Whitepaper

NAC

Network Access Control

Identity Management For Healthcare Environments Using Network Access Control

While today's healthcare practitioners continue to evolve in knowledge and best practices in treating life-threatening illnesses with promising breakthrough treatments and innovative pharmacological solutions, it is the parallel development of technology integration that will, in the coming years, define the industry's ability to make these advances possible. With EMR (Electronic Medical Records), CPR (Computerized Patient Records), and closed loop medication management on the horizon, it is the concept of trusted identity management at several levels – most notably that of network access – with which the industry has been most concerned.

Table of Contents

INTRODUCTION

While today's healthcare practitioners continue to evolve in knowledge and best practices in treating life-threatening illnesses with promising breakthrough treatments and innovative pharmacological solutions, it is the parallel development of technology integration that will, in the coming years, define the industry's ability to make these advances possible.

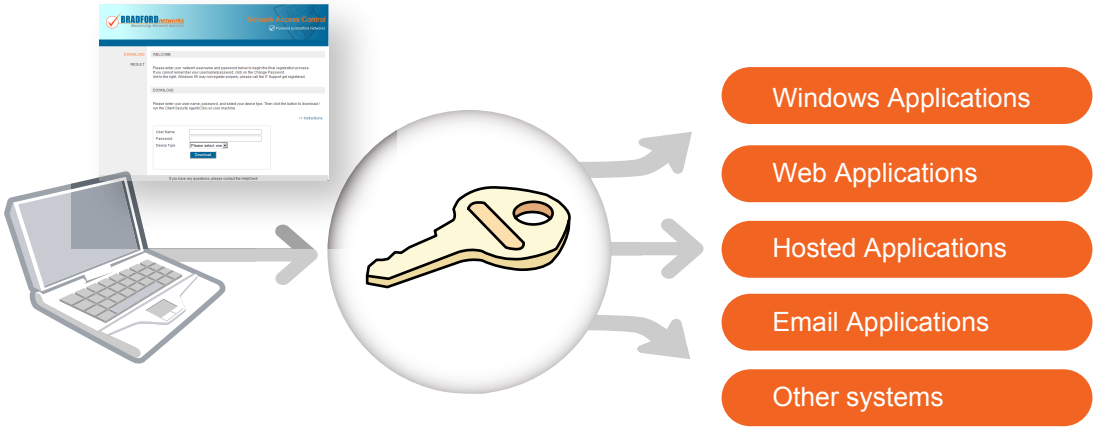
With EMR (Electronic Medical Records), CPR (Computerized Patient Records), and closed loop medication management on the horizon, it is the concept of trusted identity management at several levels – most notably that of network access – with which the industry has been most concerned. Specifically:

- **Single Sign-On Technology (SSO)**
- **Role-Based Access Control (RBAC)**
- **User Provisioning**

As a premier, innovative, and proven Network Access Control solution that incorporates Identity Management, Endpoint Compliance, and Usage Policy Enforcement into a single solution, we will outline in this white paper how NAC Director satisfies each of these concerns through a robust and proven architecture that seamlessly incorporates user authentication and policy enforcement with the roles to which the user has been individually assigned.

SINGLE SIGN-ON TECHNOLOGY (SSO)

Single sign-on (SSO) is a specialized form of software authentication that enables a user to authenticate once and gain access to the resources of multiple software systems.



SSO facilitates access to network resources and addresses, immediately, so doctors or other clinicians or caregivers do not have to recall multiple passwords; where multiple users can sign-on to a shared workstation without logging out of the desktop; where user accountability enables an administrator or compliance officer to view user access events and log files through detailed reports; and, perhaps most importantly of all, effectively prohibit security breaches in patient information.

