

Mobile Network Access Control

Extending Corporate Security
Policies to Mobile Devices

WHITE PAPER

Executive Summary

Network Access Control (NAC) systems protect corporate assets from threats posed by devices that lack adequate security measures. Using NAC in a mobile deployment, however, can be problematic if overly stringent enforcement impacts the worker's ability to use the device. The Mobility XE Mobile NAC module is especially designed to allow administrators to balance the response to a security concern based on severity, and the impact that remediation measures would have on worker productivity. Administrators can simply warn the user, or take more stringent action such as quarantining the device. Using Mobile NAC in conjunction with the Policy Management module allows automated remediation based on factors such as the speed of the connection or time-of-day. It also integrates with systems management software as part of a complete system for over-the-air device management.

The Need for NAC

Network Access Control (NAC) solutions protect organizations, and enforce corporate policies to keep devices configured correctly and operating at top efficiency. NAC solutions verify protection against viruses, spyware and other security threats that are transmitted via networks and network-enabled applications, or that take advantage of unpatched vulnerabilities in operating systems and applications. Network administrators use NAC solutions to monitor and manage computing devices to ensure they are compliant with corporate security requirements. Devices can be updated with operating system service packs and patches, antivirus and antispyware updates, software patches, etc., before being allowed access to corporate network resources.

Deploying a NAC solution to mobile workers presents a greater set of challenges than deploying to workers connecting from a corporate office. This is because mobile devices are sporadically connected to any number of wireless networks over the course of the day. Moreover, mobile workers typically access data at the point of service while working with a customer or client. This means that implementing a NAC solution designed for “always-on Ethernet access” can greatly reduce mobile worker productivity.

For example:

Home healthcare workers spend the vast majority of their workday visiting patients, updating medical records, ordering prescriptions and filing paperwork required by the healthcare system and insurance companies. They frequently make updates at the point-of-care, by connecting to a cellular carrier's wireless network. If they are forced to spend 10 or 15 minutes updating out-of-date virus signatures over a wireless connection, productive time with patients is significantly impacted.

A field service technician typically has a back-to-back schedule packed with appointments to meet with customers, install equipment and make repairs. If, while ordering parts for a customer, the technician is forced to remediate his device, it can prevent completing the current work order and will affect the remaining visits scheduled that day.

These types of productivity concerns can delay or entirely prevent organizations from deploying a NAC solution to mobile workers. But mobile devices also pose one of the greatest security risks for an organization. Mobile devices are far removed from the confines of the enterprise, are harder to manage and maintain, and can easily be lost or stolen. Thus, organizations need to implement a “Mobile NAC” that enforces corporate security policies in a way that is also sensitive to keeping mobile workers productive.

Mobility XE NAC Module

Mobility XE features an optional NAC module. It provides security controls to intelligently extend corporate security policies to mobile devices, including laptops, tablets, handheld devices and smart phones, without adversely impacting mobile worker productivity. By incorporating the NAC module in a Mobility XE deployment, network administrators can control whether a mobile device is allowed access to a Mobility server based on the mobile device’s compliance with established corporate security policies.

Using Mobility XE’s mobile NAC module, network administrators have complete control over how and when devices can connect to their enterprise network. Devices must comply with specified security policies or face remediation. Key features of the mobile NAC module include:

- **Simple deployment.** The mobile NAC module does not require network infrastructure reconfiguration in order to deploy. Using a menu-driven wizard, administrators can configure and deploy security policies in minutes.
- **Security enforcement.** Prior to connecting to the corporate network, mobile workers’ devices are scanned for compliance with NAC rules established by the system administrator. If devices fail any of the checks, the administrator has full power to enforce any number of remediation options and bring the device into compliance.
- **Flexibility and control over non-compliant devices.** Integration of mobile NAC with the Mobility XE Policy Management module affords great flexibility over when and how to remediate. Based on severity, administrators may choose from simple warnings, to triggering customizable remediation policies that can limit application access, launch websites, initiate software downloads, or even disconnect or quarantine the device. This automation allows administrators to remediate a device without user intervention.
- **Over-the-air management.** Unattended devices can be authenticated and then remediated without a user being logged on. Enterprises that use device-management solutions to apply patches and updates during non-working hours can manage the device while still in the field.
- **Defense-in-depth.** Mobile NAC is part of a three-pronged security strategy enforced by Mobility XE, which verifies that 1) the device is properly patched and configured, 2) the device is an authorized, corporate-owned asset, and 3) the user is authorized to use that particular device. Unless all are true, the administrator can configure the system to prevent a connection.

