

Policy Management Module

Granular management of wireless bandwidth,
security and mobile productivity

WHITE PAPER

NetMotion Wireless

701 N 34th Street, Suite 250

Seattle, WA 98103

206.691.5555

www.netmotionwireless.com

Policy Management Module

Executive Summary

More and more organizations are incorporating mobile access via wireless networks into their remote access strategies. These organizations are deploying mobile solutions to achieve specific business goals, NetMotion Mobility XE is an easily deployed, mobile VPN designed to resolve the key issues associated with wireless networking.

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

Mobility also offers an optional Policy Management module that provides centralized, flexible tools for managing applications, devices, and users in a wireless network environment. Mobility Policy Management enables IT managers to control network costs, improve productivity, and ensure data security over any wireless network. Ultimately, Policy Management allows IT managers to ensure that wireless network usage and performance are aligned with corporate IT policies and ROI goals.

Fine-Tuned Control of Mobile Devices

The number and types of networks an enterprise must coordinate, manage, and secure is no longer limited to networks (or devices) over which they have physical control (or even ownership). With Policy Management, IT managers have more complete control over their wireless and internal networks, including:

- Bandwidth usage
- Remote access to applications, hosts, networks, and subnets
- Types of traffic traversing a specific network
- Applications used over designated networks
- Traffic based on application name, port, or IP address
- Type or speed of a network interface
- Permitted WLAN networks

Policy Management enables IT managers to define and enforce network policies without having to change the underlying wireless infrastructure, which results in substantial cost savings. While the Mobility mobile VPN enables universal application access over wireless networks, the Policy Management module provides the ability to tune the mobile connection to best meet the bandwidth constraints of the network and comply with the security policies of the organization.

How It Works

Mobility's Policy Management module allows IT managers to enhance the security, performance and productivity of their wireless networks, internal resources, and mobile workforce. An administrator can restrict access to specific network resources either by network, host (IP) address, or application name. In addition, these access privileges can be dynamically enforced depending on the network type, location, and/or time of day that the mobile worker is connecting.

Policies are established centrally on the Mobility server and then distributed to individual clients. Companies can enforce IT and corporate security policies by assigning rules globally, to workgroups, by class of device, or to individual users and devices.

Centrally managed, remotely enforced

Mobility Policy Management is centrally managed: an administrator with appropriate permissions creates rules from Mobility's web-based management console. The administrator can then create libraries of individual rules. Drawing from the rule library, the administrator can build a policy (or rule sets), which allows them to leverage common rules repeatedly in various policies. Once the resulting policies are published, they are distributed to the appropriate devices (or clients), where they reside and are enforced.

Client-side enforcement cuts down on the transmission cost of verifying and enacting policies at the server. Distributing policies to mobile clients allows very granular control while conserving network resources. This also ensures that policies are enforced even when the client is out of range of the network or the Mobility server (by restricting access to specific Wi-Fi access points, for example).

Role-based policies

Using Policy Management, network administrators define rules associated with a set of conditions that invoke specified actions. These rules (which can be as general or specific as needed) are then aggregated into policies that are deployed to the clients.

Policies and rules can be assigned to four general classifications:

- Global—affecting all connected Mobility users
- Class of devices connected to the Mobility server
- Device name
- Individual user

Rules are enforced based on the 'most specific' classification specified: global would be the least specific while individual user would be the most specific (an individual user policy overrides a globally assigned policy).

Each rule within a policy can be configured to match conditions based on the following:

- Type of network interface
- Network speed
- Time, date, or day of the week
- Wi-Fi access point SSID or BSSID
- Operating system
- Mobility client version

When the defined conditions are met, policies can be enforced based on the following specified items:

- Applications
- IP addresses
- Subnets
- Ports/protocols

The actions that can be applied to designated network traffic are:

Allow	Allows inbound and outbound network traffic via the Mobility VPN through the Mobility server
Pass Through	Traffic is not directed through the Mobility VPN
Block	Network traffic, which would otherwise be Allowed , is paused for the duration of a defined condition (once the condition is no longer met, traffic resumes)
Disconnect	Terminates allowed or pass through traffic and closes any active sessions

When a rule is defined, the Policy Management interface provides a natural language representation of the rule so the administrator can easily verify actions to be applied.