HIMSS Analytics, which specializes in IT research for the healthcare industry, recently conducted its annual "Leadership Survey." The study findings were noted in the October 5, 2006 online issue of **Network World***. Focused on single sign-on solutions, the study included the dramatic finding that 79% of IT executives ranked SSO/identity management as the highest priority for the next two years. Among the findings:

- Senior IT executives are most concerned with the ability of SSO technology to integrate with enterprise directories and the organization's core clinical vendor products. Other requirements included the ability to integrate with other technology vendors and support for strong authentication.
- Ninety-one percent of respondents see improved user satisfaction as the top benefit of SSO technology.
- Ninety-one percent of respondents indicated a single user ID and password as a critical function, while 66% identified a quick login/logout as a key capability.

NAC Director promotes Single Sign-On through its Identity Management component, which provides administrators with the ability to identify unique users correlated to their roles as defined by the organization's Active Directory, to associate (or correlate) individuals to devices and grant access rights based on their level of authentication. Additionally, Identity Management provides the visibility into knowing where any piece of hardware or user is anytime of the day including a connection login history for each user that details what time that user logged in, what time they logged out, and what in the network they accessed in between.

NAC Director forces employees and staff to re-authenticate in a given period of time, especially when the workstation has been left unattended for a certain period of time. Automatic logoff is an effective way to prevent unauthorized users from accessing EPHI on a workstation when it is left unattended for a period of time. NAC Director re-authenticates across the network on all network devices that require re-authentication. NAC Director also scales the time interval between re-authentication events. If a user needs to be re-authenticated, it's not only a machine or device that's being re-authenticated; it's also the individual's credentials and his/her role-based access, binding machine and individual to one another. Ultimately, NAC Director enables administrators to know who is sitting behind every IP or MAC addressable device on the entire network by forcing users to re-authenticate when their device or machine is automatically logged off.

In terms of integration with other vendors the Usage Policy Enforcement feature includes events (SNMP traps) sent to NAC Director from other applications (Packeteer, IDS/IPS, Firewalls).

Additionally, through its connection-based logs, NAC Director also provides a historical and trusted record of all network activity, users, and devices that accessed the network in any given period of time requested.

ROLE-BASED ACCESS CONTROL (RBAC)

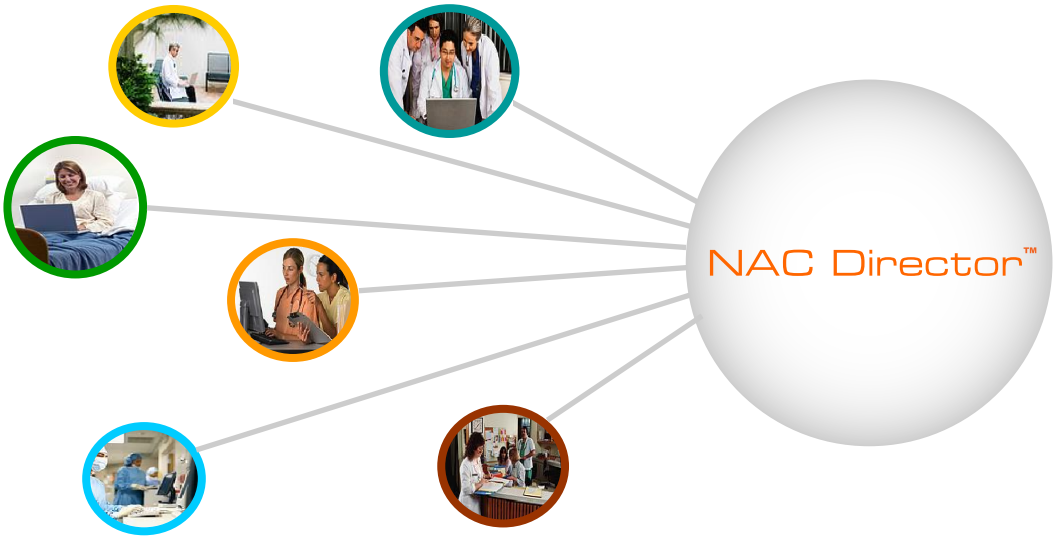
A technical means for controlling access to computer resources, RBAC controls what information computer users can utilize, the programs they can run, and the modifications that they can make. Computer-based access controls can prescribe not only who or what process may have access to a specific system resource, but also the type of access that is permitted. These controls may be implemented in the computer system or in external devices.