- **Administrator alerts.** The Mobility XE Analytics Module delivers alerts to administrators when a device fails a NAC check, at or above a specified severity level. This is useful where administrator intervention may be needed to keep the worker productive.
- **Automatic updates and compliance.** Updated rules are automatically pushed down to client devices. Devices are also automatically rescanned at regular intervals to ensure ongoing compliance.
- **Multiple platform support.** NAC is supported across all Windows-based client devices: laptops, handhelds and smart phones.

The Mobile NAC Module – How It Works

Mobility XE's mobile NAC module is designed specifically for the unique demands of mobile worker deployments. The module gathers information on antivirus, antispyware, firewall software, Windows updates and registry, installed files, and processes running on the mobile device. NAC security checks use this information to assess the health of the Mobility client device. If a device fails a security check, mobile NAC rules provide users with the information they need to bring the client device into compliance. If mobile NAC is deployed in conjunction with the Policy Management module, administrators can automatically initiate customized remediation measures to make the device compliant.

The mobile NAC module is centrally managed by a network administrator using Mobility XE's web-based Mobility console. The network administrator creates a "rule" to check a device's configuration. Groups of rules, known as a "rule set," are combined to create NAC policies suited to the organization's needs.

A NAC "wizard" makes creating the most common rules easy to do within just a few minutes. The rules can then be enforced globally, to user groups, by class of device, or to individual users and devices. When an administrator revises a NAC rule, the updates are automatically sent to all subscribed users and devices. The rules are evaluated on the mobile device at startup, and also re-evaluated every five minutes. (This interval is configurable.) If a client device fails a NAC policy check, the administrator can choose from different options for responding and remediating. If the infraction is not serious, the administrator can configure a failure message that explains what the user must do in order to bring the device into compliance. For serious security violations, the mobile device can be immediately disconnected from the corporate network and quarantined entirely.

For example:

An insurance company has claims adjusters that spend their entire workday in the field. For these workers, keeping antivirus signature files up-to-date is challenging because of their size and update frequency. The administrator can create a NAC rule, however, to display a pop-up warning message on mobile devices that are using antivirus files older than 10 days, and disconnect mobile devices using antivirus files older than 14 days.

Integration with Policy Management

By using the Policy Management module in tandem with the mobile NAC module, administrators gain unprecedented flexibility for implementing remediation measures. In particular, rules can be created that consider the network the user is connected to as well as the severity of the security concern. For users currently connected to a slower cellular data network, they could be warned that their device requires updates, whereas users connected to a fast Wi-Fi connection could be required to update immediately.

An IT administrator can also direct Mobility clients to automatically download and install software updates, operating system patches, Mobility XE updates, etc., with little or no user intervention, ensuring that devices are “healthy” before connecting to the corporate network. These automated updates can also run in an unattended mode, where the device authenticates itself for security purposes and connects via a VPN tunnel, without an active user log-in. Unattended mode enables updates in the middle of the night or when the device is not otherwise in use, and integrates with policy and remote device management solutions including Microsoft’s Active Directory Group Policies, Microsoft SC-CM, Sybase Afaria and many others. Through this integration, enterprises that use such tools may manage their mobile, remote devices as easily as devices connected to the local LAN.

In addition, if the Mobility XE Analytics Module is installed, administrators may elect to be alerted if a device fails a NAC check at or above a specified severity level (as defined under NAC enforcement below). Alerts can be sent via e-mail, or through a syslog or any SNMP compatible management system.

NAC Checks

The Mobile NAC module provides a number of checks that collectively evaluate the patch status and security posture of the device.

