

Mobile Network Access Control

Extending corporate security policies to mobile devices

WHITE PAPER

NetMotion Wireless

701 N 34th Street, Suite 250

Seattle, WA 98103

206.691.5555

www.netmotionwireless.com

Executive Summary

More and more organizations are incorporating mobile data access via wireless networks into their remote, field worker strategies. These organizations are deploying mobile solutions such as NetMotion Mobility XE™, an easily deployed mobile VPN, to provide security, management and enhanced worker productivity.

Mobility XE consists of two main components: server software that acts as a proxy to enterprise application servers, and lightweight client software that is installed on every wireless device. Through this simple architecture, Mobility XE provides continuous, secure connectivity between mobile workers and enterprise applications – over any networks they use or traverse.

Mobility XE features an optional Network Access Control (NAC) module that provides security controls to intelligently extend corporate security policies to mobile devices, including laptops, tablets, handheld devices and smartphones, without adversely impacting mobile worker productivity. By incorporating the NAC module in a Mobility XE deployment, network administrators can control whether a client device connects to a Mobility server based on the client device's compliance to pre-defined security rules.

Controlling Remote Access for Mobile Devices

Network Access Control (NAC) solutions protect organizations from security threats, denial of service attacks and enforce corporate policies to keep devices configured correctly and operating at top efficiency. NAC solutions let network administrators monitor and manage user devices to ensure they are “trusted devices,” compliant with corporate security requirements. As needed, antivirus and antispyware updates, software patches, etc., can be updated on devices so that they can meet compliance requirements and gain access to their 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. Mobile devices are sporadically connected to any number of wireless networks over the course of the day. Mobile workers typically access data at the point of service when working with a customer or client. Implementing a NAC solution designed for “always-on Ethernet access” devices 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 wide area wireless network. If they are forced to spend 10 or 15 minutes updating out-of-date virus signatures over a slow wireless connection, time spent working productively with patients is significantly impacted.

In another example, 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.

While these types of productivity concerns can delay or entirely prevent organizations from deploying a NAC solution to mobile workers, mobile devices 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 strategy that enforces corporate security policies in a way that is also sensitive to keeping mobile workers productive.

Mobility XE's NAC Module - How It Works

Mobility XE's NAC module is created specifically to handle and support mobile worker deployments. The NAC module gathers information on antivirus, antispyware, firewall software, Windows updates

and registry, installed files, and processes running on the mobile device. NAC security checks enforced by the Mobility server use this information to assess the health of the Mobility client. For clients that fail a security check, NAC rules provide users with the information they need to bring the client device into compliance.

The NAC module is centrally managed by a network administrator using Mobility XE’s web-based Mobility Console. The network administrator creates a 'rule' that can check multiple device attributes. Groups of rules, known as a 'rule set,' are combined to create NAC policies suited to the organization’s needs.

Using the NAC wizard, rules or rule sets are established to enforce security policies globally, to workgroups, by class of device, or to individual users and devices. NAC updates are automatically sent to all subscribed users and devices. The NAC rule set is evaluated by the Mobility XE client software at startup, and also re-evaluated every five minutes (this interval is configurable). If a client device fails a NAC policy check, based on severity or corporate policy, the administrator has a number of options for responding and remediating. If the infraction is not serious, they can configure a failure message that explains what the user must do in order to bring their mobile device into compliance. For serious security infractions, the mobile device can be disconnected from the corporate network or 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. The network administrator can create a NAC rule, however, to display a pop-up warning message on Mobility clients that are using antivirus files older than 10 days, and disconnecting Mobility clients using antivirus files older than 14 days. A warning message provides an explanation on how to remediate the device. NAC rules can also be flexibly created to consider which network the user is currently connected to. For users currently connected to a slower wide area network, they might be “warned” that their device requires updates, whereas users connected to a fast Wi-Fi connection might be required to update immediately.

By using the integrated Policy Management module in tandem with the NAC module, an IT administrator can also require that Mobility clients automatically download and install software updates, operating system patches, Mobility XE updates, etc., in order for the device to be considered “healthy” and thus capable of connecting to the corporate network.