With role-based access control, access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles such as doctor, nurse, teller,

manager, etc. The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in the organization.

Access rights are grouped by role name. The use of resources is restricted to individuals authorized to assume the associated role. For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests, while the role of researcher can be limited to gathering anonymous clinical information for studies.

The use of roles to control access can be an effective means for developing and enforcing enterprise-specific security policies, and for streamlining the security management process. In fact, NAC Director can dynamically create the groups based on the group structure defined within that directory.



For example, nurses can be considered, in NAC Director, as a group containing unique individuals having varying levels of access that enable them to satisfy their roles in the hospital. A Head Nurse, in this case, may have expanded attributes within the Active Directory used by NAC Director to define roles, and may be able to access an expanded part of the network based on those attributes. NAC Director also defines roles at the device level so as nurses move from one building to another in the fulfillment of their responsibilities, their attributes, authentication, and access may differ from one geographical location to the next and NAC Director is intelligent enough to know the difference. In a similar context, medical students, for example, may enjoy full access in their dorm, limited access to the medical library, and have no access at all to the administration network. With NAC Director, two unique individuals may plug into the same exact port and have two completely separate roles assigned to them resulting in ever greater or ever limited network access.

There are other examples. If a visiting cardiologist or radiologist logs onto the network, NAC Director communicates with the hospital's Active Directory or Novell e-directory and sets up a guest account or, if the account or user has specific attributes within the directory, NAC Director can "key-off" of those attributes and provide the guest user a role based on the attributes defined by the Active Directory.

The same can be said for visitors such as pharmaceutical salespersons. For example, if the salesperson is sitting with a physician interested in seeing clinical data substantiating the

outcomes that have been claimed over the course of a meeting but that particular data is not available on the salesperson's laptop but only on a remote server, the salesperson can be registered as a guest user in the directory. NAC Director then uses a guest account that enables this user to define who they are, how long they are visiting, and how long the access is going to be available and valid. In turn, NAC Director places this guest user in a VLAN for generic access to the Internet – allowing the guest user the ability to retrieve the data desired – but would not enable access to the hospital's internal network.

USER PROVISIONING

As the need for strong IT governance grows, organizations increasingly need to correlate accounts on systems to actual employees, contractors, and partners. They need to make sure that accounts have appropriate levels of permissions and that the users are directly correlated, down to the procedural level, with the policies and authentication most closely associated with them.

In the development of technology for the healthcare environment and individual practitioner, user provisioning enables administrators to better deploy and implement identity-based solutions resulting in trusted network users and more feature-rich, integrated user management policies. These include components such as:

Discovery

In healthcare and related environments where detecting anomalous behavior and maintaining control over individual users and visibility over specific devices is paramount, NAC Director employs a discovery process that not only identifies every machine and user on a network but also enables administrators to drill down to the device level. Not only does NAC Director, in performing discovery, reveal the location and IP or MAC-based address of every device on the network, it is also capable of alarming on devices if they go off-line. For example, an administrator knowing when a printer – perhaps one among hundreds – uncharacteristically goes off-line, perhaps even before the user is aware of it and before workflow, and the integrity of the network relative to privacy concerns, is compromised.

Import/Export

While NAC Director works optimally with devices that have IP or MAC based addresses, for so-called "headless devices" (such as Xbox or Play Station, a card reader, or a handheld on a nurse's cart) it does have the ability to have information on these devices entered manually via an Excel spreadsheet. This enables NAC Director to know where that device is located and even how and when it's being used.