Category	Parameters Checked
Antivirus and Antispyware	Specified product installed, real-time protection enabled, signatures up-to-date, date and result of the last scan
External Condition	Value of a system variable; this allows external programs and processes to set variables that can be evaluated by the Mobile NAC module
File	Specified file either present or not present on the client
Firewall	Specified product installed and running
Mobility Version	Version of the Mobility client
Operating System	OS version, service pack, processor and other platform information
Process Check	Specified application or service running or not running
Registry Key	Keys in the registry are present or not present, and have the expected values
Windows Update	Auto-update enabled, and/or specific patches present

NAC Enforcement

Network administrators define rules that are evaluated on each client device, with enforcement occurring at the Mobility server. Administrators also specify the severity of enforcement — from warnings, to remediation (using the Policy Management module), to disconnect or quarantine.

Status	Description/Action
Allow	The Mobility client device complies with NAC policy. Inbound and outbound network traffic allowed via the Mobility VPN through the Mobility server.
Warn	The client does not comply with one or more checks in a rule. The Mobility client device is allowed to connect, but the Mobility client displays a warning.
Remediate	The client does not comply with one or more checks in a rule that requires remediation. The action required to bring the device into compliance is determined by Policy Management rules that apply to the remediation level.
Disconnect	The client does not comply with one or more checks in a rule that causes the client to be disconnected.
Quarantine	The client does not comply with one or more checks in a rule that causes the device to be disconnected and quarantined. The system administrator must clear the quarantine before the device can connect.

Example NAC Rule Creation

Using the Mobility console's NAC wizard, the network administrator creates a base-line rule set. As necessary, additional rules for other operating systems or security configurations can be added on-the-fly. Once complete, the administrator subscribes users or devices to the rule set and the rule set is automatically sent to those mobile devices. The system provides the flexibility to subscribe NAC rule sets globally, to device classes or user groups, and to individual users and devices.

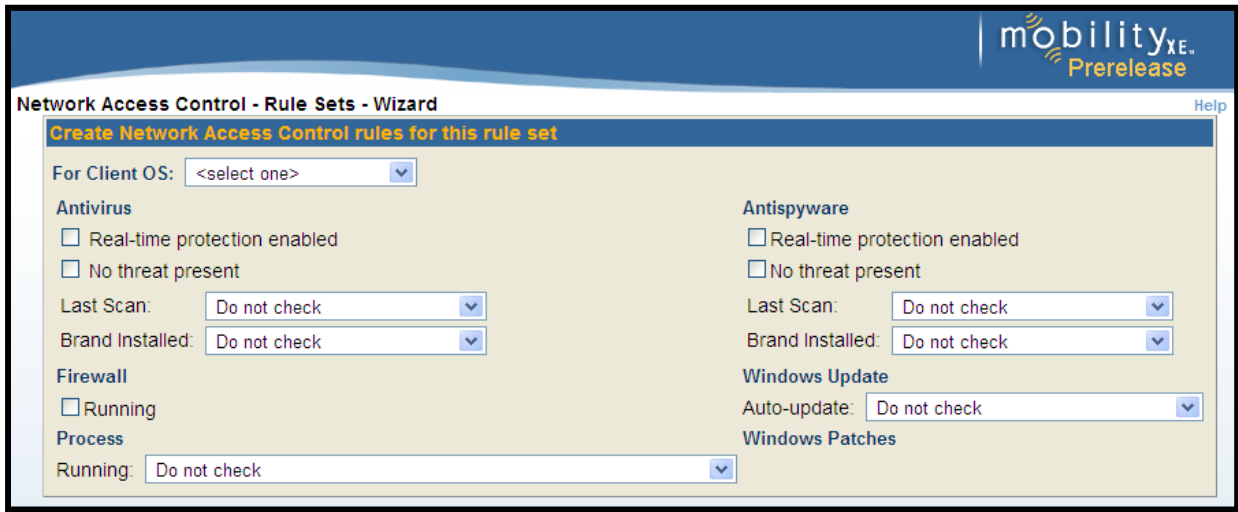
The screenshot displays the Mobility console interface for Network Access Control (NAC) rule set management. The top navigation bar includes 'Status', 'Reporting', 'Settings', 'Tools', 'Licensing', and 'About'. The 'Tools' menu is open, showing 'Policy Management' and 'Network Access Control' (highlighted with a red circle). The main content area is titled 'Network Access Control' and has tabs for 'Rules', 'Rule Sets', and 'Subscribers'. The 'Rule Sets' tab is active, showing a filter set to 'No Filter' and buttons for 'Apply' and 'Refresh'. Below the filter are action buttons: 'Add', 'Edit', 'Copy', 'Rename', 'Delete', 'Export', 'Import', and 'Publish'. A table lists the rule sets:

	Description ▲	Date Modified
<input type="checkbox"/>	bin1	06/07/2007 10:08 AM
<input type="checkbox"/>	binaryProf	06/11/2007 06:04 PM
<input type="checkbox"/>	darcy	06/12/2007 03:06 PM
<input type="checkbox"/>	darcy3	06/13/2007 05:12 PM
<input type="checkbox"/>	wiz3	06/07/2007 10:14 AM

At the bottom of the table, there are additional action buttons: 'Add', 'Edit', 'Copy', 'Rename', 'Delete', 'Export', 'Import', and 'Publish'.

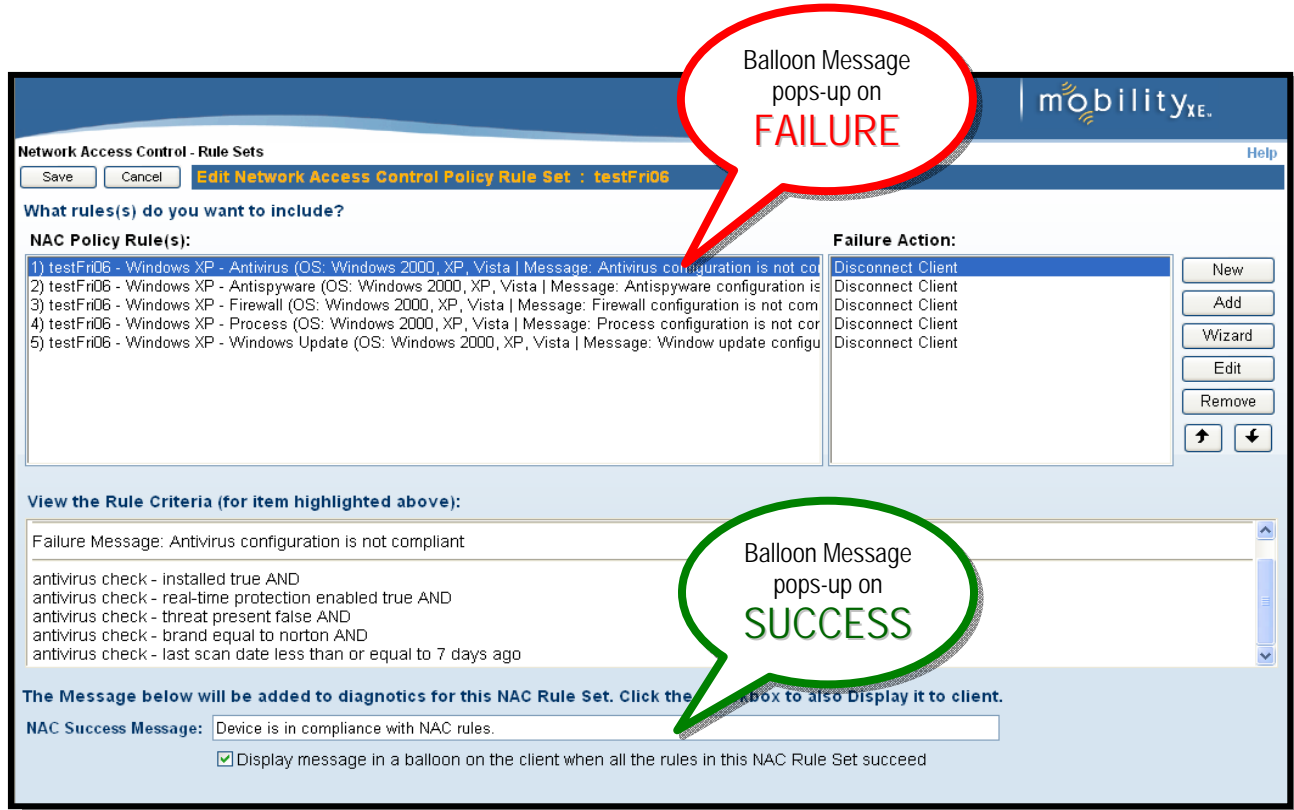
The NAC wizard features “smart” rule construction — automatically adding applicable attributes in the correct order to simplify rule creation. For more customized or complex rules, network administrators use the NAC editor to edit existing rules, add more advanced attributes and options, and create completely new rules or rule sets.