NAC Enforcement

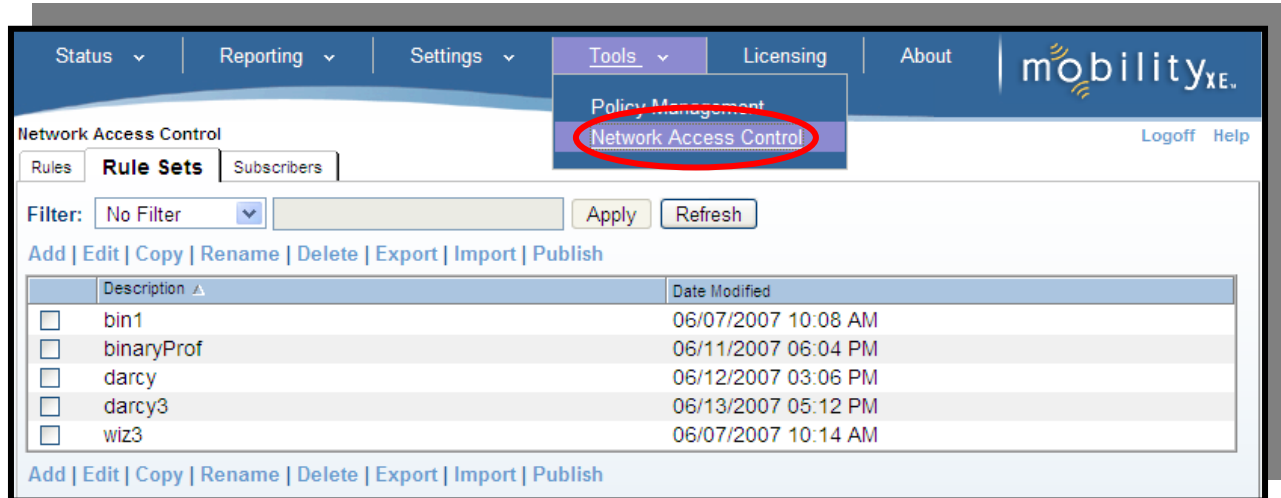
Network administrators define rules that are evaluated on each client device with enforcement occurring at the Mobility server. Administrators also determine the severity of enforcement, from warnings, to remediation (using the Policy Management module), to a disconnect or quarantine.

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 that causes the Mobility client to display 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 client into compliance is determined by the system administrator.
Disconnect	The client does not comply with one or more checks in a rule that causes the device to be disconnected.
Quarantine	The client does not comply with one or more checks in a rule that causes the device to be quarantined. The system administrator must clear this state before the device can connect.

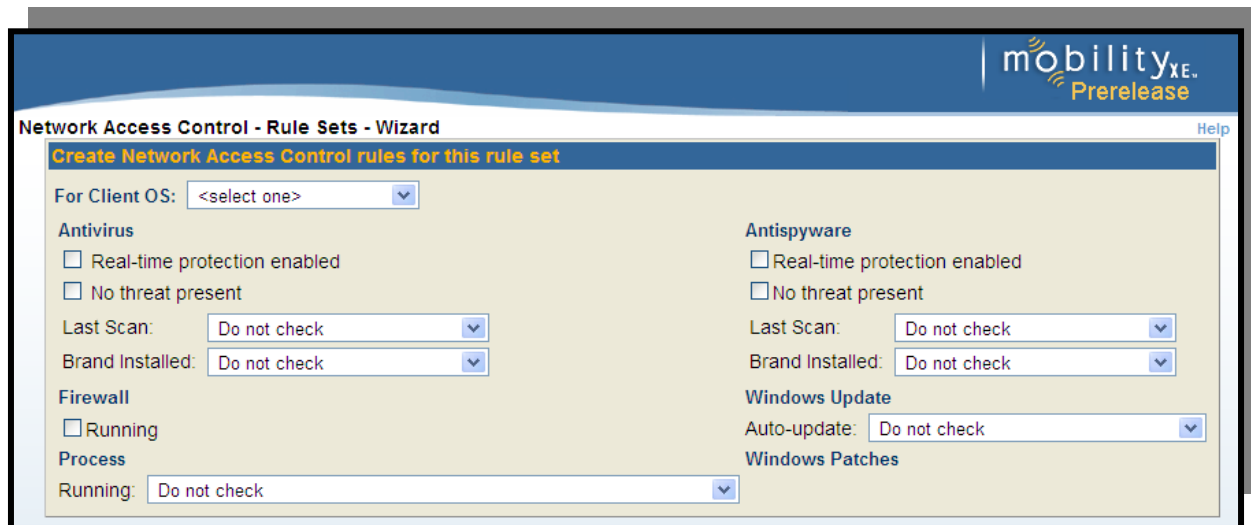
Example NAC Rule Creation

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, and the rule set is automatically sent to all the 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 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 function to edit existing rules, add more advanced attributes and options, and create completely new rules or rule sets.



To create, edit, or subscribe NAC rules and rule sets, click on "Tools > Network Access Control" menu option in the Mobility console.



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.

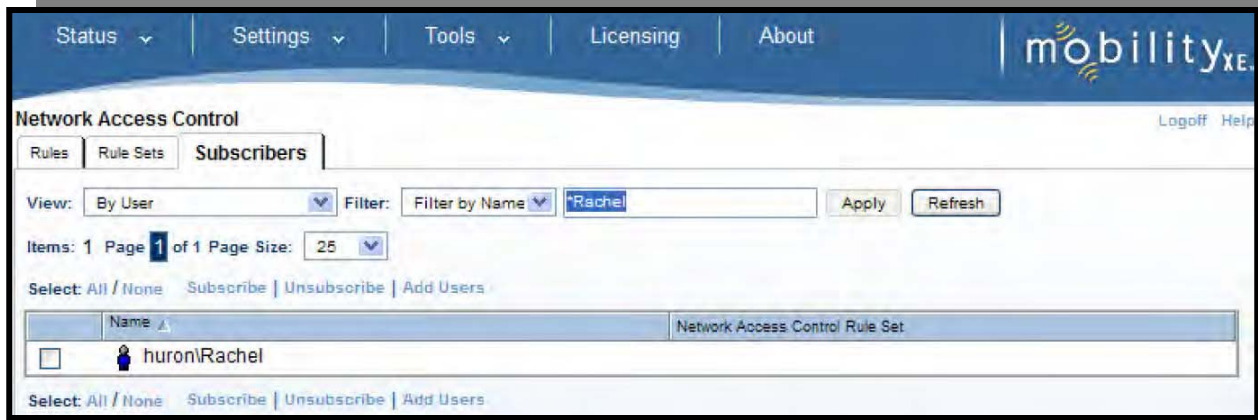
The NAC module offers flexibility in checking mobile devices for the existence and configuration of security features such as antivirus, antispysware and firewall products. If these products are not installed or configured correctly, Mobility XE can prevent the mobile device from connecting. Organizations 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, including that specific programs are running, that Windows Update is configured to meet corporate standards, or that Windows registry keys have appropriate values.