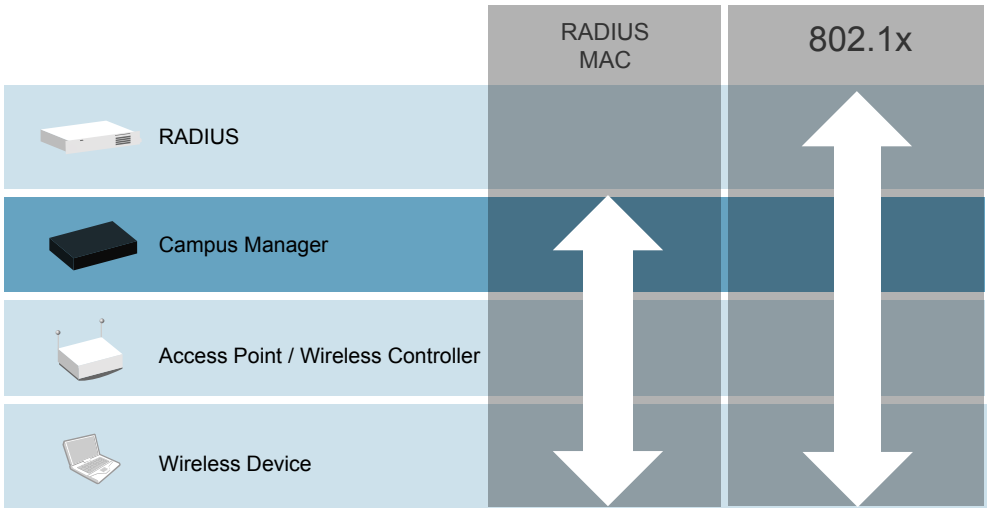
Remote Users

For users remote to the wired network who are accessing the network via a home connection, perhaps for the purpose of tele-education, NAC Director enables administrators to authenticate remotely. In this scenario a medical student could log in from home but be forced to meet specific standards for anti-virus and anti-spyware so that when the user gets onto the network through a VPN, the machine is up-to-date and meets the hospital's minimum requirements for accessing the network via the policies that are already in place. NAC Director also, through this process, anticipates the trend of users (or students in a medical learning facility within commuting distance), registering remotely. This results in lessening the need for an entire student population having to be registered and authenticated all at once.

WIRELESS

Wireless connections are becoming more and more prolific throughout the business world today. Unauthorized client connections such as wireless adapters embedded in field terminals carried by delivery and utility staff, in handheld scanners used by manufacturing and retail firms, and in laptops and PDAs used by mobile professionals are just a few examples of these types of clients.

For any wireless device managed by NAC Director, an authentication request – originating from either a controller or an intelligent access point – requires acceptance through MAC-based Radius or 802.1x in order to access network resources. For unmanageable wireless devices NAC Director uses DHCP and DNS to manage the connecting clients. If a rogue MAC address is detected, NAC Director permits access only to the isolated registration network. Devices shown not to have an account by NAC Director remain in isolation from general network access, preventing further unauthorized, wireless client proliferation.



Wireless Users

For the network administrator who has discovered a way to “lock down” hardwired access to the network, taming its wireless network counterpart to react and alarm in a similar, user-friendly, outcome-anticipated fashion can prove problematic – especially without having the necessary methodologies, solutions, and policies in place to permit authenticated access and registration without sacrificing ease of management, convenience of use, or security.

A connection-independent solution, NAC Director has been developed to assure IT administrators that the user experience doesn’t change when users switch to a different connection type (wired to wireless, for example). A device validated by NAC Director for wired access does not have to be re-validated if the interface it’s connecting through differs from the way it connected in when it first accessed the network. NAC Director is intelligent enough to differentiate between a device and a MAC address and to correlate device information, when necessary, to prevent duplicate testing. This process minimizes network authentication while eliminating the unnecessary step of asking users to be validated again if they switch their connection interface from wired to wireless.

RISKS FOR WIRELESS NETWORKS

The challenges competing for solutions in the burgeoning evolution towards securing the wireless enterprise network include both ongoing and opportunistic centers of management and control. These include:

Rogue Access Points

Rogue Access Points are unknown, unauthorized Access Points. These occur when an individual connects an unauthorized AP directly to a private network to provide backdoor access to business systems or to enable intruder attacks on the network over an extended period of time.