Network administrators may want to establish specific rules based on operating system such as Windows Mobile versus Windows XP or Vista. Alternatively, rules can also be applied to specific device type(s) such as laptops, tablet PCs, handhelds, etc. While a single rule set can contain rules applying to multiple operating systems, only rules that apply to the specific mobile device’s operating system will be evaluated.



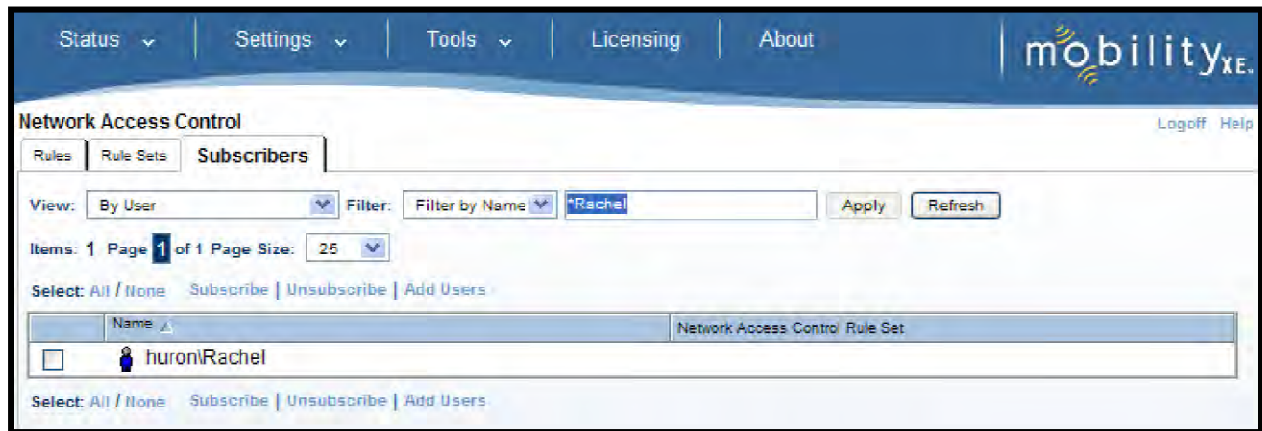
The Mobile NAC module offers flexibility in checking mobile devices for the existence and configuration of security features such as antivirus, antispyware and firewall products. If these products are not installed or configured correctly, Mobility XE can prevent the mobile device from connecting. Organizations can monitor configuration at a high level (e.g. is the software installed and running) or a more granular level (e.g. is the proper version running with the most recent update). NAC rules can inspect virtually any attribute of the device, such as that specific programs are running, that Windows Update is configured to meet corporate standards, or that Windows registry keys have appropriate values.

If a mobile device fails to satisfy any rule, the default failure action is to display a warning pop-up balloon message on the client. However, after creating a base-line rule set with the wizard, administrators can specify different failure actions, add rules for different operating systems, modify the rules, customize the message displayed on the client, or delete rules as necessary.



Subscribing and Publishing NAC Rules

Mobility XE provides the flexibility to subscribe NAC rule sets globally, or by particular device class, device type, user group, or individual user. Publishing a rule or a rule set updates it automatically to all subscribed client devices.



Conclusion

Organizations that implement NAC solutions are taking a proactive stance to secure their workers' devices and add a further layer of security to protect the confidentiality and integrity of their corporate data. Network Access Control is an essential element in an organization's overall security architecture and becomes increasingly important as workers mobilize and their numbers increase.

For More Information

Visit www.netmotionwireless.com or contact sales@netmotionwireless.com.

© 2009 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPsec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion technology is protected by one or more of the following US Patents: 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; and Canadian Patent 2,303,987. Other US and foreign patents pending.