Examples

Bandwidth Management

The following is an example of a rule that prevents mobile workers from using a bandwidth-intensive application when using an EDGE wireless WAN:

The screenshot shows the 'Policy Management' interface for 'Bandwidth_eater'. It is divided into two steps:

Step 1 - Select the target action(s):

- Applications:**
 - Allow network traffic for application(s)
 - Block network traffic for application(s)
 - Pass through network traffic for application(s)
 - Disconnect network traffic for application(s)
- Addresses:**
 - Allow network traffic for address(es)/port(s)
 - Block network traffic for address(es)/port(s)
 - Pass through network traffic for address(es)/port(s)
 - Disconnect network traffic for address(es)/port(s)
- Well-known Ports:**
 - Allow network traffic for port(s)
 - Block network traffic for port(s)
 - Pass through network traffic for port(s)

Step 2 - Edit the Rule Description (click an underlined value):

Apply this rule
 when the interface speed is less than 11000 Kbps and
 when the interface name contains EDGE
 block network traffic for application(s)
 bandwidth_eater.exe
 and all address(es)/port(s)
 with options
 display a balloon with 'This application eats too much bandwidth for this connection type' only once per process
 else
 continue to the next rule

Keep bandwidth-intensive applications off of the wireless WAN

When this rule is applied, Policy Management detects when the EDGE network is in use and temporarily blocks traffic from the “Bandwidth Eater” application, while allowing all other traffic. If the mobile worker roams to another network (802.11b for example), then network traffic from the “Bandwidth Eater” application is again allowed. Furthermore, if users try to use the “Bandwidth Eater” application on the WAN they will be presented with a Windows (pop-up) balloon informing them that the application uses too much bandwidth for the current network. This example illustrates how Policy Management can be used to control costs and preserve bandwidth for priority applications while safeguarding mobile worker data.

Access Management

The policy below illustrates restricting access to internal (trusted) network resources when on a WAN connection.

The screenshot shows the Mobility XE Policy Management interface. The top navigation bar includes links for Server Status, Client Status, Server Settings, Client Settings, Policy Management (highlighted), Licensing, and About. The Mobility XE logo is on the right. Below the navigation bar is a toolbar with buttons for Cancel, < Back, Next >, Finish, and Edit rule > Conditions(s) [Restrict_Access]. A Help link is also present.

The main content area is titled "Which condition(s) do you want to check?". It contains two steps:

Step 1 - Select the condition(s):

- For any condition
- Access Point**
 - When the access point SSID contains keyword
 - When the access point BSSID is address
- Addresses**
 - When the local address is address
 - When the WINS server address is address
- Interface**
 - When the interface name contains keyword
 - When the interface speed is less than speed Kbps
- Time**
 - On this schedule
 - When the server is reachable for time seconds
 - When the server is unreachable for time seconds

Step 2 - Edit the Rule Description (click an underlined value):

Apply this rule
 when the interface name contains [EV-DO](#)
 start [Intranet URL](#) only once per session and
 allow network traffic for [application\(s\)](#)
 firefox.exe
 and [address\(es\)/port\(s\)](#)
 to 10.1.1.100
 with [options](#)
 display a balloon with 'Access is restricted to the corporate intranet on WAN connections' only once per process
 else
 block all network traffic

Restricting access to internal network resources when on WWAN

When this rule is applied, policy management detects when the EV-DO network is in use and launches the Firefox browser to a specific URL on the organization’s intranet. Furthermore, access is restricted such that the internal URL is the only site the user has access to, either internally or externally. As a reminder of this policy, the user is presented with a Windows pop-up message about the restriction.

Here are additional examples of the types of policies that can be defined:

- Prevent an e-mail program (such as Microsoft® Outlook®) or a web browser from running over the EDGE or 1xRTT networks, but allow these applications to run whenever an 802.11b (Wi-Fi) network is in range.
- Block file downloads (such as FTP) when mobile devices roam to a network with speeds less than 11Mb per second, but allow all other traffic to pass.
- Detect the version

The Value of Policy Management

With the increasing number of applications and networks that mobile workers now use, it's a challenge for network administrators to keep data secure, maintain worker productivity, and still keep costs contained. Policy Management makes an increasingly complex wireless network landscape manageable.

Cost savings

Tight control of network traffic is especially valuable for an enterprise using wide-area networks as part of its mobile computing solution. By tailoring rules to ensure that bandwidth-intensive applications are not used over wide-area wireless, IT managers can immediately begin to control network costs by managing and reducing network traffic.

Security

Security is critical in both multi- and single-network wireless environments. Policy Management gives IT administrators tight control over network traffic and security—whether the network is private, public, or provided by a carrier. Administrators define what networks or subnets every mobile device and user has access to and the applications and resources these users and devices can use. For instance, to meet security requirements, a policy can be created to prevent access to a sensitive internal application via any external 802.11b hotspot.

The Policy Management module can restrict devices and individuals from having access to anything other than what has been explicitly allowed by an IT manager.