For its part NAC Director treats rogue access points as rogue MAC addresses and can block any rogue device from getting access to the network. Due to the solution's architecture – which relies on learning a device's MAC address and registering it – NAC Director utilizes the persistent agent (placed on the device) to communicate directly with the device to determine that it has already been registered on that network. If someone, for example, was to take a registered MAC address and place it on a rogue Access Point in an attempt to bypass the authentication process, NAC Director – which asks the device to identify its MAC or IP address – will also detect the lack of an agent on the device, quickly identify the device's rogue status, and place the device in immediate quarantine.

For devices that have NAC Director agents installed but connect behind a router or a rogue Access Point, these devices receive a private address from a rogue access point via Network Address Translation (NAT). NAC Director compares the IP address of the rogue device with the list of IP addresses received from the Agent. If the IP address does not match any in the list, NAC Director flags the device as a potential NAT device where someone hiding behind it could gain unauthorized access to the network.

Exploiting Vulnerabilities

Serious attackers often spend considerable time and effort seeking out vulnerabilities, which they can exploit in their favor. Often these "hackers" employ tools such as NetStumbler, WEP crackers (such as Airsnort), or MAC spoofing in order to gain access to data, to steal intellectual property, or to violate company regulations.

NAC Director ensures that any device allowed on the network doesn't have any prohibited applications associated with it. For example, if NetStumbler is a prohibited application, NAC Director can check the device for its presence, and if detected, effectively block that device from accessing the network.

According to Gartner** most security incidents initially appear as an IT operational issue or failure and are identified by observation of certain IT conditions, including performance issues, anomalous behavior, policy violations, and service disruptions. Identifying the scope of an attack can be very difficult if manually auditing disparate log and event data, most of which is extremely voluminous and irrelevant.

NAC Director not only identifies and knows which users, machines, and applications are accessing the network, it's also able to isolate or prohibit altogether those that are unauthorized or unauthenticated to do so. NAC Director mitigates and contains network attacks by identifying the unauthorized device through its MAC address/IP and isolating the device in a restricted portion of the network, which enables WLAN service to return to normal levels as quickly as possible.

For IT administrators wrestling with opening up their network to wireless users but reluctant to do so based on security fears that access to their network may propagate outside their walls to unauthorized users, NAC Director – a network access solution that transparently manages every device and every user regardless of how they connect to the network – makes the decision to "go wireless" easier and more secure than it's ever been.

THE COMPLIANCE FACTOR

As compliance in the enterprise network becomes ubiquitous, IT administrators are increasingly required to implement security safeguards that meet the Access Control provision of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. For each of these types, the Security Rule*** of the Act (issued in 2003), identifies various security standards and for each standard, it names both required and addressable implementation standards and specifications.

The standards and specifications include:

- Administrative Safeguards: policies and procedures designed to clearly show how the entity will comply with the Act (for example, adopting a written set of privacy procedures followed by the organization).
- Physical Safeguards: controlling physical access to protect against inappropriate access to protected sites (for example, limiting access to hardware and software to properly authorized individuals).
- Technical Safeguards: controlling access to computer systems and enabling covered entities to protect communications containing Protected Health Information (PHI) transmitted electronically over open networks from being intercepted by anyone other than the intended recipient.

NAC Director from Bradford Networks supports the physical and technical safeguards, standards, and specifications through its network access control solution, one that limits individual users and machines to increasingly wider or, conversely, narrower access depending on the level of authentication and role-based access they have been assigned. Additionally, as a result of its architecture and deployment in a network where technical safeguards are a prerequisite to compliance, NAC Director enables administrative safeguards that demonstrate how those policies and procedures are put into place to comply with the Act. For even the most scrupulous of HIPAA auditors, NAC Director knows who is on the network at any given time of the day and can document these connection times historically in order to demonstrate compliance with the Act's most demanding provisions.

ACCESS CONTROL & THE SECURITY STANDARDS RULE

Technical safeguards are becoming increasingly more important due to technology advancements in the health care industry. As technology improves, new security challenges emerge. Healthcare organizations are faced with the challenge of protecting electronic protected health information (EPHI), such as electronic health records, from various internal and external risks. To reduce risks to EPHI, covered entities must implement technical safeguards. Implementation of the Technical Safeguards standards, defined in the Security Rule (164.304) as the "technology and the policy and procedures for its use that protect electronic protected health information and control access to it."