If a Mobility client 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 rules 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.

The screenshot displays the 'Network Access Control - Rule Sets' configuration page in Mobility XE. At the top, there are buttons for 'Save', 'Cancel', and 'Edit Network Access Control Policy Rule Set : testFri06'. Below this, a section titled 'What rule(s) do you want to include?' contains a table of 'NAC Policy Rule(s)'. The first rule is selected, showing its criteria: '1) testFri06 - Windows XP - Antivirus (OS: Windows 2000, XP, Vista | Message: Antivirus configuration is not compliant)'. To the right of this table is a 'Failure Action:' dropdown menu, currently set to 'Disconnect Client'. Below the table, there are buttons for 'New', 'Add', 'Wizard', 'Edit', 'Remove', and arrow keys. A red speech bubble points to the 'Failure Action:' dropdown with the text 'Balloon Message pops-up on FAILURE'. Below the table, a section titled 'View the Rule Criteria (for item highlighted above):' shows the detailed criteria for the selected rule, including 'antivirus check - installed true AND', 'antivirus check - real-time protection enabled true AND', 'antivirus check - threat present false AND', 'antivirus check - brand equal to norton AND', and 'antivirus check - last scan date less than or equal to 7 days ago'. At the bottom, a section titled 'The Message below will be added to diagnostics for this NAC Rule Set. Click the checkbox to also Display it to client.' contains a text field for 'NAC Success Message:' with the value 'Device is in compliance with NAC rules.' and a checked checkbox for 'Display message in a balloon on the client when all the rules in this NAC Rule Set succeed'. A green speech bubble points to this checkbox area with the text 'Balloon Message pops-up on SUCCESS'.

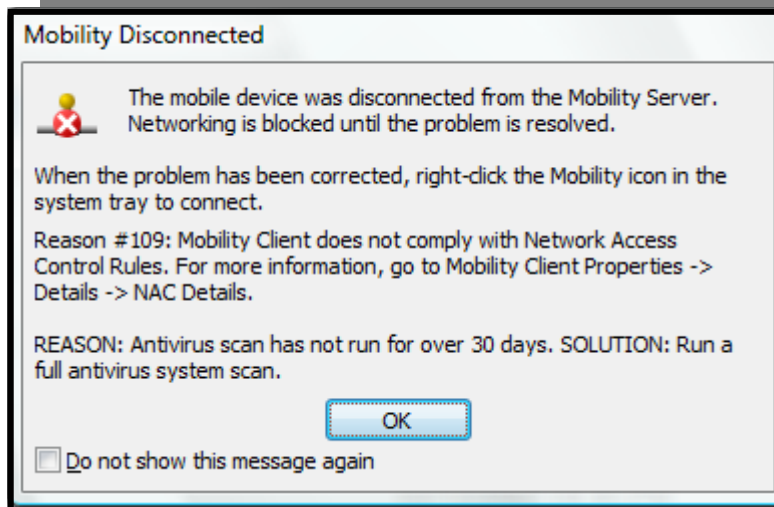
Subscribing and Publishing NAC Rules

Subscribing users and publishing the rule set is completed from the "Subscribers" tab of the main Network Access Control page. Mobility XE provides the flexibility to subscribe NAC rule sets globally, by particular device class, device type, user group, or individual user. Publishing a rule or a rule set updates it immediately to all subscribed clients.



Non-Compliant Devices

When a device fails one or more NAC rules that has a failure action of Disconnect or Quarantine, an error dialog box with the NAC failure action and disconnect message appears. The dialog box also includes a customizable message with information provided by the administrator on how to make the device compliant.



Mobility XE NAC Module Summary

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 organizations overall security architecture and becomes increasingly important as mobile worker numbers increase.

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 NAC module include:

- **Simple deployment.** The 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.

- **Ensures security compliancy.** Prior to connecting to the corporate network, mobile workers' devices are scanned for compliance to 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 to bring the device into compliance.
- **Flexibility and control over non-compliant devices.** 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.
- **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.

© 2008 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPSec, InterNetwork Roaming and Best-Bandwidth Routing are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, and Windows XP Tablet are registered trademarks and Windows Vista is a trademark 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. Other US and foreign patents pending.