Ease of use

With its simple, centralized, web-based console, Mobility Policy Management makes it easier to deploy and manage a wireless solution. IT managers log in to the server through a browser window and can define policies, monitor the status of the Mobility server, and manage connected users. They can even display a customized Windows pop-up (balloon) message explaining to users, for example, why access to a particular application or network is restricted.

Redundancy and backup protection

Policy Management lets IT managers designate a separate network repository for saving copies of policies and policy sets. This is in addition to the native Mobility Warehouse repository where the policy files are maintained. Such an approach provides redundancy in the event of an enterprise network failure and enables managers to make restoration of these policies part of an organization's standard backup procedures.

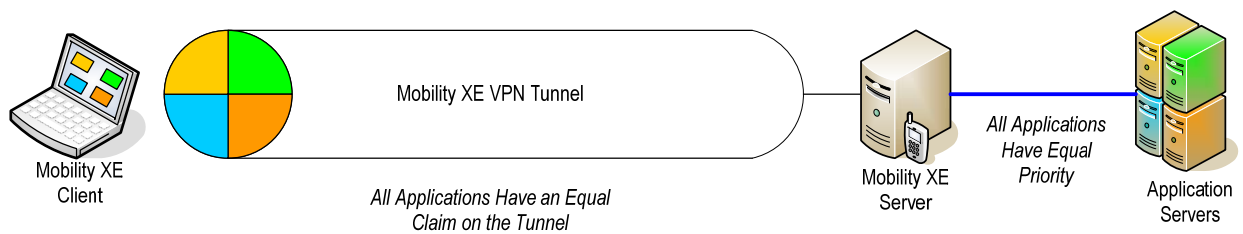
Superior user experience

Mobility simplifies mobile computing. Mobile workers can roam freely between networks, through coverage gaps or suspend-and-resume conditions, without losing data or being forced to restart

applications. Applications, connections, and VPN logins resume automatically when mobile workers re-enter network coverage. Mobility automatically selects the fastest network connection available (within the parameters defined by Policy Management). The combined effect is to make wireless computing much more like a wired computing experience.

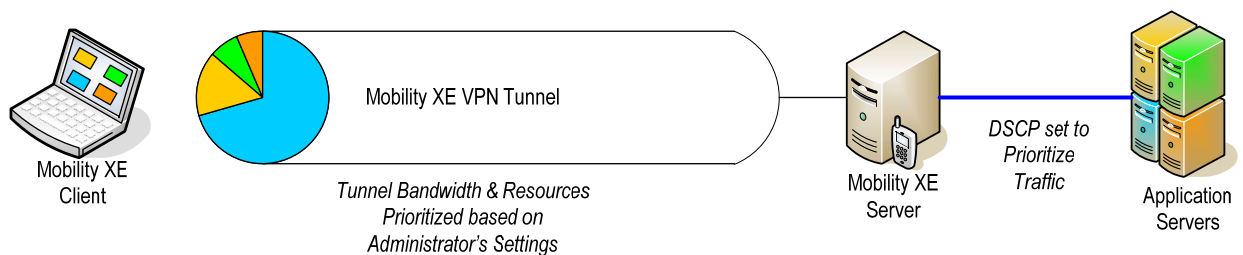
Quality of Service

QoS (Quality of Service) support, included in the Policy Management Module, can be crucial to maintaining productivity as workers move from high-speed, high-bandwidth networks, to lower capacity, high latency networks. For example, while connected to the LAN via Ethernet, performance may be just fine for the mission-critical enterprise application, running alongside e-mail, web browsing, and other applications. But on a WWAN, administrators want to prioritize use of the narrower bandwidth, and make sure that a web browser and e-mail client do not use capacity needed by the enterprise application. Other VPNs may allow administrators to shut off non-essential applications.



Without QoS: Undifferentiated Access to the tunnel and network

Mobility XE allows administrators to specify Quality of Service parameters which are applied between the Mobility client and server, and additionally put DSCP (Differentiated Services Code Point) settings which can be used as network traffic moves beyond the Mobility server. In particular, Mobility XE allows for different settings based on the network and its characteristics – there can be one set of QoS rules applied to a 1xRTT network, another to EV-DO, etc.



With QoS: Tunnel and network priorities set by Administrator

This allows an enterprise application to always have the appropriate share of network resources, but other, non-critical applications to use whatever bandwidth is available once the enterprise application has used what it needs or is assigned.

Summary

Mobility with Policy Management offers IT managers a unique and powerful mechanism to control wireless network usage and costs while increasing mobile worker productivity.

©2007 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. All other trademarks, trade names or company names referenced herein are used for identification only and are the property of their respective owners. NetMotion technology is protected by US Patents 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; and 7,136,645. Other US and foreign patents pending.

52007lj/gV72