've worked hard to balance these requirements with your security needs.

Using a dedicated database for MAC addresses, NetAttest EPS simplifies the process of issuing access for these devices:

- It gives you all the tools you need to add new devices to your network quickly
- Automatically detects non-802.1x devices and adds them to a white list
- A secure MAC address database with storage for up to 200,000 addresses
- A dedicated interface for registering new MAC addresses

# #02

## The promise of NAC

**Security**

- Allows only known and authorised users and devices onto your organisation's network
- Ensures all devices on your network meet your security policies and are considered 'safe'

**Visibility**

- Know who and what is on your network at all times
- Continuous monitoring and logging of user activity

**Control**

- Control access to specific network resources based on identity of users and/or devices
- Role based access control for "Employee" and "third party" users
- Allow "Guest" users access only to the Internet
- Deny or limit access to users or devices that do not satisfy your security policies

# #03

## NAC delivers advantages throughout the organisation

**Return on Investment (ROI)**

- Leverage your existing network infrastructure to enforce your organisation's policies
- Get more value out of your existing investments (in addition to other benefits of NAC)

**Regulatory Compliance**

- Be able to track and report on all users and devices accessing your network resources
- Provide detailed "audit trails" in the event of compliance audits

**Benefits for End-Users - Easy technology frees people up to work anytime, anywhere.**

- No need for users to take devices into the office or get IT to do any setup
- With the user-friendly app, users can self-serve certificate requests on their device
- Proactive notifications prompt users before their certificate expires, no downtime

**Benefits for IT Managers - Operational efficiency**

- Simplified and automated manual and labour-intensive IT functions
- Off-load tasks from IT and Help Desk to increase their productivity
- Prevents unauthorised network access, with straightforward and powerful (short-life) certificate management – even on unmanaged and BYO devices
- Self-enrolment drastically reduces deployment time

## Conclusion
## NAC is a foundational network security defense

The majority of breaches and data theft occur behind firewalls, making NAC a critical component of a multilayered security policy. But organizations need to understand that NAC is not a silver bullet that can protect their network against all types of threats, rather it should be used along with other systems to ensure complete network access protection. It doesn't take the place of a firewall and won't protect against data leaving through e-mail, printouts, or USB flash drives.

Nevertheless, NAC is more than a security solution; it helps you create a productive working environment for your team and create an impressive, seamless experience for your guests. It is One step before your first line of defence of IT Security.

## Soliton's NAC
## NetAttest EPS

Network administrators and IT departments often see authentication as a burden. NetAttest EPS changes that perception. Easily implement Network Access Control and provide users with the most convenient solution on any device or operating system.

NetAttest EPS is a complete, port-based network access solution and uses the IEEE 802.1X standard to act as an authentication and authorisation server. It's ideal for protecting both large networks and small networks, in one location or many, and it protects the wire, Wi-Fi and VPN.

Soliton®

## Here's what sets NetAttest EPS apart:

- Stand-alone all-in-one solution - Includes everything you need in a NAC solution, including the Certificate Authority for creating certificates and a RADIUS server for enforcing access policies
- Suitable for businesses of all sizes - available for virtual or hardware appliances
- Flexible deployment with high availability
- Cost-effective - low implementation cost and low operating costs
- Soliton KeyManager application helps users securely download and install certificates on their devices, even if those devices are private and unmanaged

## Of course, there are also a few things NetAttest EPS doesn't do:

- There's no vendor lock-in
- We don't use agents at the endpoint - avoiding complex life cycle management due to software updates and agents with security holes

**NetAttest EPS Saves Time, One Step Before Your First Line of Defence**

## Get in touch


solitonsystems.com

emea@solitonsystems.com

+31 20 896 5841


Soliton®