Foremost within the Security Standards Rule is access control. Access control provides users with rights and/or privileges to access and perform functions using information systems, programs, or files. Access controls enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges are granted to authorized

users based on a set of access roles that the covered entity is required to implement as part of the Information Access standard under the Administrative Safeguards section of the Rule. This standard specifies:

> "Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified for Information Access Management."

The standard further specifies that access controls should be appropriate for the role and/or function of the workforce member. For example, workforce members responsible for monitoring and administering information systems with EPHI, such as administrators or super users, must only have access as appropriate for their roles and/or job function.

As a premier, innovative, and proven Network Access Control solution that incorporates Identity Management, Endpoint Compliance, and Usage Policy Enforcement into a single solution, NAC Director satisfies each of these HIPAA focused requirements. In NAC Director Identity Management includes the Registration Policy, Authentication Policy, and Role-Based-Access Policy. Endpoint Compliance includes the OS patch, Hot-Fix, Anti-virus, Anti-Spyware, and Required and Prohibited Application Policies. Usage Policy Enforcement typically includes events (SNMP traps) sent to NAC Director from other applications (Packeteer, IDS/IPS, Firewalls). NAC Director enforces these policies by "isolating" a machine from the production network until compliance with the particular policy is achieved, dovetailing with the Act's Information Access standard that allows network access only to those persons or software programs that have been granted access rights.

AUTOMATIC LOGOFF

In the context of HIPAA Governance, Automatic Logoff applies to the entity being able to:

> *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*

According to this specification, users should logoff the system they are working on when their workstation is unattended. Automatic logoff, the specification continues, is an effective way to prevent unauthorized users from accessing EPHI on a workstation when it is left unattended for a period of time.

NAC Director responds to this specification by forcing employees and staff to re-authenticate in a given interval, especially when the workstation has been left unattended for a certain period of time. NAC Director re-authenticates across the network on all network devices that require this procedure. NAC Director can also scale the time interval between re-authentication events. And if a user needs to be re-authenticated, it's not only a machine or device that's being re-authenticated, it's also an individual's credentials and role-based access, binding machine and individual to one another, wherever the user is on the network. Ultimately, NAC Director enables administrators to know who is sitting behind every IP or MAC addressable device on the entire network by forcing users to re-authenticate when their device or machine has been automatically logged off.

CONCLUSION

Ultimately the litmus test for any security/role-based access/user provisioning solution is how well these technological innovations preserve patient identity and how efficient the itinerant access controls associated with successfully authenticating users and network resources to appropriate hospital personnel have been established.

NAC Director enables network administrators, working in enterprises with varying degrees of complexity, to have unparalleled visibility and control over network resources – how they're used and by whom – while having the ability to review that information through its historical connection logs. These logs not only record every transaction associated with access on the network, but also serve as a forensic audit trail for purposes of federally mandated compliance initiatives. Coupled with its ability to bind users to their machines via their attributes (or credentials) while requiring re-authentication at pre-selected intervals upon automatic logoff, NAC Director remains an intuitive and increasingly responsive solution for today's healthcare, compliance-centric, enterprise environment.

As industry practitioners – physicians and IT staff alike – contemplate their responsibilities for locking down network access and provisioning it only to those individuals associated with specific role-based access control privileges, NAC Director continues to provide industry leadership through proven, customer-validated solutions that enable hospital administrators and IT personnel alike to put into place the safeguards that define today's trusted network.

** Network World http://www.networkworld.com/newsletters/netware/2006/1002nw2.html*
***All Gartner research is copyrighted by Gartner, Inc. and/or its Affiliates. All rights reserved.*
****Note: portions of content extracted from the Centers for Medicare & Medicaid Services on the rule titled "Security Standards for the Protection of Electronic Protected Health Information" found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly known as the Security Rule. Volume 2, Copyright May 2005*